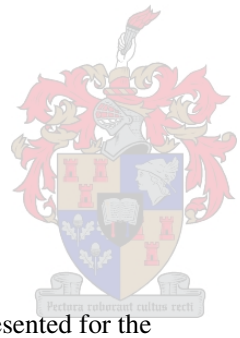
The Protection of Privacy in the Workplace: A Comparative Study

by

Mimmy Gondwe



Dissertation presented for the
Degree of Doctor of Law
at the University of Stellenbosch

Promoters: Prof Ockert Dupper and Mr Christoph Garbers
Faculty of Law
Department of Mercantile Law

December 2011

DECLARATION

By submitting this dissertation, I declare that the entirety of the work contained therein is my own, original work, and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

December 2011

ABSTRACT

The importance of privacy lies in the fact that it represents the very idea of human dignity or the preservation of the 'inner sanctum'. Not surprisingly, however, operational concerns of employers and technological developments combine continuously to challenge the preservation of privacy in the workplace. Employees the world over are exposed to numerous privacy invasive measures, including drug testing, psychological testing, polygraph testing, genetic testing, psychological testing, electronic monitoring and background checks. Hence, the issue at the heart of this dissertation is to determine to what extent privacy is protected in the South African workplace given advancements in technology and the implications (if any) for the right to privacy as such.

A secondary aim of the dissertation is to attempt to provide a realistic balance between the privacy concerns of employees and the operational needs of employers in this technological age. As such the main focus of dissertation falls within the sphere of employment law. In order to provide an answer to the research issue discussed above, the dissertation addresses five ancillary or interrelated issues. First, the broad historical development of the legal protection of privacy is traced and examined. Second, a workable definition of privacy is identified with reference to academic debate and comparative legislative and judicial developments. Third, those policies and practices, which would typically threaten privacy in the employment sphere are identified and briefly discussed. Fourth, a detailed evaluation of the tension between privacy and a number of selected policies and practices in selected countries is provided. More specifically, the dissertation considers how these policies and practices challenge privacy, the rationale for their existence and, if applicable, how these policies and practices – if necessary through appropriate regulation – may be accommodated while simultaneously accommodating both privacy and the legitimate concerns of employers. The selection of these practices and policies is guided by two considerations. At the first level the emphasis is on those challenges to privacy, which can be traced back to technological developments and which, as such, foster new and unique demands to the accommodation of privacy in the workplace. The secondary emphasis is on those policies, which are representative of the fundamental challenges created by new technologies to privacy.

To effectively address the above issues the dissertation uses the traditional legal methodology associated with comparative legal research, which includes a literature review of applicable law and legal frame work and a review of relevant case law and a comparative study of selected foreign jurisdictions.

ACKNOWLEDGEMENTS

This dissertation is dedicated to the two most important people in my life, my mother Lizah Collette Gondwe and my daughter "Little Miss Muppet", Uma Lizah Gondwe. It is also dedicated to the only family I have ever known, the Mbakile family and to the matriarch of our family, my gorgeous grandmother, Ntsatsi Mbakile and the memory of my late grandfather, Samuel Bruma Mbakile. This dissertation is further dedicated to all those who are contemplating studying for a PhD and those who have already embarked on a PhD – "if I can do it so can you", never give up no matter how rough and rugged the road may be because once you have reached your destination, the fact that you have reached your destination will be in the present and the struggles and challenges you encountered during the course of the journey will be in the past.

First and definitely foremost, I would like to thank God Almighty for all that I am and all that I am yet to become – Lord God my help comes from you and you alone. Thank you for giving me the strength, courage and armour to complete this dissertation. Thank you for also placing "angels" in my way to resuscitate my belief in myself and in this dissertation each time I felt like all hope was gone and each time I considered giving up on completing this dissertation. Lord God, please continue to light my way and guide me so that your purpose for my life will be realised.

I would also like to thank my beautiful, strong, generous and loving mother, Lizah Collete Gondwe for constantly inspiring me and encouraging me to do my best and give my all - Mummy you such a good role model and are always there for me especially when I need you the most. Thank you for your constant prayers and fasting. I am honoured and humbled to have a mother such as you; you are an exceptional mother, friend and confidante. Thank you for investing in my education and for teaching me to give without expecting nothing in return – Mummy I love you so much, thank you for your unconditional love and selflessness.

To my daughter Uma Lizah Gondwe – "Little Miss Muppet" – princess this is for you. I pray that one day you will also have the privilege of working on a doctorate. I do not know what I have done to deserve a gorgeous, intelligent and gentle daughter like you – I love you Uma.

To my dad, Franklin Clement Gondwe - thank you for your unreserved support and love and for consoling me each time I called you in a panicked and tearful state and for always answering my calls with the words "What's wrong my girl?" because when I heard you say these words I knew that everything was going to be alright.

To my brothers and siblings – Franklin Clement Gondwe Jnr and Gobe Nkosinathi Gondwe – thank you for your constant love and concern – Frankie please make me proud in all you do and Gobe I'm privileged to have a hardworking brother like you, I am so proud of you.

To my partner and the other part of our daughter, Tiroyaone Ambrose Sirang – it is now your turn to embark on this journey, I am here for you just as you are always there for me. Thank you for your love, patience and support and for never refusing to lend me you ear whenever I felt frustrated and disillusioned.

I would also like to extend my heartfelt and sincere appreciation to the two men who gave me the confidence and courage to see this dissertation through – Christoph Garbers and Professor Ockert Dupper. Christoph - you are the most brilliant person I have ever met – your ability to simplify and comprehend things astounds me. Thank you for the much needed criticism, guidance and mentorship. I would not be where I am now had you given up on me and had you not believed in me. Thank you for your efforts and for teaching me what it means and takes to be a true academic. Ockie – thank you for always being part of this dissertation not matter how near or how far you were and for taking the time to read my work and offering constructive criticism and for always prodding me in the right direction.

My auntie, Dr Christine Ega Moloi, also deserves special mention – auntie were one of my role models. Thank you for being the first in our family to get a doctorate. Thank you for your prayers honey. I looked up to you so much and I continue to pray that one day, I too, will end work for a prestigious institution such as the World Bank.

To my sponsors throughout my years of study – the NRF, Fulbright Foundation, Mellon Foundation, Fulbright South Africa and University of Stellenbosch – thank you for the financial and institutional support.

To my former boss and mentor, Larry Stein of Webber Wentzel's Banking and Finance Department – thank you for your patience and understanding and for believing in me and my abilities. You have taught me what it means and takes to be an excellent and exceptional commercial attorney –thank you Larricles and I look forward to being your client!

If I have left anyone out – I apologise- this does not mean I don't appreciate you and your love, support, encouragement and contribution towards the completion of this dissertation – God bless you all.

TABLE OF CONTENTS

CHAPTER 1:
INTRODUCTION

1.1 RESEARCH PROBLEM

The issue that constitutes the heart of this research is the extent to which advancements in technology impact on the protection of privacy in the workplace and the implications (if any) thereof for the right to privacy.

In order to determine this core issue, four ancillary and interrelated issues are addressed in this dissertation. The first ancillary issue relates to the broad historical development of the legal protection of privacy. The issue is addressed by focusing on the social conditions that have influenced the development of the legal protection of privacy and examining how early societies dealt with the notion and concept of privacy as it is known today. In addition, the gradual and somewhat laboured development of privacy protection from early times to present times is traced.

The identification of a workable definition of privacy comprises the second ancillary issue that is addressed in this dissertation. In doing so, reference is made to the extensive academic literature on the concept and value of privacy. In addition, the views of both proponents and critics of the notion of privacy are subjected to critical analysis.

The third ancillary issue to be addressed in the dissertation is the identification of workplace policies and practices of employers that typically threaten or place pressure on the notion of privacy in the employment sphere and the extent to which these policies and practices impact on the right to privacy in the workplace.

The fourth and final ancillary issue entails a detailed evaluation of the tension between privacy and a number of selected policies and practices. The selection of these practices and policies is guided by two primary considerations:

a) the primary emphasis is on those challenges to privacy that arise from technological developments and that, as such, place new and unique demands on the accommodation of privacy in the workplace;

b) a secondary focus is on those policies and practices that are representative of the fundamental challenges created by new technologies to privacy, such as genetic testing and e-mail/Internet monitoring.

Today, the rationale for the protection of privacy is not only widely accepted, but also extensively protected through a combination of international instruments, domestic constitutions, legislation, and, where applicable, the common law. This state of affairs belies the preceding, long and incremental struggle towards the legal protection of privacy that can be traced back to 1361, when the Justices of the Peace Act in England provided for the detention and arrest of peeping toms and eavesdroppers.[1] Up until the Second World War, privacy protection existed on an *ad hoc* basis through the application of existing legal principles such as the principles of the inviolability or the sanctity of the home and the secrecy of communications. In 1766, for example, the Swedish Parliament enacted the "Access to Public Records Act", requiring that all state held information be used solely for legitimate purposes. This Swedish law granted public access to government documents and upheld a principle known as *offentlighetsprincipen* (the principle of publicity) which was incorporated into the Swedish Constitution.[2] Consequently the eighteenth century was marked by a handful of countries enacting laws providing remedies for specific violations of privacy. The laws protected private property, personal and domestic affairs and state held information. However, none of these laws provided for a general right to privacy and privacy protection at this stage was largely protected on an ad hoc basis using existing law. That having been said there was growing awareness in legal circles that privacy had to be more than just a rule, but a protected right however a pronounced protection of privacy was only experienced at the end of the Second World War. The end of the Second World War and knowledge of the atrocities committed during this war resulted in increased awareness of the need to protect human rights, including the right to privacy, leading to concerted efforts to protect these international rights at an international and regional level through the adoption of various covenants[3] such as

[1] Michael *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) 15.

[2] *Supra*.

[3] Craig *Privacy and Employment Law* (1999) 5.

International Covenant on Civil and Political Rights[4] ("ICCPR"). As far as privacy protection is concerned, the early 1970s saw the incorporation or induction of the norms and principles established by the various covenants into national legal systems through the enactment of domestic privacy legislation.[5] Today a large number of countries recognise the right to privacy explicitly or implicitly in their constitutions. Although the constitutional provisions differ from country to country, at the minimum, these provisions include rights of the inviolability of the home and inviolability of communications.[6] Moreover, some countries such as South Africa include in their protection of privacy specific rights to access and control of one's personal information.[7] Even in those countries such as Ireland, the United States and India, where the Constitution is silent on the issue of the protection of privacy, the courts have imputed the protection of privacy from other constitutional rights.

1.2 HYPOTHESES

The research into the development of privacy protection revealed three significant realities with regard to right to privacy. First, the right to privacy remains an elusive concept, resulting in much debate and confusion. Not only is privacy difficult to define[8] but according to some commentators the difficulty with accurately defining privacy has also played a role in undermining its value and usefulness and has further impeded its effective legal protection.[9] Second, the fact that privacy has multiple meanings and therefore takes diverse forms means that a sense of what is private and what should be kept private differs from society to society. This means that privacy will have different consequences in different situations.[10] For this reason privacy as a concept is neither eternal nor universal, but rather a relative and contextual concept.[11] Third, the biggest continuous threat to privacy in the workplace remains developments in science and technology notwithstanding the fact that it has been

[4] Adopted and opened for signature, ratification and accession by the General Assembly of the United Nations resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976.

[5] Michael *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) 4.

[6] *Supra*.

[7] Section 14 of the Constitution of the Republic of South Africa Act 108 of 1996.

[8] Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1 3.

[9] Wacks *Privacy: Volume I The Concept of Privacy* (1993) xii.

[10] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1099 1132.

[11] See Gutwirth *Privacy and the Information Age* (2002) 29 and Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151 1153.

more than 100 years since two American lawyers, Warren and Brandeis observed that "the intensity and complexity of life and modern enterprise and invention ripened the time for the courts and judges to redefine the nature of personal rights to protect appearance, sayings acts and …personal relations, domestic or otherwise."[12]In this regard Warren and Brandeis further suggested that the law should recognise a right to "an inviolate personality" that would protect "thoughts, emotions and sensations…whether expressed in writing or in conduct, in conversation, in attitudes, or in facial expression."[13]

Present day advancements in technology and science make the recognition and protection of the right to privacy even more urgent. It is arguable that the rationale for the protection of privacy finds its most direct application in the employment sphere – a sphere where many employees spend most of their lives. The rationale for the protection of privacy in the workplace denotes the retention by the employee of a sense of autonomy, dignity and well being in the workplace. It may further be linked to the existence of the elements of good faith, trust, respect and loyalty within the employment relationship, recognised as such by the contractual basis of any employment relationship. Privacy in employment further ensures that the individual is free from conformist pressure and able to develop of fresh ideas, beliefs and attitudes which are pivotal to industrial pluralism.[14]

In contrast, those who oppose the need to protect privacy in the workplace, endeavour to justify curtailing employee privacy for the following reasons:

a) the improvement of economic conditions;
b) the need to protect the health and safety of workers, consumers and the public;
c) the need to deter and control employee abuse of the employment relationship;
d) the obligation to comply with legislation; and
e) the promotion of public interest.[15]

[12]Warren and Brandeis "The Right to Privacy" 1890 *Harvard Law Review* 193 196. According to the authors, "(t)he intensity and complexity of life attendant upon advancing civilization, have rendered necessary some retreat from the world and man under refining influence of culture has become more sensitive to publicity so that solitude and privacy have become essential to the individual…".

[13] Bible and McWhirter *Privacy in the Workplace: A Guide for Human Resource Managers* (1990) 34.

[14] Craig *Privacy and Employment Law* (1999) 20-26.

[15]*Supra*.

Thus, it may be said that the arguments advanced in opposition to the protection of privacy in the workplace do not really focus on the employee and the individual relationship of that employee with the employer instead they focus on the freedom of the employer to run its business and to exclude its possible liability, the more so where every employer operates in an environment concerned with the safety of employees and the public.

The concept of privacy in the workplace has grown in importance as technology has enabled new forms of testing and monitoring of employees. Employee monitoring is not necessarily a new trend,[16] but modern technology has enabled sophisticated forms of testing or monitoring of employees. These forms of testing or monitoring include drug tests, obtaining employees' credit history, HIV testing, genetic testing, background checks, psychological testing, polygraph tests, keystroke monitoring, listening to telephone calls and voice-mail, reading e-mail, monitoring computer, telephone and fax usage, use of electronic devices to track the location of employees, searching offices and workplaces as well as the use of video surveillance devices to monitor employees.[17] Use of these technological advancements has emphasized the tension between two conflicting sets of principles. On the one hand there is the principle of inviolability of the employee's right to privacy - employees do not cede their rights to privacy and dignity when they sign an employment contract. On the other hand, there is the right of the employer to enjoy its property and exercise its managerial powers of command to protect its property against abuse that might cause direct or indirect damage to the employer's business.[18]

Against this background, this dissertation identifies and examines some of the most prevalent technology-enabled employment practices and policies, namely background checks, polygraph testing, psychological testing, drug testing and HIV/AIDS testing and provides an illustration of how these practices and policies may invade the privacy of employees. It should be noted that the selection of the practices and

[16] Kesan *First Principle Examination of Electronic Privacy in the Workplace in Blanpain* (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 258.

[17] Solove and Rotenburg *Information Privacy Law* (2003) 618.

[18] Reinhard "Information Technology and Workers' Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law; Information Technology and Worker's Privacy: Information Technology and Worker's Privacy: Enforcement" (2002) 23 *Comparative Labour Law & Policy Journal* 527 527.

policies in this dissertation was guided by the emphasis on those challenges to privacy which arise from technological developments and foster new and unique demands for the accommodation of privacy in the workplace.

Background checks entail that employers acquire (and often store) information about an employee's credit history, employment history, school records, criminal convictions and medical history from the employee and third parties (such as previous employers, insurance companies and credit bureaus). Employers usually acquire such information during the recruitment and selection stages of employment. However, employers have also been known to undertake such checks during employment[19] and it is also important to note that in positions requiring a high degree of trustworthiness on the part of the employee, employers have a right (and perhaps a duty) to investigate the background of applicants. Background checks may infringe on an employee's privacy rights, particularly where the checks result in the disclosure of personal information that bears no relevance to the employment position or the suitability of an applicant for a position.[20]

The polygraph relies mainly on the subject's physiological reactions to a set of questions to draw an inference on the subject's truthfulness. There has been much debate as to whether the polygraph can produce empirically and scientifically reliable results.[21] Employers turn to polygraphs in the belief that the tests "detect and deter employee theft and other employee misconduct, including drug abuse, industrial espionage, and crime".[22] The widespread use of polygraph testing is especially evident in industries requiring high levels of trust and honesty, such as information

[19]See in this regard the decisions of *Smith and Grady* v *United Kingdom* [1999] ECHR 72 and *Lustig-Prean v United Kingdom* (1997) 7BHRC 65.

[20] The applicants in *Smith and Grady* v *United Kingdom* and *Lustig-Prean v United Kingdom*, members of the Royal Air Force and the Royal Navy (respectively), contented that investigations into their homosexuality and subsequent discharge on the sole ground of their homosexuality constituted a violation of their privacy right protected by Article 8 of the European Convention on Human Rights (which was drafted in 1950 by the Council of Europe and came into force on 3 September 1953). The government argued that admitting homosexuals to the armed forces would have a significant and negative impact on the fighting power, morale of armed forces personnel and the operational effectiveness of the armed forces. The European Court of Human Rights was of the view that the investigations into the applicant's homosexuality, which included detailed interviews with each of them and with third parties on matters relating to their sexual orientation and practices constituted a direct interference with the applicant's rights to have their private lives respected by others.

[21]Finkin *Privacy in Employment Law* (2003) 117.

[22] Hebert *Employee Privacy Law* (2009) § 6:5. See also Christianson "Truth, Lies and Polygraphs: Detecting Dishonesty in the Workplace" (1998) 18 *Contemporary Labour Law* 1.

technology, retail, security, criminal investigation and banking.[23] The right to privacy of individuals may be violated by the use of polygraphs particularly where the questions asked relate to personal information.

Psychological tests are used in the employment context to assess the suitability of an applicant's personality for a particular position. Employers use various psychological tests in the workplace, including personality tests, honesty tests and projective testing. Personality tests are aimed at identifying a person's "personal characteristics, thoughts, feelings and behaviour" through related questions.[24] The widespread use of personality tests as a way of identifying suitable employees has raised concerns relating to their validity and reliability.[25] Furthermore, and particularly relevant to this dissertation, personality tests infringe the privacy interests of test subjects because they consist of questions which are highly personal and sensitive in nature.[26]

Employers engage in drug and alcohol testing to identify users of illicit drugs and alcohol in the workplace to deter individuals in the workplace from using drugs and alcohol and to reduce the incidence of drug and alcohol related problems such as accidents and illnesses.[27] Urinalysis is the most common and preferred method of drug testing, because urine samples can be easily obtained and urine retains the presence of drugs for longer periods of time than, for example, blood.[28] Urinalysis as a method of drug testing has privacy implications primarily because the act of urination in itself is regarded as and has been described as highly personal and private.[29]

---

[23] Christianson "Polygraph Testing in South Africa Workplaces: Shield and Sword in the Dishonesty Detection versus Compromising Privacy Debate" (2000) 21 *Industrial Law Journal* 17.

[24] Hebert *Employee Privacy Law* (2009) § 7: 1.

[25] Critics of psychological and personality tests have argued that the tests are actually not an accurate predictor of employee performance. They further contend that the tests were developed for diagnosing psychological disorders and not best candidates for a job. Moreover in certain countries there are no rules regarding the analysis and validation of test procedures. To make matters worse no credentials are generally required for individuals and companies that develop and market the tests. Menjoge "Testing the Limits of Anti – discrimination Law: How Employers Use of Pre-employment Psychological and Personality Tests Can Circumvent Title VII and the ADA" (2003) 82 *North Carolina Law Review* 326 332. See also Ecker "To Catch A Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee" (1994) 63 *University of Missouri at Kansas City Law Review* 251259 and Hebert *Employee Privacy Law* (2009) § 7: 3.

[26] Hebert *Employee Privacy Law* (2009) § 7: 4.

[27] Hebert *Employee Privacy Law* (2009) § 2:5.

[28] Hebert *Employee Privacy Law* (2009) § 3:15.

[29] *Skinner v Railway Labour Executives Ass'n 109 S.ct* 1402 (1989) and *National Treasury Employees Union v Von Raab* 109 S.ct 1384 (1989).

HIV/AIDS tests are designed to determine if an individual has been infected with the HIV virus and do not detect the virus in individuals, but rather establish the presence of HIV virus antibodies in an individual's blood. As such, when a person tests positive for the virus, it is an indication of the fact that the person has HIV antibodies in their blood. HIV/AIDS testing in the workplace takes place not only in workplaces where the exchange of bodily fluids (or risk thereof) takes place, but also, in general, where an employer needs statistics for strategic workplace planning. However, even in those areas where there is a risk of an exchange of bodily fluids there is a reasonable expectation on employers to accommodate workers with the virus.[30] In this regard various countries have implemented legislation that substantially limits the extent to which employers carry out HIV/AIDS testing.[31] Such legislation is based on the premise that people living with HIV/AIDS should be entitled to work for as long as they can and further takes cognisance of the fact that with access to antiretroviral medication persons living with HIV/AIDS are able to lead healthy and productive lives.[32] One of the arguments made in opposition to HIV/AIDS testing in the employment sphere an employee is that such testing may infringe an individual's constitutional rights, such as the right to physical integrity and privacy and these inherent and constitutionally protected rights should trump the employer's right to contractual freedom in those instances where an employee's HIV positive status has no bearing on the job.

As previously stated the monitoring of employees by employers certainly occurred before the introduction of electronic communications. In the past employers monitored use of company resources by using onsite managers and supervisors whose job was to physically observe and monitor employees at work, to ensure that employees were being productive and efficient. Nonetheless, in the information age employers prefer other, perhaps more efficient, methods to monitor their business

[30] Bible and McWhirter *Privacy in the Workplace: A Guide for Human Resource Managers* (1990) 135.

[31] South Africa for example protects employees from HIV/AIDS testing through the Employment Equity Act 55 of 1998 and the Code of Good Practice on Key Aspects of HIV/AIDS and Employment of 2000.

[32] Bible and McWhirter *Privacy in the Workplace: A Guide for Human Resource Managers* (1990) 135.

operations in the interest of productivity such as e-mail/Internet monitoring.[33] Employers feel the need to closely regulate or monitor the use by employees of their e-mail/Internet resources to avoid the threats or risks associated with their use.[34] The monitoring of employee Internet and e-mail use involves two competing interests in the employment context: namely, the employer's right to conduct his or her business as he or she deems fit and the employee's right to privacy. On the one hand, employers are concerned about the abuse and unrestricted use of these tools by employees and the harm that could result from this unrestricted use. On the other hand, employees are concerned about their right to privacy and the use of Internet and e-mail in the workplace. The monitoring of employee Internet and e-mail use can, for example, result in the employer having knowledge of an employee's personal and private information.[35]

Genetic testing can reveal an array of existing and probable medical information concerning an individual including "presymptomatic medical information about an individual, including information about an individual's increased risk of future disease, disability, or early death…carrier status, that is, the likelihood of parents passing on to their children a genetic condition and about the health of the individual's family members".[36] That is to say, genetic testing can reveal an array of existing and probable medical information concerning an individuals' future health and an individuals' family's future health and also information relating to private decision making (such as whether or not to have a child)[37] and this is the primary reason why this type of information is considered more private than other forms of information. In the context of the workplace, employers administer genetic testing for pre-symptomatic, susceptibility and carrier testing purposes.[38] Two types of genetic

[33] Kesan "First Principle Examination of Electronic Privacy in the Workplace" in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 258.

[34] Kesan "First Principle Examination of Electronic Privacy in the Workplace" in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 253.

[35] Hebert *Employment Privacy Law* (2009) § 8A: 2.

[36] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 139 143.

[37] Annas "Genetic Privacy: There Ought To Be Law" (1999) 4 *Texas Review of Law & Politics* 9 10.

[38] United Kingdom Human Genetics Advisory Commission: Report on The Implications of Genetic Testing for Employment 1999. http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_03.htm (2006-03-27).

testing occur in the workplace, namely genetic screening and genetic monitoring. Genetic screening determines whether an individual has inherited genes that render him or her susceptible to both occupation – related or non – occupation related disease,[39]whilst genetic monitoring determines whether "occupational exposure to hazardous agents has resulted in any chromosomal or genetic damage".[40]

Insofar as this dissertation is concerned, a detailed emphasis or focus is placed on only two of the aforementioned employer practices and policies, namely genetic testing and e-mail and Internet monitoring of employees. What perhaps makes these practices and policies - e-mail/Internet monitoring and genetic testing – different from policies such as drug testing and HIV/AIDS testing is the fact that they arguably represent policies and practices that are based on the most recent and advanced technology available. As such, they represent both the essence of, and the latest in, the ongoing technological challenge to privacy in the workplace. Genetic testing and electronic surveillance therefore enhance the value of the research and thus serve as guiding principles for the further development of privacy in the workplace. At the same time, scientific and technological developments have a very real impact on the well being of employees worldwide. As such, this research focuses on the development of new technologies, their impact on the workplace and their inevitable adoption in the South African workplace. Finally, it is hoped that the research can be of practical value and enable employers to establish principles and guidelines for properly dealing with the issue of privacy in the workplace.

1.3 METHODOLOGY

In order to address the above issues, the traditional methodology associated with comparative legal research is used. This includes a literature review of the legal framework and relevant case law of a number of selected foreign jurisdictions - namely South Africa, the United Kingdom and the United States. The selection of these countries is motivated by the fact that each country presents a distinctly different approach to privacy protection: South Africa provides for and protects privacy explicitly through its Constitution; the United States has found a way to protect

[39] Hebert *Employee Privacy Law* (2009) § 12: 1.

[40]Deyerle "Genetic Testing in the Workplace: Employer Dream, Employee Nightmare Legislative Regulation in the United States and the Federal Republic of Germany" (1997) 18 *Comparative Labour Law Journal* 547 555.

privacy through other rights in its constitution despite the absence of an enumerated privacy right; and the United Kingdom (more specifically England) has no constitution, yet it protects privacy through common law principles and absorption of international human rights instruments.

1.4 SEQUENCE OF CHAPTERS

This dissertation will be structured in the following manner: Chapter 2 of the dissertation traces the historical development of the legal protection of privacy. In order to effectively do so, the chapter divides the history of the legal protection of privacy into four parts. The first part examines early conceptions of privacy and entails a brief exposition of social conditions in Greek, Roman, Ancient Hebrew, Medieval and Renaissance societies that highlight the origins of privacy concerns in these societies. The first part also discusses a number of early English cases often credited with sowing the seeds of what today is called privacy. The second part of the chapter deals with the gradual and specific protection of the right to privacy and, considers a number of legal principles and remedies that developed during the eighteenth and nineteenth centuries and which were primarily aimed at protecting various aspects of privacy. The third part, dealing with the legal protection of privacy, focuses on the international recognition of the right to privacy and examines various international instruments adopted during the twentieth century (especially after the Second World War) aimed at protecting fundamental rights, including the right to privacy. The fourth and last part of chapter 2 examines the explicit protection of privacy at domestic level and highlights the state of privacy protection today, particularly as far as its inclusion and protection in various national constitutions is concerned. The purpose of chapter 2 is therefore twofold: first, to chronologically address the development of the legal protection of privacy, and, second, to draw attention to the specific social conditions that influenced the protection of privacy.

Chapter 3 narrows down the general background picture provided by chapter 2. It focuses on the legal development of privacy protection in selected countries, namely South Africa, the United States and United Kingdom. This is done through the consideration of relevant case law and legislation that have contributed to the development of privacy protection in each jurisdiction under review. The selection of the aforementioned countries is motivated by the fact that each country has adopted a

differing approach to privacy protection. In this regard, South Africa provides for and protects privacy explicitly through its Constitution and the United States has found a way to protect privacy through other rights in its constitution, despite there being no explicit mention of this right in its Constitution. The United Kingdom has no constitution, yet it protects privacy through common law principles and absorption of international human rights instruments.

Chapter 4 of the dissertation critically assesses the possibility of a universal workable definition of privacy for purposes of the subsequent discussion. Of particular importance in this regard is the consideration of the concept and value of privacy. In doing so, various conceptions of privacy are examined, criticisms against the notion are canvassed, and, lastly (and perhaps more importantly), a workable definition of privacy is proposed.

The goal of the subsequent chapters, namely chapters 5, 6, 7 and 8, is to consider the issue that constitutes the heart of this research, namely, the extent to which privacy is protected in the workplace given advancements in technology and the implications (if any) for the right to privacy as such. In this regard, it may be said that privacy in the workplace has grown in importance as technology has enabled new forms of testing and monitoring of employees.

Chapter 5 advances the notion that employee monitoring is not necessarily a new trend,[41] but that modern technology has enabled sophisticated forms of testing or monitoring of employees. Chapter 5 proceeds to identity these various forms of testing or monitoring namely drug tests, obtaining the credit history of employees, HIV testing, genetic testing, background checks, psychological testing, polygraph tests, reading e-mail, and monitoring Internet and e-mail usage.[42] Subsequent to identifying and broadly discussing these forms of testing or monitoring, the chapter goes on to examine the two conflicting sets of principles implicated in the use of such testing or monitoring, namely the principle of inviolability of the employee's right to

[41]For instance, prior to the introduction of current technology enabling monitoring of employees, employers monitored their employee use of company resources by using onsite managers and supervisors whose job was to physically observe and monitor employees at work to ensure that they were being productive and efficient. Kesan "First Principle Examination of Electronic Privacy in the Workplace" in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 258.

[42] Solove and Rotenberg *Information Privacy Law* (2003) 618.

privacy on the one hand, and the right of the employer to enjoy its property and exercise its managerial powers of command to protect its property against abuse that might cause direct or indirect damage to the its business, on the other hand.[43] Chapter 5 also briefly considers the meaning of the phrase "privacy in the workplace" and provides an overview of the arguments for and against the need for privacy protection in the workplace.

Chapter 6 provides a more detailed and comparative discussion of the policies and practices identified in the preceding chapter in an effort to further explore the relationship between technological developments and privacy in the context of the workplace. To this end Chapter 6 sets out to do the following: first, it provides a brief introduction or overview of the extent to which a particular policy or practice is used in three selected jurisdictions, namely South Africa, the United Kingdom (as part of the European Community) and the United States; second, the chapter briefly examines the legislation, if any, regulating or impacting on the use of the particular policy or practice in these jurisdictions; third, reviews a selection of cases (where available) in respect of each jurisdiction which create a picture of how courts and tribunals in that jurisdiction have approached the application and impact of the policy or practice in question; and last, analyses the extent to which privacy is protected in light of the use of that particular policy or practice across the different jurisdictions.

Chapter 7 is the first of two chapters which give in -depth consideration of two sets of policies, namely, e-mail/Internet monitoring that are of recent origin and that illustrate the difficulty involved in resolving the tension between the rights of employers to have their property used in a beneficial and productive manner and the right of employees to the protection of their privacy. What perhaps makes these practices and policies - e – mail/internet monitoring and genetic testing – different to those considered in chapters 5 and 6 – is that e – mail/internet monitoring and genetic testing arguably represent policies and practices based on the most recent and advanced technology available. As such, they represent both the essence of, and the latest in, the ongoing technological challenge to privacy in the workplace. In this

[43] Reinhard "Information Technology and Workers' Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law; Information Technology and Worker's Privacy: Information Technology and Worker's Privacy: Enforcement" (2002) 23 *Comparative Labour Law & Policy Journal* 527.

chapter, e–mail/internet monitoring will be considered in some detail, while chapter 8 will focus on genetic testing.

As mentioned above Chapter 8 focuses on genetic testing, which perhaps is the most recent example of the way in which scientific advancement may challenge privacy. The chapter first considers what genetic testing means, an enquiry which requires, in turn, a consideration of genes, genetic testing and genetic information. Thereafter, the chapter considers the legal challenges created by genetic testing.

Chapter 9 of the dissertation draws the conclusion that even though the journey towards the legal protection of privacy has been a laboured one it was only a matter of time before the legal protection of privacy reached the level of protection that it now enjoys the world over because privacy is an essential and necessary value, right or claim without which man would cease to flourish, create and function. Chapter 9 further concludes advancements in technology remain the biggest threat to privacy in this day and age of significant scientific research and progress and as such they would invariably determine the extent to which privacy is protected. More importantly, the dissertation concludes the effective legal protection of privacy in is still in its infancy as far as South Africa is concerned and the concept of privacy as described in the Constitution is still being developed and nurtured by legal commentators and courts.

CHAPTER 2:
A BROAD HISTORY OF THE LEGAL PROTECTION OF PRIVACY

2.1 INTRODUCTION

A person's need for privacy is not a distinctly human notion, nor is it the result of the unique creative, ethical or intellectual abilities of humans. Ecological, biological and anthropological studies bring to light the fact that all animals (including humans) seek periods of seclusion or to be alone in small intimate or anonymous groups[44] without which they would cease to flourish and probably deteriorate or perish.[45] On the basis of this innate desire for privacy, Westin describes privacy as "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in state of solitude or small group intimacy, or, when among larger groups, in a condition of anonymity or reserve".[46] This state of anonymity or reserve was not always achievable or possible in early societies, which shaped and founded modern day notions of privacy (particularly the early Greek, Roman, Hebrew, as well as in medieval societies).[47] These societies were largely

[44] This seclusion is usually described as the tendency toward territoriality "in which an organism lays claim to an area of land, water, or air and defends its territory against intrusion by members of its own species. For example, the spined stickleback fish erects an invisible water wall around it and attacks any other stickleback that swim over the wall. The territorial tendency of animals, according to scientists serves the following purposes: it ensures propagation of the species by regulating density in relation to available resources; it enhances selection of "worthy" males; it provides breeding stations for animals that require male assistance in rearing their offspring; it provides a contact for group members against the entry of intruders and provides a physical frame of reference for group activity such as hiding. Animals and humans share distance setting mechanisms. An example of such distancing in the animal kingdom would be intimate distance among the bird and ape species where rules regulate the space between mates or between parents and their young. Westin *Privacy and Freedom* (1967) 7 – 8.

[45] Ecological studies show that overpopulation amongst animals can hamper the animal's ability to court, smell, feed properly or be free from constant defensive actions. In fact, overpopulation in animals can result in animals killing each other to reduce crowding or engage in mass suicides. Westin *Privacy and Freedom* (1967) 8.

[46] Contrary to Westin's assertion that privacy is an innate desire experienced by humans and animals alike, Posner argues privacy is a "cultural artefact" seeing as "[m]ost cultures have functioned tolerably well without the concept or reality of privacy in either its [sense] of seclusion or secrecy." Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1 2.

[47] These societies were chosen because they laid the foundation and shaped modern day notions of privacy. Moreover, there exist a considerable number of secondary sources detailing life in these societies.

communalistic, paternalistic and patrilineal in nature. In early societies, the need for privacy, solitude, seclusion or intimacy was not the dominant concern that it is in most contemporary societies. Nevertheless, individuals in early societies certainly felt the need for privacy. However, such a need was subjected to the existence of a range of social characteristics, such as the structure and nature of the society, the absence of words equivalent to the contemporary meaning of "private" and "public", the dominance of religion and religious practices, as well as the prevalent ideals, values or principles that excluded privacy and the public nature of "private affairs", such as marriage, relationships between men and women and child rearing.

This chapter broadly traces the development of the legal protection of privacy. To this end, the chapter divides the history of the legal protection of privacy into four parts. The first part examines early conceptions of privacy and entails a brief exposition of social conditions in Greek, Roman, Ancient Hebrew, Medieval and Renaissance societies that illustrate the privacy concerns in these societies. The first part also discusses a number of early English cases often credited with sowing the seeds of what today is called privacy. The second part dealing with the gradual and specific protection of the right to privacy, considers a number of legal principles and remedies during the eighteenth and nineteenth centuries which were primarily aimed at protecting various aspects of privacy. The third part, which deals with the legal protection of privacy, focuses on the international recognition of the right to privacy and examines various international instruments adopted during the twentieth century (especially after the Second World War) aimed at protecting fundamental rights, including the right to privacy. The last part of this chapter looks at the explicit protection of privacy at domestic level and highlights the state of privacy protection today, particularly as far as its inclusion and protection in various national constitutions is concerned.

As such, the primary purpose of this chapter is two-fold: first, to draw attention to social conditions in history that influenced the protection of privacy and, secondly, to chronologically address the development of the legal protection of privacy. Important moments in the development of such protection, at both an international and a domestic level, last-mentioned inclusive of legislation and case law, will be emphasised.

2.2 EARLY CONCEPTIONS OF PRIVACY

2.2.1 Ancient Greek Conceptions of Privacy

Early Greek conceptions of privacy dealt mainly with the refusal to seek or accept public office.[48] The individual seeking privacy and withdrawing into the private realm was no better than the Greek slave, female and child who had no role in public life. Public participation and responsibility and even competing for public office gave an individual dignity, self respect and personal honour.[49]

The *oikos* or *oikio* constituted the basic social unit in ancient Greek society. *Oikos* denoted all those living under the same roof. The oldest male headed the *oikos*, conducted all religious practices and performed all religious rites as well.[50] The social and political realm was known as the *polis*[51] and membership in this realm was guaranteed to all adult free males.[52] Women, children and slaves were excluded from participation in the *polis*. Citizenship in the *polis* meant access to sacramental or initiation ceremonies, markets, participating in public debate, policy and legislation formulation, religious festivals, the military (a primary obligation of the free male) and contributing to public opinion. Ancient Greeks, at least the Athenians, desired and lived a social life in the *polis*.[53] The ideal and accepted character was that of a man who was entirely social or of *polites* and any man displaying behaviour contrary to that of *polites* was regarded with suspicion:[54]

> "The *polis* demanded that the individual not only take part in [public activities], but he is ready to sacrifice his individual existence for it is to

[48] Moore *Privacy: Studies in Social and Cultural History* (1984) 118.

[49] Moore *Privacy: Studies in Social and Cultural History* (1984) 118.

[50] Salisbury (ed.) and Aldrette (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 25.

[51] Moore *Privacy: Studies in Social and Cultural History* (1984) 85.

[52] Citizenship in the Athenian *polis* was based strictly on descent. That is to say one had to be born of Greek parents to be considered a full citizen of the *polis*. Foreigners, women and slaves were generally excluded from citizenship in the Athenian *polis*. Nonetheless, in exceptional circumstances, the assembly of adult male citizens (the *ekklesia*) granted citizenship to a foreigner for exceptional service to the *polis*. Slaves in Athenian society also enjoyed varied degrees of social status. Moore *Privacy: Studies in Social and Cultural History* (1984) 85. See also Dickinson *The Greek View of Life* 19th ed. (1945) 77.

[53] Burns *Greek Ideals: A Study of Social Life* 2nd ed. (1919) 2.

[54] Burns *Greek Ideals: A Study of Social Life* 2nd ed. (1919) 2.

> the [*polis*] that he owes everything including the security of his very existence….".[55]

One writer described early Greek life as:

> "…one not only of public action. In this sense the social ideal may be called political… anyone who did not take part in the administration of the *polis* was looked at with suspicion…But although public activity was admired and cultivated, a quiet life was also allowed to be ideal, if it did not involve isolation. For a man should not be too busy about everything public".[56]

The Greek language drew a distinction between "private" and "public" realms. The distinction however was not clearly maintained in practice. The Greek word for private was *oikos* meaning "one's own" or "pertaining to one's self" and the word for public was *demios* meaning "having to do with other people" or *koinos* meaning "what is shared among friends" or "public affairs".[57] It is unclear what forms of social behaviour or activities fell into each realm, but there was a bias in Greek language against what is private.[58] Moreover, there was a greater emphasis on sharing what is in the public. There was debate amongst Greek philosophers centred on what private life is and whether it was preferable to public life.[59] The alternative of a life outside of public participation and responsibility, according to Greek writers such as Plato and Aristotle, was a life devoted to intellectual pursuits.[60] Plato expressed hostility towards privacy in his writing and argued that privacy posed a threat to the Greek communitarian tradition and togetherness. Plato further contended that privacy served no constructive or psychological purpose; hence any inclinations towards privacy in society should be rooted out.[61]

The distinction between the "private" and "public" realm overlapped with the distinction between the male dominated political realm and the female managed

---

[55] Burckhardt *History of Greek Culture* (1963) 13.

[56] Burns *Greek Ideals: A Study of Social Life* 2nd ed (1919) 120.

[57] Moore *Privacy: Studies in Social and Cultural History* (1984) 82.

[58] Moore *Privacy: Studies in Social and Cultural History* (1984) 82.

[59] Moore *Privacy: Studies in Social and Cultural History* (1984) 120 – 124.

[60] Moore *Privacy: Studies in Social and Cultural History* (1984) 120 – 124.

[61] Moore *Privacy: Studies in Social and Cultural History* (1984) 120 – 124.

household realm. As such, the home became tantamount to a sacred space reserved exclusively for the male and his family.[62] This theme has filtered into modern legal notions of a man's home, expressed in the adage a "man's home is his castle".[63] Despite this measure of privacy in one's home, there existed very few activities in early Greek life that individuals could partake of in isolation,[64] considering that the *polis* intervened in this household realm. The *polis*, for example, supported the punishment the husband meted out to an adulterous wife and appointed officials to keep aristocratic women and children within the confines of the home and away from the streets.[65]

The blurring of the "public" and the "private" realms in ancient Greek society is reflected in the regulation of marriage, child bearing and rearing. Philosophers like Aristotle encouraged the regulation of marriages, particularly with regard to when men and women could marry.[66] Hence, arranged marriages became the norm. Marriages were also used by privileged society to establish or cement alliances or social relations and for this reason wealth and status became criteria for choosing a suitable partner.[67]

The role of the Greek wife sheds further light on the diminished privacy individuals enjoyed. The overriding duty of a Greek wife was to provide her husband with healthy offspring to ensure succession of the household. Procreation in specific societies was also state regulated.[68] For example, in the Greek state of Sparta, the birth and rearing of children was controlled by the state. Spartan women were physically trained to enable them to successfully execute their maternal duties.[69] Moreover, children born to a man and woman were inspected by the elders for deformities. If a child upon inspection by the elders was found to be healthy, the mother was allowed to rear it,

---

[62] Moore *Privacy: Studies in Social and Cultural History* (1984) 120 – 124.

[63] Flaherty agrees that the notion of the sanctity of the home has filtered into modern law from ancient times, biblical literature and Roman law. Flaherty *Privacy in Colonial New England* (1972) 85.

[64] Dickinson *The Greek View of Life* 19th ed. (1945) 12.

[65] Moore *Privacy: Studies in Social and Cultural History* (1984) 135.

[66] Moore *Privacy: Studies in Social and Cultural History* (1984) 135.

[67] Moore agrees that marriage was not the result of romantic relationships and romantic relationships were commonly sought outside the marriage. Moore *Privacy: Studies in Social and Cultural History* (1984) 135.

[68] Dickinson *The Greek View of Life* 19th ed. (1945) 105.

[69] Dickinson *The Greek View of Life* 19th ed. (1945) 105.

but if a child upon inspection was found to be deformed, it was left to die.[70] Also in Sparta, a man could lend out his wife to another man in order to impregnate her.[71] The pressures of child bearing on the Greek woman did not only come from her household, but also from society at large and were also reinforced by prevailing medical theories.[72] Society at large expected its married people to have children to keep the population at parity and medical theory taught that abstinence from sexual activity was detrimental to one's health.[73] Plato's writings advocated the view that marriage should be conducted solely for the benefit of the *polis* – to elicit the "goodness" and "beauty" of the *polis*. Aristotle wrote that it was preferable to have sexual intercourse in winter time instead of spring or summer thereby equating sexual intercourse to a seasonal activity like the sowing or harvesting of crops.[74]

Privacy norms about marital and extramarital sexual relations existed even though Greek appreciation of artistic expression indicated that society was brazen about images of male genitalia, male and female nudity and heterosexual and homosexual fornication.[75] Sexual relations between the master and his slaves were also a common occurrence in the Greek household. Moreover, prostitution was a socially acceptable profession that was taxed and Greek prostitutes were intellectually accomplished and gifted women who charged for their companionship.[76]

No other members of Greek society experienced an absence of personal privacy to the extent of Greek slaves. Greek slaves generally had no legal status, but those who could, paid commission to their owners to live independently and carry out respectable

---

[70] Dickinson *The Greek View of Life* 19th ed. (1945) 105.

[71] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 46.

[72] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 46.

[73] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 46.

[74] Moore *Privacy: Studies in Social and Cultural History* (1984) 141.

[75] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 46.

[75] Moore *Privacy: Studies in Social and Cultural History* (2004) 148.

[76] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 46.

[76] Moore *Privacy: Studies in Social and Cultural History* (2004) 148.

positions in society as bankers, captains of trading vessels or shop managers.[77] Whereas free slaves lived independently of their master and merely handed a portion of their income to their master, chattel slaves were considered the property of their master.

2.2.2 Ancient Roman Conceptions of Privacy

Ancient Roman conceptions of privacy were largely similar to those of ancient Greece. This is not surprising given that Greek culture, art, religion and literature permeated Roman society.[78] Holding public office or engaging in public life (*bios politikis*) was expected of all males of the governing class and ensured a lifetime of honour. Persons holding no public office or deprived of public office were regarded as being persons of "no account" and not considered one of the "first men of the city".[79]

Ancient Rome[80] comprised of a male dominated society in which the father of a family, the *paterfamilias*, wielded paternal power (or *pater potestas*) and respect. The *paterfamilias* possessed unlimited authority in controlling the household and individuals living in that household. The *paterfamilias* not only negotiated and arranged marriages and divorces for his children, but acted as the "natural judge of the household".[81] As the "natural judge" of his household, the *paterfamilias* could also put his children to death[82] or sell members of his family into slavery.[83] Marriages in ancient Roman society (as in Greek society) were social and political arrangements. Roman marriages were private acts between individual families and, as such, could be

---

[77] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 112.

[78] Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 106 - 107.

[79] Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 106 - 107.

[80] Roman history spanned a considerable period of time. More specifically, ancient Roman civilisation existed from around 753 B.C.E. with the ascension of Romulus as the first King of Rome and ended with the fall of the Roman Empire to the Ottoman Turks in 1453. Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the PresentVolume 1 The Ancient World* (2004) 8 – 10.

[81] Salisbury (ed.) and Aldrette (Vol. ed.*) The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 36. See also Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 27.

[82] It was common for a *paterfamilias* to expose unwanted children for a number of reasons, including that he could not afford to keep them. A *paterfamilias* also exposed deformed children, children born out of infidelity, or children likely to disrupt his succession plans. Children could also be exposed as a sign of protest against the actions of the gods! Aries and Duby (1987) 11.

[83] Salisbury (ed.) and Aldrette (Vol. ed.*) The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 36. See also Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 27.

conducted in the absence of official sanction, a marriage contract or a formal ceremony.[84] Given that marriages were chiefly conducted to erect or cement alliances between families or political groupings, it was common for a politician to, for instance, marry, divorce and remarry to accommodate his altering political affiliations.[85]

All unmarried children were under the authority of the *paterfamilias*. The female child, once married, fell under the authority of her husband. The husband took up her father's role as her legal custodian or guardian.[86] The *manus* marriage was a popular form of marriage in which the wife figuratively speaking handed herself as property from her father to her husband.[87] Her husband consequently took ownership of her property and, like her father, was permitted by custom and law to kill his wife should she commit adultery or drink wine without his consent.[88] Whereas the female child was under the authority of her husband upon marriage, the male child (married or unmarried) remained under the authority of the *paterfamilias* unless the *paterfamilias* died or emancipated the male child.[89] Whilst the *paterfamilias* was alive or had not emancipated his male child, the male child could not without his father's consent sign a contract, engage in a career, free a slave or draw up a will and the *paterfamilias* owned whatever the male child earned or inherited.[90]

In addition to being conducted for political and economic gain, Roman marriages further sought to ensure procreation. As such a couple's duty was to bear legitimate heirs and replenish the ranks of the Roman citizenry.[91] Procreation was considered a

---

[84] Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 33.

[85] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 48.

[86] Cowell *Everyday Life in Ancient Rome* (1961) 48 - 49.

[87] The *manus* marriage had sub-categories. The first type of *manus* marriage was *co*-emptio, in which the groom literally bought his bride from her father for a price. The second type of *manus* marriage was the *usus,* in which a man and woman cohabited for an uninterrupted period of a year and after such a period the woman passed into the guardianship of the man. The period was considered interrupted if the woman spent three consecutive nights away from the man. Cowell *Everyday Life in Ancient Rome* (1961) 48 - 49.

[88] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 36.

[89] Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 27 – 28.

[90] The male child could, however, receive some money from the *paterfamilias* known as *peculum* to live on. Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 27 – 28.

[91] Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 35.

serious matter, so much so that the Emperor Augustus promulgated laws promoting marriage and procreation.[92]

Broadly speaking, Roman women led sheltered lives and had no citizenship rights such as voting, debating and running for office, but were expected to spend their days within the confines of the household and further be virtuous and modest in their behaviour. Upon venturing outside the confines of the household Roman women were carried by slaves in sheltered litters or in the company of female companions. Under the Empire wealthy women were in addition subject to laws regulating their clothing and jewellery.[93]

Slavery in Roman society also denied certain persons of individual privacy. Slaves had their fates determined by their owners and did not engage in public life. Roman slaves were obtained through military conquest or by birth and, once sold, these slaves became the property or possession of their buyer.[94] Before the slaves were sold their feet were chalked in white to indicate that they were for sale and wore signage around their collars listing their virtues and imperfections.[95] The more educated the slave was, the higher the price the slave fetched for its trader.[96] A slave could also be leased for a price and for a specified or indefinite period of time. Rural slaves usually endured manual labour on farms and were considered "articulate" tools of the farmer. Urban slaves enjoyed more freedom and undertook less arduous tasks than rural slaves, seeing that they lived in their master's household and were sometimes permitted to have families of their own.[97] Urban slaves were also more likely to receive an education and receive money from their master.[98] Slaves also had the misfortune of being branded by their masters in visible places or made to wear collars with their

[92] Salisbury (ed.) and Aldrette (Vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 37.

[93] *Supra*.

[94] Dilke *The Ancient Romans – How they Lived and Worked* (1975) 54.See also Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 63.

[95] Dilke *The Ancient Romans – How they Lived and Worked* (1975) 54. Slave traders were required to make potential buyers aware of dubious slave defects such as "religious fanaticism" and "excessive lust". Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 63.

[96] Dilke *The Ancient Romans – How they Lived and Worked* (1975) 97.

[97] Cowell *Everyday Life in Ancient Rome* (1961)108.

[98] Slaves usually saved this pocket money towards buying their freedom from their masters. A slave could also buy his freedom from savings which his master allowed him to keep. A slave could also be set free by his master as reward for his loyalty and honesty. Cowell *Everyday Life in Ancient Rome* (1961)108.

master's details.[99] Slaves had no legal rights and, furthermore, their children were born into slavery and became the property of the master.[100] A Roman slave's inferiority in society was further emphasised by the fact that a slave's evidence in court was only regarded as credible evidence under torture. Notwithstanding the inferiority of the slave, some slaves were employed by the Republic or religious temples as government officials. Roman law further provided that if a master was killed by one of his slaves, then all his slaves had to follow his fate and be put to death, usually by crucifixion.[101]

As in Greek society, sexual relations between the master and his slaves were commonplace. Ancient Romans lacked categories of sexual orientation and were therefore documented to have had sexual relations with both men and women. Prostitution was both a lawful and popular profession.[102] Prostitutes were taxpaying members of society who were required to register themselves with a local magistrate. Pornographic images adorned certain household items such as bowls and lamps. Marketplaces were sheltered by erotic murals and many homes housed paintings and mosaics depicting sexually explicit scenes.[103]

2.2.3 Ancient Hebrew Conceptions of Privacy

The social and political system of ancient Israel was also communal in nature. Ancient Hebrew society was built on kinship systems formed on the basis of blood relations and financial and social covenants.[104] That is to say, members of a household were not necessarily related by blood and households could be comprised of persons related by a covenant entered into by that household to ensure their socioeconomic survival.[105] The major difference between early Hebrew society and early Greco-

[99]Dilke *The Ancient Romans – How they Lived and Worked* (1975) 55. The master could choose to sell or keep his slave's offspring. Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 52.

[100]Dilke *The Ancient Romans – How they Lived and Worked* (1975) 55. The master could choose to sell or keep his slave's offspring. Aries and Chartier (eds.) *A History of Private Life: From Pagan Rome to Byzantium* (1987) 52.

[101]Cowell *Everyday Life in Ancient Rome* (1961) 100.

[102]Salisbury (ed.) and Aldrette (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 169.

[103]Salisbury (ed.) and Aldrette (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1 The Ancient World* (2004) 169.

[104] Matthews and Benjamin *Social World of Ancient Israel1250-587 BCE* (2002) 8 - 9.

[105] Matthews and Benjamin *Social World of Ancient Israel1250-587 BCE* (2002) 8 - 9.

Roman society was the formers' secular and religious nature, in comparison to the largely political and social nature of the latter.

The institution of marriage in early Hebrew society was far from a personal matter between a man and a woman. Rather, marriage was symbolic of the formation of political, economic and social agreements between households.[106] Men and women rarely chose their marriage partners as this was left to the father as the head of the household who had to exercise the responsibility of negotiating marriage covenants on behalf of the unmarried men and women in his household.[107] The father had the added responsibility of safeguarding the virginity of unwed women in his household before they were married off. A father's role in this regard was considered very important and a matter of honour for a household.[108]

The selection and consumption of food, especially during religious rites such as Passover, [109] defined and confirmed membership in Old Testament Hebrew society.[110] The Passover rite commemorates the time when God asked the Hebrews to mark the sides and tops of their doorframes with blood. The blood markings indicated the residence of Israelites in a particular house and such a household was spared destruction from various plagues.[111] Furthermore, the rite was a private affair performed in the intimacy of the household. The book of Deuteronomy contains a list of clean and unclean food Hebrews may (not) consume as "the children of the Lord".[112] The non – consumption or consumption of specified foods invoked religious and spiritual issues of "purity", "impurity", "holiness" and "profanity" and "sin" and "virtue".[113] In specific sections of the Old Testament, the Israelites are addressed,

[106]Matthews and Benjamin *Social World of Ancient Israel 1250-587 BCE* (2002) 13.

[107]Matthews and Benjamin *Social World of Ancient Israel 1250-587 BCE* (2002) 13.

[108] Genesis chapter 24 verse 16 and Numbers chapter 31 verse 18 refer to the virgin as a woman who has never known a man. The book of Deuteronomy, in chapter 22 verses 13-20, sets out the procedure to be followed where a woman is discovered to not be a virgin upon marriage or where a woman is married a virgin but her husband claims she was not a virgin. Matthews and Benjamin *Social World of Ancient Israel 1250-587 BCE* (2002) 177.

[109] The Passover rite (described in Exodus chapter 12) originated in Egypt. See Moore *Privacy: Studies in Social and Cultural History* (1984) 203.

[110]Moore *Privacy: Studies in Social and Cultural History* (1984) 203.

[111]See Exodus chapter 47 verses 12-13. See Moore *Privacy: Studies in Social and Cultural History* (1984) 202.

[112]Deuteronomy chapter 14.

[113] Sex, in the same vein as food, also raised questions of "purity and impurity, holiness and profanity". The Lord's commandments for example classify sexual behaviour as a subject of the highest concern

throughout the Old Testament, as "the Lord's children" or "the Lord's treasured possession" or "the Lord's chosen people".[114] The concept that Old Testament Hebrews were the Lord's property is another feature of ancient Hebrew culture that points to the fact that there was no defined conception of privacy.[115]

The Old Testament's treatment of nudity and nakedness provides insight into the fact that society recognised that the individual had some personal privacy. The book of Genesis records Adam and Eve as originally naked and not ashamed of their nudity. According to Genesis, Adam and Eve became aware and ashamed of their nakedness after they consumed fruit from the "tree of the knowledge of good and evil":

> "When the woman saw the fruit of the tree [of knowledge] was good for food and pleasing to the eye, and also desirable for gaining wisdom, she took some and ate it. She also gave some to her husband, who was with her, and he ate it. The eyes of both of them were opened and they realised they were naked; so they sewed fig trees together and made coverings for themselves."[116]

After consuming the fruit from the tree of knowledge, Adam and Eve experienced feelings of embarrassment, awkwardness, fear, shame and guilt and tried to hide themselves among the trees when God approached them.[117] Adam tells God "I heard you in the garden and I was afraid because I was naked; so I hid". Adam and Eve were said to "know instinctively without God's insight, the feeling of privacy and the fact that they had lost this feeling of privacy".[118] God in this regard gave man the right

---

to the entire community. That is not to say sexual behaviour was treated as a private matter subject to the free choice and will of the individual. Ancient Hebrew legislation and authorities used stringent sanctions to control sexual impulses within acceptable limitations. The book of Leviticus in chapter 18 and 20 respectively contain lists of unlawful sexual relations and sexual offences subject to the death penalty. Moore *Privacy: Studies in Social and Cultural History* (1984) 203.

[114]Dearman writes that the Israelites are referred to as God's peculiar treasure or prized possession three times in the Old Testament in the book of Deuteronomy chapter 7 verse 6; chapter 14 verse 2 and chapter 28 verse 18. Dearman *Religion and Culture in Ancient Israel* (1992) 130.

[115]Moore *Privacy: Studies in Social and Cultural History* (1984) 204. This reference to the Israelites as God's peculiar possession, according to Dearman, should not be construed as God asserting possession or ownership over the Israelites. Nor should it be construed as an assertion by God that the Israelites are an inherently superior people. It should rather be construed as an expression on the part of God of the fact that the Israelites are a people set apart for a particular purpose. Dearman Religion *and Culture in Ancient Israel* (1992) 130.

[116]Genesis chapter 3.

[117]Moore *Privacy: Studies in Social and Cultural History* (1984) 215.

[118]Wagner Decew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 11.

to be "reticent before the eyes of each other" by making Adam and his wife garments of skin and clothing them with these garments.[119] God is portrayed in this particular passage of the Old Testament as protecting the privacy of his children and inadvertently creating the right to personal privacy.[120]

The story of Noah and his sons also reinforces man's right to be reticent before the eyes of each other:

> "After the flood, Noah and his sons Shem, Ham and Japheth came out of the ark. Noah, a man of the soil proceeded to plant a vineyard. When he drank some of its wine, he became drunk and lay uncovered inside his tent. Ham, the father of Canaan, saw his father's nakedness and told his two brothers outside."[121]

Ham's bothers instinctively knew that Ham had violated their father's privacy by seeing their father naked and telling them that he had seen their father naked.[122] "But Shem and Japheth took a garment and laid it across their shoulders; then walked backward[123] and covered their father's nakedness. Their faces were turned the other way so that they would not see their father's nakedness."[124] The act of being naked or nakedness in the story of Noah and his sons is reinforced as private.[125]

Certain passages in the Old Testament further suggest there may have been no distinction between public and private realms of conduct and perhaps no words equivalent to "private" and "public". For example, the book of Psalms describes God as knowing the secrets of the human heart.[126] Moore writes: "There could be no secrets from God, and the most intimate affairs of what we would call private life were subject to religious norms and public intervention".[127] Some form of privacy was

---

[119] Genesis chapter 3 verse 21.

[120] Hixson *Privacy in a Public Society* (1987) 4.

[121] Genesis Chapter 9 verses 20 – 22.

[122] Wagner Decew J *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 11.

[123] Moore *Privacy: Studies in Social and Cultural History* (1984) 182.

[124] Genesis Chapter 9 verse 23.

[125] Wagner Decew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 11.The official religious position, according to Moore, was that the naked human body should be a private spectacle available only to the person enjoying marital rights. Moore *Privacy: Studies in Social and Cultural History* (1984) 215.

[126] Psalm 44 verse 21.

[127] Moore *Privacy: Studies in Social and Cultural History* (1984) 215.

observed with regards to "certain attributes of the deity and the purity of certain objects associated with religious aspects of their culture". The book of Deuteronomy explains "[t]he secret things belong to the Lord our God, but the things that are revealed belong to us and our children forever that we may follow all the words of this law".[128] For instance, on Mount Sinai, Moses points out to God: "The people cannot come up Mount Sinai, because you yourself warned us [to] [p]ut limits around the mountain and set it apart as holy."[129] This passage suggests that only God had a claim to privacy or secrecy. Religious rules also allowed the ancient Hebrew limited access to religious objects considered sacred such as the ark[130] and the Tabernacle. Limited rights to the private use and enjoyment of one's property existed, given that individuals were permitted to help themselves to their neighbours grain and grapes.[131] This is unsurprising in light of the fact that early Hebrew society was communal and individuals owned and did things for the benefit of the community as a whole.[132]

2.2.4 Medieval Conceptions of Privacy

The institution of feudalism characterised part of the Middle Ages in Europe. Feudalism essentially removed public power from the monarch and placed it into the hands of individuals holding public office and aristocrats possessing vast amounts of land and wealth.[133] Feudalism stripped the monarch of public power resulting "…in

[128] Deuteronomy chapter 29 verse 29.

[129] Exodus chapter 19 verse 23.

[130] Holiness in the Old Testament was, amongst others, associated with certain objects (such as the Ark) and places (such as Mount Sinai), specifically designated as such by God. These objects and places were also associated with God's presence. Dryness Themes *in Old Testament Theology* (1979) 51 -52.

[131] This notion of neighbourliness and generosity towards those in need is found in the story of David, Nabal and Abigail in 1 Samuel chapter 25. The story reads that David moved down into the Desert of Maon. A wealthy man named Nabal and his wife Abigail had property in Carmel and was in Maon shearing his sheep. David sent his young men to Nabal to ask for food and refreshment on his behalf. Nabal, a Calebite, was surly and mean in his dealings, so it was unsurprising when he refused David's request for food. David's men returned to tell him of Nabal's refusal. David then told some of his men to arm themselves and they set out to Nabal's property. One of Nabal's servants told Abigail, Nabal's intelligent and beautiful wife about this incident. Abigail lost no time and proceeded to pack food for David and his men. Nabal later died after the Lord had struck him. The moral of the story for Moore is that extending one's hospitality to strangers or to those in need should not be seen as an invasion of one's privacy. Moore *Privacy: Studies in Social and Cultural History* (1984) 203.

[132] Deuteronomy 23 houses a host of rules that the early Israelites were supposed to abide by. These rules range from who is to enter God's congregation and how women are to dress. Moore *Privacy: Studies in Social and Cultural History* (1984) 202.

[133] Feudalist practices occurred mainly in the following European countries France, Germany, Italy, England and Spain at varying stages and in varying forms. Thompson and Nathan *An Introduction to Medieval Europe 300 – 1500* (1965) 299. The birth of feudalism is sometimes attributed to practices

each great household becoming a sovereign unto itself, where the power exercised by the master [*dominus*] …was public", the landless and poor majority were relegated into serving as serfs for those wielding such public power.[134] Feudal lawyers described the "serf" as the lord's property as it was common to sell the serf as a slave and the serf was unable to leave the lord's service without the lord's permission. In addition the serf paid the lord taxes in money or in kind, sometimes at the Lord's discretion, and could not marry without the lord's authorization which was usually obtained after the serf paid the lord a marriage fee. The serf could further not appear against a freeman or his lord in a court of law.[135] Landed and wealthy aristocrats, as "kings" possessing their own "kingdoms", exercised a number of public duties ranging from conducting business transactions on behalf of their "kingdoms" and punishing offences committed by serfs and peasant workers inside and outside their "kingdom".[136]

In feudal Europe little privacy existed, even for the nobleman and the gentry in their "kingdoms". One writer explains:

> "[i]n feudal times, there was little space for privacy because of the paradoxical reason that all power was private. There was no public debate or public space where the common good was considered or observed".[137]

Moreover "[p]rivate interests in the middle ages were seldom honoured, for monarchies and churchmen were constantly preoccupied with constant battles for

---

of commendation, immunity and benefice. The practice of commendation took place where a landless and poor man would offer his service and honour to a landed man (such as a duke, count or court official) in exchange for food, clothing and protection. The practice of benefice was similar to that of commendation but differed in that the latter involved a less powerful man offering his land to a powerful landed aristocrat. A small landowner who found himself burdened by ownership responsibilities would cede his land to a big landowner in exchange for his continued tenancy on the land. In other words the small landowner would have a *usufruct* over the land, but in practice the small landowner also found himself in the service of the big landowner. The granting of immunities usually took place were the King would grant royal land subject to immunity to the Church through bishops and abbots. The bishops and abbots would then require that this immunity on the land be transferred to the Church. The Church as the owner of this royal immunity would then have royal prerogatives such the collection of taxes and dues. Thompson and Nathan *An Introduction to Medieval Europe 300 – 1500* (1965) 232.

[134] *Infra*.

[135] Thompson and Nathan *An Introduction to Medieval Europe 300 – 1500* (1965) 329 – 331.

[136] Salzman *English Life in the Middle Ages*(1926) 44.

[137] Gutwirth *Privacy and the Information Age* (2002) 21.

power".[138] The poor and landless classes were also unable to afford privacy given their squalid and cramped living conditions.[139] Prior to medieval feudal society, the existing power structures and relations were rarely mentioned or acknowledged in official documents.[140] Feudalism subsequently introduced the exposure and discussion of the existing power structures and relations through official documents[141] such as the English Magna Carta. The Magna Carta of 1215 accorded a range of rights and duties to freemen. The common man (known as "*villien*" - serfs, urban workers and those in the lower classes of society and their extended families) was excluded from exercising these rights and duties.[142]

The *villien* were bound by contractual obligations they owed to the lord. Lords could, as a consequence of these contractual obligations, acquire and dispose of the *villien* and the personal property of the *villien* belonged to the lord. The *villien* were

[138]Hixson *Privacy in a Public Society* (1987) 6.

[139]Strum *Privacy –The Debate in the US since 1945* (1998) 4. Thompson and Nathan also paint a grim picture of peasant or serf dwellings reinforcing the fact that they had little or no privacy. The authors describe the dwellings as "wattled cottages without windows, with thatched roofs and floors of the earth. The cottages were without chimneys; a hole in the roof let out the smoke form a small fire in the centre of the clay floor. The same hole let in rain and snow….candles were a luxury…Anyway what could a peasant do after dark, since he could neither read or write? He went to bed with the sun and was up with the sun." The authors further state that "The peasant shared his dwelling with his cats, dogs, and chickens and its thatched roof covered the stable as well." Thompson and Nathan *An Introduction to Medieval Europe 300 – 1500* (1965) 340 – 341.

[140] Aries and Duby (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 8.

[141] Aries and Duby (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 8 – 9.

[142] Mckechnie *Magna Carta: A Commentary of the Great Charter of King John* 2nded (1914) 107. The Magna Carta, sealed by King John at Runnymede, England in June 1215, granted the freemen of England and their heirs certain specified rights and liberties. The Carta arose out of a bargain between King John and members of a rebellion against his rule - in return for their renewed loyalty and allegiance, King John granted to all English freemen and their heirs the rights enumerated in the Carta. There has been debate about the legality of the Magna Carta. On the one hand the Carta is viewed as a formal piece of legislation in that it was sealed by King John with the consent of all those with political rights – such as abbots, earls, bishops and earls. On the contrary, it has been argued that the procedure followed in enacting the Carta was irregular in that (amongst other reasons) the assembly that assented to the Carta was not properly constituted. Mckechnie *Magna Carta: A Commentary of the Great Charter of King John* 2nded (1914) 105. Nonetheless the Carta is still considered an integral part of English history and politics. Mckechnie agrees that the Carta granted rights solely for the benefit of nobility. Chapter 1 of the Carta provides that the rights were granted "to all freemen of my kingdom [that is King John's Kingdom] and their heirs forever." The use of the word "freeman" for Mckechnie indicates that the application of the Carta was limited to a certain class of persons, as "freemen" in medieval times were usually landowners, barons, churchmen, merchants and yeomen. Evidence of the exclusion of the common man (*villeins*) from enjoying the rights accorded by the Carta is further provided by the fact that the executors of the Carta were themselves members of the privileged class. The Carta also makes the distinction between the villein and the freeman. Mckechnie *Magna Carta: A Commentary of the Great Charter of King John* 2nded (1914) 116.

forbidden from departing the lord's manor without permission from the lord.[143] The permission to leave the jurisdiction of the manor was usually granted if a *villien* paid his lord an annual fee. Secondary sources further indicate that the *villien* needed permission from the lord for his children to marry.[144] The *villien* usually exercised the obligations they owed to their lords by paying rent, fees and fines. Even as the *villien* served their lords, the freemen worked together with others of similar social status to protect the *res publica* (community) and the country (*patria*) against external and internal aggression by participating in military expeditions and local "peacekeeping" activities. These activities were usually directed by the magistrates charged with keeping the peace and justice in society.[145]

There seems to be no words for "public" and "private" in the Middle Ages. However, written Latin chronicles and charters made a distinction between public (*publicus*) and private (*privatus*) objects and acts. The word *publicus* denoted those things which belonged to the sovereign or were part of public office, or those acts falling under the jurisdiction of the magistrates who were charged with preserving the peace and dispensing justice[146] (such as Justices of the Peace Act in England of 1361). The Justices of the Peace Act provided for the detention and arrest of peeping toms and eavesdroppers in order to keep the peace.[147] There were also legal remedies against gossip and the scold.[148] The word *privatus* described those acts that were not performed in public or in the open, but inside one's home, in isolation and away from the prying eyes of others.[149]*Privatus* further denoted those acts, individuals and

[143] Salisbury (ed.) *Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 2 Medieval World* 312.

[144] Salisbury (ed.) *Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 2 Medieval World* 312.

[145] Salisbury (ed.) *Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 2 Medieval World* 312.

[146] Aries and Duby (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 8 – 9.

[147] Michael J *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) 15.

[148] International Commission of Jurists "The Legal Protection of Privacy: A Comparative Study of Ten Countries" (1972) 24 *International Social Science Journal* 418.

[149] Aries P and Duby G (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 5 – 6.

objects which were by law not subject to public authority. Therefore, non festive and domestic activities were often associated with the word *privatus*.[150]

Medieval society made little use of writing; written records were therefore not kept except for church, birth, death and marriage records.[151] Medieval society instead made great use of symbols such as emblems on the main gates of property and, more importantly, enclosures surrounding property.[152] Emblems decorating the gates and surrounding enclosures indicated the existence of private property and simultaneously served as a sign of ownership and privacy. Surrounding enclosures also served to "ward off violence, to drive it away from the place where people were most vulnerable…".[153] Public law encouraged the privacy provided by these enclosures, so much so that the crimes committed within these enclosures (or "private crimes") were subject to twice the penalty that "public crimes" (or crimes committed outside these enclosures) were subject to.[154] An offender committing a "private crime" within an enclosure he or she was found to be resident of could not be tried in terms of public law. The magistrate could not arrest the offender or even enter the enclosure unless the *dominus* authorised the magistrate to do so.[155] The non- application of public law or authority to the private realm illustrates the dissolution of public power during feudalism. The enclosure in early medieval society also housed the *res privatae* that is private property belonging to a household that was not *res publica*.[156] This property included reserves of food, livestock and slaves, women and minors. Persons residing in the household who were not part of *populus*, such as serfs, women and minors could only come under public authority if:

a) they went unaccompanied by the *dominus* or a freeman on public property, such as a road:
b) the *dominus* was absent and no freeman was able to protect them, and

[150]Aries P and Duby G (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 5 – 6.
[151]Strum *Privacy – The Debate in the US Since 1945* (1998) 4.
[152]Aries and Duby (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 12 – 13.
[153]Aries and Duby (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 12 – 13.
[154] Aries and Duby (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 12 – 13.
[155] Aries and Duby (eds.) *A History of Private Life: Revelations of the Medieval World* (1985) 12 – 13.
[156]Thompson and Nathan *An Introduction to Medieval Europe 300 – 1500* (1965) 291.

c) a public grievance (known as a "hue and cry") was brought by a complainant against a member of a household. [157]

Under feudalism, landowners therefore assumed the responsibility of privately regulating and protecting their "kingdoms" (against outside attacks in times of battle and controlled economic social and economic relationships). Landowners were not the only beneficiaries of a feudal state - monarchs also sought to benefit in transferring their public power and prestige to landowners.[158] This was especially true in the case of weak monarchs or where a monarch was experiencing difficulties in establishing effective administrative control over a kingdom. Due to this "numbing" of public power in the feudal state, there ceased to be a single unit of government. Instead, there were numerous small units of government known as marches, counties or duchies.[159]

Marriage in medieval Europe was characterised by a combination of economic and religious notions. For the serfs or *villien* the woman was a significant contributor to the household and a man therefore sought a wife who was skilled and industrious.[160] For the aristocrat, the woman played a less significant role in the household and so an aristocratic man sought a bride who came with a substantial dowry in the form of money or land. For the church, the overriding purpose of marriage was procreation and as such abortion and contraception were forbidden.[161] The medieval wife had the status of a child or servant of her husband. However, women were allowed to earn money by plying their trade and selling crafts and goods they made.[162]

---

[157] *Supra*.

[158] Thompson and Nathan *An Introduction to Medieval Europe 300 – 1500* (1965) 291.

[159] Thompson and Nathan *An Introduction to Medieval Europe 300 – 1500* (1965) 291.

[160] Salisbury (ed.) and Aldrette (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 2 The Medieval World* (2004) 41 -42.

[161] Salisbury (ed.) and Aldrette (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 2 The Medieval World* (2004) 41 -42.

[162] Salisbury (ed.) and Aldrette (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 2 The Medieval World* (2004) 52.

2.2.5 Renaissance and Enlightenment Conceptions of Privacy

The Renaissance and Enlightenment are often credited with the conception of contemporary notions of privacy.[163] Writers attribute the creation of contemporary notions of privacy to four cultural and political events:

a) The change in the role of the state;

b) The birth of the nuclear family;

c) The emergence of new forms of religion; and

d) The expansion of literature and the increase in the literacy rate.[164]

If the Middle Ages can be described as the period in which "all public power became private",[165] then it would be apt to describe the Renaissance as the period in which "almost all private power became public". In other words, the Renaissance epitomised the end of private power and the beginning of a powerful state.[166] The Middle Ages marked a time in history when the state was weak and played a largely symbolic role, as all public power became concentrated in feudal constituencies.[167] The Renaissance period redefined the role and status of the state to enable it to intervene in creating social order[168] and in asserting control over individuals and their actions.[169] As such, matters or individuals formerly restricted or confined to the private jurisdiction of the manor now fell under the public jurisdiction of the state. The state created at the end of the Middle Ages aimed, amongst other things, to establish peace and determined permissible and impermissible conduct.[170]

---

[163] Gutwirth *Privacy and the Information Age* (2002) 21 and Chartier R (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 2 – 4.

[164] Gutwirth *Privacy and the Information Age* (2002) 21 – 22.

[165] *Infra*.

[166] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 1.

[167] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 1.

[168] Social order was of such high concern that once literature became affordable and literacy expanded, books on civility and manners were published. These books made students and the general public aware of social conduct that was acceptable (from table manners to personal hygiene) and which would ease social intercourse and not offend religious rules. Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 181.

[169] Gutwirth *Privacy and the Information Age* (2002) 21. For instance, Justices of the Peace maintained social peace and order in England and were accordingly empowered to, amongst other things, issue warrants, make arrests and interrogate suspects. Justices of the Peace also acted as judges and mediators in petty disputes. Salisbury (ed.) and Seelig (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 4 17th and 18th Centuries* (2004) 392.

[170] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 16.

The role and status of the home also underwent transformation. The home, in the eighteenth century, became the focal point of private life and social life. The home also became a refuge or haven in which family members could seek solace and find defence against public scrutiny, outsiders or uninvited guests.[171] The home further became associated with happiness, affection and served as a symbol of morality.[172] The nuclear family emerged from the transformation of the home and individuals continued to withdraw into the privacy and comfort of the home.[173]

Along with this new role of the home came improved perceptions of the child. Whereas in the Middle Ages and earlier periods, the child had been viewed as a small adult constantly in need of correction and chastisement, the child was no longer chastised and expected to behave and dress like an adult.[174] Society celebrated the naturalness, individuality and innocence of the child and women were encouraged to remain at home with their children and to love and nurture them.[175] This tenderness and understanding expressed towards the child was encouraged by philosophers, the state and the church. Philosophers described children as "noble savages" capable of displaying noble thought and performing noble acts with the appropriate upbringing in the home.[176] The state and the church depicted the child in popular images as mystical, saint like and Christ like.[177] In addition, medieval child - rearing practices, such as swaddling the child in a corset to keep the child upright and shape its body, were replaced by less restrictive practices that allowed the child the freedom to explore.[178] The use of wet nurses was discouraged since it separated mother from the child and

[171]Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 8.

[172]Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 8.

[173]Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 16.

[174] Families, in celebration of their children, also commissioned portraits of them and begun to address them affectionately. Salisbury (ed.) and Seelig (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 4 17th and 18th Centuries* (2004) 72.

[175] Families, in celebration of their children, also commissioned portraits of them and begun to address them affectionately. Salisbury (ed.) and Seelig (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 4 17th and 18th Centuries* (2004) 72.

[176]*Supra*.

[177]Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 317.

[178] Salisbury (ed.) and Seelig (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 4 17th and 18th Centuries* (2004) 73.

further had the potential to interfere with the child's identity.[179] Instead, maternal breastfeeding was promoted, most likely in an effort to establish the bond between the mother and the child and as demonstration of affection towards the child. Places and spaces for privacy and intimacy were also created within the home.[180] Rooms within the home became smaller in size, acquired specialised functions and catered for intimacy.[181] A typical home of the well to do would have a nursery, drawing room, dressing room and reading room.[182] The study was created for the father of the house and he would read, pray and store important documents in the study.[183] This treatment of the home as a place of intimacy and privacy by the state led to perceptions of the inviolability of the home.[184]

The sixteenth and seventeenth centuries saw the firm entrenchment in society of religions such as Catholicism and Protestantism, fostering "inward piety" in addition to the pre - existing communal worship.[185] These new forms of religion also encouraged individual introspection of the conscience through confession, solitary meditation and prayer and keeping a private diary.[186] These confessions and diaries later unearthed a need for the individual to communicate with the self and to know the self.[187] For this reason, individuals began to engage in activities such as writing and painting purely for their own pleasure without the wish that their work be published.[188] This period also witnessed an excessive consumption of reading material such as histories, biographies, magazines, newspapers, sermons, novels and poetry as books became more affordable and accessible[189] and the literacy rate expanded with

[179] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 318.

[180] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 319.

[181] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 7.

[182] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 7.

[183] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 319.

[184] The early English matter of *Entick v Carrington* reiterated the inviolability of the home. See the discussion of the decision in the chapter.

[185] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 4.

[186] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 4.

[187] Chartier (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 5.

[188] For instance, in *Prince Albert v Strange and Others* 1 McN. & G. 25 (1849) (discussed in the text), the court reinforced the fact that individuals did not always wish to publish their work, no matter how famous they may be and the law was prepared to protect them. See also *Pope v Curl l*2TK. 342 (1741).

[189] Salisbury (ed.) and Lawrence (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 3 15th and 16th Centuries* (2004) 172.

the introduction of the printing press.[190] This growth of literature and the rise in the literacy rate encouraged individuals to record their private thoughts, experiences, and to further scrutinise them.[191] Diaries represented a place where these private thoughts, experiences, desires, emotions and memories could be stored. The diary generated a form of individual intimacy and solitude given that it was often written in isolation.[192]

A new form of reading also emerged during this time, namely silent reading. Silent reading fostered a private relationship between the reader and the book as it allowed the reader to engage in solitary reflection on the literature.[193] Silent reading further separated the reader from what was happening around the reader. All forms of work, including intellectual and artistic work became private, intimate and personal devotions not intended for public consumption.[194] Although the home was the primary retreat from the public, the library in the home became a secondary place of retreat especially from family and domestic responsibilities.[195] The use of the library, coupled with silent reading, ensured that reading became a private affair and as such books were often found in the more private areas of the home such as the bedroom or the study.[196]

2.2.6 Early English Cases and Privacy

It is often said that the seeds of what today is called privacy were first sown in England in the early eighteenth century.[197] Privacy in early English law often found protection in common law principles aimed at protecting other interests. As such, privacy found protection in the common law prohibitions against trespass, gossip, scolding, burglary, eavesdropping, voyeurism, libel, and slander and the adage that a "man's home is his castle".[198] For example, in *Entick v Carrington*[199], the plaintiff,

---

[190] Salisbury (ed.) and Lawrence (vol. ed.) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 3 15th and 16th Centuries* (2004) 207.

[191] *Supra*.

[192] *Supra*.

[193] Chartier R (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 125.

[194] Chartier R (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 125.

[195] Chartier R (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 134.

[196] Chartier R (ed.) *A History of Private Life: Passions of the Renaissance* (1989) 140.

[197] Ernst and Schwartz *Privacy: The Right to be Let Alone* (1962) 5.

[198] Flaherty *Privacy in Colonial New England* (1972) 85.

[199] 1558-1774 All E.R. Rep. 5.

Entick, brought an action against Carrington and three messengers of the King[200] for trespassing. The plaintiff declared that the defendants used force and arms to enter his house and searched its contents, including the plaintiff's private papers and books for four hours.[201] The defendants also seized some of the plaintiff's belongings, such as 100 printed charts and 100 printed pamphlets and delivered them to the Earl of Halifax's business premises. The plaintiff's seized books and papers were received by the Earl's assistant Lovel Stanhope for examination. The defendants denied liability on two grounds. First, they argued that they had acted under a warrant signed and sealed by the Earl of Halifax, a Lord in the King's Privy Council and one of the principal Secretaries of State.[202] The warrant was issued and sealed by Earl Halifax. The warrant, according to the Court of the Common Pleas, authorised the defendants to:

> "…make a strict and diligent search for the plaintiff, mentioned to in the warrant to be the author, or one concerned in the writing, of several weekly seditious papers, entitled, the "Monitor or British Freeholder" which contained gross and scandalous reflections and invectives upon his Majesty's government and upon both Houses of Parliament, and him, the plaintiff having been found, to seize and apprehend and bring together with his books and papers in safe custody before the Earl of Halifax to be examined concerning thepremises…".[203]

Second, it was argued that their conduct was within the scope of the Constables Protection Act of 1750. The Court found that "…neither the Secretary of State nor the messengers are within the Act of 1750" for two reasons:

a) The defendants failed to take a constable with them as required by the warrant; and
b) After the defendants carried away some of the plaintiff's private books and papers they brought them before Lovel Stanhope and not before the Earl Halifax.[204]

---

[200] The term "King" refers to the King of England.
[201] 42.
[202] 42.
[203] 42.
[204] 45.

The Court in addition found the warrant had been erroneously executed and therefore invalid, in that there was no summons, examination, hearing and proof (that the plaintiff was indeed the author of the alleged libel) preceding issuance of the warrant.[205] Lord Camden wrote the following in striking down the validity of the warrant issued by the Earl of Halifax:

> "Our law holds the property of every man sacred that no man can set his foot upon his neighbour's close without leave. If he does, he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law. The defendant's have no right to avail themselves of the usage of these warrants… and that if that would have justified them they have not averred it in their plea… We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property a man can have."[206]

Parliamentarian William Pitt enunciated similar sentiments when he wrote "the poorest man may in his cottage bid defiance to all force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement." [207]

The 1741 decision of *Pope v Curl*[208] treated a reliance on privacy as an unconventional property claim, but stressed the fact that the individual had some form of privacy in relation to any information he or she did not wish to share with the public.[209] In this case, Curl, an enterprising bookseller, unlawfully obtained and

---

[205] 45.

[206] 45.

[207] In a King's Bench decision of 1605 concerning the lawfulness of granting warrants to search for stolen goods, Sir Edward Coke interpreted the meaning of the maxim "a man's house is his castle" to mean first, "That the house of every one is to him as his Castle and Fortress , as well for his defence against injury and violence, as for his repose…" and second "…That it is not lawful for the sheriff…to break the defendant's House, to execute any process. For then thence would follow great inconven. That Men as well as in the night as in the day should have their houses (which are their castles) broke…and so mean would not be in safety or quiet in their houses." Flaherty *Privacy in Colonial New England* (1972) 85.

[208] 2 ATK.342 (1741).

[209] 608.

published certain letters to and written by well known literary figures, including Alexander Pope and Jonathan Swift. Pope successfully obtained an injunction against Curl to prevent him from selling the book, entitled *Letters from Swift, Pope and Others*, to the public.[210] Subsequently, Curl brought a motion to dissolve the injunction against any sales of the book. The question before the court was whether the letters contained in the book were protected by an Act aimed at encouraging learning and thereby vested ownership of copies of books of printed books in the authors of the relevant books or buyers of such books.[211] Curl argued that the Act did not extend to letters because "…where a man writes a letter, it is in a nature of a gift to the receiver." The Lord Chancellor found to the contrary and wrote:

> "…it would be extremely mischievous, to make a distinction between a book of letters, which comes out into the world, either by permission of the writer, or the receiver of them, and any other learned work. The same objection would hold against sermons, which the author may never intend should be published, but are collected from loose papers, and brought out after his death".[212]

In other words, with regard to letters, the rights of publication remained with the sender of the letter and not with the recipient of the letter.[213] The Lord Chancellor concluded as follows: "It is only in a special property in the receiver, possibly the property of the paper may belong to him; but this does not give licence to any person whatsoever to publish them to the world, for at most the receiver has only a joint property with the writer."[214]

The *Yovatt v Winyard*[215]decision is significant in that it not only held that personal secrets are inviolable, but took a step further and highlighted that "privacy", "plagiarism" and "unfair competition" were all included under the concept of "property". The plaintiff in this matter, a proprietor of medicines (what we would

---

[210]608.

[211]*Supra*. The Act was aptly entitled "An act for the encouragement of learning, by vesting the copies of printed books in the authors or purchasers of such copies."

[212]608.

[213]Ernst and Schwartz *Privacy: The Right to be Let Alone* (1962) 9.

[214]608.

[215]1 JAC.& W. 390.

today call a pharmacist), had employed the defendant as an assistant or journeyman.[216] In terms of the employment agreement, the defendant would get a salary and be taught generally about the business, but excluding the composition of medicines the plaintiff sold. The defendant later left their employment of the plaintiff and started his own business selling medicines. Thereafter the plaintiff discovered that the defendant, while in his employment, had surreptitiously acquired books of recipes and made copies of these to make and sell medicines of the same composition as those the plaintiff sold.[217] The plaintiff therefore sought an injunction to restrain the defendant from continuing to produce medicines from the plaintiff's recipes and selling them.[218] The Lord Chancellor granted the injunction on the ground that there been a breach of trust and confidence.[219]

Similarly, in *Truck v Priester*[220], the court reinforced an artist's or author's right to regulate the use of his work in the public domain (as the right to regulate information emanating from his person). The plaintiffs in *Truck v Priester* were art publishers, employed by the defendant, a printer based in Berlin, to make copies of a water-colour drawing called "Sounding the Charge". The defendant did this, but also made copies of the drawing for himself without the knowledge and consent of the plaintiff, and exported some of the copies to England. The plaintiffs subsequently registered their copyright in the drawing under the Act 25 & 26 Vict. c. 68.[221] After the plaintiff's registration of their copyright in the drawing, the defendant sold some of the imported copies in England. On discovering what the defendant had done, the plaintiffs claimed penalties, damages and an injunction. Lord Esher of the Court of Appeal held:

> "A copyright existed in the picture, and, without the consent of the proprietors, copies were made by the defendant. By reason of a statutory limitation the plaintiffs cannot sue the defendant for making copies, because they were made before registration. But I cannot doubt that it was absolutely wrong to make copies of that in which another

[216] 426.
[217] 426.
[218] 425.
[219] 426. See also Ernst and Schwartz *Privacy: The Right to be Let Alone* (1962) 11.
[220] 19 Q.B.D 639 (1887).
[221] This Act regulated copyright in paintings, drawings and photographs in nineteenth century England.

> man had the copyright without his consent…But then after the defendant goes on and sells the copies which he made before registration, and in respect of that sale the plaintiff can recover damages."[222]

Lord Esher thus found that the plaintiffs could not recover damages from the defendant for making unauthorised copies before registration of their copyright in the drawing, but were entitled to damages for the sale of the copies after the registration of their copyright in the drawing.[223]

The matter of *Prince Albert v Strange and Others*[224] is perhaps the most famous case with regard to early privacy protection. The plaintiffs in this matter were the British royal couple, Her Majesty Queen Victoria and her husband, Prince Albert. They brought an injunction against the reproduction and cataloguing of their etchings and drawings. The royal couple sought to restrain the defendant from cataloguing and selling reproductions of etchings done by them at a public exhibition without the royal couple's consent.[225] The royal couple argued that the etchings were intended for their private use and although copies of the etchings were occasionally made they were made using a private press and given to personal friends. The defendant's legal counsel argued that the right to privacy was distinct from the right to property:

> "It has been argued that privacy is the essence of property, and that the deprivation of privacy would make it, in fact, cease to be property…The notion of privacy is a notion altogether distinct from that of property; that another man should or should not see it is not property. There is no such property as the exclusive rights of seeing and talking about property."[226]

Despite this predictive and compelling argument from Strange's counsel, the court found for the royal couple. The case is famous for laying the legal foundation for the protection of privacy. The Vice Chancellor wrote in deciding this case: "Every man

---

[222] 637.

[223] 637.

[224] 1 McN. & G. 25 (1849).

[225] Quoted from Ernst and Schwartz *Privacy: The Right to be Let Alone* (1962) 20.

[226] Quoted from Ernst and Schwartz *Privacy: The Right to be Let Alone* (1962) 20.

has a fight to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public or commit them only to the sight of his friends. In that state the manuscript is, in every sense, his peculiar property; and no man can take it from him, or make any use of it which he has not authorized, without being guilty of a violation of his property."[227]

In summary, it may be said early English cases recognised an element of privacy under the general right to property. These cases later contributed to the general recognition of the common law right to privacy. The authors Warren and Brandeis used some of these cases to advocate the recognition of a common law right to privacy in American jurisprudence.

2.3 GRADUAL AND SPECIFIC PROTECTION OF THE RIGHT TO PRIVACY

The eighteenth century was marked by a handful of countries enacting laws providing remedies for specific violations of privacy. The laws protected private property, personal and domestic affairs and state held information. However, none of these laws provided for a general right to privacy. In 1766 the Swedish Parliament enacted the "Access to Public Records Act", requiring that all state held information be used solely for legitimate purposes. This Swedish law granted public access to government documents. This law upheld a principle known as *offentlighetsprincipen* (the principle of publicity) which was incorporated into the Swedish Constitution. In 1819 France recognised the action for defamation and further prohibited the publication of private facts and set out to fine those who broke this law. France took matters a step further in 1881 and granted the right of reply in a dispute between an individual and the press. Norway went on to prohibit the publication of information relating to personal or domestic affairs through a criminal statute in 1899.[228]

United States courts have, as far back as 1891, interpreted the Constitution as implicitly providing for the right to privacy. The Supreme Court in *Union Pacific Union Pacific R.R Co v Botsford*[229] stated that "[n]o right is held more sacred, or is

[227] Quoted from Ernst and Schwartz *Privacy: The Right to be Let Alone* (1962) 20.

[228] Michael J *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) 15.

[229] 141 US 251 11 S.Ct 1000, 35 L.Ed 734 (1891).

more carefully guarded by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference by others, unless by clear and unquestionable authority of the law".[230]

German jurists at this stage also contributed towards the rise of privacy protection. They contributed towards the creation of German law that treated privacy protection as an aspect of personality.[231] They further endorsed the theory of personality as the true theory of freedom and as such, privacy for Germans became a part of "free realisation". It is important to note that during this period Germans had strong attachments to notions of honour and respectability. It was therefore not surprising that the law of insult played a major role in legal thought. German jurists "accordingly embarked on an impressive reinterpretation of ….traditional law: the ancient Roman law of insult which they combined with the law of artistic property to create a solid foundation for a new body of personality."[232] The German law of personality was therefore reinterpreted and its reinterpretation relied on two main strands of law. The first strand was the Roman law of insult, which protected all aspects of honour and gave protection against verbal insults and other displays of disrespect. The other strand, was the law of *urheberrecht* or *droit moral de l"ateur* or the creator's rights, which were partly copyright but included "the right to control the use of one's work, in the name of protecting one's reputation as an artist".[233] Gareis, an influential German writer in the late 1870's, popularized the idea that personality was a mixture of the law of insult and the law of artistic creation. In an 1877 article, Gareis argued for "a right for the individual to organize his life as he likes a right to a person's name and to his honor".[234] Gareis's ideas also influenced a number of cases. Of note is a case concerning the prohibition of the distribution of pictures depicting Chancellor Otto Bismarck on his deathbed. The case resulted in the introduction of statutory

[230]251.

[231]Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 13-14.

[232]Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 13-14.

[233]Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 13-14.

[234]Stromholm *Right of Privacy* (1967) 29.

protection of one's image.[235] Otto von Gierke also advanced the recognition of personality rights and argued for the "right to be recognized as a personality" and "postulated rights to a person's body and life, liberty, honor, social position, free activity, commercial sphere of activity, name and marks and…intellectual property."[236] Later Kohler, like Gareis and Gierke, argued for a general right to personality. However, Kohler included in his general right to personality the limited right of the individual to a sphere of intimacy, to the name and likeness of a person.[237] In 1907, Kohler published an article on literary copyright in which he defines the right of secrecy as protecting the publication of letters, a person's name and likeness and private facts. Like the United States authors Warren and Brandeis,[238] Kohler referred to the case of *Prince Albert v Strange*[239] as the leading case protecting privacy in the unauthorized publication of private documents.[240]

To sum up, privacy protection at this stage was largely protected on an ad hoc basis using existing law. Moreover, there was growing awareness in legal circles that privacy had to be more than just a rule, but a protected right. A pronounced protection of privacy was only experienced at the end of the Second World War. The end of the Second World War and knowledge of the atrocities committed during this war resulted in increased awareness of the need to protect human rights, including the right to privacy.

2.4 INTERNATIONAL RECOGNITION OF THE RIGHT TO PRIVACY

The collapse of the Fascist and Nazi regimes and the atrocities committed by these regimes before and during the Second World War, gave birth to a need to specifically protect individual and fundamental human rights at international and regional levels.[241] Consequently, on December 10, 1948 the United Nations General Assembly

[235]Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" 113 *Yale Law Journal* (2004) 14.

[236]Stromholm *Right of Privacy* (1967) 29.

[237]Stromholm *Right of Privacy* (1967) 31.

[238]Warren and Brandeis "The Right to Privacy" 1890 *Harvard Law Review* 193. See a more detailed discussion of this benchmark article in Chapter 3.

[239]1 McN. & G. 25 (1849).

[240]Stromholm *Right of Privacy* (1967) 31.

[241]Craig *Privacy and EmploymentLaw* (1999) 5.

adopted and proclaimed the Universal Declaration of Human Rights as the yardstick for human rights protection. The Declaration also serves as the authoritative guide to the interpretation of the United Nations Charter of 1945.[242]

Article 12 of the Declaration provides:

1. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks on honour or reputation.
2. Everyone has the right to the protection of law against such interference or attacks.

Regional protection of the right to privacy is found in numerous treaties,[243] including the Council of Europe's European Convention on Human Rights[244] ("ECHR"). Article 8 of the ECHR provides that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

[242] Brownlie and Goodwin-Gill (eds.) *Basic Documents on Human Rights* 5th ed. (2006) 23.

[243] The Organisation of American States (OAS) has two human rights instruments protecting the right to privacy, namely, the American Declaration of the Rights and Duties of Man (Approved by the Ninth International Conference of American States, Bogota, Columbia 1948) and the American Convention on Human Rights (also known as the "Pact of San Jose", adopted in Costa Rica in 1969). The American Declaration of the Rights and Duties of Man was the first international human rights instrument adopted months after the Universal Declaration of Human Rights. The American Declaration protects individual honour, reputation, private life, the inviolability of the home and the inviolability of correspondence. The Declaration protects privacy in its various articles: Article V. Every person has the right to the protection of the law against abusive attacks upon his honour, his reputation, and his private life; Article X. Every person has the right to the inviolability of the home; Article XI. Every person has the right to inviolability and transmission of his correspondence. The American Convention of Human Rights is more elaborate than the American Declaration in its provisions. It protects the individual right to dignity and against arbitrary and abusive interferences of an individual's private life, family, home or correspondence. Unlawful attacks on an individual's honour or reputation are also protected. The Convention obligates the state to protect the individual against such interferences and attacks. Article 11 of the Convention reads: "Everyone has the right to have his honor respected and his dignity recognized. No one may be the object of arbitrary or abusive interference with his private life, his family, his home or correspondence, or of unlawful attacks on his honor or reputation. Everyone has the right to the protection of the law against such interference or attacks."

[244] Drafted by the Council of Europe in 1950 and came into force on 3 September 1953.

The ECHR further created the European Commission on Human Rights and the European Court of Human Rights to oversee the enforcement of the ECHR. The Commission and the Strasbourg Court have made a number of progressive decisions on the meaning and protection of privacy as articulated in Article 8 of the ECHR. One of these decisions is *X v Iceland*[245].[246] The Commission in *X v Iceland* held the following on the concept of private life:

> "For numerous Anglo-Saxon and French authors the right to respect for "private life" is the right to privacy, the right to live as far as one wishes, protected from publicity…however, the right to respect for private life does not end there. It further comprises, to a certain degree, the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's personality".[247]

The commission added that:

> "…it cannot, however accept the protection afforded by Article 8 of the Convention extends to relationships of the individual with his entire immediate surroundings, insofar as they do not involve human relationships and notwithstanding the desire of the individual to keep such as relationship within the private sphere".[248]

The question before the commission was whether the keeping of a dog contrary to the relevant provisions in the city of Reykjavik, belongs to "private life" within the meaning of Article 8 of the ECHR. The ECHR, unlike the Declaration, is binding, self executing and directly affects national legal systems. Where the treaty is incorporated into domestic law, it takes precedence over conflicting domestic legislation.[249]

On an international level, the International Covenant on Civil and Political Rights[250] ("ICCPR") is perhaps the most important international Covenant protecting privacy.

---

[245] Application No 6825/74, 87.

[246] See also *Bruggemann and Scheuten v Federal Republic of Germany* (1981) 3 E.H.R.R. 244 253.

[247] 87.

[248] 87.

[249] Gutwirth *Privacy and the Information Age* (2002) 35.

[250] Adopted and opened for signature, ratification and accession by the General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976.

Article 17 of the Covenant protecting the privacy of persons is similarly worded to Article 12 of the Universal Declaration of Human Rights. Article 17 states that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor attacks on honour or reputation.
2. Everyone has the right to the protection of law against such interference or attacks.

Article 17 does not limit the concept of privacy to individuals but embraces other zones of privacy ("kinship" zone of the family and the "physical zone" of the home and correspondence).[251] Paragraph 1 of Article 17 further prohibits the arbitrary or unlawful interference with an individual's privacy. The term "unlawful" has been defined in the General Comment of the Human Rights Committee to mean "that no interference can take place except in cases envisaged by the law. Interference authorised by States can only [occur] on the basis of law [complying] with the general provisions, aims and objectives of the Covenant." Further, the term "arbitrary interference" includes lawful interferences and such interferences have to also comply with the provisions, aims and objectives of the Covenant.[252] Paragraph 2 of Article 17 provides for the protection of the law from interference or attacks on one's privacy. The Committee explained that this provision guarantees against all such interferences and attacks emanating from both the state and from natural or legal persons. The provision also imposes obligations on the state to adopt laws and measures giving effect to the prohibition against such interferences and attacks and protection of the right.[253] Article 17 of the ICCPR is, like Article 8 of the ECHR binding, self – executing and directly affects national legal systems.[254]

[251] Harris and Joseph (eds.) *The International Covenant on Civil and Political Rights and United Kingdom Law* (1995) 334.

[252] Harris and Joseph (eds.) *The International Covenant on Civil and Political Rights and United Kingdom Law* (1995) 335.

[253] Harris and Joseph (eds.) *The International Covenant on Civil and Political Rights and United Kingdom Law* (1995) 336.

[254] Gutwirth *Privacy and the Information Age* (2002) 35.

2.5 THE PROTECTION OF PRIVACY AT THE DOMESTIC LEVEL

Today a large number of countries recognise the right to privacy explicitly or implicitly in their constitutions.[255] The constitutional provisions differ from country to country. However, at the minimum, these provisions include rights of the inviolability of the home and inviolability of communications. Moreover, some countries such as South Africa include in their protection of privacy specific rights to access and control of one's personal information. That being said, the protection of privacy at the domestic level by various countries can be divided into three categories. The first category of countries recognises the existence of a right to privacy and explicitly protects the right to privacy in their respective constitutions. Countries in this category include the Republic of South Africa[256], Belgium[257], Finland[258], Namibia[259], Spain[260] and Switzerland[261]. The second category of countries recognises the existence of the right to privacy and implicitly protects the right to privacy using other constitutional rights. Countries such as Germany[262], United States[263], Brazil[264], Canada[265], Sweden[266], Denmark[267], Portugal and India fall within this category. The final category is

[255] Remarkably, Mexico implicitly recognised the right to privacy in its 1857 Constitution in articles 13 and 14 and again in its 1917 Constitution in articles 14 and 16. International Commission of Jurists "The Legal Protection of Privacy: A Comparative Study of Ten Countries" (1972) 24 *International Social Science Journal* 418.

[256] Section 14 of the Constitution of the Republic of South Africa Act 108 of 1996.

[257] Article 22 of the Belgian Constitution of 1970.

[258] Section 10 of the Finnish Constitution of 1999.

[259] Article 13 of the Namibian Constitution of 1990.

[260] Article 18 of the Spanish Constitution of 1978.

[261] Article 13 of the Swiss Constitution of 1999.

[262] Articles 1 (personality right) and 2 (individual right to free development of one's personality) of the Basic Law of 1949

[263] 1st Amendment (religion and expression), 3rd Amendment (quartering of soldiers), 4th Amendment (search and seizure), 5th Amendment (right of persons), 9th Amendment (unenumerated rights) and penumbras of the Bill of Rights.

[264] Article 5, X (inviolability of privacy, private life, honour and image of person) of the Constitution of 1998.

[265] Sections 7 (right to life, liberty and security of the person) and 8 (protecting against unreasonable searches and seizures) of the Charter of Rights and Freedoms of 1982.

[266] Article 6 (protects citizens against physical searches and examinations of mail and other confidential correspondence and against eavesdropping, telephone tapping and recording of confidential communications) of the Constitution of 1974.

[267] Section 72 (guarantees the inviolability of the house, protects against searches and seizures and examination of letters and other papers and secrecy in respect of papers and secrecy in respect of postal, telephone and telegraph communications) of the Constitution of 1953.

comprised of countries in which there is no constitutional protection of the right to privacy. Privacy is instead protected by the common law or a specific privacy act or through the incorporation of an international instrument. The United Kingdom has no constitution, let alone a protected right to privacy, but privacy is protected by the common law doctrine of breach of confidence and the incorporation in domestic law of Article 8 of the ECHR. Australia, like the United Kingdom, does not have a constitutional right to privacy but protects the right to privacy through its Privacy Act[268].

International agreements like the International Covenant on Civil and Political Rights and the ECHR that recognise the right to privacy have also been adopted into law by certain countries, thus buttressing the protection of privacy in those countries.

2.6 CONCLUSION

This chapter sought to broadly trace the legal development of privacy protection by dividing it into four stages. The "early conceptions of privacy stage" indicated early conceptions of privacy did exist, but these were usually overshadowed by the communal tradition prevalent in these societies. Moreover, early conceptions differed from one society to another and each society defined, structured and delineated notions of privacy differently.[269] For example, the early conception of privacy in Greek society was associated with a refusal or shunning of public office or responsibility, whereas the privacy conceptions of Hebrew society were associated mostly with religious activities. A consideration of this period further shows that remnants of early conceptions of privacy, particularly those formulated during the Renaissance period, have filtered into contemporary notions of privacy. During the second broad developmental stage – that of "gradual and specific protection" - privacy was protected on an ad hoc basis using existing law in view of the growing awareness in legal circles that privacy had to be more than just a principle or value, but a protected right. The protection of privacy then went through a third stage – that of "international recognition" –where a series of international and regional legal instruments (with varying legal effect) expressly recognised and declared respect and protection for a fundamental right to privacy. The last stage of development, one we

[268] Act of 1988.

[269] Gutwirth *Privacy and the Information Age* (2002) 20.

currently find ourselves in, is marked by the seepage of the protection of privacy into various national laws and constitutions.

It is against this background that more detailed attention may be given to the regulation of privacy protection in the countries selected for this study (in chapter 3) and to use their approach to privacy (see chapter 4) as basis for the evaluation of workplace policies and practices on privacy (chapters 5 and further).

CHAPTER 3:
THE DEVELOPMENT OF PRIVACY PROTECTION IN SELECTED COUNTRIES

3.1 INTRODUCTION

The previous chapter sought generally to trace the legal development of privacy protection. The present chapter attempts to narrow the broad picture provided in chapter 2 by focussing on the legal development of privacy protection in selected countries, namely South Africa, the United States and United Kingdom. This will be done by considering case law and legislation that has significantly contributed to the development of privacy protection in each country. The selection of these countries is motivated by the fact that each country presents a different approach to privacy protection. South Africa provides for and protects privacy explicitly through its Constitution. The United States has found a way to protect privacy through other rights in its constitution, even though there is no explicit mention of this right in its Constitution. England has no constitution, yet it protects privacy through common law principles and absorption of international human rights instruments. To this end, the historical and comparative approaches in this chapter, combined with the insights gained in the previous chapter, will assist the discussion of a workable definition of privacy in chapter 4 as basis for the further discussion in this dissertation.

3.2 SOUTH AFRICA

3.2.1 Privacy Protection Prior to the Constitution

3.2.1.1 Common Law Protection

South Africa has one of the newest constitutions in the world, which explicitly protects a number of rights, including the right to privacy. The right to privacy in South Africa enjoys rich and generous protection under both the common law and the constitution. However, this dual protection of privacy has not always been in place. Prior to both the Interim[270] and Final Constitution[271] of South Africa, privacy was

[270]Constitution of the Republic of South Africa Act 200 of 1993.

protected by the common law only. In terms of the common law, every person's "rights to personality"[272]are protected by the law of personality[273], which in turn is regarded as part of the law of delict. As early as 1908, Innes CJ, in examining the essentials of an *injuria*, referred to "rights in personality" in *R v Umfaan*[274] as "those real rights, those in *rem*, related to personality, which every free man is entitled to enjoy".[275] The following personality rights are recognised under the common law: the right to physical integrity; the right to physical liberty; the right to good name or reputation; the right to dignity or honour; the right to privacy and the right to identity. The available remedy in defence of these personality rights is the *actio iniuriarum*. In *R v Umfaan*[276], Innes CJ further laid down the elements of an *injuria*: "…[the] act complained of must be wrongful; it must be intentional; and must violate one or other of those real rights, those rights in rem, related to personality, which every free man is entitled to enjoy".[277]

The idea of an independent right to privacy, distinct from the general personality right, initially was not embraced by South African courts.[278] For this reason, certain

---

[271]Constitution of the Republic of South Africa Act 108 of 1996.

[272]Neethling, Potgieter and Visser *Neethling's Law of Personality* (1996) 3.

[273] Gareis is accepted as the "father of the modern law of personality" after he formulated the notion of "a general right to personality" in 1877. Neethling, Potgieter and Visser *Neethling's Law of Personality* (1996) 7. However before 1877, Donellus, Grotius and Wolff had already begun to lay the foundation for the concept of personality. Some legal scholars credit Donellus for the critical development of the concept of personality. Donellus divided German private law into two categories: the first category consists of rights that are "truly and properly ours" and the second category consists of rights owed to us by others, including rights others owe to us as a result of an agreement or delict. Grotius proceeded to elaborate on the elements constituting personality and to what extent those elements may be alienated. Grotius asserted that a person could take another's property where this is necessary to preserve life or to obtain "the things without which life cannot be comfortably lived" such as food, clothing, water and medicine". Wolff wrote that "man's nature is to seek his perfection; we are obliged to do what is necessary for us to do; therefore we are obliged to seek our perfection and, because we are all connected to one another, the perfection of one person is tied to that of all others [and for this reason] whoever seeks to make himself as perfect as possible seeks also what others seek and desires nothing at their expense." Like Grotius, Wolff considered the right to one's life, body, bodily integrity, one's good reputation and honour as natural rights. However Wolff developed this group of inherent rights by including other rights such as *inter alia* the right to food, drink and medical care. Finkin "The Comparative Historical and Philosophical Context: Menschenbild: The Conception of the Employee as a Person in Western Law" (2002) 23 *Comparative Labour Law and Policy Journal* 577 605.

[274]*R v Umfaan* 1908 TS 62.

[275] At 66.

[276]*R v Umfaan* 1908 TS 62.

[277] At 66.

[278] In Germany the right to privacy is a fundamental part of a person's general personality right (*das allgemeines Personlichkeitsrecht*) and as such privacy and personality are indistinguishable. Klotzel

judgments limited the concept of *dignitas*[279] to dignity or honour[280] and self - respect[281] and were further reluctant to recognise the existence of an independent right to privacy. In limiting the concept of *dignitas* to dignity or honour, these decisions made insult or *contumelia* a requirement of the *injuria*.[282] This view of *dignitas* was also accepted in certain criminal law[283] and private law[284] decisions.[285]

International Privacy, Publicity & Personality Laws (2001) 157. The German general personality right has been described as [the] "right to be respected as a person, not to have one's individuality infringed, in one's right to express oneself (in appearance, writing, and speech), in one's social standing (honour), and in private and intimate spheres of one's existence." Finkin "The Comparative Historical and Philosophical Context: Menschenbild: The Conception of the Employee as a Person in Western Law" (2002) 23 *Comparative Labour Law and Policy Journal* 577 581. Privacy as a part of the general right to personality has been described as "a person's life at home, within his or her family and their private life not only within their own four walls but also – depending on the circumstances outside". Other aspects of the German general right to personality are the individual sphere (*individualsphare*) which protects the personality and the freedom of self-determination and the intimate sphere (*intimsphare*) protecting a person's thoughts, emotions and their various forms of expression. The *intimsphare* also protects information about an individual's personal health or intimate life. Klotzel *International Privacy, Publicity & Personality Laws* (2001) 158.

[279] Innes CJ defined "*dignitas*" in *R v Umfaan* 1908 T.S. 62 67 as per Melius de Villiers in *The Roman and Roman Dutch Law of Injuries* (1899) "Every person has an inborn right to tranquil enjoyment of his peace of mind, secure against aggression upon his person, against the impairment of that character for moral and social worth to which he might rightly lay claim, and of that respect and esteem of his fellow men which he is deserving, an against degrading and humiliating treatment; and there is a corresponding obligation incumbent on all others to refrain from assailing that to which he has such a right." Innes CJ further discussed the "species" of *injuria* affecting dignity and why this "species" of actions were classified as *injuria*: "As affecting dignity …insults to chastity…such as indecent proposals to a woman; forcible and wrongful intrusion into the [another's] house was looked upon as an *injuria*, not because it was trespass on the property, but because it was a violation of family sanctity of that peace and dignity which a free man was entitled to enjoy." *R v Umfaan* 1908 T.S. 62 67 – 68.

[280] Botha AJ *S v A* 1971 (2) SA 293 (T) 297 H accepted that the recognition of a right to privacy as an independent personality right but clouded this recognition by restricting *dignitas* to dignity or honour thereby also negating the existence of an independent right to privacy. Botha AJ, in addition, stated the defendants had intent (*dolus eventualis*) and must have foreseen that the plaintiff would be insulted or hurt by their recklessness. The defendants were charged with bugging the plaintiff's apartment. *S v A* 1971 (2) SA 293 (T) 299 F.

[281] For example in *R v Holiday* 1927 CPD 395 401 the accused was charged with spying on a woman while she was undressing through a skylight. Gardiner JP held that "…among the rights of personality to which under our civilisation a woman is entitled, is the right to privacy in regard to her body…this right was violated in this present case by the accused." Gardiner JP further held that for *injuria* there must be *animus injuriandi* "[b]ut this does not mean there must be the intention to convey to the mind of the woman the insult". The intention required according to Gardiner JP is "the intention to do the insulting." *R v Holiday* 1927 CPD 395 402.Neethling is of the view that by requiring that the intention to do insulting be present, Gardiner JP equated *dignitas* to "self-respect". Neethling, Potgieter and Visser *Neethling's Law of Personality* (1996) 7 footnote 34.

[282] For example *Stoffberg v Elliot* 1923 CPD 148 (A) 152 Watermeyer J stated "The rule is that unless there is an element of insult …then the plaintiff cannot recover unless he proves some actual damage, that pecuniary loss or pain and suffering." See also *Walker v Van Wezel* 1940 W.L.D. 66 70 in which Ramsbottom J concluded "In considering the meaning of the words which are alleged to constitute a verbal injury to dignity…the words complained of must be injurious in their natural meaning or in such other meaning as they may derive from special circumstances; and where a special meaning is attributed to the words the circumstances in which they are said to bear such meaning must be alleged and proved. A declaration which alleges the use of words which are incapable of bearing a meaning

The *locus classicus* for the recognition of an independent right to privacy in South African is *O'Keeffe v Argus Printing and Publishing Co Ltd*.[286] The plaintiff in *O' Keefe*, an unmarried woman, brought the *actio iniuriarum* for the unauthorised use of her photograph and name in an advertisement for a company distributing rifles, pistols revolvers and ammunition.[287] The plaintiff brought the action on the basis that the advertisement had violated her dignity or *dignitas*. The defendant argued that insult had to be present in an *injuria*. Watermeyer AJ preferred to take the view that whether an act involves "an insult, indignity, humiliation or vexation depends…upon the modes of thought prevalent amongst any particular community or at any period of time, or upon those of different classes or grades of society, and the question must be left to the discretion of the Court where an action…is brought".[288] In determining whether "the plaintiff can be reasonably held to have been subjected to offensive, degrading or humiliating treatment" Watermeyer JA considered "modern conditions and thought" (namely English and American jurisprudence on the use of a person's name and photograph without consent) and concluded that "[t]he unauthorised publication of a person's photograph and name for advertising purposes [constitutes] an aggression upon the person's *dignitas*".[289] Neethling criticises the *O'Keeffe* decision for failing to offer a comprehensive definition of privacy, resulting in "identity as a personality right [being] equated with privacy".[290] The view of privacy

---

injurious to dignity in either their primary sense or in the circumstances alleged does not disclose a cause of action is open to exception".

[283]In *R v* S 1955 (3) SA 313 (SWA) Hofmeyer AJ stressed the requirement of intent to insult and impair one's dignity in finding the defendant's act "wrongful and … in contempt of the complainant's personal rights of security, privacy and dignity". *R v* S 1955 (3) SA 313 (SWA) 315.

[284] For instance in *Mhlongo v Bailey* 1958 (1) SA 370 (W) the issue before the court was whether the unauthorised publication of photographs in a popular magazine constituted an aggression upon a person's *dignitas*. The court found that certain factors should be taken into account in determining the issue but further stated that "The remedy [if the photographs are found to constitute an aggression upon the plaintiff's *dignitas*] should be given only when the words or conduct …involves an element of degradation, insult or *contumelia*". *Mhlongo v Bailey* 1958 (1) SA 370 (W) 372 H.

[285]Neethling Potgieter and Visser *Neethling's Law of Personality* (1996) 7 footnote 34 and 35.

[286]*O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 1954 (3) SA 244 (C). The appellate court in *Jansen Van Vuuren v Kruger* 1993 4 SA 842 (A) also found that the *actio iniuriarum* protects a person's *dignitas* and *dignitas* embraces privacy.

[287]Even after the *O'Keefe* decision the view that the right to the right to privacy should only be protected where the intention to insult still found favour in certain decisions. See also *Kidson v SA Associated Newspapers Ltd* 1957 (3) SA 461.

[288]Watermeyer AJ referring to Melius de Villiers in *The Roman and Roman Dutch Law of Injuries* (1899).*O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) 248 C -D

[289]*O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C) 249 D.

[290]Neethling, Potgieter and Visser *Neethling's Law of Personality* (1996) 240 footnote 20.

as an independent right of personality was firmly established in subsequent decisions.[291]

The current view of the South African common law on privacy is twofold: first, the equation of privacy with dignity and identity is outdated and, secondly, privacy is an independent personality right.[292] Moreover, courts are willing to have regard to the "prevailing *boni mores*" (public opinion) in deciding whether particular encroachments constitute a serious impairment of an individual's *dignitas*. In *S v A*[293] two private detectives placed a listening device under the dressing table of the complainant at the request of her estranged spouse. The court found the two private detectives liable for invading the complainant's privacy. In reaching this decision, Botha AJ reiterated that the right to privacy is included in the concept of *dignitas*[294] and further that the "infringement of a person's privacy prima facie constitutes an impairment of his *dignitas*".[295] Botha AJ concluded that the punishment meted out in response to a particular encroachment on *dignitas* is dependent on the "time", "place", "modes of thought and ways of life prevalent amongst a particular community." In applying this to the facts, it was found that "encroachment on a person's privacy by… a private detective, by means of planting a [listening] device in his apartment and listening on his conversations…[amounts] to a serious impairment of [such a person's *dignitas*]".[296]

Courts are also willing to weigh up competing interests in determining the unlawfulness of a factual infringement of a person's right to privacy. For example, in *S v I* [297], the Appellate Division of Rhodesia found an estranged wife and a private detective employed by her not guilty of *crimen injuria* after they peeped into her husband's room at night. Although the court found their actions in this regard

---

[291] See for example *Mr and Mrs "X" v Rhodesia and Publishing Co Ltd 1974* (4) SA 508 (R) and *Financial Mail v Sage Holdings* 1993 (2) SA 451 (A) and *Jansen van Vuuren v Kruger* 1993 (4) SA 842 (A).

[292] The Constitutional Court in *Bernstein v Bester* 1996 (2) SA 751 accepted that the common law recognized the right to privacy as an independent personality right included within the broader concept of *dignitas*.

[293] *S v A* 1971 (2) SA 293.

[294] *S v A* 1971 (2) SA 293 297 H.

[295] *S v A* 1971 (2) SA 293 297 D.

[296] *S v A* 1971 (2) SA 293 299.

[297] *S v I* 1976 (1) SA 781 (RA).

amounted to an invasion of privacy, this invasion was seen to be justified given that these actions were done with the bona fide intention of obtaining evidence of her husband's adultery. According to Corbett CJ, the court weighed the husband's privacy interest against the wife's interest in obtaining evidence of her husband's adultery.[298] The cases of *S v A* and *S v I* highlight the grey area between justifiable and unjustifiable actions.[299]

In *Financial Mail (Pty) Ltd v Sage Holdings Ltd*,[300] Corbett CJ identified two ways in which the right to privacy can be breached: through the unlawful intrusion upon the personal privacy of another and the unlawful disclosure of a person's private facts.[301] The court moreover held that the unlawfulness of a breach of privacy is determined by the prevailing *boni mores* and a general sense of justice perceived by the community.[302] Nonetheless, in *National Media Ltd v Jooste*,[303] the court cautioned that personal facts are not necessarily private facts. Private facts for the court encompassed only those facts "whose disclosure will cause mental distress and injury to anyone possessed of ordinary feelings and intelligence…".[304] The court further agreed with the *Financial Mail* decision in that the unlawfulness of a factual infringement of a person's right to privacy should be determined by taking into consideration the competing interests, contemporary *boni mores* and the community's general sense of justice.[305] The *National Media* decision defined privacy as "[encompassing] the competence to determine the destiny of private facts…The individual concerned is entitled to dictate the ambit of disclosure…[and] may prescribe the purpose and method of the disclosure…".[306]

---

[298] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 462 H – J.

[299] Van Niekerk "The Right to Privacy in Employment" (1994) 3 *Contemporary Labor Law* 105.

[300] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 1993 (2) SA 451 (A).

[301] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 462 E – F.

[302] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 462 E – F. In other words "in demarcating the boundary between lawfulness and unlawfulness , the court will have regard to the particular facts of the case and judge them in light of the contemporary bona mores and the general sense of justice of the community as perceived by the court." Van Niekerk "The Right to Privacy in Employment" (1994) 3 Contemporary *Labor Law* 105.

[303] *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 270 I –J.

[304] *Supra*.

[305] *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 270 I –J.

[306] *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271 G – H.

The Constitutional Court, in discussing the common law right to privacy, has pointed out the following examples of wrongful intrusion and disclosure which have come before the courts: illegal entry into a private residence,[307] eavesdropping on private conversations,[308] secretly watching a person undress, [309]disclosure of private facts acquired by a wrongful act of intrusion, [310]and the disclosure of private facts in breach of a confidential relationship[311]. [312]

Prior to the adoption of the Interim Constitution, courts recognised the right to privacy as one of the personality rights - "those real rights, those rights *in rem* related to personality, which every free man is entitled to enjoy"[313]. The courts further regarded the invasion of privacy as an impairment of *dignitas*. Despite recognising the existence of the right to privacy, the courts did not expressly attempt to define the concept of privacy. Some academics have attempted to offer general definitions of the right to privacy, but most of the definitions, according to McQuoid – Mason, were synonymous with amongst others "solitude", "anonymity and reserve", "intimacy" and "being let alone".[314] The definitions, more importantly, also failed to give guidance on "the circumstances in which the courts will consider a breach of that right as an actionable invasion of privacy".[315]

3.2.2 Constitutional Protection of Privacy

3.2.2.1 Interim Constitution

Sachs J described South Africa before the enactment of the Interim Constitution as a place where "generations of systemised and egregious violations of personal privacy established norms of disrespect for citizens that seeped generally into public administration and promoted amongst a great many officials habits and practices

[307] *S v I* 1976 (1) SA 781 (RA).

[308] *S v A* 1971 (2) SA 293.

[309] *R v Holiday* 1927 CPD 395.

[310] *Financial Mail* (Pty) Ltd v Sage Holdings Ltd 1993 (2) SA 451 (A).

[311] *Jansen Van Vuuren v Kruger* 1993 4 SA 842 (A).

[312] *Bernstein v Bester* 1996 (2) SA 751 789 D – E. See also Woolman, Roux, Klaaren, Stein, Chaskalson and Bishop *Constitutional Law of South Africa* 2nd ed. (2005) 38 – 7.

[313] *S v A* 1971 (2) SA 293 297.

[314] McQouid – Mason *The Law of Privacy in South Africa* (1978) 98 – 99.

[315] McQouid – Mason *The Law of Privacy in South Africa* (1978) 98 – 99.

inconsistent with the standards of conduct required by the Bill of Rights".[316] The new (Interim) Constitution "accordingly requires us to repudiate the past practices which were repugnant to the new constitutional values, while at the same time re-affirming and building on those that were inconsistent with these values".[317]

In 1993 South Africa enacted its first democratic Constitution of the Republic of South Africa, Act 200 of 1993. The Bill of Rights provided for a right to privacy in section 13. Section 13 read as follows:

> "Every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violation of private communications".

Section 13 of the Interim Constitution reinforced the importance of a right to privacy[318] and further enjoined courts to consider its provisions in deciding matters affecting privacy. The Interim Constitution also had direct and indirect application. That is to say, the right to privacy in the Interim Constitution applied with regard to state action and private law disputes.[319]

3.2.2.2 Final Constitution

The Final Constitution[320] provides in section 14:

"Everyone has the right to privacy, which shall include the right not to have;

a) their person or home searched;
b) their property searched;
c) their possessions seized; or
d) the privacy of their communications infringed."[321]

There are no substantive differences between the privacy provisions in both constitutions. The first part of section14 guarantees a general right to privacy and the second part protects against specific breaches of privacy. The use of the word

[316] *Mistry v Interim Medical and Dental Council of South* 1998 (4) SA 1127 1143 B.
[317] *Mistry v Interim Medical and Dental Council of South* 1998 (4) SA 1127 1143 C.
[318] Neethling, Potgieter and Visser *Neethling's Law of Personality* (1996) 239.
[319] *Supra*.
[320] Section 14 of Act 108 of 1996.
[321] Section 14 of Act 108 of 1996.

"include" in the second part of section 14 indicates that the specific breaches listed are not a closed list and accommodates other unlisted breaches of privacy.[322] Moreover the second part of section 14 is part and parcel of the first part, the general right to privacy.[323]

Section 2 of the Constitution provides for the supremacy of the Constitution. It expressly provides that the Constitution is the supreme law of South Africa and any law, or conduct inconsistent with the Constitution is invalid. This means that the Bill of Rights is applicable to all law, including the right to privacy.[324] The Bill of Rights further binds the state and therefore has vertical application. The Bill also binds natural and juristic persons and for this reason has horizontal application. The vertical and horizontal application of the Bill can be direct or indirect. The direct vertical application of the Constitution requires the state to respect the fundamental rights housed in the Bill of Rights unless such an infringement is reasonable and justifiable in terms of the limitations clause in section 36 of the Constitution. Direct horizontal application requires the courts to give effect to specific fundamental rights in applying and developing the common law where legislation fails to do as such. Indirect application of the Bill of requires that all rules, principles or norms be subjected to and construed in light of the spirit, object and purport of the Bill of Rights.[325]

The obligation on the courts to develop the common law does not, however, mean that courts can alter the common law without first considering inter alia whether such development is necessary and the manner in which it should occur.[326] It means that the court has to "retain those existing common law actions which are in harmony with the values of the Constitution".[327] The Constitutional Court, in *Bernstein v Bester* cautioned against projecting "common law principles onto the interpretation of

---

[322]Devenish *A Commentary on the South African Bill of Rights* (1999) 138.

[323] Currie and de Waal *Bill of Rights Handbook* 5th ed. (2005) 141.

[324] Chaskalson in *Pharmaceutical Manufacturers Association of South Africa* 2000 (2) SA 674 (CC) 698 reinforced the supremacy of the Constitution by stating "There is…only one system of law and within that system the Constitution is the supreme law which all other law must comply."

[325]South African Law Reform Commission *Privacy and Data Protection* Project 124 Discussion Paper 109 October 2005.

[326] Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study*(2003) 548 Thesis Submitted at the University of South Africa 548.

[327] Woolman, Roux, Klaaren, Stein, Chaskalson and Bishop *Constitutional Law of South Africa* 2nd ed. (2005) 38 - 42.

fundamental rights and their limitation…". The Court differentiated between the common law action for invasion of privacy and the constitutional protection of the right to privacy. The former, according to the Court, entails a single policy based inquiry into whether there has been an unlawful infringement of privacy, while the latter entails a dual inquiry into whether the conduct has infringed the constitutional right to privacy and, if so, whether the infringement is justifiable in terms of the limitations clause.[328] The infringement of the constitutional right to privacy is established where a subjective expectation of privacy that society considers objectively reasonable exists and the justifiability of the infringement is established by weighing the individual's privacy against competing fundamental rights.[329]

Section 14 of the Constitution has in effect done the following for the protection of privacy:

1. It has bolstered the existing protection of privacy provided by the common law;
2. It has sealed the status of privacy as an independent and fundamental right;
3. It has provided for a general right to privacy;
4. It has created new classes of privacy rights. The new classes of rights created by the constitutional are substantive and informational privacy rights. Substantive privacy rights protect "personal autonomy" whereas informational privacy rights "prevent [disclosure] and access to information".
5. It requires courts to develop the common law right to privacy. The Constitution enjoins the courts to develop the common law with regard to the spirit, purport and object of the Bill of Rights. As previously indicated, this means the courts have to retain those common law principles which are in line with the Constitution and alter those principles viewed as contrary to the values of the Constitution. [330]

[328]Woolman, Roux, Klaaren, Stein, Chaskalson and Bishop *Constitutional Law of South Africa* 2nd ed. (2005) 38-21.

[329]*Supra*.

[330]Devenish *A Commentary on the South African Bill of Rights* (1999) 147. See also

Woolman, Roux, Klaaren, Stein, Chaskalson and *Bishop Constitutional Law of South Africa* 2nd ed. (2005) 38-19.

3.2.2.3 Constitutional Court Decisions on the Right to Privacy

The Constitutional Court has decided a number of cases on the right to privacy, which decisions have related to the possession of obscene material,[331] the general scope of privacy in society,[332] sexual orientation,[333] searches,[334] and in challenging the statutory prohibition of prostitution.[335]

The Constitutional Court has not as yet dealt with the right to privacy in the employment context. The general tenor of the constitutional court as regards privacy is that the right to privacy merits respect given its explicit mention in the Constitution. However, respect of the right does not mean that it cannot be limited where it is in conflict with societal interests. The Constitutional Court has also linked the right to privacy to other core rights such as human dignity[336] and autonomous identity[337] equality[338].

3.2.2.3.1 Bernstein v Bester

Bernstein v Bester remains the *locus classicus* on the constitutional right to privacy. Although the decision concerned the Interim Constitution, the decision represents the "richest and most comprehensive interpretation of the right to privacy" provided by a South African court.[339] The issue before the court in *Bernstein* was the constitutionality of sections 417 and 418 of the Companies Act 61 of 1973, providing for the examination of persons and the disclosure of documents on company affairs. The applicants contended that section 417 and section 418 were unconstitutional on a number of grounds. One argument was that these sections violated a cluster of interrelated and overlapping constitutional rights, *inter alia* the right to privacy in section 13 of the Interim Constitution. More specifically, the applicants argued that section 417 and section 418 of the Companies Act of 1968 violated the privacy of a witness by forcing the witness to disclose books and documents the witness would

[331] *Case v Minister of safety and Security* 1996 (3) SA 165 (CC).

[332] *Bernstein v Bester* NO 1996 (2) SA 751 (CC).

[333] *National Coalition for Lesbian and Gay Equality v Minister of Justice* 1999 (1) SA 6 (CC).

[334] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).

[335] *S v Jordan* 2002 (6) SA 642 (CC).

[336] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors Pty Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit NO* 2001 (1) SA 545 (CC).

[337] *Bernstein v Bester NO* 1996 (2) SA 751 (CC).

[338] *National Coalition for Lesbian and Gay Equality v Minister of Justice* 1999 (1) SA 6 (CC).

[339] De Waal and Currie *Bills of Rights Handbook* 5th ed (2005) 14.2 – 14.3.

under normal circumstances like to keep undisclosed and confidential. The applicants further argued that the compulsory production of documents under section417 constituted a seizure within the meaning of section 13.[340] Ackerman J reasoned:

> "The truism that no right is to be considered absolute, implies that from the outset of interpretation each right is always already limited to every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his or her family life, sexual preferences and home environment, which is shielded from erosion by conflicting rights of the community. This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly".[341]

Ackerman J further found that the scope of privacy is "closely related to the concept of identity" and rights like the right to privacy are not based on the notion of the unencumbered self, but on the notion of what is necessary to have one's own autonomous identity. *Bernstein*, as the first Constitutional Court judgement to interpret the constitutional right to privacy, viewed the right to privacy as a subjective expectation that society must consider reasonable. The judgment further established a reasonable expectation of privacy existed in the "inner sanctum" and the "truly personal realm",[342] but acknowledged that privacy concerns may diminish depending on the activities of persons. This is of particular importance with regard to privacy in employment.

---

[340] *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 784 I – J and 785 A.

[341] *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 784 E - F.

[342] De Waal and Currie *Bills of Rights Handbook* 5th ed. (2005) 143.

3.2.2.3.2 Mistry v Interim Dental Council of South Africa

Mistry v Interim Dental Council of South Africa[343] concerned section 28 (1) of the Medicines and Related Substances Control Act 101 of 1965, which granted inspectors of medicines the authority to enter and inspect any premises, place, vehicle, vessel or aircraft in which they reasonably believe medicines or substances regulated by the Act are housed. The section further authorised these inspectors to seize any books, records or documents found in such premises, place, vehicle, vessel or aircraft. The applicant's surgery in *Mistry* was searched and numerous items seized by investigating officers of the Interim Medical and Dental Council of South Africa. At issue was the constitutionality of the said section 28(1) of the Act and whether the communication of information by one of the investigators to the inspector of medicines, or the manner in which the search was conducted, constituted a breach of the applicant's right to privacy. As to the nature of the right to privacy and its importance in an open and democratic society based on freedom and equality, the court held that "[t]he existence of safeguards to regulate the way in which State officials may enter the private domains of ordinary citizens is one of the features that distinguish a constitutional democracy from a police state".[344] The Court also held that the degree of privacy that a citizen can reasonably expect would vary significantly according to the activity that brings him or her in contact with the state.[345] The Court further observed:

> "[t]the more public the undertaking and the more closely regulated, the more attenuated would the right to privacy [be] and the less intense [the] invasion" and "[i]n the case of any regulated enterprise, proprietor's expectation of privacy with regard to the premises, equipment, materials and records must be attenuated by the obligation to comply with reasonable regulations and to tolerate the administrative inspections that are an inseparable part of an effective regime of regulation".[346]

[343] *Mistry v Interim Dental Council of South Africa 1998* (4) SA 1127 (CC).

[343] *S v Jordan* 2002 (6) SA 642 (CC).

[344] *Mistry v Interim Dental Council of South Africa* 1998 (4) SA 1127 (CC) 1142 E.

[345] *Mistry v Interim Dental Council of South Africa* 1998 (4) SA 1127 (CC) 1144 C.

[346] *Mistry v Interim Dental Council of South Africa* 1998 (4) SA 1127 (CC) 1145 A.

According to the court, in modern industrial society many activities that individuals engage in are regulated by the state to ensure that the individual's pursuits are compatible with those of the community.[347] Hence, the limitation imposed on the right to privacy by the Act protected the general public and honest health professionals:

> "People involved in such undertakings must be taken to know from the outset that their activities will be monitored. If they are licensed to function in a competitive environment, they accept as a condition of their licence that they will adhere to the same reasonable controls as are applicable to their competitors. Members of professional bodies, for example, share an interest in seeing to it that the standards, reputation and integrity of their professions are maintained".[348]

The court concluded that the communication by one of the investigating officers to the inspector of medicines had not been a violation of the applicant's right to privacy for a number of reasons. These include: the information communicated had been volunteered by a member of the public and not obtained in an obtrusive manner; the information related to the way in which the applicant conducted his medical practice and did not concern intimate aspects of the applicant's personal life; the information had not been communicated to the press or general public or other persons the applicants could reasonably have expected that such information should be withheld from but had been communicated to persons charged with carrying out the regulatory inspections; and the information constituted information that led to the search and not information from a search.[349]

3.2.2.3.3 Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors

In contrast to the *Bernstein* and *Mistry* decisions, *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* [350] was decided under the Final Constitution. At issue was whether section 28(13) and section 28 (14) read with section 29 (5) of the National Prosecuting Authority Act 32 of 1998 was inconsistent

[347] *Mistry v Interim Dental Council of South Africa* 1998 (4) SA 1127 (CC) 1145 B – C.

[348] *Supra*.

[349] *Mistry v Interim Dental Council of South Africa 1998* (4) SA 1127 (CC) 1155 B – D, 1155 F – G and 1156 C.

[350] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2001 (1) SA 545.

with the Final Constitution, specifically whether these provisions authorising the seizure of documents, records and data breached the right to privacy in section 14 of the Constitution. Langa DP held that section 14 does not only relate to the "truly personal realm" or "inner sanctum". In other words individuals still retained their privacy when venturing outside the "truly personal realm" or "inner sanctum":

> "Thus when people are in their offices, in their cars or on mobile telephones, they retain the right to be left alone by the state unless certain conditions are satisfied. Wherever a person has the ability to decide what he or she reveals to the public, the expectation that such a decision warrants respect is reasonable and the right to privacy comes into play".[351]

The Court further stated: "[p]rivacy is a right which becomes intense the closer it moves to the intimate personal sphere of the life of human beings, and less intense as it moves away from the core".[352] The court also held that juristic persons enjoyed some right to privacy although "their privacy rights cannot be as intense as those of human beings".[353]

3.2.2.3.4 National Coalition for Gay and Lesbian Equality v Minister of Justice

The Constitutional Court, in *National Coalition for Gay and Lesbian Equality v Minister of Justice*,[354] considered the constitutional validity of the common law blanket prohibition on sodomy criminalising sexual intercourse between men. The court held that the criminalisation of sodomy infringed the right to privacy. Ackermann J stated that:

> "privacy recognises that we all have a right to a sphere of private intimacy and autonomy, which allows us to establish and nurture human relations without interference from the outside community. The way in which we give expression to our sexuality is at the core of this area of private intimacy. If in expressing our sexuality, we act

[351] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2001 (1) SA 545 557 B - C.

[352] *Supra*.

[353] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2001 (1) SA 545 557 F.

[354] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6.

> consensually and without harming one another, invasion of that precinct will be a breach of privacy".[355]

Sachs J, in a separate concurring judgment, rejected the idea that the privacy argument reinforces the view "that homosexuality is shameful and [deserves protection only when confined to the private bedroom]" for two reasons: first, the argument "subjects equality and privacy rights to inappropriate sequential order" and second, "it undervalues the scope and significance of privacy rights".[356] Sachs J held in this regard that rights cannot be compartmentalised or ranked:

> "equality and privacy cannot be separated, because they are both violated by anti – sodomy laws…such laws deny equal respect for difference, which lies at the heart of equality, and become the basis for the invasion of privacy."[357]

Sachs J also pointed out that "privacy protects people not places" and this right to be left alone is not merely "a negative right to occupy a space free from government intrusion" but is also a right to get on with your life, express your personality and make fundamental decisions about your intimate relationships without penalisation.[358]

Privacy, according to Sachs J further imposes a duty in creating an environment in which personal realisation can thrive.[359] He concluded that although privacy was violated by anti – sodomy law, this did not mean that the "the concept of privacy should be extended to give blanket libertarian permission for people to do anything they like provided that what they do is sexual and is done in private".[360]

3.2.2.3.5 S v Jordan

The applicants in *S v Jordan*[361] contested the prohibition on prostitution contained in section 2 and section 20 (1) of the Sexual Offences Act 23 of 1957. The Court supported the reasoning of Sachs J in *National Coalition for Gay and Lesbian*

[355] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 30 B.
[356] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 57 E – F.
[357] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 60 D – E.
[358] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 60 D – E.
[359] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 61 A.
[360] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 61 F.
[361] *S v Jordan* 2002 (6) SA 642.

Equality v Minister of Justice by holding that "the law may continue to proscribe what is acceptable and what is unacceptable even in relation to sexual expression and even in the sanctum of the home, and may within justifiable limits, penalise what is harmful and regulate what is offensive".[362] Ngcobo J stated that "a person who commits a crime in private, the nature of which can only be committed in private can necessarily claim [a right of privacy]. What compounds the difficulty is that the prostitute invites the public generally to come and engage in unlawful conduct in private. The law should be as concerned with crimes that are committed in private as it is with crimes that are committed in public." [363] Ngcobo J distinguished the facts in *S v Jordan* from those in *National Coalition for Gay and Lesbian Equality v Minister of Justice* in that *S v Jordan* concerned the commercial exploitation of sex which involves neither an infringement of dignity nor unfair discrimination.[364]

3.2.3 Summary

In summary, the preceding discussion on the legal protection of privacy in South African has shown that prior to the adoption of the Interim Constitution, South African courts recognised the right to privacy as one of the bundle of personality rights - "those real rights, those rights *in rem* related to personality, which every free man is entitled to enjoy".[365] The courts further regarded the invasion of privacy as an impairment of *dignitas*. Despite recognising the existence of the right to privacy, the courts did not expressly attempt to define the concept of privacy. Attempts by academics to offer general definitions yielded unsatisfactory results and failed to point the courts towards circumstances in which they should regard the breach of privacy as an actionable invasion.

Privacy is still not defined in the Constitution, but the Constitutional Court did initially (in deciding cases under the Constitutional dispensation) speak of protection of the "inner sanctum" and "truly personal realm" and by relating privacy to the concept of identity (and thus individualising privacy). Under the Final Constitution, the Constitutional Court has still not ventured to define privacy and seems to accept that privacy is "an amorphous and elusive concept" and as such difficult to define.

[362] *S v Jordan* 2002 (6) SA 642 654 I – 655 A.
[363] *S v Jordan* 2002 (6) SA 642 654 I – 655 A.
[364] *Supra*.
[365] *S v A* 1971 (2) SA 293 297.

Even so it has continued to build on the nature of right by linking it with additional concepts such as human dignity[366] and equality[367]. Ackermann J explained privacy in *National Coalition for Gay and Lesbian Equality v Minister of Justice* as "a right to a sphere of private intimacy and autonomy, which allows us to establish and nurture human relations without interference from the outside community".[368] Perhaps most importantly for purposes of the further discussion, the Court has further concluded that privacy becomes less intense as an individual moves away from the "inner sanctum" or "truly personal realm"[369] and explicitly stated that privacy depends on a subjective expectation that is objectively reasonable.

3.3 UNITED STATES

3.3.1 Development of Privacy Concerns

The year 1850 marked the transition of America from a rural, agrarian and private society to an urban and public society as a result of technological advancements. Technological devices such as the reaper, power loom, sewing machine, telegraph, and typewriter transformed both city and farm life.[370] Increased newspaper circulation not only improved the reliability of the means of communication that had previously been hearsay, but also generated a hunger for more information. By the end of the nineteenth century, the United States printing press had grown to such an extent that any literate person had access to daily newspapers.[371] The emergence of cheap gazettes, journals and tribunals created a small yet significant revolution in social curiosity. This hunger for information extended "beyond the local neighbourhood and country"[372] and subsequently led to the birth of an aggressive press and journalism known as the "yellow press".[373] The "yellow press" subscribed to populist journalism,

---

[366] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors Pty Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit* NO 2001 (1) SA 545 (CC).

[367] *National Coalition for Lesbian and Gay Equality v Minister of Justice* 1999 (1) SA 6 (CC).

[368] *National Coalition for Lesbian and Gay Equality v Minister of Justice* 1999 (1) SA 6 (CC) 1538 A – B. See also De Waal and Currie *Bills of Rights Handbook* 5th ed. (2005) 272.

[369] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2001 (1) SA 545 557F.

[370] Hixson *Privacy in a Public Society* (1967) 16.

[371] Hixson *Privacy in a Public Society* (1967) 16.

[372] Hixson *Privacy in a Public Society* (1967) 16.

[373] Solove and Rotenburg *Information Privacy Law* (2003) 3.

which featured sensational, colourful and interesting news about the lives of the upper class and alleged criminals and wholly fuelled this social curiosity.[374]

United States constitutional jurisprudence failed to immediately provide the necessary relief from this spate of aggressive journalism. United States jurists declined to depart from a rigid and literal interpretation of the Constitution and the Bill of Rights; first, because of the non-existence of privacy as a right in English common law and in the United States Constitution and, secondly, because the Bill of Rights assured aspects of privacy such as religious belief and practice.[375] However, some social writers such as Godkin had already begun to write about the effect of the "yellow press" on personal privacy. In 1890 Godkin wrote that:

> "[t]he chief enemy of privacy in modern life is that interest in other people and their affairs known as curiosity, which in the days before newspapers created personal gossip. As soon in the progress of civilization as men left the tent, or wigwam, or tribal dwelling, and retreated into private houses, a desire on the part of their neighbours to know what was going on in the private houses sprang up rapidly, and had flourished ever since the world over".[376]

He further wrote"[i]n all this the advent of the newspaper, or rather of a particular class of newspaper, had made a great change. It has converted curiosity into what economists call an ineffectual demand and gossip into a marketable commodity".[377] Godkin further adds that:

> " [i]n other words gossip about private individuals is now printed, and makes its victim, with all his imperfections on his head, known to hundreds or thousands of miles away from his place of abode; and,

[374]Hixson *Privacy in a Public Society* (1967) 28.

[375]Wagner DeCew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997)15. According to Wagner DeCew up until 1890, the law had been wary of protecting emotional harm because of: first, the difficulty associated with assessing damages for emotional harm and second, the subjective nature of findings based on the state of an individual's mind.

[376] Godkin "The Rights of the Citizen: IV. To His Own Reputation" (1890) *Scribner's Magazine* 66.

[377]Hixson *Privacy in a Public Society* (1967) 29. Godkin further stated that "the eagerness of men to know [all he can about his neighbour's private life]… finds defence in that the love of gossip is after all human and that everything that is human concerns us deeply. The most absorbing topic for the bulk of mankind must always be other men's doings and sayings, and it can hardly be denied that there is some substance in this apology." Godkin "The Rights of the Citizen: IV. To His Own Reputation" (1890) *Scribner's Magazine* 66.

> what is worst of all, brings to his knowledge exactly what is said about him, with all its details. It thus inflicts what is, to many men, the great pain of believing that everybody he meets in the street is perfectly familiar with some folly, or misfortune, or indiscretion, or weakness, which he had previously supposed had never got beyond his domestic circle".[378]

3.3.2 Early Privacy Cases

One of the earliest mention of privacy concerns appeared in Judge Thomas Cooley's *Treatise on the Law of Torts*, in which he wrote the following with regard to personal immunity: "The right to one's person may be said to be a right to be let alone".[379] However, even before Judge Cooley's legal treatise, the Supreme Court in *Wheaton v Peters*[380] had already alluded to the "right to be alone" when the copyright over twelve books known as the "Wheaton reports" containing reports of cases argued and decided in the United States Supreme Court from 1816 to 1827, was contested. The court observed that "[t]he defendant asks nothing-wants nothing, but to be let alone until it can be shown that he has violated the rights of another".[381] Privacy concerns were also raised in two nineteenth century American cases, namely, *Newell v Witcher*[382] and *De May v Roberts*[383].

In *Newell v Witcher*[384] the defendant, a married man, entered the room in which the plaintiff was sleeping for the night, sat on her bed and urged her to have sexual intercourse with him. The defendant argued that his entry into the plaintiff's room did not meet the requirements of trespass because the room in which the plaintiff was sleeping for the night was in his home. Redfield J, however, was of the opinion that the defendant's actions, although carried out in his own house, amounted to trespass

---

[378] Godkin "The Rights of the Citizen: IV. To His Own Reputation" (1890) *Scribner's Magazine* 66.

[379] Ernst and Schwartz *Privacy: The Right to be Let Alone* (1962) 49.

[380] *Wheaton v Peters* 33 U.S. 591(1834). The court was of opinion "that no reporter has or can have any copyright in the written opinions delivered by this court; and that the judges thereof cannot confer on any reporter any such right". *Wheaton v Peters* 33 U.S. 591(1834) 668.

[381] *Wheaton v Peters* 33 U.S. 591(1834) 634.

[382] *Newell v Witcher* 53 Vt 589, 1880 WL 4800 (Vt.).

[383] *De May v Roberts* 46 Mich. 160, 9 N.W. 146 154.

[384] *Newell v Witcher* 53 Vt 589, 1880 WL 4800 (Vt.).

as the plaintiff had a right to some privacy, even though she had not been sleeping at home in her own bedroom. Redfield J stated the plaintiff's:

> "right to her private sleeping room…was as ample and exclusive against the inmates of the house, as if entry had been made into her private dwelling house…Her right of quiet occupancy and privacy was absolute and exclusive; the entry by stealth into the night into the room the plaintiff was sleeping in for the night without licence or justifiable cause, was a trespass; and if with felonious intent, was a crime".[385]

The court in *De May v Roberts* expressly mentioned that there existed a legal right to privacy, especially as regards the home and in certain events taking place in that home. In *De May v Roberts* a physician permitted a friend to accompany him in attending to the plaintiff who was in labour. The plaintiff assumed the physician's friend was also a physician, so she voiced no objections to him being within hearing or seeing distance of her. The court found both men guilty of deceit for not disclosing to the plaintiff that the physician's friend was not a physician. The court found that the occasion for the plaintiff "was a most sacred one and no one had a right to intrude unless invited or because of some real and pressing necessity...". [386] Based on the sacred nature of the occasion and perhaps the existing notion of the sanctity of the home, the court concluded that the plaintiff "had a legal right to privacy of her apartment at such a time and the law secures to her this right by requiring others to observe it, and to abstain from its violation".[387]

3.3.3 Common Law

The right to privacy in United States common law has its roots in the famous Harvard Law Review article by the authors Warren and Brandeis.[388] The article took the argument that the right to privacy was separate from the rights of property, contract and trust. The article was supposedly borne out of Warren's annoyance with the

[385] *Newell v Witcher* 53 Vt 589, 1880 WL 4800 (Vt.) 2.

[386] *De May v Roberts* 46 Mich. 160, 9 N.W. 146 149.

[387] *De May v Roberts* 46 Mich. 160, 9 N.W. 146 149.

[388] Warren and Brandeis "The Right to Privacy" (1890) *Harvard Law Review* 193. The article was published on the 15th of December 1890, led to the authors becoming the first common law scholars to recognise that the importance of the legal protection of privacy to individuals and society.

interest of the Boston yellow press in his family's social activities. The article drew its influence from two sources.[389]

First, Warren and Brandeis credited Judge Cooley's treatise on torts. As stated earlier, Judge Cooley spoke of the "right to be let alone" as a matter of personal immunity: "The right to one's person may be said to be a right of complete immunity".[390] Second, Warren and Brandeis cited Godkin and his *Scribner's Essay* on privacy in which he traced the history of man's desire for privacy from the days of communal life in Native American wigwams to the industrialisation of his time.[391] Godkin wrote:

> "To have a house of one's own is the ambition of nearly all civilized men and women, and the reason which most makes them enjoy it is the opportunity it affords of deciding for themselves how much or how little publicity should surround their lives".[392]

According to Warren and Brandeis the right to privacy sought to protect the plaintiff's "right to be let alone". Warren and Brandeis wrote about privacy as "an inviolate personality" right that would protect "thoughts, emotions and sensations…whether expressed in writing or in conduct, in conversation, in attitudes, or in facial expression".[393] This did not mean that the authors rejected the property aspects of privacy, but the authors simply sought a distinct right.[394] They also argued that "the intensity and complexity of life" and modern enterprise and invention "ripened the time for the courts and judges to redefine the nature of personal rights to protect appearance, sayings, acts and …personal relations, domestic or otherwise".[395]

The recognition of a distinct right to privacy, according to the authors, would not require the law to be rewritten because at that time case law had already come close to

---

[389] Wagner DeCew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 29.

[390] Wagner DeCew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 30.

[391] *Supra*.

[392] Godkin "The Rights of the Citizen: IV. To His Own Reputation" (1890) *Scribner's Magazine* 66.

[393] According to the authors "the intensity and complexity of life attendant upon advancing civilization, have rendered necessary some retreat from the world and man under refining influence of culture has become more sensitive to publicity so that solitude and privacy have become essential to the individual." Warren and Brandeis "The Right to Privacy" (1890) *Harvard Law Review* 193 196.

[394] Bible and McWhirter *Privacy in the Workplace: A Guide for Human Resource Managers* (1990) 34.

[395] Warren and Brandeis "The Right to Privacy" (1890) *Harvard Law Review* 193 196.

recognising a legally enforceable right.[396] The authors further argued in favour of a legal remedy for the anguish caused to an individual where the injury had not been to property or contractual rights.[397] This extension of jurisprudence as pleaded by Warren and Brandeis would protect the feelings of individuals who had been subjected to some form of intrusion.[398] To support their argument, Warren and Brandeis referred to cases in which "protection had been afforded against wrongful publication" where the "jurisdiction" that was asserted had been based on an "alleged breach of an implied contract or of a trust or confidence".[399] In sum, the authors believed that these cases were really protecting privacy and as such there was no need for the courts to recognise a 'new' right to privacy. The authors in effect argued that everyone should own the facts relating to his or her own private life.[400] It is sometimes argued that the purpose of Warren and Brandeis's article, in calling as it did for the recognition of a general right to privacy, was to serve as a conduit for the authors to express their frustrations towards the press.[401] The authors felt the press were "overstepping in every direction the obvious bounds of propriety and of decency.[402] Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery". Warren and Brandeis further believed "modern enterprise and invention have through invasions upon [the individual's] privacy subjected [the individual] to mental pain and distress, far greater than could be inflicted by mere bodily injury".[403]

---

[396] *Supra*.

[397] Warren and Brandeis "The Right to Privacy" (1890) *Harvard Law Review* 193 196.

[398] Bible and McWhirter *Privacy in the Workplace: A Guide for Human Resource Managers* (1990) 34.

[399] Warren and Brandeis "The Right to Privacy" (1890) *Harvard Law Review* 193 196.

[400] Bible and McWhirter *Privacy in the Workplace: A Guide for Human Resource Managers* (1990) 76.

[401] It is often suggested that Warren and Brandeis wrote the article in response to the press's interest in Mrs Samuel D. Warren. Mrs Samuel D. Warren was the daughter of Senator Bayard Delaware and held a host of popular elaborate social functions at her home for the Boston elite and as such newspapers reported on her social affairs in detail. Mrs Warren did not appreciate the coverage of her social affairs and especially not pleased with the lurid coverage of her daughter's wedding and turned to her husband, a retired paper magnate and lawyer. Bible and McWhirter *Privacy in the Workplace: A Guide for Human Resource Managers* (1990) 35.

[402] Warren and Brandeis "The Right to Privacy" *Harvard Law Review* (1890) 193 196.

[403] *Supra*.

Though the article initially had little effect upon the law, it encouraged courts to start thinking about privacy protection at common law level.[404] For instance, in the 1905 Georgia Supreme Court case of *Pavesich v New England Insurance Company*[405], Cobb J outlined the development of the right to privacy and conceded that before 1890:

> "every adjudicated case, both in this country and in England, which might be said to have involved a right of privacy, was not based upon the existence of such right, but was founded upon a supposed right of property, or a breach of trust or confidence, or the like, and that therefore a claim to a right of privacy, independent of a property or contractual right, or some right of a similar nature, had, up to that time, never been recognized in terms in any decision".[406]

Cobb J further differed from the judgment in *Robertson v Rochester Folding Box Co*[407], in which it was held that a right to privacy does not exist or will never exist as a legal and enforceable right.[408] Parker CJ argued in *Robertson* that the incorporation of the right to privacy in United States law would "result not only in vast amount of litigation, but in litigation bordering upon absurd". He added that if the right to privacy were to be "established as a legal doctrine [it would be impossible to confine it] to the restraint of the publication of a likeness, but [it would also have to include] publication of a word picture, a comment upon one's looks, conduct, domestic relations or habits".[409] Parker CJ further refused the existence of a right to privacy with reference to decided cases in both United States and England: every case relied upon to support the existence of the right was based on other grounds and no reference to the existence of the right is made by common law commentators or

---

[404]Wagner DeCew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 17. Although the article had minimal effect on the law it was accepted by New York's lower courts. See *Schuyler v. Curtis* (Sup. 1892) 15 N. Y. Supp. 787 (injunction granted against the making and public exhibition of a statue of a deceased person not shown to be a public character) and *Marks v Jaffa* (1893), 26 N.Y. Supp. 908, 6 Misc. Rep. 290 (injunction granted against the publication of a the plaintiff's picture in a newspaper for purposes of a popularity contest). McQuoid – Mason *The Law of Privacy in South Africa* (1978) 36.

[405]*Pavesich v New England Insurance Company* 122 Ga. 190 (1905).

[406]*Pavesich v New England Insurance Company* 122 Ga. 190 (1905) 69.

[407]*Robertson v Rochester Folding Box Co* 171 N.Y. 538, 64 N.E. 442.

[408]*Pavesich v New England Insurance Company* 122 Ga. 190 (1905) 77.

[409]*Robertson v Rochester Folding Box Co* 171N.Y. 538 545.

writers on common law principles of equity.[410] In contrast, in *Pavesich* Cobb J found that the existence of the right to privacy can reasonably be inferred from common law commentaries and judgments that really protected the right to privacy based on principles derived from the law of property, trust and contract. The learned judge further found the proper precedent in the circumstances to have been the dissenting judgment of Gray J in *Robertson*. Gray J held at 561:

> "[t]he right of privacy, or the right of the individual to be let alone, is a personal right, which is not without judicial recognition. It is the complement of the right to the immunity of one's person. The individual has always been entitled to be protected in the exclusive use and enjoyment of that which is his own. The common law regarded his person and property as inviolate, and he has the absolute right to be let alone. The principle is fundamental and essential in organized society that every one, in exercising a personal right and in the use of his property, shall respect the rights and properties of others. He must so conduct himself, in the enjoyment of the rights and privileges which belong to him as a member of society, as that he shall prejudice no one in the possession and enjoyment of those which are exclusively his. When, as here, there is an alleged invasion of some personal right or privilege, the absence of exact precedent, and the fact that early commentators upon the common law have no discussion upon the subject, is of no material importance in awarding equitable relief."

Even after the progressive argument by Cobb J in favour of the recognition of a right to privacy in *Paveisch*, American courts continued to be split over whether or not the right to privacy existed.[411]

The courts were ultimately convinced to adopt a common law right to privacy by two events. The first was the inclusion of the right in the first Restatement of Torts and the second Restatement of Torts. The Restatement adopted the view that "the law of privacy has not developed as a single tort, but as a complex of four [related] kinds of invasion of four different interests [with a common focus on the plaintiff's "right to be

[410] *Robertson v Rochester Folding Box Co* 171 N.Y. 538 545.

[411] McQouid – Mason *The Law of Privacy in South Africa* (1978) 37.

let alone"] of the plaintiff, which are tied together by the common name, but otherwise have nothing in common except that each represents an interference with the right of the plaintiff to be alone". The four kinds of invasions described by the Restatement are:

1. Intrusion upon seclusion;
2. Appropriation of likeness;
3. Public disclosure of private facts and;
4. False light publicity.

The second event was the publication of Prosser's article on the right to privacy (referred to in chapter 1). Prosser essentially identifies from the reported cases on privacy four distinct categories of invasions namely: appropriation of one's name or likeness[412]; intrusion upon the seclusion of another[413]; public disclosure of private facts[414] and placing another in a false light before the public[415]. [416]

3.3.4 Constitutional Protection of Privacy

The United States Constitution does not explicitly protect a right to privacy. The constitutional protection of privacy in the United States is the product of a long line of Supreme Court decisions, in which the Court went beyond the literal and sometimes narrow meaning of the constitutional language to strike down federal or state legislation, thereby in effect recognising a constitutional right to privacy.[417] The

[412] This invasion of privacy is the first to be recognised by US courts and requires that the appropriation of one's name or likeness benefit the defendant. McQouid – Mason *The Law of Privacy in South Africa* (1978) 40.

[413] The requirements of this category of invasions of privacy are three fold. First, there must be intrusion into the plaintiff's seclusion of solitude; second, the intrusion must be "offensive or objectionable to a reasonable man" and third, the intrusion must concern something private. McQouid – Mason *The Law of Privacy in South Africa* (1978) 37.

[414] The invasion of privacy under this category requires that the private information be given publicly and be highly objectionable in nature even where this private information is true. McQouid – Mason *The Law of Privacy in South Africa* (1978) 38.

[415] This invasion of privacy requires that the "publicity which places an individual in a false light in the public eye" be "objectionable to the ordinary reasonable man." McQouid – Mason *The Law of Privacy in South Africa* (1978) 40.

[416] McQouid – Mason DJ *The Law of Privacy in South Africa* (1978) 37. See also Jacques "Common Law Right to Privacy in the Employment Context" (2004) *Practising Law Institute* 788.

[417] Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law Review* 737. Rubenfield argues that the genealogy of the right of privacy in the US Constitution can be traced as far back as the *Marbury v Madison*1 Cranch 137, 5 U.S. 137, 1803 WL 893 (U.S.Dist.Col.), 2 L.Ed. 60). The Marbury decision marked the beginning of a long line of decisions which have used the due process clause in the Fourteenth Amendment to protect certain liberties. See *Lochner v New York* 198 U.S. 45 (1905) in which the Supreme court invalidated a maximum hours law for bakers on the basis that it interfered

discussion here will focus on only a select number of Supreme Court decisions that paved the way towards the constitutional protection of privacy. The Supreme Court has recognised that a right of privacy exists, or a guarantee of areas or zones of privacy, exist in the Constitution, namely in the First Amendment guaranteeing freedom of thought and expression[418]; the Fourth Amendment affirming the right of persons to be secure in their persons and the Fifth Amendment creating a zone for the individual in against self – incrimination clause[419]; in the penumbras of the Bill of Rights[420] and in Ninth Amendment which provides that the enumeration of certain rights in the Constitution shall not be interpreted to deny or disparage others.[421]

3.3.4.1 Boyd v United States

Perhaps the earliest Supreme Court case to recognise that the United States Constitution protects a right to privacy is *Boyd v United States*.[422] The Supreme Court interpreted privacy rights as generalisations of two maxims, namely "a man's home is his castle" or "sanctity of the home" which were regarded as enforceable legal principles by the English common law.[423] The court identified the "…Bill of Rights with its vigorous circumscription of state power [as the point of departure for understanding privacy]." The Court in *Boyd* explained the right to privacy as "the right against unlawful searches and seizures. It is thus the right that inheres in us as free and sovereign political actors, masters in our own houses, which the state is ordinarily forbidden to invade." The court cited with approval Lord Camden's opinion in *Entick v Carrington* and then proceeded to state:

---

with the freedom to contract; *Trustees of Dartmouth College v Woodward* 17 U.S. (4 Wheat.) 518 (1819) where the court struck down New Hampshire's attempt to legislatively control Dartmouth College; *Meyer v Nebraska* 262 U.S. 390 (1923) in which the Court held that state could not prevent the education of foreign languages at an elementary school; and *Pierce v Society of Sisters* 268 U.S. 510 (1925) in which the Supreme Court struck done legislation which required all children to attend public school.

[418] *Stanley v Georgia* 394 U.S. 557 (1969).

[419] *Katz v United States* 389 U.S. 347 (1967).

[420] *Griswold v Connecticut* 381 U.S. 477 (1965).

[421] *Griswold v Connecticut* 381 U.S. 477 (1965).

[422] *Boyd v United States* 116 U.S. 616 (1886) 616.

[423] *Boyd v United States* 116 U.S. 616 (1886) 616.For Whitman the history of modern privacy rights in America should ideally begin with the *Boyd* decision and not with the "right to be let alone" as espoused by Warren and Brandeis since the "right to be let alone" was borne of the *Boyd* interpretation of privacy. Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151 1212-1213.

> "[t]he principles laid down in [*Entick v Carrington*] affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence …Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of that judgment".[424]

3.3.4.2 Griswold v Connecticut

Griswold v Connecticut[425] was the first of many United States Supreme Court decisions to articulate constitutional privacy.[426] The appellants in *Griswold* were fined for contravening a Connecticut statute prohibiting the use of contraception for giving medical advice to a married couple on preventing conception. Douglas J found that various guarantees in the Bill of Rights create zones of privacy, namely, the First Amendment guaranteeing right of association; the Third Amendment prohibiting the quartering of soldiers in any house in times of peace without the consent of the owner; the Fourth Amendment affirming the right of persons to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures; the Fifth Amendment creates a zone for the individual against self – incrimination; and the Ninth Amendment which provides that the enumeration of certain rights in the

[424] *Boyd v United States* 116 U.S. 616 (1886) 616.

[425] *Griswold v Connecticut* 381 U.S. 477 (1965).

[426] The reasoning in *Griswold* was later used by the court in *Einsenstadt v Baird*405 U.S. 438 (1972) the Court protected the distribution of contraceptives to unmarried persons, thereby extending the decisions regard sexual conduct beyond the marital relationship. The Court stated the following "If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted government intrusion into matters, so fundamentally affecting a person as the decision whether to bear or beget a child." *Einsenstadt v Baird* 405 U.S. 438 (1972) 453.

Constitution shall not be interpreted to deny or disparage others. The Court concluded that marriage was covered within the zone of privacy created by several constitutional guarantees and the legislation concerned "seeks to achieve its goals by means of having a maximum destructive impact upon the marriage".[427]

3.3.4.3 Katz v United States

In *Katz v United States*[428], the Supreme Court formulated the "reasonable expectation test" of the right to privacy. In *Katz*, the defendant received a conviction in a United States district court for violating a statute proscribing interstate transmission by wire communication of bets and wagers, after the FBI had listened to and recorded conversations the defendant had from a public telephone booth. The defendant appealed this decision on the basis that the recordings had been obtained in violation of the Fourth Amendment. However, the Court of Appeals rejected this argument because there was no physical entrance by the FBI into the public telephone booth while the defendant was conducting the telephone conversations in question. The United States Supreme Court chose to reverse the decision of the Court of Appeals. The Court found that the government's listening and recording of the defendant's conversations while using a public telephone booth violated his right to privacy and constituted a search and seizure within the ambit of the Fourth Amendment. Stewart J reasoned that the defendant, in entering the telephone booth did not seek "to avoid the intruding eye" but "the uninvited ear". Stewart J added that the defendant:

> "did not shed his right to [privacy] simply because he made his calls from a place where he might be seen. No less that an individual in a business office, in a friend's apartment, or in a tax cab, a person in a telephone booth may rely upon protection of the Fourth Amendment."[429]

The Supreme Court thus altered the face of United States privacy protection in two ways. First, the Court departed from the narrow stance taken in *Olmstead v United States*[430] that the Fourth Amendment limited only searches and seizures of tangible objects (i.e. that trespass without the seizure of tangible material objects fell outside

[427] *Griswold v Connecticut* 381 U.S. 477 (1965) 484.
[428] *Katz v United States* 389 U.S. 347 (1967).
[429] *Katz v United States* 389 U.S. 347 (1967) 352.
[430] 277 U.S. 438, 471 - 485 (1928).

the ambit of the Fourth Amendment). The Court instead construed the Fourth Amendment as governing not only the seizure of tangible material objects but as also governing the recording of words. The Fourth Amendment, according to Court, "protects people not simply areas against unreasonable searches and seizures".[431]

Second, the court balanced the interest of individuals from governmental intrusion against the state's interest in protecting society from criminals. The two pronged reasonable expectation test - resulted from this. Harlan J expressed the test as follows:

> "…[F]irst, that a person has exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as reasonable (objective). Thus, a man's home is, for most purposes, a place where he expects privacy but objects, activities, or statements that he exposes to the plain view of outsiders remain unprotected because he expresses no intention to keep them to himself. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable".[432]

3.3.4.4 Stanley v Georgia

The question before the court in *Stanley v Georgia*[433] was whether a state of Georgia statute criminalising the possession of obscene material violated the First Amendment. The state contended that the possession of obscene material is not consistent with the right to free thought and expression guaranteed by the First Amendment (.i.e. the First Amendment did not protect obscenity). The Court acknowledged that the government had a legitimate interest in regulating the commercial distribution of obscenity but found that insofar as it punished the mere private possession of obscene material by an adult, the state violated the First Amendment. In reaching this finding, the Court noted that it had been established the Constitution protected that right to receive information and ideas regardless of their social worth. In asserting this right, the individual was at liberty to "read or observe what he [or she] pleases to satisfy his [or her] intellectual needs in the privacy of his [or her] home." In so doing, the individual "is asserting the right to be free from state

[431] *Katz v United States* 389 U.S. 347 (1967) 353.

[432] *Katz v United States* 389 U.S. 347 (1967) 353.

[433] *Stanley v Georgia* 394 U.S. 557.

inquiry into the contents of his library".[434] The Court added that United States "constitutional heritage rebels at the thought of giving government the power to control men's minds."[435] The Court further construed the First Amendment to mean that "a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch"[436]. [437]

3.3.5 Summary

In summary, the development of legal protection in the United States began with the invention of the printing press. The printing press increased individual access to information. In 1890 the authors Warren and Brandeis called for the recognition of a common law right to privacy. This and other events encouraged certain courts to argue for the recognition and development of a right to privacy in the United States jurisprudence. At common law level, these developments, as well as the inclusion of privacy in the Restatement of Torts and Prosser's classification of privacy into four distinct categories convinced the courts to develop a common law right to privacy (albeit in a negative ay as a bundle of related torts). Thereafter, the United States Supreme Court held that the United States Constitution, which does not explicitly protect or guarantee the right to privacy, guaranteed zones of privacy through its various amendments. Again, perhaps most importantly for the further discussion, the United States Supreme Court formulated the reasonable expectation test which balances privacy interests against other competing interests.

---

[434] *Stanley v Georgia* 394 U.S. 557 565.

[435] *Stanley v Georgia* 394 U.S. 557 565.

[436] *Stanley v Georgia* 394 U.S. 557 565.

[437] See also *Lawrence v Texas* 539 U.S. 558 (2003). The court in *Lawrence* found a Texas statute criminalising sexual relations between two persons of the same sex unconstitutional. The court stated the following: "…[This] case[involves] two adults who, with full and mutual consent from each other engaged in sexual practices common to the homosexual lifestyle…[they] are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government. It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter". Justice Kennedy in delivering the opinion of the court also cited with approval decisions of the European Court of Human Rights and other foreign jurisdictions that affirmed the rights of homosexual adults to engage in sexual conduct. *Lawrence v Texas* 539 U.S. 558 (2003) 578.

3.4 UNITED KINGDOM

3.4.1 Privacy Prior to the Incorporation of the ECHR

Prior to the incorporation of the European Convention on Human Rights[438] ("ECHR") into English domestic law, there was no explicit recognition of a right to privacy in English law. Before the incorporation of the ECHR into domestic law, Britain had neither a statutory nor common law right to privacy.[439] English law did, however, provide and continues to provide remedies for invasions of privacy in the absence of a written constitution.[440] For some commentators the remedies provided for privacy protection were "patchy, incomplete and hidden within a large number of disparate laws".[441]

Various authors give the following as reasons for the absence of a statutory or common law right of privacy in English law:

a) The absence of a written constitution within which to use a liberal interpretation to find a right to privacy. The United States, as mentioned, possesses a written constitution, which has allowed for an interpretation it in favour of an implied right to privacy in view of the First, Fourth, Fifth and Ninth Amendments. A written constitution therefore aids the extension and the scope of other fundamental rights by analogy and implication.[442]

b) Restricted focus on the development of existing related rights. English law has historically focussed on the protection of property and physical rights, rather than on the protection of social rights or on the creation of new types of rights such as the right to privacy. Consequently, most of the law protecting privacy in theory protects the property and physical rights of individuals.[443]

c) Deference to the supremacy and sovereignty of parliament.

---

[438] Drafted by the Council of Europe in 1950 and came into force on 3 September 1953.

[439] Carnegie "Privacy and the Press: The Impact of Incorporating the European Convention on Human Rights in the United Kingdom" (1998) 9 *Duke Journal of Comparative and International Law* 311 311.

[440] Krotoszynski "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law" 1990 *Duke Law Journal* 1398 1404.

[441] Shorts and De Than *Human Rights Law in the UK* (2001) 535.

[442] That is to say, because English rights emanate from different and individual sources it becomes difficult to argue that other fundamental rights exist within those individual sources. Shorts and De Than *Human Rights Law in the UK* (2001) 535.

[443] Shorts and De Than *Human Rights Law in the UK* (2001) 535.

d) Fears that changes to existing law may result in legal uncertainty.[444]

Some legal commentators have argued that, even before the incorporation of the ECHR, Britain could have developed a right to privacy within the framework of its existing common law.[445] Some of these commentators argue that if the United States (with Warren and Brandeis the catalysts) was capable of claiming a common law right to privacy and base this claim on an English case (*Prince Albert v Strange*[446]), surely English jurisprudence could reach the same conclusion by relying on the existing principles of trespass, nuisance, copyright and confidence. [447]

3.4.1.1 Parliamentary Attempts to Create a Right of Privacy

The English Parliament has made several (unsuccessful) attempts to address the right to privacy. The Younger Committee made perhaps the most well known attempt. This Committee was given the primary task of reviewing privacy under English law.[448] The terms of reference of the Younger Committee were "[t]o consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons and organisations, or by companies, and to make recommendations".[449] In its 1972 report, the Committee concluded that England did not require a general right to privacy as the existing doctrine of breach of confidence was able to protect privacy.[450] The Younger Committee primarily based its conclusion on two reasons: first, the concept of privacy is difficult to define and, secondly, it is difficult to balance privacy interests against

---

[444] Krotoszynski "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law" 1990 *Duke Law Journal* 1398 1404.

[445] Legal commentators such as Arnheim *The Handbook of Human Rights Law: An Accessible Approach to The Issues and Principle*s (2004) 176 and Shorts and De Than *Human Rights Law in the UK* (2001) 536 use this reasoning to advance arguments in favour of the development of English privacy law.

[446] 1 McN. & G. 25 (1849).

[447] Arnheim *The Handbook of Human Rights Law: An Accessible Approach to The Issues and Principle*s (2004) 176 and Shorts and De Than *Human Rights Law in the UK* (2001) 536.

[448] Before the English parliament authorised the Younger Committee in 1972 to look into the creation of a right of privacy, a number of bills in the 1960's purported to create a general right to privacy. These bills were however unsuccessful for a number of reasons and one of those reasons was that the Bills accorded courts too much discretion. Carnegie "Privacy and the Press: The Impact of Incorporating the European Convention on Human Rights in the United Kingdom" (1998) 9 *Duke Journal of Comparative and International Law* 311 317.

[449] Wacks *Privacy and Press Freedom* (1995) 4.

[450] Carnegie "Privacy and the Press: The Impact of Incorporating the European Convention on Human Rights in the United Kingdom" (1998) 9 *Duke Journal of Comparative and International Law* 311 317.

other competing interests.[451] The second major committee charged with looking into developing a privacy tort, was the Calcutt Committee on Privacy and Related Matters. The Calcutt Committee's terms of reference were "to consider what measures (whether legislative or otherwise) are needed to give further protection to individual privacy from the activities of the press and improve recourse against the press for the individual citizen."[452] In its 1990 report, the Calcutt Committee also concluded there was no need for a right of privacy in tort law and based its conclusion on a number of practical and legal reasons[453].[454]

3.4.1.2 Judicial Reluctance towards Recognising Privacy

Judicial decisions prior to the incorporation of the ECHR "lacked any notion of privacy" and expressed a reluctance to recognise a general right to privacy.[455] Certain judges, such as Vice Chancellor Sir Robert Megarry in *Malone v Metropolitan Police Commissioner* opined that the creation of a right to privacy was a task to be borne by parliament and not by judges.[456] The view that the general right to privacy could not be developed by the courts was not shared by some English judges. For instance, Lord Keith in the House of Lords decision of *Attorney General v Guardian Newspapers Ltd and Other (No 2)*,[457] suggested, in discussing the law of breach of confidence, that a

[451] MacCormick "Privacy: A Problematic" (1974) 1 *British Journal of Law and Society* 75.

[452] Munro "Press Freedom – How the Beast was Tamed" (1991) 54 *The Modern Law Review* 104.

[453] Munro "Press Freedom – How the Beast was Tamed" (1991) 54 *The Modern Law Review* 104 107.

[454] Krotoszynski attributes the failure of these Committees to the fact that their terms of reference were restricted to private intrusions of privacy and not extended to governmental intrusions of privacy. The problem with British law for Krotoszynski is not a lack of a general right to privacy per se but "a lack of a right to privacy that can be asserted against the state." Krotoszynski "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law" 1990 *Duke Law Journal* 398 406.

[455] 192. The following UK decisions that have held there is no right to privacy in English law: see *R v Khan (Sultan)* [1997] AC 558 (at issue was whether the covert installation of electronic device amounted to trespass, damage to property and an invasion of privacy) *Bernstein v Skyviews Ltd*. [1978] Q.B. 479 (at issue was whether a flight over property for the purpose of taking aerial photographs amounted to trespass or invasion of privacy) and *Wainright and Another v Home Office* [2003] UKHL 53 (question before court was whether strip search of mother and her son on a prison visit infringed their right to respect for private life).

[456] *Malone v Metropolitan Police Commissioner* [1979] 1 Ch. 344. The question before the court in *Malone v Metropolitan Police Commissioner* [1979] 1 Ch. 344 was whether tapping of post office telephone by police lawful on grounds of right to property, privacy and confidentiality.

[457] *Morris v Beardmore* [1981] A.C. 446 464.

tort of privacy could be developed by the courts.[458] In addition, Lord Scarman in *Morris v Beardmore*[459] declared that:

> "[i]n formulating my reasons for allowing the appeal…I have deliberately used an adjective which has an unfamiliar ring in the ears of common law lawyers. I have described the right of privacy as "fundamental"…it is apt to describe the importance attached by the common law to the privacy of the home. It is still true as was said by Lord Camden C.J. in *Entick v Carrington* (1765) 19 State Tr. 1029, 1066, that: "No man can set his foot upon my ground without my licence, but he is liable to an action, though the damage be nothing;…If he admits the fact, he is bound to show by way of justification, that some positive law has empowered or excused him."[460]

Lord Scarman concluded: "The present appeal is concerned exclusively with the suspect's right to privacy of his home…The appeal turns on the respect which parliament must be understood… to pay to the fundamental right of privacy in one's own home, which has for centuries been recognized by the common law". Lord Scarman here is suggesting that there is no need to develop a right to privacy as the right already exists in English law and (even though English courts do not expressly describe the right as a "the right of privacy") is clearly recognised by the common law and international law. [461]

3.4.2 Remedies for Privacy Invasions Prior to the ECHR

As previously indicated, in the absence of a written constitution and legislation explicitly protecting privacy, English law provided remedies for various privacy

---

[458] See discussion on law of breach of confidence below which discusses the findings of the court in *Attorney General Guardian Newspapers Ltd and Others*.

[459] *Morris v Beardmore* [1981] A.C. 446 cited in Fiddick "The Human Rights Bill [House of Lords], Bill 119 of 1997-98: Privacy and the Press" *98/25Research Paper Home Affairs Section* House of Commons Library 7.

[460] *Morris v Beardmore* [1981] A.C. 446464.

[461] *Morris v Beardmore* [1998] All ER 446 464. See also Fiddick "The Human Rights Bill [HL], Bill 119 of 1997-98: Privacy and the Press" *Research Paper 98/25Home Affairs Section* House of Commons Library 7.

invasions. Two of these remedies are the torts of trespass to land and goods and the doctrine of breach of confidence.[462]

3.4.2.1 Tort of Trespass to Land and Goods

The tort of trespass to land and goods essentially protects individuals against direct intrusions into their home.[463] Lord Camden in *Entick v Carrington* confirmed the existence of the tort of trespass relating to goods in English law:

> "Our law holds the property of every man sacred that no man can set his foot upon his neighbour's close without his leave. If he does, he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law and concluded "[t]he defendants have no right to avail themselves of the usage of these warrant…".[464]

English common law has always treated the right to freedom from interference with personal property as a predominant interest and the remedy for this earliest form of tort was a writ of trespass.[465] This treatment of individual property rights as fundamental gave birth to the English maxim, "An Englishman's home is his castle". Donaldson LJ in *McLorie v Oxford*[466] traced the importance of this maxim in English common law to *Seymane's Case*[467] : "That an Englishman's home is his castle" is one of the few principles of the law known to every citizen and was affirmed as early as 1604 in *Seymane's Case*... and reaffirmed as recently as 1980 in *Morris v Beadmore*[468]...". [469]

---

[462] Clayton and Tomlinson "Privacy and Freedom of Expression" (2001) 6-7.

[463] Clayton and Tomlinson "Privacy and Freedom of Expression" (2001) 6 – 7.

[464] In *Entick v Carrington* Lord 1558-1774 All ER Rep 45.

[465] In *Entick v Carrington* 1558-1774 All ER Rep 45 Lord Camden confirmed the existence of the tort of trespass relating to personal goods in English law: "Our law holds the property of every man sacred that no man can set his foot upon his neighbour's close without his leave. If he does, he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law and concluded "[t]he defendants have no right to avail themselves of the usage of these warrant…".

[466] *McLorie v Oxford* [1982] 1 QB 1290 1296.

[467] *Seymane's Case* [1558-1774] All E.R. Rep.

[468] *Morris v Beardmore* [1981] A.C. 446.

[469] *McLorie v Oxford* [1982] 1 QB 1290 1296.

In *Seymane's Case*[470]Sir Edward Coke held that "…the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose….".[471] Sir Coke further held "[t]hat the house of everyone is not a castle or privilege but for himself, and shall not extend to protect any person who flies to his house or goods of any other…for the privilege of his house extends only to him and his family, and his own proper goods …".[472]

3.4.2.2 Doctrine of Breach of Confidence

The doctrine of breach of confidence evolved from the decision of *Albert v Strange*.[473] In *Albert v Strange*, one of the grounds on which the Court allowed the injunction to remain was that there had been a breach of confidence or trust on the part of the defendant. The doctrine has since found expression in a number of decisions. *Malone v Metropolitan Police Commissioner*.[474]

One of the leading cases on the doctrine of breach of confidence in English law is *Attorney General v Guardian Newspapers Ltd and Others (No 2)*[475]. The matter concerned the book *Spycatcher*, written by an ex officer of MI5 (British security service), which purported to be the memoirs of the ex officer's 20 years in MI5. The Attorney General (AG) sought to prevent or restrict publication of the book and publication of any comment or reports of its contents, on the ground of national security and that publication represented a breach by the ex - officer of the duty of confidence he owed to his country. On appeal, Sir John Donaldson described breach of confidence as a right to have the confidentiality of information maintained, which arises out of contract (whereby one party undertakes to maintain the confidentiality of information made available to them by another party), or arises as a necessary or traditional incident of a relationship between the confidant and confider (e.g. priest and penitent, doctor and patient, lawyer and client, banker and customer and husband and wife).[476]

---

[470]*Seymane's Case* [1558-1774] All E.R. Rep 63.

[471]*Seymane's Case* [1558-1774] All E.R. Rep 63.

[472]*Seymane's Case* [1558-1774] All E.R. Rep 65.

[473]1 McN. & G. 25 (1849).

[474]*Malone v Metropolitan Police Commissioner* [1979] Ch. 344.

[475]*Attorney General v Guardian Newspapers Ltd and Others* (No 2) [1988] 3 All ER 545.

[476]*Attorney General v Guardian Newspapers Ltd and Others* (No 2) [1988] 3 All ER 545 595 and 596.

In the House of Lords decision of *Attorney General v Guardian Newspaper Ltd.* (No 2), Lord Keith, in considering whether detriment to the confider of confidential information is an essential ingredient of the cause of action alluded to the right to privacy:

> "The Crown's case on all the issues which arise invokes the law of confidentiality…The law has long recognized than an obligation of confidence can arise out of particular relationships. Examples are the relationships of doctor and patient, priest and penitent, solicitor and client, banker and customer. The obligation may be imposed by an express and implied term in a contract but it may also exist independently of any contract on the basis of an independent equitable principle of confidence: see *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) [1963] 3 All ER 413. It is worthy of some examination whether or not detriment to the confider of confidential information is an essential ingredient of his cause of action in seeking to restrain by injunction a breach of confidence. Presumably that may be so as regards an action for damages in respect of a past breach of confidence. If the confider has suffered no detriment thereby he can hardly be in a position to recover compensatory damages. However, the true view may be that he would be entitled to nominal damages. Most of the cases have arisen in circumstances where there has been a threatened or actual breach of confidence by an employee or ex-employee of the plaintiff, or where information about the plaintiff's business affairs has been given in confidence to someone who has proceeded to exploit it for his own benefit: an example of the latter type of case is *Seager v Copydex Ltd* [1967] 2 All ER 415, [1967] 1 WLR. In such cases the detriment to the confider is clear, since the breach involves no more than an invasion of personal privacy. Thus in, *Margaret Duchess of Argyll v Duke of Argyll* [1965] 1 All ER 611, [1967] Ch 302 an injunction was granted against the revelation of

> marital confidences. The right to personal privacy is clearly one which the law should in this field seek to protect".[477]

Lord Keith is suggesting in the last sentence that a tort of breach of privacy could be developed by the courts.[478] Several commentators have suggested that breach of confidence cannot effectively protect privacy interests and, as such, English courts or parliament should look into the creation of a tort based on breach of independent right of privacy.[479]It is true that the tort of breach of confidence is perhaps the closest relative of privacy as far as both actions prevent the public disclosure of private or personal information. At first glance, privacy and breach of confidence may seem similar and even overlap at times, but ultimately the two actions are different. The difference primarily is that the underlying issue in case of breach of privacy is publicity whilst at issue in case of breach of confidence is disclosure.[480] Schreiber argues the tort of breach of confidence should not protect invasions of privacy and an independent tort of invasion of privacy should be recognised in English law.[481] The recognition of a an independent invasion of privacy will permit the growth and development of each action and ultimately a less strenuous protection of privacy, in Schreiber's words: "[it] will enable breach of confidence to grow without jeopardizing the right to privacy, and will likewise allow for the protection of privacy to develop without affecting the action in breach of confidence. Confidence cannot transmogrify into privacy, the courts or Parliament must facilitate the emergence of privacy independently of confidence".[482]

Schreiber advances seven arguments in support of this: first, the jurisprudential beginnings of breach of contract and privacy are different. Privacy is a natural law right to self - determination, that inheres in every human being and is enforceable against everyone regardless of whether they are known to us or not, whereas breach of confidence is a relationship based action, i.e. an action based on the existence of a

---

[477] *Attorney General v Guardian Newspapers Ltd and Others* (No 2) [1988] 3 All ER 545 639.

[478] Fiddick "The Human Rights Bill [House of Lords], Bill 119 of 1997-98: Privacy and the Press" *98/25 Research Paper Home Affairs Section House of Commons* Library 6.

[479] Shorts and De Than *Human Rights Law in the UK* (2001) 550.

[480] Shorts and De Than *Human Rights Law in the UK* (2001) 550.

[481] Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy Should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160.

[482] Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy Should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160 191.

relationship of trust between parties;[483] secondly, privacy can be and deserves to be treated as a common law tort and a constitutional right whereas breach of confidence is simply a common law tort;[484] thirdly, the protection of privacy through breach of confidence has resulted in the dilution of the action;[485] fourthly, because breach of confidence is a commercially orientated action, it should by and large protect commercial information or confidences; privacy is a human right and aims to protect personal information;[486] fifthly, breach of confidence may constitute inadequate protection for privacy invasions;[487] sixthly, breach of confidence cannot adequately protect privacy because it fails to give effect to the privacy provisions of Human Rights Act and the ECHR;[488] lastly, the protection of privacy through breach of confidence fails to accord privacy its due recognition as an independent and important right in society.[489]

3.4.3 Privacy Protection Post the ECHR

The ECHR was the first convention signed under the Council of Europe. In 1998 Britain incorporated the ECHR into English law with the enactment of the Human

---

[483] Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160 168. For Schreiber for privacy to have carry some weight and have meaning it needs to be more than a tort, it needs to be strengthened by constitutional recognition. For this reason, the use of breach of contract to protect privacy in English law creates two problems: first, it "creates two types of privacy unrelated at law, requiring separate definition..." and second, "[breach of contract is] tied to a constitutional law and must evolve with it. Thus the constitutional law of privacy (e.g. ECHR, Article 8) will determine the path of the common law breach of confidence…." Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy Should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160 169.

[484] *Supra*.

[485] Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy Should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160 171. For example there are 3 requirements for the breach of contract action (the information must have a necessary quality of confidence; the defendant must have known or ought to have known that the information was imparted in confidence; there must have been a breach of that information) however the first and second requirements have been dissolved by courts in privacy cases resulting in an "uncertain and indeterminate action". Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160 170.

[486] Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy Should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160 177 – 178.

[487] Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy Should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160 180- 181.

[488] Schreiber "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy Should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160 190.

[489] *Supra*.

Rights Act[490].[491]Prior to the Human Rights Act English law had no single document housing individual and fundamental rights.[492]

3.4.3.1 Article 8 of the ECHR

Article 8 of the ECHR provides:

1. Everyone has the right to respect for his private and family life, his home and correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 (1) outlines the interests that are protected by the Article, being an individual's private life, family life, home and correspondence and further places an obligation on the state to "respect" those interests. Article 8(2) goes on to provide the circumstances under which states may lawfully interfere with the respect they are required to have for an individuals' private and family life, the individual's home and correspondence.

3.4.3.2 Meaning of "Private Life" in Article 8

In *Niemetz v Germany*[493]it was held that the meaning of "private life" in Article 8 extends beyond the Anglo-American idea of privacy with its emphasis on secrecy of personal information and seclusion. In this regard, courts have held certain areas to constitute private life within the meaning of Article 8: physical and moral integrity of

[490]Act of 1998.

[491] For Hoffman and Rowe, the Convention was incorporated into the English legal system: first, to avoid the cost and delay involved in taking a case to the European Court in the absence of a local remedy; second, to allow Convention rights to enter full into English law and lastly, to allow judges to contribute to Convention jurisprudence. Hoffman and Rowe *Human Rights in the United Kingdom: A General Introduction to the Human Rights Act 1998* (2003) 29.

[492]Hoffman and Rowe *Human Rights in the United Kingdom: A General Introduction to the Human Rights Act 1998* (2003) 17.

[493]*Niemetz v Germany* [1992] EHRR 97.

a person[494]; personal identity[495]; personal information[496]; personal sexuality[497]; and personal or private space[498].

3.4.3.3 Privacy Protection under Article 8

The incorporation of the ECHR into English domestic law has ignited debate on the existence of a common law right to privacy.[499] However, Article 8 presents two

[494] "Private life" within the meaning of Article 8 also covers a person's his or sexual life, protects against physical or sexual assaults on a person(*X and Y v Netherlands* (1985) 8 EHRR 235). It has also been held to cover some forms of intrusive testing such as compulsory blood testing (*X v Austria* (1979) 18 DR 154, EComm HR) and urine (*Peters v Netherlands* (1994) 77-A DR 75, EComm HR).

[495] Also at the root of private life is the capacity of the individual to formulate a perception of himself or herself and to choose his or her personal identity.

[496] In *Z v Finland* (1997) 25 EHRR 371 at 405 the court emphasized that "…the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention". The Court added that respecting the confidentiality of health data is a vital principle in the legal systems of all states to the Convention and that this confidentiality went beyond respecting the privacy of a patient but also encompassed preservation of the patient's confidence in the medical profession and in health services. Both the storing and release of information relating to an individual's private life in a secret police register have been found to constitute an interference with the person's right to respect for his or private life(*Leander v Sweden* (1987) 9 EHRR 433).

[497] Private life also encompasses an individual's personal relationships with others including social and sexual activities with others. See *Dudgeon v United Kingdom* (1981) 4 EHRR 149 the court described sexual activity as very intimate and private and in *Lustig-Prean v United Kingdom* (1997) 7BHRC 65 homosexuality as a sexual preference was held to fall under private life and this was confirmed by the court in. The court found in *Lustig-Prean v United Kingdom* (1997) 7 BHRC further found only weighty and convincing evidence could justify with the private life of certain members of the armed forces by investigating and dismissing them on the basis of their homosexuality.

[498] A breach of private life can be invoked in places where an individual has exclusive rights of enjoyment, such as the home, on the ground that there has been an infringement of private space which is to be enjoyed free from interference. The difficulty arises in considering whether private space includes those areas in which the applicant has no exclusive rights of ownership like the workplace and whether private space includes those areas in which the individual has no exclusive rights of ownership like the workplace. The Court in *Klass v Germany* (1979-80) 2 EHRR 214 230 stated in this regard that although telephone conversations are not expressly mentioned in paragraph 1 of Article 8, it considers that such conversations are covered by the notions of "private life" and "correspondence" referred to by the provision. In *Halford v United Kingdom* (1997) 24 EHRR 523 the Court stated that it was clear from the Court case law that telephone calls made from business premises as well as from home may be covered by notions of "private life" and "correspondence" within the meaning of Article 8(1). In *Klass v Germany*, *Malone v United Kingdom*, *Huvig v France* (1990) 12 EHRR 528, *A v France* (1994) 17 EHHR 462 and *Kopp v Switzerland* (1999) 27 EHRR 91. The applicant in *Halford*, formerly an Assistant Chief Constable, complained that calls she made from her home and office telephones were intercepted by the police in order to gather information to use against her in sex discrimination proceedings she was instituting against the police. The Court held she had a reasonable expectation of privacy for calls made from both telephones more so because she had been assured that she could use her both her office telephone for personal purposes including a sex discrimination claim she was pursuing against her employer and as Assistant Chief Constable she has sole use of her office and telephones in that office, one of which had been designated for her private use. In *Anderson v Sweden* (1992) 14 EHRR 615 the court held telephone conversations between family members were covered by the concepts of "family life" and "correspondence" in Article 8 (1).

[499] Carnegie 'Privacy and the Press: The Impact of Incorporating the European Convention on Human Rights in the United Kingdom' (1998) 9 *Duke Journal of Comparative and International Law* 311.

problems in its protection of privacy. First and foremost, Article 8 does not protect privacy.[500] The use of the word "respect" in the article means the obligation merely guarantees a "respect" for these rights[501] and does not protect privacy of family or the home or correspondence of the individual.[502] Second, a technical interpretation of the whole ECHR (including Article 8), points to the fact that the ECHR is intended to have a vertical effect and not a horizontal effect.[503] The question then arises whether Article 8 of the ECHR imposes positive or negative obligations. If positive obligations flow from Article 8, then the state is obliged to take steps to protect individuals from the negative effects of inaction and further require that third parties take positive action where there is a possibility of interference with an individual's life.[504] On the other hand, if negative obligations flow from Article 8, such obligations prohibit the state from committing any acts that might unduly infringe an individual's private life.[505]

The European Court has read the provisions of Article 8 as encompassing both positive and negative obligations. In *Airey v Ireland*[506] it was held that "…although the object of Article 8 is chiefly aimed at protecting the individual against arbitrary interference by public authorities, it does not merely compel the state to abstain from such interference: in addition to this primary negative undertaking, there may be positive obligations inherent in an effective respect for private or family life".[507] The Court in *Hokannen v Finland* [508] further found that although the boundaries between the State's positive and negative obligations under Article 8 do not lend themselves to precise definition, the applicable principles are similar – in both contexts due regard must be paid to the fair balance that has to be struck between the competing interests

[500] Arnheim *The Handbook of Human Rights Law: An Accessible Approach to The Issues and Principle*s (2004) 176.

[501] Clayton and Tomlinson *Privacy and Freedom of Expression* (2001) 46.

[502] Clayton and Tomlinson *Privacy and Freedom of Expression* (2001) 46.

[503] *Supra*.

[504] Clayton and Tomlinson *Privacy and Freedom of Expression* (2001) 46.

[505] *Supra*.

[506] *Airey v Ireland* (1979-80) 2 EHRR 305 319.

[507] See also *X and Y v Netherlands* (1985) 8 EHRR 235 and *Marckx v Belgium* (1979) 2 EHRR 330. Clayton and Tomlinson *Privacy and Freedom of Expression* (2001) 47.

[508] *Hokannen v Finland* (1995) 19 EHRR 139.

of the individual and the community as a whole, and in both contexts the State is recognized as enjoying a certain margin of appreciation.[509]

Article 8(2) provides for the justification of an interference with the right to privacy and the home.[510] It states:

> [t]here shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Conduct that has been found to constitute "interferences" include, amongst others, house searches and seizures,[511] storage and release of personal information on an applicant[512] and interception of telephone conversations.[513] In *Leander v Sweden*[514] the following principles were established in respect of the phrase "in accordance with the law":

> "[the expression] requires…that the interference must have some basis in domestic law. Compliance with domestic law, however does not

[509] *Hokannen v Finland* (1995) 19 EHRR 139 168-169.

[510] Clayton and Tomlinson *Privacy and Freedom of Expression* (2001) 36-37.

[511] *Klass v Germany* (1979-80) 2 EHRR 214.

[512] *Leander v Sweden* (1987) 9 EHRR 433.

[513] Malone v Metropolitan Police Commissioner [1979] 1 Ch 344 ,*Huvig v France* (1990) 12 EHRR and *Ludi v Switzerland* (1992) 15 EHRR 173.

[514] *Leander v Sweden* (1987) 9 EHRR 433. See also *Hewitt and Harman v United Kingdom* (1992) 14 EHRR 657 664. In *Hewitt* the Court stated that the phrase "in accordance with the law" goes beyond mere compliance with the domestic law. In *The Sunday Times v United Kingdom* [1979-80] 2 EHRR 245 271, the Court outlined two of the requirements flowing from the expression: " Firstly, the law adequately accessible in the sense that the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct. He must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty: experience shows this to be unattainable. Again, whilst certainty is highly desirable, it may be bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which to, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice."

> suffice: the law in question must be accessible…and its consequences [must be] foreseeable [for the individual concerned]"[515].

The Court has found that the following requirements flow from the expression "in accordance with the law":

1. Acts or activities complained of must have a basis in domestic law.[516]
2. The law must be accessible and foreseeable.[517]
3. A law conferring discretion (such as a norm) may be foreseeable provided the scope of its discretion and the manner of its exercise are clear[518].[519]

Article 8 further requires public authorities to prove that the interference was "necessary in a democratic society". The Court in *Handyside v United Kingdom*[520] noted that "…whilst the adjective "necessary"…is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "useful", "ordinary" or "desirable" and it implies the existence of a "pressing social need". The court further noted that "…it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion "necessity", in this context".[521] In terms of assessing this "necessity", States have a "certain margin of appreciation" or a degree of flexibility.[522] Thus the margin of appreciation recognises that States may take differing approaches to similar issues.

For Hoffmann and Rowe the idea of a margin of appreciation is:

> "appropriate because states that are bound by the Convention cover the whole of Europe and have different cultures and histories, different dominant religions, different traditions about how people should

[515] *Leander v Sweden* (1987) 9 EHRR 433 at 450.

[516] *Leander v Sweden* (1987) 9 EHRR 433.

[517] *The Sunday Times v United Kingdom* [1979-80] 2 EHRR 245 271.

[518] *Malone v Metropolitan Police Commissioner* [1979] 1 Ch 344 .

[519] See also Clayton and Tomlinson *Privacy and Freedom of Expression* (2001) 53-55.

[520] *Handyside v United Kingdom* (1976) 1 EHRR 754. In *Handyside* the applicant, an English publisher, was charged and convicted under the Obscene Publications Act of 1959 for possessing obscene books. The Court held that there had been interference by a public authority with the applicant's freedom of expression but such interference was justified in terms of Article 10(2) of the Convention, which is worded similar to Article 8(2). See also Clayton and Tomlinson *Privacy and Freedom of Expression* (2001) 53 - 55.

[521] *Handyside v United Kingdom* (1976) 1 EHRR 754.

[522] See *Handyside v United Kingdom* (1976) 1 EHRR 754 for an exhaustive discussion of the implications of the margin of appreciation afforded to contracting states.

> behave and when and to what extent interference is necessary. In some areas, there may be no consensus across Europe about what should be tolerated and what should not, and that would suggest to the judges popular feelings about their citizens about a particular issue".[523]

It is normally on complex moral issues (such as abortion or the treatment of transsexuals) that states have a margin of appreciation afforded by the ECHR.[524]

The phrase "legitimate aim" implies that the domestic law at issue is justified for one or more exceptions listed (that is national security, public safety, the economic well-being of the country, the prevention of crime and disorder, the protection of health or morals and the protection of rights and freedoms of others) under the second paragraph of Article 8(2).[525] Hence, where a state fails to show that an exception justified its interference, Article 8 is violated.[526]

3.4.3.4 ECHR and Right to Privacy in English Law

Several legal commentators have argued that the idea that there is no right to privacy in English law is no longer valid, particularly in light of certain decisions which, according to them, are indicative of the existence of a right to privacy in English law. In *Morris v Beardmore*[527]Lord Scarman declared the following regarding privacy in English law post the ECHR: "the right enjoys the protection of the European ECHR for the Protection of Human Rights and Fundamental Freedoms (1953) ("the ECHR"), which the United Kingdom has ratified and which the United Kingdom permits to those within its jurisdiction and the individual right of petition: see articles 8 and 25".[528]

---

[523] Shorts E and De Than C *Human Rights Law in the UK* (2001) 615.
[523]*Supra*.
[523] Shorts E and De Than C *Human Rights Law in the UK* (2001) 615.
[523]*Supra*.
[523] Shorts E and De Than C *Human Rights Law in the UK* (2001) 615.
[524]*Supra*.
[525] Shorts E and De Than C *Human Rights Law in the UK* (2001) 615.
[526] Shorts E and De Than C *Human Rights Law in the UK* (2001) 615.
[527]*Morris v Beardmore* [1981] A.C. 446.
[528]*Morris v Beardmore* [1981] A.C. 446 464.

3.4.3.4.1 Kaye v Robertson

These commentators further contend that the *Kaye v Robertson*[529]decision did not establish that there was no right to privacy in English law or that there was no room for developing such a right using existing principles. Rather, it is argued that in that case Lord Justice Glidewell was lamenting the inability of English judges to rely on the right to privacy found in the Human Rights Act[530] and further found that the enactment of the Human Rights Act introduced a right to privacy in English law.[531]

In *Douglas v Hello*,[532]Lord Justice Bingham, agreeing Lord Justice Glidewell's words in *Kaye v Robertson*, observed that that case highlights the failure of both the common law of England and statute to protect personal privacy and individual citizens.[533] Also in agreement, Lord Justice Leggatt, commended United States law for responding to the need for privacy, a need which English judges are unable to fulfil should circumstances arise. Lord Justice Leggatt further asserted that the right had been disregarded so long in English law that the only body that can effectively recognise it is the legislature.[534]

3.4.3.4.2 Hellewell v Chief Constable of Derbyshire

The second case is that of *Hellewell v Chief Constable of Derbyshire*[535]. In May 1989 the plaintiff, who had 32 previous convictions, 19 of which were for theft, was arrested and taken to a police station and charged with (attempted) theft. The plaintiff was fingerprinted, photographed and subsequently convicted of the offences. In 1992, an organization of shopkeepers, concerned about the level of shoplifting, asked the

[529]*Kaye v Robertson* [1991] FSR 62. The plaintiff in *Kaye v Robertson* was a well-known actor who had undergone extensive surgery at Charing Cross Hospital after a piece of wood during a storm smashed through his car windscreen and struck him on the head. The first defendant was the editor of a tabloid newspaper named the "Sunday Sport" and the second defendant was the publisher of the same newspaper. A journalist and photographer acting under the instructions of the first defendant gained access to Kaye's private hospital room, interviewed, and photographed the plaintiff before being ejected by security staff. The defendants then expressed their intention to publish the article on the plaintiff. The plaintiff, through a friend sought to prevent publication of the article through an interlocutory injunction alleging malicious falsehood, libel, passing off and trespass to the person. The injunction was granted and the defendants appealed. The Court of Appeal allowed the appeal in part and discharged the injunction but substituted with a new order.

[530]Act of 1998.

[531]*Kaye v Robertson* [1991] FSR 62 66.

[532]*Douglas v Hello! Ltd* [2006] QB 125.

[533]*Douglas v Hello! Ltd* [2006] QB 125 236 paragraph 114.

[534]*Douglas v Hello! Ltd* [2006] QB 125236 paragraph 115

[535]*Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804.

police to supply photographs of individuals known to be causing trouble in the area so that their staff would recognize them. The police provided a number of photographs, including one of the plaintiff, which had been taken when he was in police custody. The police also told the shopkeepers to only show the photographs to their staff but not to display the photographs publicly. The plaintiff learnt of the use being made of the photograph and applied for an injunction restraining the Chief Constable from disclosing his photograph to the public. Justice Laws, in granting the application, held that a duty of confidence could arise when the police took a photograph of a suspect at a police station in circumstances where his consent was not required, but where the photograph was used reasonably for the prevention and detection of a crime, the investigation of alleged offences or the apprehension of suspects or persons unlawfully at large, the police would have a public interest defence to any action for breach of confidence. Justice Laws concluded that the police in disclosing the plaintiff's photograph had acted entirely in good faith for the prevention or detection of a crime and had distributed it only to persons who had reasonable need to make use of it. The court further gave an example to illustrate that the tort of breach of confidence contains all the necessary elements for the fair protection of privacy. In other words, the court was convinced that privacy interests are protected in particular instances under the law of confidentiality:

> "If someone with a telephoto lens were to take from a distance with no authority a picture of another engaged in some private act, his subsequent disclosure of the photograph would, in my judgment as surely amount to a breach of confidence as if he found a stolen letter or diary in which the act was recounted and proceeded to publish it. In such a case, the law would protect what might reasonably be called a right to privacy, although the name accorded to the cause of action would be breach of confidence".[536]

[536] *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804 807.

3.4.3.4.3 Thompson and Venables v News Group Newspapers

In the third case, *Thompson and Venables v News Group Newspapers*,[537] the limitations of the development of breach of confidence in protecting rights of privacy under Article 8 were recognised. Dame Elizabeth Butler –Sloss stated that:

> "[u]nder the umbrella of confidentiality there will be information which may require a special quality of protection. In the present case the reason for advancing that special quality is that, if the information is published , the publication is likely to lead to grave and possibly fatal consequences …the court has jurisdiction, in exceptional cases, to extend the protection of confidentiality of information…where not to do so would be likely to lead to serious physical injury, or to death, of the person seeking that confidentiality, and there is no other way to protect the applicants other than by seeking relief from court".[538]

The approach in *Thompson and Venables* was adopted in *Naomi Campell v Mirror Group Newspapers Ltd*[539] in which decision Justice Morland found that celebrities and public figures are entitled to some privacy:

> "Although many aspects of the private lives of celebrities and public figures will inevitably enter the public domain…it does not follow that even with self-publicists every aspect and detail of their private lives are legitimate quarry for the journalist. They are entitled to some space of privacy…the media to conform with Article 8 should respect information about aspects or details of private life of celebrities and public figures which they legitimately choose to keep private, certainly

[537] *Thompson and Venables v News Group Newspapers* [2001] EWHC 32 (QB). The claimants in *Thompson and Venables* had killed a two-year-old boy when they were both aged ten and a half years old and were both subsequently convicted and detained for the crime. The shocking and distressing facts of their case were widely publicized. Injunctions restricting the information which the media had been entitled to publish during their detention came to an end on their eighteenth birthdays, the claimants therefore sought injunctions against specific newspaper publishers and against the whole world to restrain the solicitation or publication of information as to the physical appearance, whereabouts or movements, their new identities upon release and personal and historical information on their care, treatment and progress during their minority. The claimants sought the injunctions on the basis that they were necessary to protect their right of confidentiality and rights to life and freedom from persecution and harassment conferred by the Convention.

[538] *Thompson and Venables v News Group Newspapers* [2001] EWHC 32 (QB)162.

[539] *Naomi Campell v Mirror Group Newspapers Ltd* [2003] EMLR 39.

> "sensitive personal data", unless there is an overriding public interest duty to publish…". [540]

The court further held that the development of the law of confidentiality since the Human Rights Act[541]came into force has seen information described as "confidential" in instances where it had not been confided by one person to another, but where it relates to an aspect of an individual's private life which he does not choose to make public. The court added that the unjustifiable publication of such information should be described as breach of privacy rather than breach of confidence.[542]

3.4.3.4.4 Douglas v Hello! Ltd

The fourth case, *Douglas v Hello! Ltd*,[543] touches on the reluctance of some English courts to interpret the provision under Article 8 of "private life" as protecting the right to privacy. Instead, such courts prefer to adhere to the conclusions of the Younger Committee and protect all privacy interests, including those which clearly necessitate a right to privacy be recognised and protected, with the tort of breach of confidence. These courts further ignore the fact that the tort of breach of confidence has shortcomings in that it cannot effectively remedy those cases in which no prior confidential relationship existed between the parties.[544]

In *Douglas*, the first and second claimants were the film stars Michael Douglas and Catherine Zeta-Jones. The third claimant was the publisher OK! Magazine. The defendant was the publisher of Hello! Magazine. The claimants had entered into an agreement under which the third claimant was given exclusive rights to publish photographs of their wedding in 2000. The first and second claimants further requested their guests and employees not to take photographs or videos, and were required to pass through a security check at which a notice prohibiting photography and videos was posted. The third claimants later learned that the defendant intended to publish an article containing photographs of the wedding and applied for an injunction

---

[540] *Naomi Campell v Mirror Group Newspapers Ltd* [2003] EMLR 3946.

[541] Act of 1998.

[542] *Naomi Campell v Mirror Group Newspapers Ltd* [2003] EMLR 3946.

[543] *Douglas v Hello! Ltd* [2006] QB 125.

[544] Carnegie 'Privacy and the Press: The Impact of Incorporating the European Convention on Human Rights in the United Kingdom' (1998) 9 *Duke Journal of Comparative and International Law* 311 320.

restraining publication. The claimants, in support of or alternatively to their breach of confidence action argued the first and second claimants had a right to privacy under English law by virtue of the Human Rights Act and Article 8 of the ECHR, Lord Justice Sedley, as a point of departure, considered the question whether there is a right to privacy in English law in the context of the case, as it had been established that an intruder with whom no relationship of confidence existed took the photograph. Had a guest or an employee of a contractor taken the photographs, there would have been cause for a breach of confidence action. Lord Justice Sedley held that English law:

> "…has reached a point at which it can be said with confidence that the law recognizes and will appropriately protect a right of personal privacy. The reasons are two-fold: First, equity and the common law are today in a position to respond to an increasingly invasive social environment by affirming that everybody has a right to some private space. Secondly, the Human Rights Act requires the courts to give an appropriate effect to respect for private and family life set out in Article 8 of the European Convention on Human Rights and Fundamental Freedoms".[545]

3.4.3.5 The European Court's Interpretation of Article 8

The European Court seems to be taking the opposite direction in terms of its interpretation of Article 8. The Court prefers to interpret Article 8 as protecting the right to privacy. For instance in *Peck v United Kingdom*[546], Peck was captured on CCTV (Closed Circuit Television) walking through his local town centre, wielding a large knife in the process of committing suicide. The police were alerted to the situation because of the CCTV footage and recovered the knife from the applicant. The CCTV footage, owned by the local council, was released to the local press to demonstrate the effectiveness of CCTV in preventing crime and enabling the police to respond to situations. A photograph of Peck was used in the publicity material and at all times Peck's face was not masked. The footage was also given to the BBC and a commercial broadcast news agency who both took inadequate steps to mask Peck's identity. Peck made media appearances to speak out against the publication of the footage and photographs from the CCTV.

---

[545] *Douglas v Hello! Ltd* [2006] QB 125235 paragraph 111.

[546] *Peck v UK* (2003) Application No. 4464/98.

The court, referring to *PG and JH v United Kingdom*[547], noted that there are a number of elements [such as gender identification, name, sexual orientation and sexual life] important to a consideration of whether a person's private life is impacted on outside a person's home or private premises:

> "Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be significant …A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example a security guard viewing through closed circuit television) is of a similar character. Private life considerations may arise however once any systematic or permanent record comes into existence of such material from the public domain. The monitoring of the actions of an individual in a public space by use of photographic equipment, which does not record the visual data, does not, as such, give rise to an interference with the individual's private life. On the other hand, the recording of the data and systematic or permanent nature of the record may give rise to such considerations".[548]

The court further observed that Peck did not complain that the collection of data through the CCTV monitoring his movements and the creation of a permanent record amounted to an interference with his private life.[549] Rather, he argued that it was the disclosure of that record of his movements to the public in a manner in which he could not have foreseen that amounted to interference. The court concluded that disclosure of the relevant footage constituted a serious interference with the applicant's right to respect for his private life. The court based its conclusion on the following factors: Peck was walking in a public street and was not there to participate in a public event; it was late at night and Peck was distressed and perturbed; he was not charged with any offence; the footage of the aftermath of his suicide attempt was disclosed to the media and the applicant's identity is some instances was not

[547] *PG and JH v United Kingdom* (2001) Application No. 44787/98S57.

[548] *PG and JH v United Kingdom* (2001) Application No. 44787/98S57 (2001) paragraph 57.

[549] *Peck v UK* (2003) Application No. 4464/98 paragraph 60.

masked.[550] In determining whether the disclosure was "necessary in a democratic society", the court considered whether the reasons adduced to justify the disclosure were "relevant and sufficient" and whether the measures were proportionate to legitimate aims. The court found that Peck's voluntary media appearances did not diminish the seriousness of the interferences or reduce the correlative requirement of care concerning disclosures.[551]

3.4.4 Summary

Prior to the incorporation of the ECHR into English domestic law, there was no statutory or common law right of privacy. Moreover, English courts expressed both a reluctance to recognise a general right to privacy or under the umbrella of the tort of breach of confidence. After the incorporation of the ECHR, some English courts continued to rely on the tort of breach of confidence to protect privacy interests, but other courts emphasised the limitations in relying on breach of confidence. The latter courts further observed Article 8 of the ECHR as protecting a right to privacy. The European Court's interpretation of the Article 8 phrase of "private life" as including "privacy" has led some legal commentators to conclude there is a general right to privacy in English law.

3.5 CONCLUSION

This chapter sought to narrow the broad discussion in chapter 2 on the general development of the legal protection of privacy by concentrating on the development of the legal protection of privacy in selected countries, namely South Africa, England and the United States, because they protect the privacy of their citizens in distinct and varying ways. This already shows that privacy as a concept is elusive and that there is hardly agreement on exactly what it entails, nor the extent to which and how it should be protected.

In South Africa, privacy now is protected through a combination of explicit protection in the Constitution and the common law (applicable legislation will be discussed in the chapters to follow). The United States has found a way to protect zones of privacy through other rights in its constitution even though there is no explicit mention of the

[550] *Peck v UK* (2003) Application No. 4464/98 paragraph 62.

[551] *Peck v UK* (2003) Application No. 4464/98 paragraph 86-87.

right to privacy in its Constitution. In addition, common law protection exists for privacy infringements. The discussion also showed that England has no constitution and does not recognise that there is a right to privacy, yet it protects privacy through other common law principles and an international human rights instrument.

Looking ahead to the discussion to follow, perhaps the most important insight to be gathered, especially from the experience in South Africa (in the new constitutional dispensation) and the United States is what courts have said about the meaning of privacy. It seems as if the prevailing view is that, for purposes of legal protection, privacy cannot be accurately defined, but that it is a context –dependent right and that the phrase "right to privacy" is actually a misnomer. Rather, existence of the right is made subject to the expectation of privacy – subjectively held and objectively reasonable. This seems to imply that the existence of the right (and its infringement) already becomes dependant on a balancing of interests. But that is not all, the review of case law in this chapter shows that even if the right does exist, and even though it is infringed, a further balancing of rights takes place to enquire into the justification for that infringement (that is especially true in the constitutional context.) As such, the right to privacy becomes a rather tenuous right. Looking ahead to the further discussion in this dissertation, which aim to locate the right to privacy in the workplace and the policies and practices employers engage in, one can already submit that the right to privacy faces a battle for survival in that context. After all, employers, as the owners of the means of production and with a legitimate interest in directing their affairs will more often than not argue that their policies and practices do not infringe on privacy (as the right, being dependent on the reasonableness of the expectation, does not exist in the particular circumstances of the matter) or, to the extent that these policies and practices do infringe on privacy, that their conduct was justified in light of their legitimate concerns.

CHAPTER 4:
A WORKABLE DEFINITION OF PRIVACY

4.1 INTRODUCTION

Many people (as do courts and legislators) have an idea of what privacy is, but cannot adequately and satisfactorily define it. Chapter 2 gave an overview of the historical development of privacy protection whereas Chapter 3 presented a brief comparative overview of the development of privacy protection in South Africa, the United States and the United Kingdom, discussions which, to some extent, already illustrate this point. In view of these developments, this chapter critically assesses the possibility of a universal workable definition of privacy for purposes of the further discussion. In particular, the purpose of this chapter is to consider the concept and value of privacy, discuss the various conceptions of privacy advanced by proponents of privacy, outline the criticisms levelled against the notion of privacy and endeavour to identify a workable definition of privacy.

4.2 THE DIFFICULTIES IN DEFINING PRIVACY

The majority of commentators "proclaim privacy as a supremely important human good, as a value somehow at the core of what makes life worth living"[552]. As such, commentators generally think and talk about privacy as a useful concept. Although there is broad consensus on the distinctness and importance of privacy, there are those, such as the reductionists, who do not think and talk of privacy as a useful, coherent and distinct concept.[553] For proponents of privacy, privacy is useful because it "denote[s] something distinct and coherent". Privacy is further useful, distinct and coherent where there are losses of privacy, invasions of privacy and actionable violations of privacy.[554]

4.2.1 The Meaning of Privacy

There is not only broad consensus about the importance and distinctness of privacy, but also about the fact that privacy cannot be clearly and satisfactorily defined. In fact,

[552] Whitman "The Two Western Cultures of Privacy" (2004) 113 *Yale Law Journal* 1153.

[553] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 422.

[554] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 422 – 423.

it has been said that, "[t]he term "privacy" is notoriously difficult to define".[555] The view as to the difficulty of defining privacy is shared by both critics and proponents of privacy. Michael, for example, states that "of all human rights in the international catalogue, privacy is perhaps the most difficult to circumscribe and define".[556] Similarly, Parker observes that "[c]urrently there is no consensus in legal and philosophical literature on a definition of privacy".[557] Thomson writes that "[p]erhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea what [privacy] is".[558] Posner laments that "[m]uch ink has been spilled in trying to clarify the elusive and ill defined concept of privacy".[559] For Wacks, "an acceptable definition of privacy remains elusive" and the concept of privacy "has become too vague and the concept of privacy is "nebulous", thereby undermining the value of privacy and [impeding] its effective legal protection".[560] Laurie also finds "the concept of privacy… problematic" and goes on to state that "the problems it causes relates to its definition, its function, its nature, its usefulness, its value and its protection".[561]

Post mentions that "privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with the various distinct meanings, that I sometimes despair whether it can be usefully addressed at all".[562] Gutwirth argues that privacy is virtually impossible to define because "it has multiple meanings. It is not a tangible object that can easily be corralled into a confined definition".[563] Whitman attributes the complexity in defining privacy to the fact that it takes "disconcertingly diverse forms"[564] and "the sense of what must be kept "private", of what must be

[555] Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1 3.

[556]Michael *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) 1.

[557]Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275. See also Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* (1979) 1 2.

[558]Thompson "The Right to Privacy"(1975) 2 *Philosophy and Public Affairs* 95.

[559] Posner *An Economic Theory of Privacy* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 333.

[560]Wacks *Privacy: Volume I The Concept of Privacy* (1993) xii.

[561] For Laurie the scope of privacy is so wide ranging that is it is almost impossible to examine the concept in its entirety. Laurie *Genetic Privacy* (2002) 1.

[562]Post "Three Concepts of Privacy" (2001) 89 *Georgetown Law Review* 2087 2087.

[563]Gutwirth *Privacy and the Information Age* (2002) 29.

[564]Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151.

hidden before the eyes of others, seems to differ strangely from society to society".[565] Gutwirth adds that privacy "is not a natural element nor is it a part of reality. It is neither eternal nor universal and it has different consequences in different situations" and "[p]rivacy only exists in context, meaning privacy is a relative, contextual concept".[566]

Gross contends that it is not the function of the law to determine what privacy is. The function of the law, according to Gross, is to identify "situations of privacy that will be afforded legal protection or will be made private by virtue of legal protection", because "privacy…is a creature of life in a human community and not the contrivance of a legal system concerned with its protection"[567]. This, of course, begs the question, if it is not the function of the law to determine what privacy is, what or who determines what privacy is? In answering this question, the value of privacy becomes important. This value determines the meaning given to privacy in a particular context. At the same time, this means that the question of what privacy is, is devoid of any moral consideration, because privacy is not an "eternal" or "universal" concept and has "different consequences in different situations".

4.2.2 The Value of Privacy

In contrast to the approach mentioned above, Gavison is of the view that the value of privacy can only be determined after it has been established "what privacy is, and when and why losses of privacy are undesirable".[568] The value of privacy can be gleaned from an examination of its positive functions;[569] the values served by privacy;[570] and those aspects of human life that would be impossible or unlikely in the total absence of privacy.[571]

---

[565] Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151 1153.

[566] Gutwirth *Privacy and the Information Age* (2002) 29.

[567] Gross "The Concept of Privacy" (1977) 42 *New York University Law Review* 36. Whitman contends "[p]rivacy law is not the product of logic. But neither is it [the] product of "experience" or of supposed "felt necessities" that are shared in all modern societies." Whitman also observes privacy to be a "product of local anxieties and local ideals". Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151 1219.

[568] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 425.

[569] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 441.

[570] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 442.

[571] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 443.

Commentators on privacy have determined the value of privacy by identifying differing functions of privacy and values served by privacy. The functions and values of privacy identified further circumscribe the meaning of privacy. For example, Benn asserts that, in the absence of privacy the following ideals would be inconceivable: the ideal of personal relations;[572] the ideal of the politically free man[573] and the ideal of the morally autonomous man.[574] Privacy, for Benn, thus implies a general respect for persons.[575]

Privacy serves a number of values and in the absence of privacy these values would be non – existent. These values include happiness, justice, liberty, dignity and autonomy. McCloskey contends that privacy is grounded on values such as human happiness, justice and liberty.[576] The values served by privacy are inextricably linked to its functions.

One of the most important functions of privacy is the creation and maintenance of social and personal relations. Personal relations would be inconceivable in the absence of privacy, because personal relations are by their very nature private.[577]

In so much as privacy functions to create relations with others, it also functions to limit access to the individual in order to insulate the individual inhibitive effects of close proximity with others.[578] In this regard, Rachels argues that we need to regulate or vary our behaviour with different people according to the different types of human

[572] The ideal of personal relations relates to relations between persons we consider important and valuable i.e. personal relations. These include relations with friends, lovers and family members. Personal relations relationships according to Benn are by their very nature private and "could not exist if it were not possible to create excluding conditions." Benn *Privacy, Freedom and Respect for Persons* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 17.

[573] The ideal of the politically free man recognises the individual has to exist "in a minimally regulated society", subject to the power of others within reasonable and legally safeguarded limits. However, the ideal also recognises the individual possesses a breadth of choice in the way he lives despite social obligations. Benn *Privacy, Freedom and Respect for Persons* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 21.

[574] The ideal of the morally autonomous man, recognises the individual can be principled as such capable of carrying out morally responsible action. Benn *Privacy, Freedom and Respect for Persons* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 24.

[575] Benn *Privacy, Freedom and Respect for Persons* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 26.

[576] McCloskey "The Political Ideal of Privacy" (1971) 21 *Philosophical Quarterly* 303 311.

[577] Benn *Privacy, Freedom and Respect for Persons* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 17.

[578] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 446 - 447.

relationships we have with them.[579] This means we need to control who has access to us because "[i]f we cannot control who has access to us sometimes including and sometimes excluding various people, then we cannot control the patterns of behaviour we need to adopt or the kinds of relations with other people that we will have".[580]

In addition, privacy is credited with perfecting political understanding.[581] In a democracy, privacy encourages individuals to deliberate on and make political decisions. Moreover, a respect for privacy in a democracy attracts the participation of talented individuals in government.[582]

McCloskey is of the view that an invasion of privacy causes feelings of outrage, shame, hurt and humiliation. For this reason, privacy is viewed by some of its proponents as a mechanism for insulating the individual from such feelings.[583] Gavison also shares the view that privacy protects individuals from societal ridicule and censure.[584] Rachels argues that privacy protects a number of interests, including interests in keeping information on embarrassing or shameful aspects of life and behaviour from others.[585] Gross similarly sees privacy as protecting certain types of information, specifically information concerning our individuality (our identity, appearance, personality traits, character, talents, habits and weaknesses amongst others) and our lives (our past, present and future, our feelings, what we own and our desires or needs).[586] In this sense, by preventing unwanted shameful and embarrassing exposures concerning an individual privacy further enhances human dignity.[587]

Comment [OD1]: Mimmy – please check page numbers in this footnote – does not make sense – the first page of the article must be cheked and inserted

In considering "why privacy is commonly considered a right or a value to be protected by law," Negley suggests that "privacy is necessary to ensure that the

[579] Rachels "Why Privacy is Important" (1975) 6 *Philosophy and Public Affairs* 323 327 – 328.

[580] Rachels "Why Privacy is Important" (1975) 6 *Philosophy and Public Affairs* 323 331.

[581] Weinstein *The Uses of Privacy in the Good Life* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984)96.

[582] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 455 - 456

[583] McCloskey "The Political Ideal of Privacy" (1971) 21 *Philosophical Quarterly* 303 311.

[584] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421448.

[585] Rachels "Why Privacy is Important" (1975) 6 *Philosophy and Public Affairs* 323.

[586] Gross "The Concept of Privacy" (1977) 42 *New York University Law Review* 36 172-174.

[587] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 455.

individual has the possibility of moral choice and action".[588] Also, in this regard, privacy equips the individual with the ability to exercise moral judgment in an open, pluralistic and tolerant society.[589]

Privacy creates the personhood of persons and promotes individuality of persons. Reiman asserts that "privacy is necessary for the creation of "selves" out of human beings".[590] Reiman describes a "self" as partly "a human being who regards his existence – his thoughts, his body, his actions – as his own".[591] As such, privacy constitutes an essential ingredient in the creation of personhood in developing persons and further "confirms and demonstrates" the personhood of developed persons.[592] Privacy, understood in this sense, is "a condition of the original and continuing creation of "selves" or "persons"[593] and the right to privacy therefore "protects the individual's interest in becoming, being and remaining a person".[594]

4.3 PROPONENTS OF PRIVACY

Notwithstanding general agreement on the fact that privacy cannot be satisfactorily defined, several proponents of privacy[595] have made attempts to define or at least propose a conception of privacy. The various definitions or conceptions have focused on privacy as a psychological condition,[596] a form of control,[597] a claim,[598] and a

[588]Negley "Philosophical View on the Value of Privacy" (1966) 31 *Law and Contemporary Problems* 319.

[589] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 450.

[590] Reiman "Privacy, Intimacy and Personhood" (1976) 6 *Philosophy and Public Affairs* 26 40.

[591] Reiman "Privacy, Intimacy and Personhood" (1976) 6 *Philosophy and Public Affairs* 26 39.

[592]*Supra*.

[593] Reiman "Privacy, Intimacy and Personhood" (1976) 6 *Philosophy and Public Affairs* 26 40.

[594]*Supra*.

[595] "Proponents of privacy" are those writers who have found privacy to be a useful and coherent concept and have accordingly attempted to define it or offer an approach towards understanding it. It is important to note in this regard, that some writers do not find privacy to be a useful and coherent concept and for this reason have not defined or attempted to define the concept. See discussion on "Criticisms of Privacy".

[596] For Weinstein privacy is a psychological condition of being apart from others. Weinstein *The Uses of Privacy in the Good Life* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 94.

[597] Fried has defined privacy as "the control we have over information about ourselves". Fried *An Anatomy of Values: Problems of Personal and Social Choice* (1970) 141. Gross also defines privacy as "the condition under which there is control over acquaintance with one's personal affairs by the one enjoying it". Gross *Privacy and Autonomy*in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 169.

right[599].[600] Thus, although commentators agree that privacy is distinct and coherent, there is disagreement as to what makes privacy distinct and coherent.[601]

4.3.1 Theoretical Approaches to Privacy

Proponents of privacy have advanced different approaches or conceptions of privacy. Solove identifies six dominant approaches or conceptions of privacy postulated in legal and scholarly literature:

a) The right to be let alone;
b) Limited access to the self
c) Secrecy;
d) Control over information;
e) Personhood; and
f) Intimacy.[602]

Each one of these approaches to, or concepts of, privacy will be discussed below by focussing on the definition of privacy in terms of the different conceptions, what the value of privacy is in terms of each conception, as well as criticisms levelled at each.

4.3.1.1 Right to be Let Alone

The phrase the "right to be let alone" was coined by Judge Cooley in his 1880 Treatise on Torts.[603] Judge Cooley used the phrase to articulate that physical touching was a tort injury. The phrase was later adopted by Warren and Brandeis, when they authors defined privacy as the "right to be let alone" in their seminal article on privacy.[604]

---

[598] Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others". Westin *Privacy and Freedom* (1970) 7 - 8.

[599] Van Den Haag for example, views privacy as "the right not to let others participate in one's activities" or right to exclude others from participating in your life activities. Van Den Haag *On Privacy* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 149.

[600] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275 276.

[601] Schoeman *Privacy: Philosophical Dimensions of the Literature in Schoeman ed. Philosophical Dimensions of Privacy: An Anthology* (1984) 6.

[602]This discussion on the various conceptions of privacy relies heavily on Solove's article titled "Conceptualising Privacy" (2002) 90 *California Law Review* 1087. Solove deals with the different conceptions of privacy and identifies six primary conceptions of privacy.

[603] Godkin "The Rights of the Citizen: IV. To His Own Reputation" (1890) *Scribner's Magazine* 66.

[604] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1100 - 1101.

4.3.1.1.1 Meaning

Proponents of this conception of privacy define it as the "right to be alone". Privacy, understood in this sense, is a form of "immunity", "solitude", or "seclusion".[605]

4.3.1.1.2 Value

The conception locates the value of privacy in its ability to provide the individual with physical space away from others.

4.3.1.1.3 Criticism

Even though the conception of privacy as the "right to be let alone" has made a profound contribution to the development of privacy, it has been the subject of much criticism.

Solove argues that the conception "merely describes an attribute of privacy" and neglects to indicate how privacy should be valued or to identify instances where the individual should "be let alone".[606]

Thomson argues that the conception restricts violations of privacy to those violations which can be proved and not all violations of privacy can be proved. Thompson uses the following example to illustrate the shortcoming of this conception: Y uses an X - ray hearing device to hear everything X says via the walls of X's house. Y would admit to using the device to listen to X's conversation, but Y would deny her conduct violated X's privacy because she operated the hearing device at a distance and did not go anywhere near X (she let him alone and did not even touch him).[607]

The conception has also been criticised for being antiquated, "archaic" and "belonging to the period when physical space was very limited – when people lived in such crowded conditions that to get some privacy required withdrawal to an isolated spot [in the] countryside".[608] The phrase the "right to be let alone" was apt during a time in human history when individuals generally lacked physical space. This is no

[605] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review*1087 1102.
[606] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review*1087 1102.
[607]Thompson "The Right to Privacy" (1975) 4 *Philosophy and Public Affairs* 295.
[608] Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1 4.

longer the case in modern society because the "opportunities for physical privacy are so much greater" and "abundant".[609]

Parker observes that privacy in this sense may result in every loss of privacy qualifying as not being let alone. That is to say, there are numerous instances in which not being let alone will not necessarily result in a loss of privacy.[610]

4.3.1.1.4 Conclusion

The conception of privacy as the "right to be alone" has its roots in Warren and Brandeis's 1890 article on privacy. As fundamental as the conception may be, it has a number of shortcomings: first, it does not indicate how privacy should be valued; second, it obscures the fact that not every violation is a violation of privacy; third, it overlooks the fact that not being let alone does not always result in a loss of privacy; lastly, it is outdated in its sense of privacy as seclusion or solitude.[611]

4.3.1.2 Limited Access to the Self

The conception of privacy as the limited access to oneself is closely related to the "right to be let alone". The conception under discussion recognises the individual's desire for concealment and in being apart from others.[612]

4.3.1.2.1 Meaning

Proponents of this conception often describe privacy as a condition. Simmel, for example, defines privacy as a condition in which our interests are sovereign and we have ownership over all our initiatives.[613] Gross suggests privacy is "the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited".[614] Similarly, Weinstein writes of privacy as the "condition

---

[609] Posner "Privacy, Secrecy and Reputation" 1979 28 *Buffalo Law Review* 1 4.

[610] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275 276.

[611] Gavison also criticises the conception in so far as it is similar with the conception of privacy as non-interference by the state in personal decisions, for two reasons. First, the discussion of privacy as non-interference by the state in personal decisions obscures the fact privacy is a claim for legal protection against other individuals by the state. Second, the conception restricts privacy claims to interests concerning personal decisions. Gavison "Privacy and Limits of Law" (1980) 89 *Yale Law Journal* 421 438.

[612] Solove defines solitude as "a form of seclusion, of withdrawal from other individuals, of being alone". Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1102.

[613] Simmel *Privacy Is not an Isolated Freedom in Pennock and Chapman* (eds.) *Privacy: Nomos XIII* (1984) 72.

[614] Gross *Privacy and Autonomy in Pennock and Chapman* (eds.) *Privacy: Nomos XIII* (1984) 169.

of voluntary limitation of communication to or from certain others for the purpose of conducting an activity in pursuit of a perceived good" or simply a "condition of being apart from others".[615]

4.3.1.2.2 Value

Privacy, in terms of this conception, allows individuals to be apart from others by limiting access to themselves and information about themselves. In this regard, Weinstein finds privacy to be similar to "alienation, loneliness, ostracism, and isolation" in that they all represent conditions or states "of being apart from others."[616] Privacy is however different from the conditions of loneliness, shame, ostracism, alienation and unhappiness because, unlike such conditions, privacy is sought after and desirable: "alienation is suffered, loneliness is dreaded, and ostracism and isolation are borne with resignation or panic".[617]

Although Van Den Haag subscribes to the conception under discussion, Van den Haag prefers to see privacy as a right, namely, a "right not to let others participate in one's activities, be it only by watching or publicizing them".[618] Privacy thus enables an individual to exclude others from watching, using and invading his private realm and to control his or her living space, image, expression and communications.[619]

In attempting to show that privacy is a distinct and coherent concept, Gavison advances a limited access conception of privacy. In Gavison's view, privacy is "related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are subjects of others".[620] More importantly, Gavison rejects the idea of "privacy as a claim, a psychological state, or an area that should not be invaded" and

---

[615] Weinstein *The Uses of Privacy in the Good Life in Pennock and Chapman* (eds.) *Privacy: Nomos XIII* (1984) 94.

[616] Weinstein *The Uses of Privacy in the Good Life in Pennock and Chapman* (eds.) *Privacy: Nomos XIII* (1984) 88.

[617] *Supra*.

[618] Van Den Haag *On Privacy in Pennock and Chapman* (eds.) *Privacy: Nomos XIII* (1984)160.

[619] Van Den Haag *On Privacy*in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 149 - 150.

[620] Gavison "Privacy and Limits of Law" (1980) 89 *Yale Law Journal* 421 453.

of "privacy as a form of control". Gavison prefers instead to see privacy as a neutral concept comprised of secrecy, anonymity and solitude.[621]

4.3.1.2.3 Criticism

The main point of criticism against the conception of privacy as limited access to oneself is its failure to identify instances in which access to the self violates privacy, given that access to the self does not always result in a violation of privacy. That is to say, a violation of privacy occurs only when others have access to those aspects of an individual's life or affairs which are personal or private.[622]

4.3.1.2.4 Conclusion

Privacy in terms of the limited access conception is a condition which enables individuals to be apart from others by way of limiting access to themselves and information about themselves. The conception however fails to identify situations in which access to the self will result in a violation of privacy.

4.3.1.3 Secrecy

Some commentators conceive of privacy as a sense of secrecy, or the concealment of information. This conception of privacy has been identified as a subset of the limited access conception.[623] That being said, the conception of privacy as secrecy is narrower than the limited access conception, because it entails only an aspect of access to the self, namely, the concealment of personal facts.[624]

4.3.1.3.1 Meaning

Posner defines privacy as the withholding or concealment of particularly personal information[625]and his analysis of privacy identifies one of the interests privacy embraces as the concealment of information.[626] This interest of concealment of information is invaded "whenever private information is obtained against the wishes of the person to whom the information pertains".[627]

---

[621]*Supra*.

[622]Solove "Conceptualizing Privacy" (2002) 90 *California Law Review*10871104.

[623] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review*1087 1104.

[624] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review*1087 1104.

[625]Posner *The Economics of Justice* (1981) 231.

[626]Posner *The Economics of Justice* (1981) 272 – 273.

[627]Posner *The Economics of Justice* (1981) 273.

4.3.1.3.2 Value

The value of privacy according to this conception is that it enables individuals to keep certain information private. Friedrich, in focussing on the public or political implications of privacy, also links privacy to secrecy and defines privacy as "a special form of secrecy" prevalent in all social relations.[628] Friedrich further makes a distinction between functional and dysfunctional secrecy. Functional secrecy is seen as secrecy necessary in certain circumstances (for example with regard foreign and military diplomacy). Dysfunctional secrecy on the other hand, is usually not required as it concerns morally objectionable or dubious circumstances (for example in the case of fraud or corruption).[629]

4.3.1.3.3 Criticism

The conception of privacy as secrecy has been criticised for not taking cognisance of the fact "that individuals [may] want to keep things private from some people but not others".[630] In this sense the conception equates secrecy with total non - disclosure and overlooks that, as individuals, "ordinarily we deal with an interest in selective disclosure" and "not with an interest in non – disclosure".[631] Commentators such as Beardsley recognise this and conceive of privacy as tantamount to selective disclosure, which finds expression in the following statement: "[D]o not seek or disseminate information about X which X does not wish to have known or disseminated"[632].

Posner is further of the view that "when people decry lack of privacy, what they want [is] more power to conceal information about themselves that others might use to their disadvantage".[633] Posner reasons that people conceal personal facts about themselves in order to "mislead others"[634] and "to manipulate other people's opinion of them"[635]or

---

[628] *Friedrich Secrecy versus Privacy: The Democratic Dilemma* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 119.

[629] *Friedrich Secrecy versus Privacy: The Democratic Dilemma* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 106.

[630] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review*1087 1106 referring to observation made by legal scholar Kenneth L. Karst in "The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data" (1966) 31 *Law & Contemporary Problems*342 344.

[631] *Supra*.

[632] Beardsley "Privacy: Autonomy and Selective Disclosure" in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984)65-70.

[633] Posner *The Economics of Justice* (1981) 271.

[634] Posner *The Economics of Justice* (1981) 235.

to "manipulate the world around them by selective disclosure of [personal] facts about them".[636] In other words, for Posner, privacy is a tool individuals use to manipulate and defraud others.

This conception of privacy has been further criticised for equating privacy with secrecy. For Wagner DeCew "privacy and secrecy are not co extensional." Wagner DeCew provides two reasons as to why privacy is not tantamount to secrecy. First, secret information is not always private. For instance, secret treaties or military plans are kept from the public, but this does not make them private because authorised military personnel can view them. Secondly, not all private matters (such as one's debts or behaviour) are tantamount to secrets. Such information may be publicised for the public benefit. Solove agrees with Wagner DeCew in this regard and argues that the disclosure of secrets does not necessarily result in violations of privacy and some violations of privacy do not involve a disclosure of secrets.[637]

4.3.1.3.4 Conclusion

The conception of privacy as secrecy locates the value of privacy in the fact that it enables individuals to keep certain information private. The conception, however, equates secrecy with total non –disclosure, thus overlooking the fact "that individuals [may] want to keep things private from some people but not others".[638] The notion of privacy as a form of secrecy further (incorrectly) equates privacy with secrecy.

4.3.1.4 Control over Information about Oneself

The majority of commentators prefer to conceive of privacy as control over information about oneself. In so doing, proponents of this conception often refer to privacy as a claim, form of control or condition.

4.3.1.4.1 Meaning

Parent prefers to view privacy as a condition "of not having undocumented personal information about oneself possessed by others" and as such "a person's privacy is diminished exactly to the degree that others possess this kind of knowledge about

---

[635]Posner *The Economics of Justice* (1981) 233.

[636]Posner The *Economics of Justice* (1981) 234.

[637] Wagner DeCew *In Pursuit of Privacy: Law, Ethics, and Rise of Technology* (1997) 48.

[638]Beardsley "Privacy: Autonomy and Selective Disclosure" in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 65-70.

him". [639]Westin also subscribes to this conception and identifies privacy as a claim by "individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[640] Parker and Gross see privacy as a form of control. Parker sees privacy as "control over when and by whom parts of us can be seen or heard, touched, smelled or tasted by others"[641] whilst Gross sees privacy as "control over acquaintance with one's personal affairs".[642]

4.3.1.4.2 Value

The value of privacy in terms of this conception is the ability to keep information about ourselves from others.

4.3.1.4.3 Criticism

As already indicated, proponents of this conception often construe privacy a claim, a psychological state or form of control.[643] Gavison, in arguing that privacy is a distinct and coherent concept, advances a neutral conception of privacy, which rejects the construction of privacy as a claim, a psychological state, as a form of control or as an area that should not be invaded.[644]

Similar to Gavison, Parker is of the opinion that privacy cannot be defined as a psychological condition or state given that some losses of privacy have no effect on an individual's psychological state or consciousness.[645] This is especially the case where an individual's privacy is temporarily invaded without his knowledge.[646] Parker further finds that defining privacy as a form of power or control is problematic, because not every loss or gain of control over information about us is tantamount to a loss or gain of privacy.[647] Furthermore, some losses or gains of privacy are not related to information about ourselves.[648]

---

[639] Parent *Privacy, Morality and the Law* in Barendt (ed.) *Privacy* (2001) 297.
[640] Westin *Privacy and Freedom* (1967) 7 -8.
[641] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 238 275.
[642] Gross "The Concept of Privacy" (1977) 42 *New York University Law Review* 172-174.
[643] Gavison "Privacy and Limits of Law" (1980) 89 *Yale Law Journal* 421 453.
[644] Gavison "Privacy and Limits of Law" (1980) 89 *Yale Law Journal* 421 453.
[645] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275 278.
[646] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275 278.
[647] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275 279-280.
[648] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275 279-280.

Like the conception of privacy as a form of secrecy, the conception under discussion represents a (too) narrow subset of the limited access conception, in that it excludes non informational aspects of privacy such as the right to make decisions regarding one's body, health and sexual conduct.[649] The conception, at the same time, is overbroad in that it fails to adequately define the types of information individuals should have control over.[650] The conception also fails to define what is meant by "control" in relation to personal information. Nonetheless, theorists often construe "control" over personal information as "ownership" in such information. The assignment of ownership over personal information is an extension of personality.[651] For Solove, assigning ownership to personal information is problematic, because information (unlike physical property) can easily be transmitted and, once transmitted, such information can be possessed in the mind of many other persons. Moreover, ownership rights in personal information rarely rest in one person, particularly given the fact that such information is often created in relationships with others.[652]

4.3.1.4.4 Conclusion

This conception of privacy as control over personal information is perhaps too narrow in that it excludes non – informational aspects of privacy. It is further perhaps too broad in that it fails to sufficiently define the types of information individuals should have control over and what is meant by "control". The conception also assigns ownership over information. The assignment of ownership over information is problematic because of the nature of information. Information, unlike physical property, is easy to transmit, can be possessed by more than one person and its ownership often rests in more than one person.

4.3.1.5 Personhood

Professor Freund coined the term "personhood" on the basis of Warren and Brandeis's notion of the "inviolate personality". He further made the following observation regarding usage of the term "personhood" in privacy jurisprudence:

> "[personhood is] sometimes called privacy, inaptly it would seem…; autonomy perhaps, though that seems too dangerously broad. But the

[649] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1113 -1114.
[650] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1113 -1114.
[651] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1113 -1114.
[652] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1113 -1114.

> idea is that of personhood in the sense of those attributes of an in individual which are irreducible in his selfhood".[653]

In Rubenfeld's view, the essence of "personhood" encompasses those "acts, faculties or qualities so [necessary] to our identity as persons [and] human beings that they must remain inviolable, at least against the state."[654] Rubenfeld identifies two strands to "personhood": the first concerns our identity as persons and the second concerns our identity as individual's i.e. personal identity.[655] Privacy is often linked to the latter. Rubenfeld states that at the heart of the personhood and privacy relationship is the notion that the individual should be at liberty to "define himself" without state interference. Personhood further equates the right to privacy with the right to "self definition".[656] Rubenfeld further observes that the link between "personhood" and privacy has been forged to such an extent that personhood is seen as either the underlying principle of privacy or a synonym for the right to privacy.[657]

For Solove, the articulation of privacy as a form of protecting personhood stands apart from other conceptions of privacy "because it is constructed around a normative end of privacy, namely the protection of integrity of the personality".[658]

4.3.1.5.1 Meaning

This conception has been criticised for not adequately defining privacy. However, Rubenfeld has suggested that "the right to privacy is not the freedom to do certain, particular acts determined to be fundamental through some ever – progressing

[653] The observation on the usage of "personhood" was made by Professor Freund in 1975. Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law* 737 752. See also Solove "Conceptualizing Privacy" (2002) 90 *California Law Review*1087 1116.

[654]Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law* 737 753.

[655] The term "self – definition" is lent from Justice Blackmum's dissent in *Bowers v Hadwick* 478 US 186 (1986)205. Blackmum J stated the US Constitution protected the "decision whether to have a child because parenthood alters so dramatically an individual's self – definition." Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law* 737 753.

[656] The term "self – definition" is lent from Justice Blackmum's dissent in *Bowers v Hadwick* 478 US 186 (1986)205. Blackmum J stated the US Constitution protected the "decision whether to have a child because parenthood alters so dramatically an individual's self – definition." Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law* 737 753.

[657]Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law* 737 753.

[658] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1116.

normative lens…[i]t is [instead] the fundamental freedom not to have one's life too totally determined by a progressively more normalising state." [659]

4.3.1.5.2 Value

Bloustein believes, similar to Warren and Brandeis, that privacy tort cases involve a single tort and that the social value or interest at stake in privacy violations is "spiritual" in nature.[660] It is not a social value, nor does it concern interests in property or reputation. In Bloustein's view, the "spiritual" interest at stake in privacy violations includes individuality, "liberty as individuals to do as we will", personal dignity and integrity.[661] Bloustein further observes that a lack of privacy and continual public scrutiny deprives the individual of individuality and human dignity:

> "Such an individual merges with the masses. His opinions, being public tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique and personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual".[662]

Reiman argues that the right to privacy is "fundamentally connected to personhood"[663] and "protects the individual's interest in becoming, being and remaining a person".[664] Reiman describes privacy as:

> "…a very complicated… social ritual by means of which an individual's moral title to his existence is conferred…an essential part of the complex social practice by means of which [a] social group

[659]Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law* 737 784.

[660]Bloustein "Privacy as an Aspect of Human Dignity" in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 187 – 189.

[661] Bloustein *Privacy as an Aspect of Human Dignity* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 187 – 189.

[662]*Supra*.

[663] Reiman *Privacy, Intimacy and Personhood* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 314.

[664] Reiman *Privacy, Intimacy and Personhood* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 308.

> recognises – communicates to [an] individual – that his existence is his own…this a precondition of personhood." [665]

The complex social ritual of privacy serves two purposes for Reiman. First, it conveys to the individual that he has exclusive moral rights over his person. Second, it "confirms" and "demonstrates" respect for other persons.[666] For this reason, for an individual to qualify as a person according to Reiman, the individual has to recognise his capacity to control his destiny and further recognise that he possesses a moral right to control his destiny.[667]

Benn suggests that the principle of privacy is grounded upon the principle of respect for persons. Like Reiman, Benn is of the opinion that for an individual to qualify as a person, that individual must *inter alia* possess the capacity to shape his destiny. Benn explains a person to be "a subject with a consciousness of himself as [an] agent capable of having projects, and assessing his achievements in relation to [his projects]."[668] Respecting an individual as a person entails recognising that individual as "a chooser, as one attempting to steer his own course through the world, adjusting his behaviour as his perception of the world changes, correcting course as he perceives his errors". Respecting a person means recognising that every human being "is entitled to minimal degree of consideration" for his choices and courses he chooses to travel through the world.[669]

4.3.1.5.3 Criticism

The personhood conception of privacy, in particular those United States privacy cases "espousing a personhood theory of privacy",[670] have been criticised for focussing on

---

[665] Reiman *Privacy, Intimacy and Personhood* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 308.

[666] Reiman *Privacy, Intimacy and Personhood* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 310.

[667] Reiman *Privacy, Intimacy and Personhood* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 310.

[668] Benn *Privacy, Freedom and Respect for Persons* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 228.

[669] Benn *Privacy, Freedom and Respect for Persons* in Pennock and Chapman (eds.) *Privacy: Nomos XIII* (1984) 229.

[670] A number of US privacy cases have accepted that certain decisions relating to marriage, family relationships, child rearing, reproduction and contraception are fundamental to the idea of self-definition. See for example *Eisenstadt v Bard* 405 US 438 (1972), *Roe v Wade* 410 US 113 (1973), *Whalen v Roe* 429 US 589 (1977) and *Griswold v Connecticut* 381 US 479 (1965). Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1099, 1116.

liberty and autonomy instead of privacy. The conception has also been critiqued for allowing "personhood" and privacy to remain "ill – defined".[671] Rubenfeld criticises the personhood conception for not defining the concept of personal identity and those "acts, faculties or qualities so [necessary] to our identity as persons [and] human beings that they must remain inviolable, at least against the state".[672] As such, most actions taken by individuals could be said to involve an element of self - definition. Although Rubenfeld aptly pinpoints the primary flaw with the personhood conception, Rubenfeld fails to remedy this flaw by advancing a definition of personal identity. Rubenfeld merely offers an alternative definition of privacy as "the fundamental freedom not to have one's life too totally determined by a progressively more normalising state". [673]

Posner is also critical of the conception of privacy as a sense of personhood or individuality, particularly for suggesting that the absence of privacy negates any expression of individuality.[674] Posner argues that history teaches us that even in those societies in which privacy was perceived negatively or in a restricted way, such as ancient Greek and Roman society, individuals were able to express their individuality and creativity. [675]

4.3.1.5.4 Conclusion

The conception of privacy as personhood views privacy as protecting an individual's personhood and identity. The conception has been criticised for equating privacy in this sense with liberty and autonomy. A further criticism relates to the suggestion that the absence of privacy negates expression of individuality. Furthermore, this approach has also not adequately defined privacy, personhood and the concept of personal identity, as well as those inviolable aspects of an individual's identity.

4.3.1.6 Intimacy

The conception of privacy as a form of intimacy places the value of privacy primarily in the creation and maintenance of personal relationships.[676] Murphy asserts in his

[671] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1120.
[672] Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law Review* 737 784.
[673] Rubenfeld "The Right to Privacy" (1989) 102 *Harvard Law Review* 737 784.
[674] Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 393 407.
[675] *Supra*.
[676] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1121.

essay on "Social Distance and the Veil" that through "aloofness, removal and reserve" individuals are able to establish social relationships and maintain social interaction with others.[677] For Murphy, privacy is realised through expressions or displays of distance in social relationships. Intimate relationships, according to Murphy, are demanding of expressions of distance because such relationships are the "most affect laden and central to the life of the individual, most difficult to maintain, and most ambivalent."[678] Gerstein writes that "privacy and intimacy seem to go together" and argues "intimate relationships could not exist if we did not continue to insist on privacy for them".[679]

4.3.1.6.1 Meaning

Gerety defines privacy as "an autonomy or control over the intimacies of personal identity" and argues "intimacy [is] necessary for the proper invocation of the concept of privacy".[680] Gerety furnishes a number of definitions for intimacy. Intimacy, according to Gerety, is "the chief restricting concept in the definition of privacy"[681] and "always the consciousness of the mind in its access to its own and other bodies and minds, insofar, at least, as these are generally and specifically secluded from access of the uninvited".[682] Intimacy is further "a kind of knowledge…personal, immediate, and consented to…and…private".[683]

4.3.1.6.2 Value

Rachels[684] also gives an account of the value of privacy that is centred on the creation and maintenance of interpersonal relationships. According to Rachels, privacy is important to us because it protects a number of interests, including interests in gaining advantage in competitive situations and keeping embarrassing aspects of our life or

---

[677] Murphy *Social Distance and The Veil* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984)34.

[678] Murphy *Social Distance and The Veil* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984)37.

[679] Gerstein *Intimacy and Privacy*in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 265.

[680] Gerety "Redefining Privacy" (1977) 12 *Harvard Civil Right Civil Liberties Law Review* 233 236.

[681] Gerety "Redefining Privacy" (1977) 12 *Harvard Civil Right Civil Liberties Law Review* 233 263.

[682] *Supra*.

[683] Gerety "Redefining Privacy" (1977) 12 *Harvard Civil Right Civil Liberties Law Review* 233 268.

[684] Rachels *Why Privacy is Important* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 291.

behaviour private.[685] For this reason, Rachels argues "a close connection [exists] between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people" and, as such, "privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have".[686]

Fried also explores the meaning and significance of privacy in its relation to love, friendship and trust.[687] Fried is of the view that privacy is implicated in notions of respect, self – respect, love, friendship, affection and trust.[688] For Fried, the existence of privacy is crucial to these notions and these notions are inconceivable without privacy. Fried notes in this regard:

> "To respect, love, trust, feel affection for others and regard ourselves as objects of love, trust and affection is at the heart of our notion of ourselves as persons among persons, and privacy is a necessary atmosphere for these attitudes and actions, as oxygen is for combustion".[689]

4.3.1.6.3 Criticism

Solove criticises Gerety's attempt to place conceptual limits on privacy with broad terms, namely, "identity" and "autonomy".[690] This, according to Solove, results in the word "intimacy" being a substitute for the word "privacy". Solove further criticises the formulation of privacy as intimacy for being too narrow, in that it focuses exclusively on intimate human relationships and the feelings produced by such relationships, to the exclusion of other ends facilitated by privacy outside of interpersonal relationships.[691]

---

[685] *Supra*.

[686] Rachels *Why Privacy is Important* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 292.

[687] Fried *Privacy: A Moral Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 209 – 210.

[688] Fried *Privacy: A Moral Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 209.

[689] Fried *Privacy: A Moral Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 205.

[690] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1123.

[691] *Supra*.

Reiman criticises the suggestion by Fried and Rachels that intimate information is information we want to keep others from accessing, because such a suggestion assumes intimacy makes the revelation of personal information significant, whereas the context of caring is what really makes the sharing or revelation of such information significant. This context of caring is located in the "reciprocal desire [relating to] present and future and intense and important experiences… [t]he more one knows about the other, the more one is able to understand how the other experiences things, what they mean to him, how they feel to him. In other words the more each knows about the other, the more they are able to really share an intense experience instead of merely having an intense experience alongside each other."[692]

4.3.1.6.4 Conclusion

The conception of privacy as intimacy tends to be too broad, particularly where the scope of "intimacy" is inadequately defined. The conception is also narrow in its focus on intimate human relationships and the feelings produced by human relationships.[693]

4.4 A PRAGMATIC APPROACH TO PRIVACY

Even though there clearly exists disagreement as to what makes privacy distinct and coherent, there exists broad consensus on the core realities of privacy namely that privacy is "dynamic", "fluid", "contextual" and "evolving". A number of commentators have raised practicable approaches to privacy in their attempt to define privacy.[694] These approaches accept the dynamic and evolving nature of privacy and offer an understanding of privacy, which embraces the nature and core realities of privacy.

Craig proposes a functional approach which "recognises that the role of the right to privacy is to protect certain aspects of life from public scrutiny".[695] For Craig efforts by commentators to provide "greater specificity to the concept of privacy" and to

[692] Reiman *Privacy, Intimacy and Personhood* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 305 – 306.

[693] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1124.

[694] See for instance Craig *Privacy and Employment Law* (1999) 13, Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 and Gutwirth *Privacy and the Information Age* (2002) 29.

[695] Craig *Privacy and Employment Law* (1999) 13.

devise a "perfect privacy definition" have proved futile.[696] For this reason, Craig argues that the focus should be on developing a workable legal definition of privacy as opposed to an ideal legal definition of privacy.[697]

A workable definition of privacy, according to Craig, has to take into account the following: firstly, the yardstick for determining the sufficiency of any conception of privacy should be legal certainty rather than legal perfection; secondly, privacy is a dynamic and evolving concept and as such it occurs in varied contexts, can be compromised in diverse circumstances and its interests can evolve; thirdly, the quest to define privacy should not overshadow the legal protection of privacy.[698]

Gutwirth's approach recognises an important aspect of privacy, namely, that privacy is context specific. Gutwirth's approach begins with the basic premise that privacy has a plethora of meanings and it cannot "be corralled into a confined definition".[699] Gutwirth further asserts that privacy cannot be conjured up by listing a series of human activities -"[i]t is not a natural element, nor is it a part of reality. It is neither eternal nor universal and it has different consequences in different situations".[700]

Solove recommends a pragmatic approach to "understanding privacy rather than a definition or formula for privacy".[701] Solove advances pragmatism as an approach to understanding privacy because it avoids conceptualising[702] privacy through "necessary and sufficient conditions" and "rigid conceptual boundaries and common denominators". The pragmatic approach, instead, "emphasises the contextual and dynamic nature of privacy".[703]

---

[696] Craig *Privacy and Employment Law* (1999) 11 – 12.

[697] Craig *Privacy and Employment Law* (1999) 13.

[698] Craig *Privacy and Employment Law* (1999) 14.

[699] Gutwirth *Privacy and the Information Age* (2002) 29.

[700] Gutwirth *Privacy and the Information Age* (2002) 29.

[701] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1129.

[702] Solove defines conceptualising privacy as "an attempt to articulate what separates privacy from other things, what makes it unique and what identifies it in various manifestations". Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1095.

[703] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1091.

In terms of the pragmatic approach, privacy is an aspect of practices such as customs, norms and traditions and activities such as letter writing, engaging in sexual activity and conversing with a therapist. Solove adds:

> "[u]nderstanding privacy requires us to look to specific ways in which privacy manifests itself within [such] practices and the degree to which privacy is linked to the purposes of [such practices]. When we state that we are protecting "privacy", we are claiming to guard against disruptions to certain practices. Privacy invasions disrupt and sometimes annihilate certain practices. Practices can be disrupted in certain ways, such as interference with peace of mind and tranquillity, invasion of solitude, breach of confidentiality, loss of control over facts about oneself, searches of one's property, threats to or violations of personal security, destruction of reputation, surveillance."[704]

Privacy in this sense is "the practices we want to protect and the protections against disruptions to these practices."[705] These social practices cannot for Solove be reduced into the public or private sphere because the practices we consider private have evolved over time and the divide between public and private practices is often blurred or nebulous. Solove states "[t]o say things are private is imprecise because what it means for them to be private is different today than what it was in the past."[706]That is to say, Solove's pragmatic approach recognises that "what was privacy yesterday is not necessarily privacy tomorrow" and places emphasis on the contextual and dynamic nature of privacy.

Privacy is unquestionably a fluid and dynamic concept that is impossible to place in a mould to be used in the same manner over and over again. Any workable definition of privacy in this age of large scale and complex technological developments has to embrace this particular attribute of privacy.

---

[704] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1091.

[705] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1093.

[706] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1132.

4.5 THE APPROACH TO PRIVACY IN SELECTED COUNTRIES

4.5.1 Introduction

This section will consider the approaches taken by the countries under review to the notion of privacy.

4.5.2 South Africa

The South African common law recognises the right to privacy as an independent personality right. Further, a person's privacy is breached when there has been an unlawful intrusion on his or her personal privacy or an unlawful disclosure of private facts concerning such a person. The Constitutional court in *Bernstein v Bester*[707] identified a number of instances which amount to a breach of privacy in terms of the common law: entry into private residence, the reading of private documents, the disclosure of private facts acquired through an unlawful intrusion and the disclosure of private facts in breach of confidentiality. For this reason, the common law seems to subscribe primarily to the limited access to the self and control over information conceptions of privacy.

This is also true of the general right to privacy provided for in the Constitution, which primarily conceives of privacy as the limited access to the self and the control over information about oneself. The right protects the privacy of an individual's person or home, their property, possessions and communications. The Constitutional Court has, however, extended the scope of the constitutional privacy provision to protect personhood and intimacy.

In *Bernstein v Bester* the court viewed privacy as protecting personhood when it observed that privacy can be reasonably expected in the "truly personal realm" and in the "inner sanctum".[708] This inner sanctum includes family life, sexual preferences and the home environment. The court further observed that the scope of privacy is in close relation with the concept of identity and that privacy is based on the "notion of

[707] *Bernstein v Bester NO* 1996 (2) SA 751 (CC).

[708] *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 784 E - F.

what is necessary to have one's autonomous identity" and not on the "notion of the unencumbered self".[709]

In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors*[710] the Constitutional Court described privacy as the right to be let alone when it pointed out individuals did not lose their right to privacy once they ventured outside the "truly personal realm" and "inner sanctum". The Court in this regard stated that "when people are in their offices, in their cars or on mobile telephones, they retain the right to be left alone by the state". [711]

In *National Coalition for Gay and Lesbian Equality v Minister of Justice*[712] adopted a personhood conception of privacy when it stated that privacy "recognises that we all have a right to a sphere of private intimacy and autonomy". The court further advanced a conception of privacy as a form of intimacy. The court in this regard stated privacy:

> "allows us to establish and nurture human relations without interference from the outside community. The way in which we give expression to our sexuality is at the core of this area of private intimacy."[713]

In this case, and in a separate concurring judgment, Sachs J observed that "privacy protects people not places" and further described privacy as the right to be left alone, which went beyond being "a negative right to occupy a space free from government intrusion" but also protected personhood. Privacy protected personhood in providing for "a right to get on with your life, express your personality and make fundamental decisions about your intimate relationships without penalisation."[714]

---

[709] *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 783 F - G.

[710] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2000 (10) BCLR 1079 (CC).

[711] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2000 (10) BCLR 1079 (CC) 1087 C - D.

[712] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6.

[713] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 30 B.

[714] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 60 D – E.

Although *S v Jordan*[715] also concerned the intimate activity of sex, the Constitutional Court refused to afford the concerned intimate activity the privacy protection it previously afforded to other forms of intimacy. The Court's refusal was based on the fact that the sexual expression involved was not "nurturing relationships or taking life affirming decisions about birth, marriage or family" but was instead done for commercial gain. The Court held in this regard:

> "[b]y making the sexual services available for hire to strangers in the marketplace, the sex worker empties the sex act of much of its private and intimate character. She is not nurturing relationships or taking life – affirming decisions about birth, marriage or family; she is making money." [716]

4.5.3 United States

In evaluating the approach in the United States to privacy protection, it should be said that privacy protection occurs both at the common law and constitutional level. Privacy under the common law has been described as "the right to be let alone". Warren and Brandeis emphasised the legal recognition of "a privacy right that gives an individual the power to control absolutely the limits of publicity about him or herself" or the protection of an inviolate personality.[717] In 1960, Prosser's description of the law of privacy into four distinction kinds of tort invasion also referred to the need to control access and information about oneself.[718]

The Fourth Amendment has also been invoked in protecting privacy interests, particularly in unreasonable seizures.[719] The Supreme Court in *Katz v United States*[720] clarified that the Fourth Amendment protected people and not places. Therefore, the

---

[715] *S v Jordan* 2002 (6) SA 642.

[716] *S v Jordan* 2002 (6) SA 642 654 I – 655

[717] Warren and Brandeis "The Right to Privacy" (1890) *Harvard Law Review* 193 196.

[718] Prosser "Privacy" (1960) 48 *California Law Review* 383.

[719] See for example in the decisions of *Ex Parte Jackson* 96 U.S. 727 (1877) and *Boyd v United Sates* 116 U.S. 616 (1886). In the former, the Supreme Court held that a sealed letter sent through the mail is subject to Fourth Amendment warrant protections. In the latter, the same court held that a person's private correspondence is protected from seizure by Fourth and Fifth Amendment provisions. Wagner DeCew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 18 -19.

[720] *Katz v United States* 389 U.S. 347 (1967).

early recognition and protection of privacy concerned the protection of personal information and linked privacy to the concepts of liberty and personhood.[721]

Whitman asserts that "suspicion of the state" is the cornerstone of United States privacy jurisprudence and, as such, the United States privacy conception has been moulded around the idea that the "state is the prime enemy". Whitman observes:

> "American "privacy" law, however ingenious its elaborations, always tends to imagine the home as the primary defence, and the state as the primary enemy…[w]here American law perceives a threat to privacy, it is typically precisely because the state has become involved in the transaction".[722]

For this reason, the United States privacy protection tradition according to Whitman espouses the core value of liberty, particularly liberty against the state or freedom from state intrusions. Furthermore, United States privacy anxieties are focussed on "maintaining a kind of private sovereignty within the walls of our homes".[723]

In 1886 the decision of *Boyd v United States* deduced a right to privacy from the Fourth Amendment:

> "[a]t its origin, the right to privacy is the right against unlawful searches and seizures. It is thus a right that inheres in us as free and sovereign political actors, masters in our own houses, which the state is ordinarily forbidden to invade." [724]

The Court in *Boyd* further cited with approval Lord Camden's proclamation on the "sanctity of the home" in *Entick v Carrington* and in so doing advanced an understanding of "privacy" rights as generalisations of the principle of the "sanctity of

---

[721] Wagner DeCew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 16 – 17.

[722] Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151 1215.

[723] Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151 1161. By contrast, continental Europe privacy protection generally espouses the core value of a right to one's image, name, reputation and self – determination. In other words continental Europe protects individual privacy serves to: shield an individual from unwanted public exposure, spare embarrassment or suffering any indignity or humiliation. Moreover, unlike in the US where anxieties are focuses against state intrusions or interferences, continental Europe privacy anxieties are focussed towards the media. Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151 1162.

[724] *Boyd v United States* 116 U.S. 616 (1886) 616.

the home".[725] Three years later, in *Union Pacific Railway Co. v Botsford*,[726]the Court extended the sanctity of the home to the individual right "to the possession and control of his own person free from all restraint or interference of others unless by clear and unquestionable authority of law".[727]

The understanding of privacy as protecting the "sanctity of the home" was later extended to privacy decisions involving "attributes of personhood" namely marriage, procreation, contraception and child rearing. The Supreme Court espoused in such decisions a conception of privacy as personhood. For example, Douglas J stated in *Griswold v Connecticut* [728]that the constitutional right to privacy protected "zones" of privacy and, protected in these zones of privacy, was the intimacy shared between individuals in certain relationships such as between man and wife and doctor and patient. Subsequently, in *Einsenstadt v Baird*,[729] Brennan J wrote that the right to privacy is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision of whether or not to have a child. Later, in *Lawrence v Texas*,[730] Kennedy J, in protecting homosexual relations between adults, stated that the right to liberty under the Due Process Clause prevented government intrusion in this personal realm of the individuals concerned.

The conception of personhood was articulated in *Planned Parenthood v Casey*[731]. In *Casey* the Supreme Court stated that the constitutional right to privacy encompassed:

> "matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the

[725]*Boyd v United States* 116 U.S. 616 (1886) 616.
[726]*Union Pacific Railway Co. v Botsford* 141 US (1891) 250.
[727] Solove "Conceptualizing Privacy" (2002) 90*California Law Review*1087 1117.
[728]*Griswold v Connecticut* 381 U.S. 477 (1965).
[729]*Einsenstadt v Baird* 405 U.S. 438 (1972).
[730]*Lawrence v Texas* 539 U.S. 558 (2003).
[731]*Planned Parenthood v Casey* 505 US 833 (1992).

attributes of personhood were they formed under compulsion of the State".[732]

The constitutional right to privacy in United States law protects the individual's interest in independently making certain types of decisions, whereas the common law right to privacy protects the individual's interest in avoiding the disclosure of personal information.[733]

4.5.4 United Kingdom

There is no right to privacy in English law. However, Article 8 of the ECHR provides for an individual's right to respect for his private and family life, his home and correspondence. The European Court has held in *Niemetz v Germany*[734] that the meaning of "private life" in Article 8 went beyond the Anglo-American idea of privacy with its emphasis on secrecy of personal information and seclusion to include: the physical and moral integrity of a person, including his or sexual life; the capacity of the individual to formulate a perception of himself or herself and to choose his or her personal identity; the protection of personal information; personal relationships with others including social and sexual activities with others; and an individual's personal or private space or any place or space in which the individual has exclusive rights of enjoyment, such as the home.

4.6 CRITICS OF PRIVACY

Although there is broad consensus about the importance and distinctness of privacy, some commentators[735] suggest that privacy rhetoric is misleading because the violation of privacy actually involves the violation of some other interest. These commentators further assert that for a true understanding of privacy, the rhetoric surrounding it has to be ignored and the focus should be on the particular interest in

[732] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1117. Critics of the personhood theory of privacy have argued that if privacy is construed as protecting the liberty or personhood of an individual against the state or anyone else, then privacy cases do not necessarily concern privacy but liberty and autonomy. Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1118.

[733] Wagner DeCew *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997) 25.

[734] *Niemetz v Germany* [1992] EHRR 97.

[735] See for instance Gavison 'Privacy and Limits of Law' (1980) 89 *Yale Law Journal* 421, Botswick "A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision" (1976) 64 *California Law Review* 1447 and Prosser *Privacy: A Legal Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 104.

question. [736] They conclude that there is nothing distinctive and integrated about privacy cases, as these cases concern "diverse and disparate" issues. Other commentators argue that there is nothing morally distinctive about privacy claims, because the moral justification of privacy claims cannot be defended by principles distinctive to privacy.[737] Commentators denying the coherence and distinctiveness of privacy are referred to as reductionists because they reduce privacy to some other right or interest.[738]

One of the earliest reductionist positions on privacy was advanced by Prosser.[739] Prosser stated in his analysis of the privacy tort that Warren and Brandeis not only had erred in observing that the law of privacy involved a single tort, but also in identifying the interest at stake in violations of privacy as the "inviolate personality".[740] Prosser, after examining more than three hundred cases, concluded that the law of privacy comprises "four distinct kinds of torts"[741] and "four different interests"[742]. [743] Prosser concluded that privacy is not a single coherent and distinct value, but a complex of different interests - mental, reputation and proprietary interests.[744]

Botswick, in cataloguing privacy cases in different classes, also reduces privacy to other rights.[745] Botswick reduces privacy into three separate and distinct rights, namely repose, sanctuary and intimate decision. Botswick, like Prosser, is of the view

---

[736] Gavison 'Privacy and Limits of Law' (1980) 89 *Yale Law Journal* 421 421 – 422.

[737] Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 5.

[738] *Supra*.

[739] Prosser *Privacy: A Legal Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 104 - 107.

[740] *Supra*.

[741] The law of privacy for Prosser is comprised of the following four torts: first, intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; second, public disclosure of embarrassing private facts about the plaintiff; third, publicity which places the plaintiff in a false light in the public eye; and fourth, appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

[742] The interests at stake in the violations of privacy according to Prosser are: reputation (in respect of the public disclosure and false light torts), emotional tranquillity (in respect of the intrusion upon seclusion or solitude tort) and proprietary gain (in respect of the name and likeness tort).

[743] Prosser *Privacy: A Legal Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 104 - 107.

[744] *Supra*.

[745] Botswick "A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision" (1976) 64 *California Law Review* 1447 1448.

that the rubric of "privacy issues" does not sufficiently recognise and protect the different interests at stake in privacy concerns.[746]

Thompson suggests that privacy interests are reducible into other rights such as property rights and personal rights and argues against the coherence and distinctiveness of privacy.[747] Thompson writes "…the right to privacy is itself a cluster of rights and [is not] a distinct cluster of rights [but] intersects with the cluster of [personal rights and property rights]." Thompson concludes that privacy is a "derivative" right that can be justified without "ever once mentioning the right to privacy".[748]

Schoeman contends that the right to privacy breeds "deceit and hypocrisy" in that it conceals wrongdoings by individuals and prevents wrongdoers from being held morally responsible for their wrongdoings.[749] Schoeman further contends that privacy impedes necessary moral debate on different practices.[750] For this reason, certain practices are deemed to be legal simply because they have been left "unexamined" and "unexposed" when in fact they are illegal.[751] More so, privacy enables individuals to conceal their true position. In this regard Schoeman concludes that:

> "[p]rivacy may be seen as a culturally conditioned sensitivity that makes people more vulnerable than they would otherwise be to selective disclosures and the sense of comparative inferiority and abject shame – a sense engendered by ignorance about the inner lives of others".[752]

Reductionists primarily criticise the distinctiveness and coherence of privacy. Moral idealists and realists, on the other hand, criticise the moral effects of privacy on the

---

[746] Botswick "A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision" (1976) 64 *California Law Review* 1447 1448.

[747] Thompson "The Right to Privacy" (1975) 4 *Philosophy and Public Affairs* 295 306.

[748] Thompson "The Right to Privacy" (1975) 4 *Philosophy and Public Affairs* 295 313.

[749] Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 1.

[750] Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 1.

[751] Prosser *Privacy: A Legal Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 1.

[752] Prosser *Privacy: A Legal Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 1.

individual and society.[753] Moral idealists and realists associate privacy with negative attributes such as "hysteric neurosis", "anonymity", "unbridled individualism", or "alienation" and "loneliness".[754] They also view privacy as breeding violence, fear and shame. They further view privacy as depressing social relations and erecting artificial boundaries between individuals.[755]

Moral idealists and realists further contend that the seeds of privacy were sown by bourgeois efforts to alienate themselves from the rest of society. Consequently, privacy is a product of ethnic and social class distinction.[756] The proposition that privacy is borne of ethnic and class distinction finds support amongst those writers who suggest that Warren and Brandeis - particularly Warren who is said to have been a member of the Boston blue blood in the 1890's - were in fact expressing their frustrations at interest in their private affairs which they preferred not to be pursued by the public when they wrote their seminal article on privacy. That is to say, the authors intended to vent their frustrations at the prying eyes and ears of the "yellow press" and did not intend to contribute towards the development of privacy in United States common law.[757]

Moral realists assert that privacy furnishes individuals with an excuse not to fulfil their social obligations and to not involve themselves with other people. Moral idealists construe privacy as a paradigm shift from the human essence of "personal

---

[753] Weinstein *The Uses of Privacy in the Good Life* in Pennock and Chapman (eds) *Privacy: Nomos XIII* (1984) 88.

[754] Weinstein *The Uses of Privacy in the Good Life* in Pennock and Chapman (eds) *Privacy: Nomos XIII* (1984) 88.

[755] *Supra*.

[756] Weinstein *The Uses of Privacy in the Good Life* in Pennock and Chapman (eds) *Privacy: Nomos XIII* (1984) 88.

[757] Whitman writes that because Warren and Brandeis worked and lived amongst Boston's high society, the "high – status tenor" of their article is apparent to its readers considering the article was written "in a fit of outrage over newspaper reports of a party given by the Warrens and its main target was the gossip pages of the "yellow press". Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151 1204. Benzanson in drawing our attention to the fact that the object of privacy has altered since Warren and Brandeis penned their seminal article in 1890 also observes the Warren and Brandeis conception was class based in character. By contrast, contemporary notions of privacy according to Benzanson are democratic in character. The Warren and Brandeis idea of privacy was further a manifestation of social tensions between established institutions (such as family and local community) and an impersonal social culture undergoing inter alia industrialisation and growth of the mass media. For Benzanson privacy in the 1890's represented "generalised social controls on information whereas privacy today entails the individual's control of information in a "more complex milieu of personal and social relationships. Benzanson "The Right to Privacy Revisited: Privacy, News and Social Change 1890-1990" (1992) 80 *California Law Review* 1133.

wholeness" or "social communion" to feelings of loneliness, shame, alienation and unhappiness.[758]

Posner suggests an economic approach to privacy, and as such defines privacy as the "concealment of information".[759] Posner's economic approach views privacy and prying or curiosity as intermediate economic goods which people use "as inputs into the production of income or some other broad measure of utility of welfare". Prying or curiosity provides individuals with valuable and accurate pictures of friends or colleagues for subsequent use in social and professional dealings,[760] whilst privacy enables individuals to "manipulate by misrepresentation other people's opinion of them" or to "control others' perceptions and beliefs" regarding them.[761] As such, for Posner, privacy enables individuals to manipulate private information and defraud others with this private information.[762]

Etzioni observes "[a]lthough we cherish privacy in a free society, we also value other goods. Hence, we must address the moral, legal, and social issues that arise when serving the common good entails violating privacy".[763] Etzioni is therefore of the view that we are "justified in implementing measures that diminish privacy" particularly for the realisation of the common good. Etzioni further asserts that the "best way to curtail the need for government control and intrusion is to have somewhat less privacy" in order to serve the common good.[764]

4.7 CONCLUSION

The literature on the privacy as a concept indicates that there two schools of thought with respect to the value or usefulness of privacy. There are proponents of privacy who proclaim privacy as a useful value that is distinct and coherent. On the other hand, the reductionists, who assert that privacy is incoherent and further, contend that there is nothing morally distinctive about privacy claims, because privacy can be

[758] Weinstein *The Uses of Privacy in the Good Life* in Pennock and Chapman (eds) *Privacy: Nomos XIII* (1984) 92.

[759] Posner "The Economics of Privacy" (1981) 71 *American Economic Review* 405.

[760] Posner "The Right of Privacy" (1978) 12 *Georgia Law Review* 393 394.

[761] Posner 'The Right to Privacy' (1978) 12 *Georgia Law Review* 393 395.

[762] Gavison "Privacy and Limits of Law" (1980) 89 *Yale Law Journal* 421 422.

[763] Etzioni *The Limits of Privacy* (1999) 38.

[764] *Supra*.

protected through other interests, or reduced to some underlying right or interest such as freedom from mental stress, property and reputation. That being said, the majority of commentators proclaim privacy as a value at the core of human existence and well being. The majority of commentators also, however, lament the fact that privacy is difficult to define. Some of these commentators propose that the difficulty in defining privacy has played a role in undermining its value and usefulness and has further impeded its effective legal protection. What is clear is that privacy has multiple meanings and can therefore take diverse forms to such an extent that a sense of what is private and what should be kept private differs from society to society. There is definitely truth in the observation and remark by most mainstream legal and philosophical commentators that privacy will have different consequences in different situations. For this reason it is a concept that is neither eternal nor universal, it is a relative and contextual concept. The value of privacy lies in the function of privacy, the values privacy promotes and those aspects of human life that would be impossible or unlikely in the absence of privacy. Privacy serves a number of functions including the creation and maintenance of social and personal relations, limiting access to the individual and perfecting political understanding. Privacy promotes and is grounded on values such as happiness, justice and liberty. In the absence of privacy, ideals like persona relations, the politically free man and the morally autonomous man would not in existence.

Notwithstanding general agreement on the fact that privacy cannot be satisfactorily defined, several proponents of privacy have made attempts to define or at least propose a conception of privacy.

There are different definitions or conceptions advanced by proponents of privacy. Although the majority of commentators agree that privacy is distinct and coherent, there is disagreement as to what makes privacy distinct and coherent. There are a number of approaches to or conceptions of privacy postulated in legal and philosophical literature, namely the right to be let alone, limited access to the self, secrecy, control over information, personhood and intimacy. The right to be let alone is perhaps the most commonly postulated and one of the earliest conceptions of privacy. The conception locates the value of privacy in its ability to provide the individual with physical space away from others. One of the criticisms levelled at this

conception is that it is merely descriptive of an attribute of privacy. The conception has also been criticised for being antiquated, "archaic" and conception was appropriate during a time in human history when individuals generally lacked physical space but now that is no longer the case because the "opportunities for physical privacy are so much greater" and "abundant". As fundamental as the conception may be, it has a number of other shortcomings: first, it does not indicate how privacy should be valued[765]; secondly, it obscures the fact that not every violation is a violation of privacy[766]; thirdly, it overlooks the fact that not being let alone does not always result in a loss of privacy[767]; lastly, it is outdated in its sense of privacy as seclusion or solitude.[768]The majority of commentators prefer to conceive of privacy as control over information about oneself. In so doing, proponents of this conception often refer to privacy as a claim, form of control or condition. Even so, this conception is also open to criticism. Ultimately, the pragmatic approach is perhaps the more realistic and workable approach to privacy because the approach embraces the dynamic and evolving nature of privacy. In terms of this approach privacy is seen as a dynamic and evolving concept, it occurs in varied contexts, can be compromised in diverse circumstances and its underlying interests may evolve. Put differently, privacy is an aspect of customs, norms and traditions that may change from time to time and activities that we want to protect from disruptions and interferences.

The different conceptions have all featured at different times, to different degrees and in different contexts in case law across the jurisdictions under review. To go back to what was said at the end of Chapter 3, perhaps the most important point remains that whatever the nature of privacy, or its value, it is still regarded to be a fluid concept and to exist only where there is a reasonable expectation of privacy. In this sense, the different conceptions may play a role to assist in locating the right in a particular context. At the same time, these conceptions may inform the justifiability of infringement where the right has been found to exist. However, the overarching approach – a reasonable expectation coupled with a pragmatic approach informed by contemporary customs and norms – may well not only make for uncertainty in many

[765] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1102.

[766] Thompson "The Right to Privacy" (1975) 4 *Philosophy and Public Affairs* 295 295.

[767] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 275 276.

[768] Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1 4.

contexts (it is indeterminate in advance), but lopsided certainty in other contexts, such as the workplace. It is to privacy in the workplace that the remainder of this dissertation is devoted.

CHAPTER 5:
PRIVACY IN THE WORKPLACE

5.1 INTRODUCTION

Chapter 2 of this dissertation provided an overview of the privacy protection in early societies and identified the extent to which privacy was protected in those societies. That chapter also sought to illustrate that the seeds of what we view or refer to as privacy today were sown at a very early period, this notwithstanding the fact that the development of the concept and its concomitant protection progressed at a slow pace. Chapter 3 proceeded to investigate the development of privacy protection in countries selected for purposes of this study and critically assessed the current status of the general protection of privacy in these countries. Chapter 4 considered the numerous conceptions of privacy, outlined the criticisms levelled at each conception and assessed the possibility of a universal workable definition of privacy, or at least a practicable approach to privacy.

The goal of the next four chapters is to consider the issue that constitutes the heart of this research, namely, the extent to which privacy is protected in the workplace given advancements in technology and the implications (if any) for the right to privacy as such. In this regard, it may be said that privacy in the workplace has grown in importance as technology has enabled new forms of testing and monitoring of employees. Employee monitoring is not necessarily a new trend,[769] but modern technology has enabled sophisticated forms of testing or monitoring of employees. These forms of testing or monitoring include drug tests, obtaining employees' credit history, HIV testing, genetic testing, background checks, psychological testing, polygraph tests, keystroke monitoring, listening to telephone calls and voicemail, reading e-mail, monitoring computer, telephone and fax usage, use of electronic devices to track the location of employees, searching offices and workplaces as well

[769]For instance, prior to the introduction of current technology, which enables the monitoring of employees, employers monitored their employee use of company resources by using onsite managers and supervisors whose job was to physically observe and monitor employees at work to ensure that they were being productive and efficient. Kesan "First Principle Examination of Electronic Privacy in the Workplace" in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 258.

as the use of video surveillance devices to monitor employees.[770] Use of these technological advancements has emphasized the tension between two conflicting sets of principles. On the one hand there is the principle of inviolability of the employee's right to privacy - employees do not cede their rights to privacy and dignity when they sign an employment contract. On the other hand, there is the right of the employer to enjoy its property and exercise its managerial powers of command to protect its property against abuse that might cause direct or indirect damage to the employer's business.[771]

As a first step towards evaluating the implications of new technology for privacy in the workplace, the aim of this chapter is to set the tone and briefly consider, in turn, what is meant by the phrase "privacy in the workplace", the arguments for and against the need for privacy protection in the workplace, a number of policies and practices in the workplace that typically threaten or pressurise the protection of privacy in the workplace, as well as the implication of these policies and practices for privacy. In conclusion, it will be argued that there is indeed a need for privacy protection in the workplace, particularly in light of technological advancements. The following chapter (chapter 6) will provide a synopsis of what the selected countries have done in protecting privacy in the workplace in light of the policies and practices identified in this chapter. Chapters 7 and 8, in turn, will respectively focus in depth on two of further employer practices and policies, namely e – mail/internet monitoring and genetic testing, these being the most recent and, arguably, the most technologically advanced of the policies and practices identified. It is important to bear in mind that the selection of the practices considered in the chapters to follow was guided by an emphasis on challenges to privacy, which relate to technological developments and foster new and unique demands for the accommodation of privacy in the workplace.

[770] Solove and Rotenburg *Information Privacy Law* (2003) 618.

[771] Reinhard "Information Technology and Workers' Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law; Information Technology and Worker's Privacy: Information Technology and Worker's Privacy: Enforcement" (2002) 23 *Comparative Labour Law & Policy Journal* 527.

5.2 ARGUMENTS FOR PRIVACY PROTECTION IN THE WORKPLACE

In order to determine what is meant by the phrase "privacy in the workplace", it is important to first examine the arguments raised on behalf of employees in favour of the protection of their right to privacy in the workplace. Broadly speaking, employees insist on the protection of their privacy in the workplace for the following four reasons[772]:

a) Employees argue that the protection of the right to privacy in the workplace preserves their autonomy (that is, the ability to choose freely and independently one's own goals and relations).[773] For this reason, their autonomy may be unreasonably affected where (for example) a management policy threatens to penalise employees for conduct outside the workplace. The problem of employer control over employees' private lives becomes complicated as the boundaries between off duty and on duty time and conduct becomes blurred.[774] More and more employees spend a lot of time in the workplace and the workplace becomes a second home, yet at the same time technology enables decentralisation of the workplace.[775]

b) Certain commentators such as Craig have linked privacy to the individual dignity, health and well-being of employees. Employees contend that all forms of employer practices may adversely affect the dignity and well- being of employees.[776]

c) It is also argued that privacy is inherent in notions of respect, love, friendship and trust and that close relationships are only a possibility if individuals accord each other a measure of privacy.[777] The employment relationship transcends the contractual framework and operates on a social level as a relationship based on good faith, trust, respect and loyalty. As such, some

[772]Craig *Privacy and Employment Law*(1999) 20 -26.
[773]*Supra*.
[774]*Supra*.
[775]*Supra*.
[776]Craig *Privacy and Employment Law* (1999) 20 -26.
[777]*Supra*.

employees may construe employer policies infringing on their privacy interests as an attack on their dignity, respect and loyalty by employers.[778]

d) Employees further argue that privacy breeds diversity and its protection not only works against conformist pressures, but also nurtures the development of fresh ideas, beliefs and attitudes.[779] Pluralism (industrial pluralism) plays a vital in the workplace where innovation is pivotal to any successful enterprise. Industrial pluralism is unlikely to be achieved where employers implement policies inhibiting employee autonomy. As such, any threat to the privacy of individuals, regardless of whether they are in the workplace or at home, is a cause for serious concern for both employee and employer.[780]

It appears from these arguments that the phrase "privacy is in the workplace" in the first place denotes a retention by the employee of a sense of autonomy, dignity and well being in the workplace. It may further be linked to the existence of the elements of good faith, trust, respect and loyalty within the employment relationship, recognised as such by the contractual basis of any employment relationship. Privacy in employment further ensures that the individual is free from conformist pressure and able to develop of fresh ideas, beliefs and attitudes which are pivotal to industrial pluralism. As such, 'privacy in the workplace' is shorthand for, and a reflection of, individual concerns, the contractual nature of the employment relationship, and good business sense.

5.3 ARGUMENTS AGAINST PRIVACY PROTECTION IN THE WORKPLACE

In contrast, employers and the public may endeavour to justify curtailing employee privacy for the following reasons:

a) The improvement of economic conditions. Employers are concerned about the way employees perform at work since this is linked to the efficiency and profitability of their enterprises. Employers want to hire competent workers who are unlikely to cause workplace disruptions or be careless or reckless while they work (thus exposing the employer to liability). Employers want

[778] Craig *Privacy and Employment Law* (1999) 20 -26

[779] Craig *Privacy and Employment Law* (1999) 20 -26.

[780] Craig *Privacy and Employment Law* (1999) 20 -26.

employees who are not likely to suffer health and personal problems that will result in employees being absent from work or being unproductive;[781]

b) The protection of the health and safety of employees, consumers and the public.[782] Employers will often raise safety concerns to justify, for example, drug or medical testing. Moreover, under health and safety legislation (and, in some jurisdictions, in terms of the common law), employers are obligated to provide a safe working place and protect the health of employees;[783]

c) The deterrence of and control over employee abuse of the employment relationship.[784] Employers have justified, for example, search and surveillance policies on the basis of the need to deter employee abuse of employer facilities and to identify perpetrators of such abuse... In short, employers may wish to engage in searches and surveillance to investigate misconduct;[785] and

d) The need to comply with legislation.[786] Legislation sometimes authorises employers to implement privacy invasive policies. Other legislation compels employers to train and monitor its employees to ensure that they are competent to perform their specific jobs. Such legislation holds the employer responsible where the employer fails to train or monitor employees, especially when the concerned jobs impact on the safety of others. For instance, in professions involving child care there is pressure on employers to scrutinize an employee's past and previous work experience to reduce the risk of employee misconduct.[787]

In summary, it may be said that the arguments against privacy protection do not really focus on the employee and the individual relationship of that employee with the employer (as do the arguments in favour of privacy protection). Rather, arguments against privacy protection focus on the freedom of the employer to run its business and to exclude its possible liability, the more so where every employer operates in an environment concerned with the safety of employees and the public.

---

[781] Solove and Rotenburg *Information Privacy Law* (2003) 619.

[782] *Supra*.

[783] Solove and Rotenburg *Information Privacy Law* (2003) 619.

[784] *Supra*.

[785] Solove and Rotenburg *Information Privacy Law* (2003) 619.

[786] *Supra*.

[787] Solove and Rotenburg *Information Privacy Law* (2003) 619.

5.4 IDENTIFICATION OF POLICIES AND PRACTICES

Technological developments have increased the ability of employers to monitor and survey their employee's performance in the workplace. As already alluded to, this chapter briefly identifies and examines some of the most prevalent technology enabled employment practices and policies, namely background checks, polygraph testing, psychological testing, drug testing and HIV/AIDS testing. This part of the chapter will provide an illustration of how these practices and policies may invade the privacy of employees, while Chapter 6 will focus on the manner in which selected countries have addressed the privacy concerns raised by these practices and policies. It bears repeating that chapters 7 and 8 will focus in detail on two further employer practices and policies impacting on privacy, namely e – mail/internet monitoring and genetic testing. Furthermore, it should again be noted that the selection of the practices and policies in this and subsequent chapters is not meant to provide a comprehensive list, but was guided by the emphasis on those challenges to privacy, which arise from technological developments and which foster new and unique demands for the accommodation of privacy in the workplace.

5.4.1 Background Checks

Background checks entail that employers acquire(and often store) information about an employee's credit history, employment history, school records, criminal convictions and medical history from the employee and third parties (such as previous employers, insurance companies and credit bureaus). Employers usually acquire such information during the recruitment and selection stages of employment. However, employers have also been known to undertake such checks during employment.[788] Employers primarily conduct background checks to determine the suitability of an employee for a specific job or position. Such checks are commonplace for positions requiring high levels of trust, honesty and integrity such as in banking, security and financial management. These checks may infringe on an employee's privacy rights, particularly where the checks result in the disclosure of personal information that bears no relevance to the employment position or the suitability of an applicant for a

[788] For example the applicants in *Smith and Grady* v *United Kingdom* [1999] ECHR 72 and *Lustig-Prean v United Kingdom* (1997) 7 BHRC 65 underwent investigations (which included detailed interviews with each of them and with third parties on matters relating to their sexual orientation and practices into their homosexuality) whilst employed.

position.[789] In so much as the checks may implicate an individual's privacy interests, employer's (in particular United States employers) conduct the checks to prevent liability for the illegal or negligent acts of an employee in terms of the doctrine of negligent employment.[790] Similarly, United Kingdom and South African employers may be held liable under the doctrine of vicarious liability. For example, the employer in the United States decision of *Tallahassee Furniture Co. Inc.v Harrison*[791] was held liable for negligent employment after an employee brutally stabbed and bludgeoned a client (Harrison) while delivering furniture to her home. South African and United Kingdom courts have also held employers liable for the negligent and intentional acts of their employees in terms of the principle of vicarious liability, where the concerned employees' conduct is determined to be sufficiently related to the business of the employer. For example, the House of Lords in *Lister and Others v Hesley Hall Ltd*[792], held a school liable for the sexual abuse of some of its students by a warden in its employment, because the wardens' conduct was sufficiently related to the obligations the school owed to children placed in its care. Similarly, in *K v Minister of Safety and Security*[793] the South African Constitutional Court found the conduct of three policemen who assaulted and raped a woman sufficiently related to the business of the employer to render the employer liable.

---

[789] The applicants in *Smith and Grady* v *United Kingdom* and *Lustig-Prean v United Kingdom* members of the Royal Air Force and the Royal Navy (respectively) complained of investigations into their homosexuality and their subsequent discharge on the sole ground of their homosexuality constituted a violation of their right to respect for their lives protected by Article 8 of the ECHR. The government argued that admitting homosexuals to the armed forces would have a significant and negative impact on the fighting power, morale of armed forces personnel and the operational effectiveness of the armed forces. The European Court of Human Rights was of the view that "the investigations…into the applicants homosexuality, which included detailed interviews with each of them and with third parties on matters relating to their sexual orientation and practices…constituted a direct interference with the applicant's right to respect for their private lives." The Court added that "Their consequent administrative discharge on the sole ground of their sexual orientation also constituted an interference with that right". The Court further found there was a lack of concrete evidence provided by the government to substantiate the alleged damage to morale and fighting power that any change in policy would entail, that is, the admission or presence of homosexuals to the armed forces. In other words the Court found that neither the investigations conducted into the applicant's sexual orientation nor their discharge on the grounds of their homosexuality was justified under Article 8 of the ECHR.

[790] *Tallahassee Furniture Co. Inc. v Harrison* 583 So.2d 744, 747 (Fla. Dist. Ct. App. 1991).

[791] *Tallahassee Furniture Co. Inc. v Harrison* 583 So.2d 744, 747 (Fla. Dist. Ct. App. 1991).

[792] [2002] 1 AC 215 (HL).

[793] [2005] 8 BLLR 749 (CC).

5.4.2 Psychological Testing

A psychological test has been described as 'an observation of a sample of human behaviour made under standard controlled conditions which results in a linear evaluation called a score'.[794] Psychological tests are used in the employment context to assess the suitability of an applicant's personality for a particular position.[795] For example, the employer in *Soroka v Dayton Hudson Corporation*[796] required applicants for the position of store security officer to undergo psychological testing in order to identify rational and emotionally stable applicants. The employer viewed good judgment and emotional stability as ideal personality traits for the position.[797] Employers use various psychological tests in the workplace, including personality tests, honesty tests and projective testing. Personality tests are aimed at identifying a person's "personal characteristics, thoughts, feelings and behaviour" through related questions.[798]One example of a personality test is the Minnesota Multiphasic Personality Inventory, which consists of over 500 numbered statements which the test subject has to decide are true, false, and mostly true or mostly not true. The statements relate to "opinions, attitudes, observable behaviour and feelings" and a test subject's responses to the statements represent personality characteristics such as depression, hysteria, social introversion and paranoia.[799] Honesty tests also consist of written tests. However, unlike personality tests they are aimed at identifying a particular personality trait, in particular honesty or integrity.[800] The test results represent applicants' attitude towards dishonesty and whether they are likely to engage in dishonest or counterproductive behaviour. Projective tests require applicants to engage in various mental exercises, from drawing a person or human figure, through the interpretation

---

[794] Hoffman "Pre – placement Examinations and Job Relatedness: How to Enhance Privacy and Diminish Discrimination in the Workplace"(2001) 49 *University of Kansas Law Review* 517 539.

[795] Hebert *Employee Privacy Law* (2009) § 7: 1.

[796]235 Cal. App. 3d 654 (1991).

[797] Camara "Using Personality Testing in Pre-Employment Screening: Issues Raised in *Soroka v Dayton Hudson*" (2000) 6 *Psychology, Public Policy and Law*1164 1165. See also *International Brotherhood of Electrical Workers* 856 F 2d 1174 (CA 8 1998) which involved the psychological testing of employees who were security risk at a nuclear power plant and *McKenna v Fargo* 451 F. Supp. 1355 involving the personality testing of applicants for fire fighting positions in order to determine their ability to withstand stress.

[798] Hebert *Employee Privacy Law* (2009) § 7: 1.

[799]*McKenna v Fargo* 451 F. Supp. 1355, 1359 – 1360.

[800] Hebert *Employee Privacy Law* § 7: 1.

of drawings and pictures to the completion of sentences.[801] The Rorschach Inkblot Test is an example of a projective test. The test consists of a series of inkblots in various shapes, colours and forms which test subjects are required to interpret. The responses of the test subjects are analysed to reveal "emotional and personality traits".[802] The widespread use of personality tests as a way of identifying suitable employees has raised concerns relating to their validity and reliability.[803] Furthermore, and particularly relevant to this study, personality tests infringe the privacy interests of test subjects because they consist of questions which are highly personal and sensitive in nature.[804]

The United States Supreme Court in *Osborn v United States*[805] explained why the use of personality tests raised privacy concerns: 'Personality tests seek to ferret out a man's inner most thoughts on family, life, religion, racial attitudes, national origin, politics, atheism, ideology, sex, and the like'.[806] The appellants in *Soroka v Hudson*, for example, argued that some of the questions they were required to respond to in a personality test aimed at assessing their emotional stability, were related to religious

[801] Hebert *Employee Privacy Law* § 7: 1.

[802] *McKenna v Fargo* 451 F. Supp. 1355, 1360.

[803] Critics of psychological and personality have argued that the tests are actually not an accurate predictor of employee performance. They further contend that the tests were developed for diagnosing psychological disorders and not best candidates for a job. Moreover in certain countries there are no rules regarding the analysis and validation of test procedures. To make matters worse no credentials are generally required for individuals and companies that develop and market the tests. Menjoge "Testing the Limits of Anti – discrimination Law: How Employers Use of Pre-employment Psychological and Personality Tests Can Circumvent Title VII and the ADA" (2003) 82 *North Carolina Law Review* 326, 332. See also Ecker "To Catch A Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee" (1994) 63 *University of Missouri at Kansas City Law Review* 251 259 and Hebert LC "Employee Privacy Law" (2009) § 7: 3. Other critics have argued the tests may discriminate against subjects in the following ways: first, the tests may contain questions that employers would normally be prohibited from asking in the pre-employment interview; second, the tests may eliminate candidates on the basis of specific traits traditionally possessed by persons of a certain group; and third the tests may be standardized in a way that reflects the cultural bias against those persons who do not fit into the middle-class, racial and religious norm. Menjoge "Testing the Limits of Anti – discrimination Law: How Employers Use of Pre-employment Psychological and Personality Tests Can Circumvent Title VII and the ADA" (2003) 82 *North Carolina Law Review* 326. See also the matter of *Griggs v Duke Power* Co. 91 S.Ct. 849. In *Griggs*, the Supreme Court held that the employer was prohibited by provisions of the Civil Rights from requiring a high school education or the passing of a standardised general intelligence test as a condition of employment because neither requirement was shown to be significantly related to successful job performance. The court found that both requirements operated to disqualify Negroes at a substantially higher rate than white applicants, and only white employees formerly had filled the jobs in question as part of a long-standing practice of giving preference to whites.

[804] Hebert *Employee Privacy Law* (2009) § 7: 4.50.

[805] 385 U.S. 323 (1966).

[806] 342.

beliefs and sexual orientation and as such had no bearing on their emotional stability or ability to perform the job of store security officer. For this reason, the appellants argued, the personality testing they were required to undergo violated their constitutional right to privacy. The appellants in Soroka were required to respond to questions related to religious attitudes such as: "I believe there is a Devil and a Hell in afterlife" and "I believe my sins are unpardonable". The appellants were also required to respond to questions related to sexual orientation such as: "I have been in trouble because of my sex behaviour" and "Many of my dreams are about sex".[807]

5.4.3 Polygraph Testing

The polygraph is a lie detection device measuring and recording physiological changes in blood pressure, heart rate, pulse rate, respiration and perspiration. A polygraph machine usually consists of a sphygmograph, pneumograph tubes and electrodes.[808] The sphygmograph is strapped around a subject's arms and measures heart beat, blood pressure and pulse rate. The pneumograph tubes are positioned on the chest and abdomen and measure the subject's respiration. The electrodes are placed on two of the subject's fingers to measure perspiration.[809] The polygraph relies mainly on the subject's physiological reactions to a set of questions to draw an inference on the subject's truthfulness.[810] There has been much debate as to whether the polygraph can produce empirically and scientifically reliable results.[811] Employers turn to polygraphs in the belief that the tests "detect and deter employee theft and

[807] 79 – 80.

[808] Hebert *Employee Privacy Law* (2009) § 6:2.

[809] Hebert *Employee Privacy Law* (2009) § 6:2.

[810] Hebert *Employee Privacy Law* (2009) § 6:2.

[811] The US in its 1983 Office of Technology Assessment concluded that there was limited evidence for establishing the validity of polygraph testing. The assessment further concluded that polygraph accuracy may be affected by a series of factors including: the training, orientation and experience of the examiner, the examinee's emotional stability and intelligence, the use of countermeasures and the examinee's willingness to be tested. Finkin *Privacy in Employment Law* (2003) 117. Similar concerns regarding the reliability and accuracy of polygraph testing have been expressed by South African legal commentators. See for example Christianson M "Polygraph Testing in South Africa Workplaces: Shield and Sword in the Dishonesty Detection versus Compromising Privacy Debate" (2000) 21 *Industrial Law Journal* 17 and Tredoux and Pooley "Polygraph Based Testing of Deception and Truthfulness: An Evaluation and Commentary" (2001) 22 *Industrial Law Journal* 819. The authors correctly point out that polygraphs do not measure the presence or absence of deception or lying (in fact there is no known instrument that directly records whether a subject is lying or deceptive) but merely measure a subject's physiological activity.

other employee misconduct, including drug abuse, industrial espionage, and crime".[812] The widespread use of polygraph testing is especially evident in industries requiring high levels of trust and honesty, such as information technology, retail, security, criminal investigation and banking.[813] Certain companies go as far as making the passing of a polygraph test a decisive factor in pre-employment selection and others include provision for testing in their employment contracts, in that the employment contract will require the employee to submit to the test on demand by the employer.[814] Employers commonly require employees to under polygraph testing as part of the pre – employment process for a number of purposes. Employers may use polygraph tests for pre – employment screening to verify information given by an applicant; to determine if an applicant had engaged in any misconduct with their previous employer or to determine if an employee has engaged in any unlawful activities such as theft and fraud.[815] Employers may also subject employees to random or periodic testing for the purpose of determining whether employees are engaged in counter-productive behaviour or to deter theft in the workplace. Polygraph tests in employment may also be used as part of an investigation into an employee's misconduct.[816]The right to privacy of individuals may be violated by the use of polygraphs particularly where the questions asked relate to personal information. It has been argued that the use of these polygraph tests in employment implicates the privacy of employees in a number of ways:

a) these tests attempt to penetrate the inner domain of individual belief in violation of the distinction between conduct and belief;[817]

---

[812] Hebert *Employee Privacy Law* (2009) § 6:5. See also Christianson "Truth, Lies and Polygraphs: Detecting Dishonesty in the Workplace" (1998) 18 *Contemporary Labour Law* 1.

[813] Christianson "Polygraph Testing in South Africa Workplaces: Shield and Sword in the Dishonesty Detection versus Compromising Privacy Debate" (2000) 21 *Industrial Law Journal* 17.

[814] Christianson "Polygraph Testing in South Africa Workplaces: Shield and Sword in the Dishonesty Detection versus Compromising Privacy Debate" (2000) 21 *Industrial Law Journal* 17.

[815] Hebert *Employee Privacy Law* (2009) § 6:5.

[816] Hebert *Employee Privacy Law* (2009) § 6:5.

[817] The court in the US decision of *Long Beach City Employees Association v City of Long Beach*41 Cal.3d 937, 227 Cal.Rptr. 90 Cal. 198 , 944 stated the following regarding the inner domain of the individual "If there is a quintessential zone of human privacy it is the mind. Our ability to exclude others from our mental processes is intrinsic to the human personality. In their seminal article on the right to privacy, Warren and Brandeis stated: the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others". The court further added that it was for the reason that "A polygraph examination is specifically designed to overcome this privacy by compelling communication of thoughts, sentiments, and emotions which the examinee may have chosen not to communicate".

b) they interfere with the individual's sense of autonomy and reserve through use of a machine or instrument which senses an employee's emotional responses to personal questions; and

c) these tests increase the psychological power employers have over individuals seeking employment or already employed.[818]

5.4.4 Drug and Alcohol Testing

Employers engage in drug and alcohol testing to identify users of illicit drugs and alcohol in the workplace, deter individuals in the workplace from using drugs and alcohol and to reduce the incidence of drug and alcohol related problems such as accidents and illnesses.[819] Drug tests are able to detect the presence of drugs such as "opiates, phencyclidine (PCP), cocaine, methamphetamine, amphetamine, Phenobarbital and marijuana".[820] There are five known methods of drug testing. [821]

Urinalysis is the most common and preferred method, because urine samples can be easily obtained and urine retains the presence of drugs for longer periods of time than, for example, blood.[822] Urinalysis as a method of drug testing has privacy implications. The act of urination has been described as highly personal and private. First, in the leading United States decision of *National Treasury Employees Union v Von Raab* the court observed that '[t]here are few activities in our society more personal or private than the passing of urine. Most people describe it by euphemisms if they talk about it at all. It is a function traditionally performed without public observation; indeed, its

[818] Christianson "Truth, Lies and Polygraphs: Detecting Dishonesty in the Workplace" (1998) 18 *Contemporary Labour Law* 12. Some of the psychological power play present in the use of polygraph in the employment scenario were referred to by the court in *State v Community Distributors Inc.* (See note 19) when the court stated "Admittedly, [the] defendant did not physically compel its employees to submit to lie detector tests. Nor did [the] defendant orally threaten its employees with loss of their jobs if they did not submit to the tests. From a realistic viewpoint, however, defendant-employer stands in the supreme bargaining position and, should it please, may adopt a 'take it or leave it' attitude toward prospective and present employees...Compelling psychological factors nonetheless enter into a situation wherein someone who wants a job is asked if he will volunteer to take a lie detector test. The court does not envision…that prospective or current employees would initiate the administering of a lie detector test. The requests and suggestions clearly come from the employer." The defendant in *State v Community Distributors Inc*., an owner and operator of drugstore, was convicted in Freehold Township Municipal Court of statutory violations in influencing, requesting or requiring employees, as condition of employment or continued employment, to take or submit to lie detector tests. See also *SACCAWU obo Chauke v Mass Discounters* (2004) 13 CCMA [2004] 6 BALR 767 (CCMA).

[819] Hebert *Employee Privacy Law* (2009) § 2:5.

[820] Hebert *Employee Privacy Law* (2009) § 2:5.

[821] Hebert *Employee Privacy Law* (2009) § 2:5.

[822] Hebert *Employee Privacy Law* (2009) § 3:15.

performance in public is generally prohibited by law as well as social custom.' Secondly, urinalysis can reveal more than the presence of illegal drugs, it can also reveal what medications an employee is taking[823] and consequently reveal "a host of medical facts including whether or not [an employee] is epileptic, pregnant or diabetic".[824] Thirdly, the manner in which urine samples are collected may intrude on the privacy of employees, particularly where the samples are to be provided under direct observation to prevent adulteration or substitution of the sample. Some United States courts have held that the requirement of direct observation in the collection of a urine sample for drug testing heightened the existing invasive and intrusive nature of the testing[825].[826] Fourthly, the results of a drug test are not always treated as confidential medical records given that they are often shared with third parties such as supervisors, prospective employers, health insurers and management. For example, post – incident drug testing after an occupational accident have to be shared with insurance companies to provide information whether industrial injuries benefits have to be paid out.[827]

Blood samples can also be examined for the presence of drugs and are better indicators of recent drug use than urine samples. That being said, blood samples are not often used to detect drugs, because the drawing of a blood sample is a complex procedure that involves "a physical intrusion into the body" which is best done by trained persons.[828]

Another method of drug testing is hair sample analysis. Hair retains the presence of drugs for longer periods than urine or blood.[829] Nonetheless, the collection of hair samples for drug analysis is not entirely unproblematic.[830] For example, an individual's hair sample may test positive for marijuana as a result of exposure to

---

[823] *Supra*.

[824] *Skinner v Railway Labour Executives Association* 489 US 602 (1989) 617.

[825] See *American Federation of Government Employees v Sullivan* 744 F Supp 294, 305 (D DC 1990) and *American Federation of Government Employees v Thornburgh* 720 F Supp 154, 155 n 1 (ND Cal 1989).

[826] Hebert *Employee Privacy Law* (2009) § 3:15.

[827] Rothstein "Workplace Drug Testing: A Case study in the Misapplication of Technology" (1991) 5 *Harvard Journal of Law and Technology* 65 77 – 79.

[828] Hebert *Employee Privacy Law* (2009) § 2:4.

[829] Hebert *Employee Privacy Law* (2009) § 2:4.

[830] Hebert *Employee Privacy Law* (2009) § 2:4.

marijuana smoke that has become embedded in the hair. In other words, a positive drug test based on hair sample analysis is not always an indication of the personal use of drugs.[831]

The collection of saliva samples for drug analysis is one of the less invasive and intrusive methods of drug testing. The method is also a good indicator of present drug usage and intoxication.[832]

Sweat analysis is another less invasive method that may reveal the presence of drugs. However, as is the case with hair samples, exposure to drugs from environmental sources may affect sweat samples and consequently yield an incorrect positive test result.[833]

All the aforementioned forms of testing raise privacy concerns about the way in which sample are obtained, not to mention the information gathered by the testing.[834]

The information obtained through drug tests, even though at first glance not private, may further concern the off duty conduct of employees in the privacy of their homes. In other words, drug tests are able to expose and reveal aspects of the personal life of employees (including any illegal activities they may wish to engage in) outside of working hours. This means that while employers may be entitled to monitor the conduct of employees while on duty, these tests may well ignore the fact that employees have privacy interests outside the workplace.[835]

The United States district court, in *Beattie v St Petersburg*[836] recognised that drug tests may deprive employees of their privacy interests in off duty conduct (in this case fire fighters) and in this regard stated that drug tests "reveal activities of a fire fighters' personal life. The fire fighters have a legitimate interest in keeping their personal life shielded from the government's prying eyes, especially when the activity revealed is frowned upon by a large segment of the community and may constitute a crime. In order to pass constitutional muster the City must demonstrate a compelling interest

[831] Hebert *Employee Privacy Law* (2009) § 2:4.
[832] Hebert *Employee Privacy Law* (2009) §2:4.
[833] Hebert *Employee Privacy Law* (2009) § 2:4.
[834] *Supra*.
[835] Hebert *Employee Privacy Law* (2009) § 2:4.
[836] 733 F Supp 1455 (MD Fla 1990).

that outweighs these privacy concerns".[837] These compelling interests may, as already indicated, be based on the identification of users of illicit drugs in the workplace; the deterrence of individuals from using drugs in the workplace; and to reduce the incidence of drug related problems such as accidents and illnesses.[838]

Drug testing in employment typically occurs at the following stages:

a) Pre – employment testing. Pre – employment testing occurs where applicants are required to undergo drug testing as a condition of employment. For example, in the United States case of *Willner v Thornburgh*,[839] an applicant for the position of attorney in the Antitrust Division of the Department of Justice was required to undergo pre – employment drug testing as a condition of employment. The Department argued that the testing was justified by an interest in promoting a public image of integrity and in minimising the costs of hiring and retention.[840]
b) Periodic routine testing. Routine testing may occur periodically as part of an annual physical examination or in response to a triggering event such as promotion or transfer. For example, the employees in *National Treasury Employees Union v Von Raab*,[841] had applied for promotion to positions requiring them to carry firearms and handle classified materials. They were required to undergo routine testing. The Court stated that for routine testing to be constitutional it had to be sufficiently justified by a compelling interest (such as an interest in public safety, interest in the integrity of the workforce and interest in protecting sensitive information); conducted in a manner that preserves the privacy interests of employees and with prior notice of testing to employees.[842]

[837] Hebert *Employee Privacy Law* (2009) § 2:4.
[838] Hebert *Employee Privacy Law* (2009) § 2:5.
[839] 738 F Supp 1 (D DC 1990).
[840] Hebert *Employee Privacy Law* (2009) § 3:9.
[841] 816 F. 2d 170, 175 (CA51987).
[842] Hebert *Employee Privacy Law* (2009) § 3:10.

c) Post accident testing. In *Skinner v Railway Labour Executives' Association*,[843]the court upheld the post accident testing of railway crew involved in serious accidents because of the governmental interest in determining the cause of rail accidents and in deterring future accidents by ferreting out drug abuse by employees in safety sensitive positions. Courts are also likely to uphold post accident testing where the employee was responsible or at fault with respect to an accident, the accident was grave in nature and the employees' duties implicate safety concerns. [844]

d) Random testing. Random testing occurs randomly, without prior notice, any number of times and is not based on a triggering event or a reasonable suspicion. As a consequence, courts have found random testing more intrusive than other types of drug testing.[845]In the United States, employers have justified this type of testing based on safety concerns and courts have upheld the random testing of employees in safety sensitive positions such as air traffic controllers, water treatment plant operators, crane operators, physicians and dentists[846]. [847] The employer in *Chetty and Kaymac Rotomoulders (Pty) Ltd*,[848] for example, conducted random drug tests on employees, The arbitrator took issue with the manner in which the testing took place, specifically with the fact that the employer dismissed one of the employees (in a safety sensitive position concerned with the manufacture of fuel tanks for the motor industry) after he admitted his drug problem to the employer and expressed willingness to let the employer assist him with his problem;

e) Reasonable suspicion testing.[849] Employers may engage in reasonable suspicion testing of employees where they suspect an employee had been using drugs or is under the influence of drugs. In the United States, courts uphold reasonable suspicion testing of employees where an employer can

[843] 489 US 602 (1989).

[844] See *Skinner v Railway Labour Executives' Association*.

[845] See *Transportation Institute v United States Coast Guard* 727 F Supp 648 (D DC 1989).Hebert *Employee Privacy Law* (2009) §3:11.

[846] Hebert *Employee Privacy Law* (2009) §3:11.

[847] Hebert *Employee Privacy Law* (2009) § 3:12 .

[848] (2004) 25 *ILJ* 2391 (BCA).

[849] Wefig "Employer Drug Testing: Disparate Judicial and Legislative Responses" (2000) 63 *Albany Law Review* 799 799.

prove that his or her suspicion was based on "the existence of illustrative facts" that would guide a reasonable person to suspect that an employee has been using drugs or is under the influence of drugs. Symptoms of drug use and direct observation of drug use or possession have been accepted by courts as facts that can guide an employer to engage in reasonable suspicion testing.[850]

5.4.5 HIV/AIDS Testing

Notwithstanding global efforts to manage and contain the HIV/AIDS epidemic, it continues to grow. Less than two decades ago, in 1990, around 8 million people were estimated to be living with HIV/AIDS globally. Today the number of people with the epidemic has increased to nearly 35 million.[851] The latest global HIV/AIDS statistics published by UNAIDS/WHO estimate that at the end of 2007, 33, 2 million people were living with HIV/AIDS, 2,5 million people were infected with HIV during 2007 and 2,1 million people died of AIDS during the same year. [852]

According to the UNAIDS/WHO report, sub–Saharan Africa continues to be the most affected region in the world, because 22,5 million individuals are reported to be living with HIV/AIDS in the region and in 2007 an estimated 1, 7 million people were infected with HIV/AIDS in the region. A further estimated 1, 6 million people died of the pandemic in sub – Saharan Africa during 2007. This means that 76 % of global AIDS deaths in 2007 occurred in the sub – Saharan region. The sub-region of Southern Africa accounts for 68 % of individuals living with HIV/AIDS globally and 76 % of global AIDS deaths.[853]

A further reality in these regions is that the majority of people living with HIV/AIDS are "between the ages of 15 and 49 - in the prime of the working lives". As such, the epidemic has adversely affected all sectors of society in these regions with negative social and economic consequences. A 2001 report - "The Economic Impact of

[850] Hebert *Employee Privacy Law* (2009) § 3:13.

[851] AIDS Epidemic Update: Special Report on HIV/AIDS: December 2007 Published by Joint United Nations Programme on HIV/AIDS (UNAIDS) and the World Health Organisation (WHO).

[852] AIDS Epidemic Update: Special Report on HIV/AIDS: December 2007 Published by Joint United Nations Programme on HIV/AIDS (UNAIDS) and the World Health Organisation (WHO).

[853] AIDS Epidemic Update: Special Report on HIV/AIDS: December 2007 Published by Joint United Nations Programme on HIV/AIDS (UNAIDS) and the World Health Organisation (WHO).

HIV/AIDS in Southern Africa" - expounded on the major impact of HIV/AIDS on labour productivity, economic growth and social development:

> "The spread of HIV/AIDS reduces labour productivity, raises private and public consumption, and thereby reduces income and savings, with lower savings, the rate of investment falls, reinforcing the decline in economic growth. The loss of labour productivity occurs because a larger share of the work force becomes debilitated and dies causing organizations to lose workers with critical skills. Skilled personnel are lost and valuable labour time is consumed when workers become debilitated, and work schedules are disrupted when organizations replace workers and managers who are ill or have died. The loss of capacity reduces economic growth."

HIV/AIDS tests are designed to determine if an individual has been infected with the HIV virus and as such do not detect the virus in individuals, but rather to establish the presence of HIV virus antibodies in an individual's blood. As such, when a person tests positive for the virus, it is an indication of the fact that the person has HIV antibodies in their blood. Blood samples, as well as saliva and urine samples can be tested to reveal the presence of HIV antibodies. Research has indicated that the testing of urine samples for HIV antibodies is more reliable and accurate than the testing of saliva samples. In fact, the testing of urine samples is as accurate as the testing of blood samples and may also become as prevalent as blood testing given that the virus cannot be transmitted through urine.[854]

5.4.5.1 Arguments for Workplace HIV/AIDS Testing

In response to the spread and the devastating effects of the epidemic employers (in order to provide a safe work environment and maintain productivity in the age of HIV/AIDS) often resort to mandatory HIV/AIDS testing in the recruitments stages or during employment. Employers usually justify the HIV/AIDS testing of employees by arguing that:

a) the employer has a freedom of choice as to whom to hire, which freedom is founded on the legal principles of freedom of association and freedom to contract;

[854] Hebert *Employee Privacy Law* (2009) § 11:7.

b) it is well known that the risk of occupational transmission of the HIV virus is unlikely, but this does not mean the risk is non-existent. For this reason, some employers feel they have a responsibility to prevent occupational transmission of the virus by testing both prospective and existing employees. This occupational safety argument has led to health care workers being prevented from performing certain duties in countries such as the United States. Certain United States decisions have held that HIV positive medical workers who pose a less than significant risk of transmitting the virus can be prevented from performing certain invasive procedures.[855] The argument has also been extended to military officials[856] and persons employed in emergency services;[857]

c) HIV positive persons, although not yet symptomatic, may experience psycho-neurological symptoms such as dementia. As such, in some occupations (for example in the case of an aircraft/airline pilot and mine lift operator) a sudden onset of AIDS dementia may be very risky;

d) the employment of persons with HIV has costs associated with recruitment, training and support of such employees;[858]

---

[855] See for example *Doe v University of Maryland Medical System Corporation* 50 F 3d 1261 (1995) where the court stated the following in this regards "[a]lthough there may presently be no documented case of surgeon-patient transmission such transmission is clearly possible". Doe was a resident in neurosurgery; in *Leckelt v Board of Commissioners* 909 F 2d 820 (1990) where the court found that "even though the probability that a health care worker might transmit HIV to a patient may be extremely low and can be further minimized through the use of universal precautions, there is no cure for AIDS at this time and the potential of HIV infection is extremely high." Leckelt in this decision was a licensed practical nurse*;* and in *Doe v Washington University* 780 F.Supp. 628 632-34 (E.D. Mo. 1991) the court found that the HIV positive dental student not otherwise qualified to perform invasive procedures because the risks defy the axiom to at least do no harm.

[856] For instance in *X v Commonwealth of Australia* [1999] HCA 63, at issue was the ability of the Australian Defence Force to terminate the enlistment of a solider based on his HIV positive status. Such was the case in Namibia in the matter of *N v Minister of Defence (Namibia)* Labour Court of Namibia, delivered 2005 05 10, Case No: LC 24/98 and in India's *A v Union of India* Writ Petition No. 162 3 01 2000, High Court of Judicature at Bombay (28 Nov 2000). Canadian HIV/AIDS Legal Network *HIV Testing of UN Peacekeeping Forces: Legal and Human Rights Issues* 9 September 2001. http://www.aidslaw.ca/Maincontent/issues/testing/peacekeepingforces.pdf (2005-02-21).

[857] In *Anonymous Fireman v City of Willoughby* 779 F. Supp 402 (1991) a federal district court in the US found that the possibility of HIV transmission during the provision of emergency care could justify the exclusion of applicants for employment with HIV. http://www.law.wits.ac.za/salc/salc.html (2005-02-21).

[858] The economic argument was primarily used by South African Airways (SAA) in the case of *Hoffmann v SAA* [2000]12 BLLR 1365 (CC). In response to the economic argument used by SAA Justice Ngcobo stated that legitimate economic concerns were important but they cannot serve to disguise stereotyping and prejudice, which have no place in South Africa's era of respect for human dignity, compassion and understanding – *ubuntu*. He further noted that the "greater interests of society require the recognition of inherent dignity of every human being…".

e) in service industries, such as restaurants and hotels, the employment of HIV persons may give rise to irrational fears amongst clientele or co-workers.[859]

5.4.5.2 Arguments against Workplace HIV/AIDS

The following arguments have been raised in opposition to the testing of employees for HIV/AIDS:

a) Requiring an employee or a prospective employee to undergo an HIV test as a general condition of employment may infringe an individual's constitutional rights, such as the right to physical integrity and privacy. These inherent and constitutionally protected rights should trump the employer's right to contractual freedom in those instances where an employee's HIV positive status has no bearing on the job;[860]

b) The risk of occupational transmission argument is valid only where an employee is exposed or will be exposed to procedures constituting possible modes of transmission, such as surgical procedures in the case of a surgeon. However, even in such high-risk occupations employees can take the necessary precautions. Moreover, in most occupations (including the exposure prone occupations) the risk of occupational transmission is often low;[861]

c) HIV is not a reliable or conclusive indicator of dementia; in fact, psychometric testing is perhaps the better indicator of any neurological impairment; [862]

d) HIV positive employees may continue to be productive members of society (by paying taxes, paying for their own medical aid and by supporting their families and dependants) for a long period of time after contracting the virus. Moreover, the costs associated with employing HIV positive persons are similar to those borne by commitments to equality and the prohibition on unfair discrimination;[863]

---

[859] http://www.law.wits.ac.za/salc/salc.html (2005-02-21).

[860] http://www.law.wits.ac.za/salc/salc.html (2005-02-21).

[861] For instance in *Doe v University of Maryland Medical System Corporation* the court noted that there was between a 1 in 42,000 and a 1 in 417,000 chance of a transmission from doctor to patient during blood prone procedures.

[862] http://www.law.wits.ac.za/salc/salc.html (2005-02-21).

[863] http://www.law.wits.ac.za/salc/salc.html (2005-02-21).

e) The fear and antagonism surrounding HIV/AIDS cannot justify the discrimination against individuals living with the illness, particularly in those countries with a history of discrimination. Ngcobo J, in *Hoffmann v South African Airways*[864] aptly stated the following in this regard and with particular reference to South Africa: "Prejudice can never justify unfair discrimination. This country has recently emerged from institutionalised prejudice…Our constitutional democracy has ushered in a new era – it is an era characterised by a respect for human dignity of all human beings. In this era, prejudice and stereotyping have no place." [865]

Further consideration of HIV/AIDS testing of employees, also in the South African context, will be given in Chapter 6.

5.5 CONCLUSION

The need for privacy is not created by people. Instead it inheres in all people. Privacy is something that all persons yearn. Without it, people would cease to flourish and probably perish or deteriorate. The arguments advanced in favour of the protection of privacy emphasise this value of privacy as well as its constituent elements (outlined in Chapter 4). In the workplace, and despite the existence of arguments to the contrary, privacy protection is essential because it preserves and maintains the autonomy, dignity and well being of employees in an environment where the employer in general yields more influence and authority than the employee. Furthermore, privacy is inherent in the notions of good faith, loyalty, respect and trust which underpin the employment relationship. In addition, privacy breeds diversity and nurtures the development of fresh and different ideas, beliefs and attitudes, which are crucial for innovation and creativity in individuals. At the same time, employers (and, indirectly, the public) often have a legitimate interest in policies and practices that may impact on privacy.

In this chapter, a number of these policies and practices engaged in by employers were identified. The way in which these policies and practices impact on privacy and the extent to which they do so were also described. What these policies and practices have in common, is that all of them are based on recent and continued technological

[864] [2000] 12 BLLR 1365 (CC).
[865] 1374 – 1376.

advances. As such, it seems clear that the biggest continuous threat to privacy in the workplace remains developments in science and technology. At the same time, it may be said, even at this early stage, that it does not appear as if the challenge lies in a changed conception of privacy and the values it seeks to protect. Rather, it would seem that technological developments demand no more than a continuous balancing of the interests of employer and employee in the different contexts created by new policies and practices made possible by technology. In what follows, specific attention will be given to how different jurisdictions have responded to what may be termed this 'contextual challenge' to the accommodation of privacy in the workplace. As mentioned, Chapter 6 will elaborate on legal responses across the different jurisdictions to the challenges raised by the policies and practices identified in this chapter, while Chapter 7 and 8 will focus on the contextual challenge raised by the most recent advances in technology – e-mail/ internet monitoring and genetic testing.

CHAPTER 6:
A COMPARATIVE SURVEY OF POLICIES AND PRACTICES IMPACTING ON PRIVACY IN THE WORKPLACE

6.1 INTRODUCTION

The previous chapter briefly considered the meaning of the phrase "privacy in the workplace" and also gave brief consideration to the arguments for and against the need for privacy protection in the workplace. The chapter then went on to identify a number of policies and practices in the workplace that typically threaten or pressurise privacy in the workplace. The general impact of these policies and practices on privacy was discussed and it was found that these policies and practices, to an extent which depends on the manner and circumstances in which they are used, infringe on an individual's privacy. Finally, it was argued that there is indeed a need for privacy protection in the workplace, particularly in light of technological advancements.

As a further step in exploring the relationship between technological developments and privacy in the context of the workplace, this chapter provides a more elaborate and comparative discussion of the policies and practices identified in the previous chapter. This is done by:

a) first, providing a brief introduction or overview of the extent to which a particular policy or practice is used in three selected jurisdictions, namely South Africa, the United Kingdom (as part of the European Community) and the United States;
b) second, briefly examining the legislation, if any, regulating or impacting on the use of the particular policy or practice in these jurisdictions;
c) third, reviewing a selection of cases (where available) in respect of each jurisdiction to form a picture of how courts and tribunals in that jurisdiction have approached the application and impact of the policy or practice in question; and
d) lastly, analysing the extent to which privacy is protected in light of the use of that particular policy or practice across the different jurisdictions.

6.2 BACKGROUND CHECKS

The previous chapter explained that background checks in essence entailed the acquisition and storage by an employer of information about an employee, which information ranges from an employee's credit history to an employee's criminal convictions or medical records. Because the range of information that an employer can obtain in this manner is so vast, it was submitted that employers should restrict background checks on employees to only that information which has a bearing on the position sought or occupied by the employee. For instance, it would be prudent and arguably justifiable for an employer to do a background check on employees applying for the position of driver (only) to determine whether they have been convicted of any traffic related or drug related offences (as opposed to an extensive background check likely to disclose other personal information which has no bearing on whether or not the concerned employee will be a suitable and fit driver).

6.2.1 South Africa

Grogan is of the view that background checks are used by South African employers primarily to ensure the veracity of information given by an applicant for a position.[866] Grogan adds that a high premium is placed on dishonest conduct in employment because it is capable of destroying or causing irreparable harm to the trust on which the employment relationship is founded.[867] Dishonest conduct can "consist of any act or omission which entails deceit. This may include withholding information from the employer, or making a false statement or misrepresentation with the intention of deceiving the employer."[868]

Grogan's views are supported by a number of South African decisions, which depart from the premise that the employment relationship is one requiring the utmost trust. As such, any conduct of a dishonest nature, constitutes a breach of this relationship.[869] Included in this expectation of trust, is a duty on the parties to disclose material facts before entering into a contract of employment. It follows that the non- disclosure of

[866]Grogan *Dismissal, Discrimination and Unfair Labour Practices2nd ed*. (2007) 301.

[867]Grogan *Dismissal, Discrimination and Unfair Labour Practices2nd ed*. (2007) 301.

[868]Grogan *Dismissal, Discrimination and Unfair Labour Practices2nd ed*. (2007) 301.

[869] See for instance the decisions of *Standard Bank of South Africa Ltd v CCMA & Others* [1998] t BLLR 622 (LC), *De Beers Consolidated Mines Ltd v CCMA & Others* (2000) 21 ILJ 1051 (LAC) and *Toyota SA Motors (Pty) Ltd v Radebe & Others* (2000) ILJ 340 (LAC).

material facts by a party may well result in the other party justifiably terminating the contract.[870] A number of Labour Court and Commission for Conciliation Medication and Arbitration ("CCMA") decisions have upheld the dismissal of employees where misrepresentation or non–disclosure by an employee was found to have destroyed the relationship of trust between the employee and the employer.[871]

6.2.1.1 Legislation

There is no legislation regulating the use of background checks by employers as such. However, there is legislation that ensures that employers conducting background checks on individuals do not discriminate against individuals. Section 6(1) of the Employment Equity Act[872] ("EEA") prohibits direct or indirect unfair discrimination in any employment practice or policy on various grounds. The EEA's definition of an "employment practice or policy" in section 1 "includes advertising a position and the selection criteria for employment". To avoid any suggestions of unfair discrimination during the selection stages of employment an employer should not request information about an employee that has no bearing on the inherent requirements of the job or the suitability of an applicant for a position.[873]

6.2.1.2 Case Law

There are no reported decisions directly related to the use of backgrounds checks by employers in South Africa. However, the Labour Court and CCMA have often pronounced on misrepresentation and non-disclosure by employees of their qualifications, previous misconduct under an old employer, or previous convictions.[874] These pronouncements suggest that South African tribunals are likely to uphold the dismissal of employees who misrepresent themselves or fail to disclose material facts, particularly if those employees are occupying positions requiring high levels of trust, honesty and integrity. In fact, the Labour Court has gone so far as to disregard the materiality of a misrepresentation and uphold the dismissal of an employee simply on

---

[870] See for example *Hoffmann v Monis's Wineries Ltd* 1948 (2) SA 163 (C) *and Dilks v Postma's Diamond Prospect Ltd* 1921 (WLD). *Grogan Dismissal, Discrimination and Unfair Labour Practices 2nd ed.* (2007) 301.

[871] Decisions such as *De Beers Consolidated Mines Ltd v CCMA & Others* (2000) 21 ILJ 1051 (LAC) and *Mlotshwa/SABC (1)* [2002] 12 BALR 1292 (CCMA).

[872] Act 55 of 1998.

[873] Van Niekerk *The Right to Privacy in Employment* (2001) Unpublished Paper presented at seminar for Advanced Diploma in Labour Law hosted by Rand Afrikaans University 5.

[874] *Grogan Dismissal, Discrimination and Unfair Labour Practices 2nd ed* (2007) 301.

the basis that the employee stood in a unique relationship of trust and honesty with the employer. In *Hoch v Mustek Electronics*[875] the applicant was dismissed for misrepresenting her qualifications. The Court upheld the dismissal of the applicant notwithstanding the fact that the applicant had been working for the employer for a considerable number of years and had been honest and trustworthy in her work and notwithstanding the fact that her disputed qualifications were irrelevant to her position. The Court held that because the applicant "stood in a unique relationship of trust and confidence" towards her employer,[876] her employer was justified in considering her misrepresentation material enough to "have irreparably damaged the unique trust relationship" they once shared.[877]

The applicant in *Wium v Zondi & Others*[878] had been previously convicted of theft and had failed to point this out in his curriculum vitae when applying for a position as deputy principal of a school. For this reason, the employer charged the employee with making a false statement and subsequently dismissed the employee. The employee argued that he was entitled to conceal his previous conviction because the appeal against the conviction was pending and he assumed the employer was aware of his conviction by virtue of the fact that his previous and potential employer both were in the field of education. Ntsebeza AJ reasoned that the dismissal of the employee was an appropriate sanction for his intentional non-disclosure seeing as his act of dishonesty in this regard had resulted in a breakdown of the relationship of trust between the employee and the employer.[879]

Although *Mashava v Cuzen & Woods Attorneys*[880] did not involve the non-disclosure of previous misdeeds, the decision is nonetheless important in that the Labour Court weighed the employee's non-disclosure of her pregnancy against her constitutional right to privacy. The employer in Mashava dismissed the employee for dishonesty in that she concealed the fact that she was pregnant. The employee claimed her dismissal was based on her pregnancy and, as such, automatically unfair in terms of section

[875][1999] 12 BLLR 1297 (LC).
[876]1292 J.
[877]1293 B.
[878][2002] 11 BLLR 1117 (LC).
[879]1125 C.
[880][2000] 6 BLLR 691 (LC).

187(1)(e) of the Labour Relations.[881] Landman J reasoned that the employee had tried to conceal her condition for the sole reason that she feared her employer would treat her disadvantageously and her fear had to be "measured against [her] right to privacy and [the] duty to relinquish that privacy". Landman J found that there is no duty on an employee to inform an employer of her pregnancy except where such information is in an employee's interest or in the interests of her unborn child.[882]

6.2.2 United Kingdom

The practice of screening employees during recruitment and selection is a long standing tradition in the United Kingdom. The creation of the Criminal Records Bureau in 2002 to manage and organise aspects of employee screening confirms the widespread practice engaged in by employers to check whether applicants have any previous convictions rendering them unsuitable for certain positions. It is important to note that the Bureau's primary aim is to prevent the abuse of children and vulnerable persons and for this reason the information it discloses to various organisations is limited and related to achieving this aim. As a consequence, the Bureau discloses only information related to a person's criminal background and then only pertaining only to persons who want to work with children and vulnerable adults. As such, the Bureau would not be in a position to, for example, disclose criminal record information about persons who want to work in the financial sector.[883]

The Rehabilitation of Offenders Act[884] limits the disclosure of previous convictions by applicants to allow them unprejudiced access to employment. The Exceptions Order provides that after a certain period of time has elapsed certain convictions, referred to as 'spent' convictions, need not be disclosed to an employer.[885] "Unspent" convictions are those convictions which an individual is under a duty to reveal because the period of time required to attain "spent status" has not passed. The general rule is that applicants with 'spent' convictions have a right, when asked about previous convictions, to indicate that they have no criminal record during a job interview

[881] Act 66 of 1995.

[882] 698 B – C.

[883] Thomas "Employment Screening and the Criminal Records Bureau" (2002) 31 *Industrial Law Journal* 55 – 56.

[884] Act of 1974, (Exceptions Order 1975).

[885] The period of time which must elapse for a conviction to become "spent" is dependent on a number of factors including the nature of the offence and the sentence given for the particular offence. http://www.emplaw.co.uk (2007-02-05).

(unless the type of employment falls within the ambit of the Exceptions Order of the Rehabilitation of Offenders Act).[886] However, applicants are under a duty to disclose 'unspent' convictions to potential employers when requested to do so.

6.2.2.1 Legislation

Apart from the impact of the Rehabilitation of Offenders Act[887] discussed above, the Data Protection Act[888] ("DPA") generally regulates the processing of personal[889] and sensitive data. Part I of the DPA defines "personal information" as information about a living person and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. "Sensitive information" is described, in Part I of the DPA, as information concerning an individual's racial or ethnic origin; political opinions; commission or alleged commission of any offence; proceedings for any offence committed or alleged to have been committed; trade union membership; sexual life; religious beliefs or other beliefs of a similar nature; and physical or mental health. The term "processing" in the DPA is defined as, in relation to information or data, obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including, amongst others, the retrieval, consultation or use of the information or data or the organisation, adaptation or alteration of the information or data. The scope of the DPA with respect to the regulation of the processing of personal and sensitive data is also extended through a wide definition of the term "data controller" in Part I of the DPA as a person who alone or jointly with others determines the purposes for which and the manner in which any personal data is processed or is to be processed. The DPA's wide and far reaching definition of "data controller" invariably suggests that it applies to both private and public sector employers. Perhaps the most important aspect to the DPA is that it places a duty on a

[886] An applicant will, however, be required to disclose "spent" convictions if he or she intends applying for a position in the following categories: professional occupations (e.g. barristers, accountants, opticians and vets); administration of justice (judges, police officers and prison and traffic wardens); regulated occupations (e.g. directors of insurance companies and firearm dealers); caregivers and child minders (e.g. old age nurse, nanny and teachers); and national security providers (e.g. air traffic controllers). http://www.emplaw.co.uk (2007-02-05).

[887] Act of 1974.

[888] Act of 1988.

[889] Examples of personal information would be details of an employee's salary and bank account or a completed set of applications. http://www.emplaw.co.uk (2007-02-05).

data controller to comply with the data protection principles in relation to all personal data with respect to which he, she or it is the data controller.[890]

Generally speaking, the DPA does not prevent employers from processing sensitive data. The DPA merely limits the circumstances under which such data can be processed. The DPA recognises that employers may process sensitive data with regard to individuals in order to assess their suitability for employment and requires that employers, prior to processing such data, should obtain the explicit and voluntary consent of their employees.[891] This denotes that the consent to the processing must be voluntary by the related individual and such individual must not feel coerced to give his or her consent. This further means that the related individual must not be penalised for refusing to give his or her consent to the processing.[892]

The voluntary consent requirement in section 4 of the DPA ensures that an individual has some autonomy and control over his or her personal information and furthermore advances the conception of privacy as limited access to oneself (see chapter 3 above). This approach describes privacy as, amongst other things, a condition in which acquaintance with a person or a person's personal affairs is limited by the person him- or herself. As indicated above, the DPA requires employers, when processing sensitive data, to obtain the explicit and unequivocal consent of employees, failing which the processing becomes unfair and, more importantly, unlawful. The DPA takes matters a step further and requires employers to notify employees of all intended purposes of the information processed, even where the intended purposes appear obvious.[893] The DPA sets out a number of requirements to be met by employers before they can collect, store, use, disclose or process sensitive personal information concerning employees. This includes the requirement that before employers collect and use sensitive personal information they must do so only if a legal right or obligation requires them to do so for purposes of ensuring the health, safety and welfare of employees and the selection of safe and competent employees and a safe working environment.[894]

---

[890] Section 4 (4) of the DPA.
[891] Employment Practices Code Guidance 12.
[892] *Supra*.
[893] Employment Practices Code Guidance 12.
[894] Employment Practices Code Guidance 12.

It is apparent from the DPA's definition of the terms "personal information" and "sensitive information" that United Kingdom employers conducting background checks on employees have a duty to observe and comply with the data protection principles of the DPA, simply because these checks undoubtedly relate to the processing of data of an individual. In fact, United Kingdom employers implementing any of the policies and practices discussed in this chapter – also those impacting on employees during employment - have to ensure that the manner in which they employ these policies and practices complies with the DPA data protection principles, again because the employment of the said policies and practices entail a processing of personal and sensitive data as defined in the DPA. In this regard, the Information Commissioner has issued comprehensive and explanatory guidelines, in the form of the Employment Practices Data Protection Code of 2005 [895] ("Employment Practices Code") and the Supplementary Guidance ("Employment Practices Code Supplementary Guidance") in order to assist compliance by employers and the adoption of good practice. The Employment Practices Code also aims to strike a balance between, on the one hand, the legitimate expectations of workers that personal information about them will be handled properly and, on the other hand, the legitimate business interests of employers.[896]

With respect to applications for employment, the Employment Practices Code guides employers to seek only relevant and necessary information for purposes of reaching a recruitment decision. The Employment Practices Code further requires employers to limit the collection of criminal record information to offences that have a direct bearing on the suitability of an applicant for a particular position.[897] The Employment Practices Code recognises that employers may need to verify the accuracy of information given by applicants and as such provides that employers inform

[895] The Employment Practices Code is intended to assist and guide employers to comply with the legal requirements of data protection. Although the Employment Practices Code has no legal status and is not legally enforceable, it stands as an important guideline for employers in meeting the legal requirements of the DPA. Given that the Employment Practices Code covers amongst others successful and unsuccessful applicants and former applicants and affects recruitment and selection exercises by employers, UK employers are obligated to consider its provisions when conducting background checks on individuals. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/about_the_code.html (2009-05-16).

[896] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/about_the_code.html (2009-05-16).

[897] Employment Practices Code Guidance 11.

applicants of the fact that their information may need to be verified. The Employment Practices Code Supplementary Guidance also discourages employers from requiring applicants to obtain their records from third parties as a condition of employment.[898] Of particular importance is the fact that the Employment Practices Code Supplementary Guidance emphasises that obtaining information about an applicant from the CRB or Disclosure Scotland amounts to an intrusion into that particular individual's privacy and, as such, should be only be done during the final stages of the employment process (i.e. once the applicant has been shortlisted and only if it is necessary in light of the nature and character of the position concerned).[899]

Although the Employment Practices Code provides guidelines on pre – employment vetting, the Employment Practices Code warns employers that vetting is more intrusive than verification. The Employment Practices Code Supplementary Guidance requires that an employer's decision to vet an employee should be proportionate to the risks that the employer is likely to face. As such, an employer who wants to safeguard against risks such as breaches of national security, theft or disclosure of trade may be justified in vetting its employees.[900] The Employment Practices Code recommends that employers inform applicants early on in the recruitment process that vetting may take place at a later stage.[901] The Employment Practices Code further advises against the use of vetting as a means of gathering intelligence on an employee and that it should be used as a means of obtaining specific information concerning an employee.[902] Moreover, the signed consent of an applicant must be obtained especially where vetting involves the release of documents or information from a third party.[903]

6.2.2.2 Case Law

The appellant in *Kawol v Craig Homes Ltd*[904] was employed as a nurse, a profession which is exempt from the provisions of the Rehabilitation of Offenders Act. The employee worked largely unsupervised at night and further supervised junior staff in his position of unit manager. It subsequently emerged (after the employer conducted a

[898] Employment Practices Code Guidance 12.
[899] Employment Practices Code Guidance 13.
[900] Employment Practices Code Guidance 14.
[901] Employment Practices Code 22.
[902] Employment Practices Code 22.
[903] Employment Practices Code Guidance 15.
[904] Appeal No. UKEAT/0833/DM 2005.

criminal record search) that the employee had failed to disclose his previous conviction for assault occasioning actual bodily harm in his application form for employment. The employee was dismissed after a disciplinary hearing for failing to disclose his previous conviction to the employer.

The employment tribunal upheld the decision of the employer to dismiss the employee, not only in view of the requirements of the Rehabilitation of Offenders Act, but also because the application form for employment that the employee was required to complete plainly indicated that he had to make this disclosure. The appeal tribunal found that the employer had no choice but to dismiss the appellant because of the nature of the business they owned, which required them to exercise care in the staff they chose and employed. The appeal tribunal further found the decision to dismiss the appellant justified because it was not based on his conviction, but on his failure to voluntarily disclose his conviction, a fact which destroyed or breached the trust and confidence the employer had in him.

The employee in *X v Y*[905] was employed as a development officer by a charity organisation that, amongst other things, organised activities for young offenders and those at risk of offending. The employee was arrested, following an incident with another male in a public toilet whilst off duty, and taken to a police station where he signed a caution in which he acknowledged he had committed an offence in terms of the Sexual Offences Act[906]. The employee chose not disclose this incident to his employer. The employer became aware of the incident six months after its occurrence and dismissed the employee for gross misconduct in that he had committed a criminal offence with a direct bearing on his employment and for failing to disclose his offence to the employer. The employee filed a complaint with the employment tribunal arguing that he had been unfairly dismissed in a manner inconsistent with respect for private life under Article 8 of the ECHR and in breach of the prohibition of discrimination in Article 14 of ECHR.

The employment tribunal upheld the dismissal on the ground that the conduct in question was a criminal offence, not trivial in nature and showed an inappropriate lack of self control and serious lack of judgment, which had a direct bearing on his

[905][2004] EWCA Civ 662.

[906]Act of 1956.

employment in a position which dealt mainly with vulnerable youngsters. The conduct had also undermined the employer's trust and confidence in the employee. With respect to the question whether the dismissal was incompatible with Articles 8 and 14 of the ECHR, the employment tribunal held there were no headings under which these claims could be brought in terms of the Human Rights Act.[907] In any event, the argument was held to be irrelevant because the employee acknowledged that he should have told his employer of his conviction and caution and elected not to do so. This, in itself, could be construed as an acknowledgment by the employee that he was wrong to have withheld the information about his conviction and caution from his employer.

On appeal, the appeal tribunal directed its attention to whether the dismissal of the employee breached Article 8 of the Human Rights Act. The applicant submitted that the conduct in question took place outside his work life and in his private life and his dismissal therefore involved a breach of right to respect for his private life. The appeal tribunal found that the conduct in question was not covered by the right to respect for private life in terms of Article 8 as the conduct in question was not private. Rather, it was a transitory sexual encounter between two strangers in a place to which the public had and were permitted access to.

The court of appeal came to a similar conclusion, namely, that the conduct concerned did not take place in the employee's private life. The court of appeal further determined that because the conduct under discussion was a criminal offence, it would be of legitimate concern or interest to the public and as such could not be labelled as a purely private matter. In this sense, the employer had a legitimate concern or interest in knowing of the employee's conduct because it set off alarm bells regarding the employee and his suitability for the type of employment at issue.

6.2.3 United States

It appears from case law that United States employers do carry out background checks on applicants. It further emerges from case law that employers may and are in certain instances compelled to take into consideration an individual's criminal record in making appointments, particularly where the conviction relates to or has any bearing

[907] Act of 1998.

on the position sought by the applicant. In the event that that an applicant's criminal record is significantly unrelated to the position sought by the applicant and the employer still investigates this, the employer faces the risk of contravening federal and state antidiscrimination legislation that explicitly prohibits employers from discriminating against individuals with criminal records.[908]

6.2.3.1 Legislation

There is no legislation directly regulating the use of background checks by employers in United States law. However, as pointed out above, employees can protect and preserve their privacy interests by using the Fourth Amendment (in relation to which it has been held that it protects people and not just places from unreasonable searches). It may be argued that an unwarranted background check by an employer amounts to a search and, perhaps, a seizure (if the employer decides to store the information acquired in conducting a background check on a particular employee). In this regard, United States courts have given the words "unreasonable search and seizures" in the Fourth Amendment a wide and purposive meaning to include other forms of intrusions such as drug testing and HIV/AIDS testing.[909] However, a number of states prohibit persons with criminal convictions from seeking employment in positions related to or in connection with caring for children, nursing and education.[910] As a consequence, employers are legally obliged to carry out background checks aimed at discovering if an applicant has any criminal record in respect of certain positions.[911] Despite this, it is submitted that employees who have been subjected to background checks they feel were unwarranted or unjustified in light of the nature or character of the employment they sought, may be able to use constitutional protection, particularly, the Fourth Amendment the challenge these checks. In *Griswold v*

[908]Scales "Employer Catch – 22: The Paradox between Employer Liability for Employee Criminal Acts and the Prohibition against Ex-Convict Discrimination" (2002) 11 *George Mason Law Review* 419 421. For example in states such as Connecticut, New York and Wisconsin it is unlawful for employers to discriminate against individuals with criminal record unless the record has bearing on the position sought. Scales "Employer Catch – 22: The Paradox between Employer Liability for Employee Criminal Acts and the Prohibition against Ex-Convict Discrimination" (2002) 11 *George Mason Law Review* 419 427.

[909] See in this regard the decisions of *National Treasury Employees Union v Von Raab and Skinner v Railway Labour Executives' Association* which held that the drug testing of employees amounted to a search in relation to the concerned individuals.

[910] Ecker "To Catch A Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee" (1994) 63 *University of Missouri at Kansas City Law Review* 251 256.

[911]Finkin *Privacy in Employment Law* (2003) 175.

Connecticut [912] the Fourth Amendment was held to protect both individuals and places against unreasonable searches and seizures, where individuals argue that their privacy interests were violated

6.2.3.2 Case Law

Although the United States is a highly litigious society, the different policies and practices impacting on privacy have only featured in a handful of cases. This does not mean that there is no case law pertaining to the issue of background checks. In certain states, employers may be held liable under claims of negligent employment and negligent retention if they knew or should have known of an employee's propensities and the employer's negligence in employing or retaining that employee caused harm to third parties. The employer in *Tallahassee Furniture Co. Inc. v Harrison* [913] was found to have failed in its duty of care in hiring an employee who had been previously convicted of serious crimes (including aggravated assault), after the employee (a furniture delivery man) brutally stabbed and bludgeoned a client whilst delivering furniture to her home. The employer was found liable because it had failed to interview the employee, ask him for references or to ask him to fill out a job application.[914] Religious employers may also be held liable under the doctrine of negligent employment. In *Jones v Trane*[915] the court held a church could be held liable in terms of the doctrine of negligent employment where it is shown that "the church placed or continued to place a clergy man in contact with boys despite actual or constructive notice of the priest's perverted proclivities".[916]

6.2.4 Analysis

The discussion above shows that employers carry out background checks on applicants and current employees to not only determine their suitability but also to avoid liability for the conduct of their employees. At the same time, all three jurisdictions impose limitations on the freedom of employers to do so, even though

[912] *Griswold v Connecticut* 381 U.S. 477 (1965).

[913] 583 So. 2d 744, 747 (Fla. Dist. Ct. App. 1991).

[914] Scales "Employer Catch – 22: The Paradox between Employer Liability for Employee Criminal Acts and the Prohibition against Ex-Convict Discrimination" (2002) 11 *George Mason Law Review* 419 422.

[915] (1992, Supp) 153 Misc 2d 822, 830.

[916] (1992, Supp) 153 Misc 2d 822, 830.See also *Foster v Loft Inc.* 26 Mass App 289 (1988) where an employer was held liable for the negligent employment of bartender with a criminal record after the employee injured a customer.

these limitations are uneven across the three jurisdictions. These limitations range from direct regulation of access to certain types of information (such as criminal records in the United Kingdom) relating to specific categories of employment (as in some states of the United States), regulation of the access and use of personal data (in the United Kingdom), the indirect application of the principles of unfair discrimination (across all three jurisdictions) and the application of constitutional protections (in the United States). The question whether employees are under a duty to make disclosures where employers neglect to conduct background checks depends on the materiality of the disclosure. A disclosure is considered sufficiently material where if it can influence an employer's employment decision and has a bearing on the position concerned.

6.3 PSYCHOMETRIC TESTING

The previous chapter described how psychological tests are used in the employment context to assess the suitability of an applicant's personality for a particular position. It was pointed out that some of these tests, such as the MMPI test, consists of statements relating to, amongst other things, an individual's opinions, attitudes, beliefs, behaviour and feelings and could determine, on the basis of a test subject's responses, the individual's personality (even, for example, whether the individual suffered from depression, hysteria or paranoia). Much like polygraph testing, these tests may infringe an individual's privacy in that they are able to reveal a person's inner thoughts and feelings. However, unlike polygraph testing which tends to reveal specific information about an individual (such as whether or not he, for example, committed a specified act), personality tests are structured in such a way that they are able to give the person administering the test a wide range of information concerning the person taking the test.

6.3.1 South Africa

Published research indicates that certain South African employers, particularly those in the banking, insurance and security industries[917] use psychological tests for training and development, selection and recruitment, team development and succession

[917] See Van Der Merwe "Psychometric Testing and Human Resource Management' (2002) 28(2) *South African Journal of Industrial Psychology* 77.

planning purposes.[918] Perhaps the most commonly used form of psychological testing is psychometric tests. Psychometric tests concern the "larger project of assessment which includes forms of evaluation such as structured and unstructured interviews, self assessment and projective techniques like the Rorschach Inkblot Test".[919] Consequently, psychometric tests measure not only psychological traits but also occupational abilities and skills.[920] Research further indicates South African employers do not use psychometric tests in isolation but in combination with other methods, such as interviews and simulation exercises.[921]

6.3.1.1 Legislation

Although South African courts have yet to deal with the issue of psychometric testing in the employment context, South Africa has legislation specifically regulating such testing in employment in the form of section 8 of the EEA. Section 8 of the EEA explicitly prohibits psychometric testing and other similar assessment of employees unless the test:

a) has been shown to be scientifically valid and reliable;

b) can be applied fairly to all employees; and

c) is not biased against any employee or group.

Section 8 of the EEA aims to prevent the psychometric testing of employees which is discriminatory and unjust in nature. According to Grogan, the prohibition on psychometric testing does not apply to all forms of pre – employment testing and would not, for example, prohibit tests designed to establish a person's knowledge of a specific area or field.[922]

---

[918] This is according to the Human Sciences Research Council (HRSC) Psychological Assessment Needs Analysis Project of 2004 referred to in Paterson and Uys "Critical Issues in Psychological Test Use in the South African Workplace" (2005) 31 (3) *SA Tydskrif vir Bedrysfsielkunde* 12 – 22.

[919] Bonthuys "Counting Flying Pigs: Psychometric Testing and the Law" (2002) 23 *Industrial Law Journal* 1175 – 1176. See also Stabile "The Use of Personality Tests as a Hiring Tool: Is the Benefit Worth the Cost" (2002) 4 *University of Pennsylvania Journal of Labour and* Employment Law 279 281.

[920] Bonthuys "Counting Flying Pigs: Psychometric Testing and the Law" (2002) 23 *Industrial Law Journal* 1175 – 1176. See also Stabile "The Use of Personality Tests as a Hiring Tool: Is the Benefit Worth the Cost" (2002) 4 *University of Pennsylvania Journal of Labour and* Employment Law 279 281.

[921] Van Der Merwe "Psychometric Testing and Human Resource Management" (2002) 28(2) *South African Journal of Industrial Psychology* 77 – 78.

[922] Grogan *Dismissal, Discrimination and Unfair Labour Practices 2nd ed.* (2007) 160.

The Health Professions Act[923] ("HPA") allows only registered psychologists[924] to perform "psychological acts" which are defined in sections 37(2)(a)(c)(d) and (e) of the Act as being:

a) *The evaluation of behaviour or mental processes or personality adjustments or adjustments of individuals or groups of persons, through the interpretation of tests for the determination of intellectual abilities, aptitude, interests, personality make-up or personality functioning, and the diagnosis of personality and emotional functions and mental functioning deficiencies according to a recognised scientific system for the classification of mental deficiencies;*

b) *The use of any method or practice aimed at aiding persons or groups of persons in the adjustment of personality, emotional or behavioural problems or at the promotion of positive personality change, growth and development, and the identification and evaluation of personality dynamics and personality functioning according to psychological scientific methods;*

c) *The evaluation of emotional, behavioural and cognitive processes or adjustment of personality of individuals or groups of persons by the usage and interpretation of questionnaires, tests, projections or other techniques or any apparatus, whether of South African origin or imported, for the determination of intellectual abilities aptitude, personality make-up, personality functioning, pscyhophysiological functioning or psychopathology;*

d) *The exercising of control over prescribed questionnaires or tests or prescribed techniques, apparatus or instruments for the determination of intellectual abilities, aptitude, personality make-up, personality functioning, pscyhophysiological functioning or psychopathology;*

e) *The development of and control over the development of intellectual abilities aptitude, personality make-up, personality functioning, pscyhophysiological functioning or psychopathology.*[925]

[923] Act 56 of 1974.

[924] Section 56. The HPA not only regulates the use of psychological tests by psychologists but also the use of such tests by psychometrists and psychotechicians amongst others in for example assisting speech and occupational therapy patients.

[925] Health Professions Council of South Africa Form – *Lists of Tests Classified as being Psychological* Tests Form 207 2.

Because this definition of psychological tests is couched in such wide terms it may be argued that it includes the use of psychometric tests in the employment context. This means that an employer wishing to administer psychometric tests would have to employ the services of a trained psychologist to do so on its behalf.[926] The Professional Board of Psychology on the Classification of Psychometric Measuring Devices, Instruments, Methods and Techniques provides in its policy that use of a psychometric instrument, or any instrument "that assesses intellectual or cognitive ability of functioning, aptitude, interest, personality make-up or personality functioning", amounts to a psychological act.[927] The policy further requires that before a psychometric instrument may be used in the workplace an employer should assure itself of that instrument's validity, reliability and fairness. Scientific proof of this must be provided to the employer by the person making use of the psychometric instrument (i.e. the psychometric test).[928]

The Psychometrics Committee, as mandated by the Professional Board for Psychology, further regulates the use of psychometric tests.[929] The Committee is not only responsible for the classification of psychological tests but is also responsible for the accreditation of tests. It also endeavours to inform the public of any danger associated with the use or misuse of tests, questionnaires, techniques, apparatus or instruments.[930] What this all means is that there is a statutory duty on South African employers making use of psychological tests to ensure a number of things: first, that the test has been classified as valid and reliable by the Psychometrics Committee; second, that the test has been accredited and certified by the Board; third, to ensure that the tests and persons administering the tests meet the requirements of the HPA;

[926]Paterson and Uys "Critical Issues in Psychological Test Use in the South African Workplace" (2005) 31 (3) *SA Tydskrif vir Bedrysfsielkunde* 12 – 22.

[927]Paterson and Uys "Critical Issues in Psychological Test Use in the South African Workplace" (2005) 31 (3) *SA Tydskrif vir Bedrysfsielkunde* 12 – 22.

[928]Paterson and Uys "Critical Issues in Psychological Test Use in the South African Workplace" (2005) 31 (3) *SA Tydskrif vir Bedrysfsielkunde* 12 – 22.

[929]Christianson "The Testing of Employee: The Selective Prohibition of Medical, Psychological and Other Testing in terms of the Employment Equity Act" (1999) Vol. 9 *Contemporary Labour Law* 11 15.

[930]Christianson "The Testing of Employee: The Selective Prohibition of Medical, Psychological and Other Testing in terms of the Employment Equity Act" (1999) Vol. 9 *Contemporary Labour Law* 11 15.

fourth, that the test can be applied fairly to all employees; and fifth, that the test is not biased against any employee or group.[931]

6.3.1.2 Case Law

There are no clear judicial guidelines about the principles applicable to the use of psychometric tests in the employment context. However, a handful of decisions have addressed the use of these tests in employment. Psychometric testing as a precondition for applicants for the position of team leader at a leading brewery came before the CCMA in *X and SA Breweries Ltd*.[932] The employee alleged that the employer's failure to promote the employee amounted to an unfair labour practice (in terms of section 186(2)(a) of the Labour Relations Act[933] ("LRA"). The employee had been required to meet five criteria for the position of team leader, which included psychometric testing. The employee managed to meet only four of the five criteria. The results of his psychometric test came back as "not recommended" and, on this basis, the employee was not appointed to the position concerned. The employee contended that he met the criteria for team leader because he possessed the necessary qualifications and had acted in the position for some time. The employer argued that the tests were administered as part of company policy pertaining to promotions. The employer further argued that the tests were designed by experts and administered by independent psychologists for a valid business purpose. The arbitrator, in analysing the evidence and arguments, found that the decision by the employer to use psychometric testing along with other criteria amounted to a sound business decision.

The employer in *FAWU & Others v SA Breweries Ltd*[934] had used a general adult education test ("ABET") for purposes of determining the suitability of its employees for posts in a new operation and to retrench those who did not do well in the test. The Court found that the use of ABET constituted an unfair basis for selecting employees for retrenchment because it was not workplace specific and did not in actual fact test whether employees who had years of practical experience in the old operation could adequately perform in the new operation. The Court was also critical of ABET for

[931] Christianson "The Testing of Employee: The Selective Prohibition of Medical, Psychological and Other Testing in terms of the Employment Equity Act" (1999) Vol. 9 *Contemporary Labour Law* 11 15.

[932] (2006) 27 ILJ 435 (ARB).

[933] Act 66 of 1995

[934] 2004 25 ILJ 1979 (LC).

being too generalised and for having a negative impact on older black employees who were products of an inferior education. The Court further held that pre – employment tests would be acceptable only if the employer showed the tests were "professionally proven, predictive or significantly correlated with important elements of work behaviour which compromise or are relevant to the job or jobs" in respect of which employees were evaluated.[935]

6.3.2 United Kingdom

The Employment Practices Code recognises that employers may need to administer psychological tests on applicants during recruitment and selection, but does not provide guidelines on how selection testing (such as psychological testing) should be undertaken by employers.[936] It is unclear to what extent psychometric testing is carried out in the United Kingdom by employers, but it appears from the literature that it is firmly established in certain workplaces.[937] Employers use the tests for, amongst other things, recruitment and selection, job profiling and team building purposes.[938]

6.3.2.1 Legislation

There is no legislation directly regulating the use of psychometric or psychological tests in workplaces in the United Kingdom. Notwithstanding the fact that the Employment Practices Code does not provide employers with detailed guidelines on how to carry out psychometric testing in the workplace, it does remind employers that such testing must comply with the data protection principles of the DPA (this Act was discussed earlier in the chapter in the context of background checks). The DPA requires such testing not to be discriminatory in nature and to be lawful and fair.[939] As such, the DPA requirements are similar to the requirements of section 8 of South Africa's EEA. This means that employers in the United Kingdom, like their South African counterparts, will have to ensure that the psychometrics tests that they use in the workplace are scientifically valid and reliable, can be applied fairly and in a non –

[935] Grogan *Dismissal, Discrimination and Unfair Labour Practices 2nd ed* (2007) 147 – 148.

[936] Employment Practices Code 13.

[937] Bake and Cooper "Fair Play or Foul" (1995) Volume 24 No.3 *Personnel Review* 3 – 18.

[938] *Supra*. For example a recent article in the Nursing Standard indicated that nursing students and staff In England would be required to undergo psychometric tests as part of the recruitment process and a test would be developed to assist in identifying candidates with the skill and personal attributes for the job. *Nursing Standard* (2009) Volume 24 No 6 11.

[939] Bake and Cooper "Fair Play or Foul" (1995) Volume 24 No.3 *Personnel Review* 3 – 18.

discriminatory manner to all employees and are not biased against any employee or group.

The results of psychological tests may qualify as sensitive personal information in terms of section 2 of the DPA, particularly where the tests comprise of questions which promise to reveal information about an individual's political opinions, religious beliefs and sexual life. As previously indicated, the DPA does not prohibit the processing of personal sensitive data, but limits the processing of such data to instances where employers are required to process the data in order to exercise or perform a legal right or obligation.

Section 12 of the DPA deals with the situation where an employment decision is taken by the employer solely on the basis of the results of a psychological test to be taken by applicants. Employers are mandated to inform applicants that the results of the psychological test shall constitute the sole basis of the employment decision.[940] Applicants are afforded a number of rights. First, applicants have a right to make representations which must be considered before a final decision is taken. Secondly, applicants have a right to request the employer to explain the rationale behind the decision it took.[941] Thirdly, applicants have a right to request the employer to reconsider its decision on a different basis, particularly where applicants have been rejected or treated differently from other applicants.[942] Applicants are not allowed to exercise these rights if the results of the psychological test constitute one of a number of factors considered by the employer in taking the employment decision.[943] More importantly, the Employment Practices Code advises employers to ensure that psychological tests are administered and their results interpreted only by qualified persons or persons with appropriate training.[944]

At policy level, professional bodies such as the British Psychology Society ("BPS") has also tried to develop an industry standard and to provide best practice guidelines on the use of psychometrics in the workplace, aimed at assuring quality, fairness and

[940] Employment Practices Code 20.
[941] Employment Practices Code 20.
[942] Employment Practices Code Guidance 13.
[943] Employment Practices Code Guidance 14.
[944] Employment Practices Code 20 and Employment Practices Code Guidance 14.

ethics in the use of these tests.[945] In this regard, for instance, an employer who is interested in carrying out psychometric testing in his or her workplace may consult the BPS's directory of Chartered Psychologists to gain independent advice from a BPS registered psychologist about the use of such testing.[946]

6.3.2.2 Case Law

There appears to be few reported cases directly addressing the issues of psychological testing and privacy in the employment context. However, the issue of psychometric testing or assessments in the context of discrimination has been considered by United Kingdom tribunals and the European Commission.

The Employment Appeal Tribunal decision in *Teva (United Kingdom) V Goubatcher*[947] concerned a race discrimination claim brought against an employer after the employee was not promoted to the position of deputy team leader. The employer had chosen to appoint a candidate who had scored 2 more marks more at the interview and 3 marks more in written tests than the employee. The Employment Tribunal reasoned that an adverse inference could be drawn from the employer's conduct as it had failed to provide adequate and satisfactory reasons for its decision to prefer another candidate over the employee. The Employment Tribunal concluded that the employer had discriminated against the employee on racial grounds. The Employment Appeal Tribunal took the Employment Tribunal to task for a number of reasons: first, for not explaining how its factual findings had led to its conclusions (particularly how it arrived at the conclusion that the employer's reasons for failing to appoint the employee were racially motivated); secondly, for approaching the issue of the burden of proof erroneously because it had negated to explain why the difference in the scores between the successful candidate and the employee was not treated as a decisive factor against a finding of discrimination; and thirdly, for mistakenly assuming that an unsatisfactory explanation on the part of the employer translated into a presumption of racial discrimination.

---

[945] Cooper, Raker, Maddocks "Occupational Testing Practice: Sustaining Quality Testing Processes through CPD: A Case Study" (1996) 20/7 *Journal of European Industrial Training* 3 – 9.

[946] *Supra*.

[947] Employment Appeal Tribunal (EAT) 27 April 2009.

The applicant in the European decision of *Neophytos Neophytou v Commission of the European Communities*[948] had applied for the position of administrative assistant. Candidates for the position were required to undergo 3 pre - selection tests, 2 written tests and an oral test. In order to be admitted to the written tests, candidates had to obtain a pass mark in respect of each of the pre – selection tests (which were in written form) and only candidates who obtained the highest marks for the written and oral tests were included on the shortlist. The applicant in question contended that the selection criteria applied to him was unjustifiably different to those applied to the other candidates. The applicant based his contention on a number of arguments, which included that the competition notice had stated that candidates who obtained the highest marks in *all* written and oral tests (including the pre - selection tests) would be on the shortlist (and not only candidates with the highest marks for the written and oral tests only). The Civil Service Tribunal dismissed his claim and found that an appointing authority had the discretion to require candidates to undergo pre – selection test for purposes of identifying candidates who qualified for the written and oral tests, which would determine the suitable candidate for the position.

Although the decision did not delve into whether or not use of the tests was discriminatory, the decision nonetheless appears to suggest that employers have a fairly unfettered discretion to use psychometric testing to shortlist candidates or to identify which candidates qualify for the written and oral tests which will finally determine who should be employed.

6.3.3 United States

Personality or psychological tests were first used by the United States military in both World Wars to identify soldiers who were likely to 'freeze' or experience shell shock in battle.[949] The tests were subsequently developed for use by employers in the employment context. According to the United States Equal Employment Opportunity Commission ("EEOC") a number of United States employers use psychometric tests which assess, amongst other things, reasoning, perceptual speed and accuracy,

[948] Case F -22/05.

[949] Stabile "The Use of Personality Tests as a Hiring Tool: Is the Benefit Worth the Cost?" (2002) 4 *University of Pennsylvania Journal of Labour & Employment Law* 279. See also Menjoge "Testing the Limits of Anti – discrimination Law: How Employers Use of Pre-employment Psychological and Personality Tests Can Circumvent Title VII and the ADA" (2003) 82 *North Carolina Law Review* 326 329.

memory, reading comprehension and arithmetic skills.[950] For instance, in *EEOC v Ford Motor Co. and United Automobile Workers of America*[951] the use of a written test for skilled trades apprentice positions in Ford Motor Company came under scrutiny. In this case a nationwide class action was instituted on behalf of African Americans who were rejected for apprentice positions at Ford Motor Company after taking the test. The test used in this case is known as the Apprenticeship Training Selection System and is a cognitive test that seeks to evaluate mechanical aptitude by measuring verbal, numerical, and spatial reasoning.

The EEOC rightly cautions that although the use of these tests can be effective in determining which employees are qualified for a position, their use may violate anti - discrimination legislation. This is particularly so where an employer uses tests which intentionally or unintentionally (in their effect) discriminates on the grounds of race, colour, religion, sex and national origin and thus violates Title VII of the Civil Rights Act[952] ("Title VII").[953] Notably in this regard, is that the use of psychological testing in the United States played a significant role in the development of the notion of indirect discrimination (also called the "disparate impact model" of discrimination endorsed in *Griggs v Duke Power Co*[954]. For instance, the applicants in *EEOC v Ford Motor Co. and United Automobile Workers of America* (mentioned above) contended that, although the ATSS had been validated over a decade before the action was instituted, statistics indicated that it had a significant disparate impact in excluding African American applicants. A settlement was reached between the parties as Ford agreed to replace the ATSS with a less discriminatory employment selection procedure and to pay $8.55 million in monetary relief. [955]

6.3.3.1 Legislation

The use of personality tests increased markedly after the enactment of the Employee Polygraph Testing Act[956] ("EPPA").[957] The EPPA restricts the use of polygraph tests

[950] http://www.eeoc.gov/policy/docs/factemployment_procedures.html (2010 05-23).
[951] No. 1:04 – CV – 00845 (S.D. Ohio June 16, 2005).
[952] Act of 1964.
[953] http://www.eeoc.gov/policy/docs/factemployment_procedures.html (2010 05-23).
[954] 401 U.S. 424 (1971).
[955] http://www.eeoc.gov/policy/docs/factemployment_procedures.html (2010 05-23).
[956] Act of 1998.

in the employment context[958] and was enacted in response to complaints and evidence of the abuse of such tests by employers in the private sector. As such, the EPPA specifically prohibits the use of polygraph tests and similar devices by private sector employers.[959] The legislative history of the Act indicates honesty tests are not covered by the Act's prohibition. To be precise, the Act expressly excludes honesty tests in its definition of the term "lie detector". [960]

Title VII permits psychometric or psychological tests (and other forms of employment tests such as physical ability tests, sample job tests and medical tests) provided such tests are not designed, intended or implemented to discriminate on the grounds of race, colour, religion, sex or national origin.[961] Title VII further prohibits employers, from adjusting the scores of, using different cut-off scores for, or otherwise altering the results of, employment related tests, including psychometric tests, on the basis of race, colour, religion, sex, or national origin.[962]

Both disparate treatment (direct) and disparate impact (indirect) discrimination are prohibited under Title VII in relation to the use of the tests.[963] Disparate treatment discrimination refers to intentional discrimination based on race, colour, religion, sex and national origin. An employer is prohibited from, for example, requiring only its' black employees from undergoing a psychometric test aimed at assessing their reading comprehension and not requiring its' white employees to undergo a similar test.[964] Disparate impact discrimination, on the other hand, refers to discrimination which appears neutral but has the effect of disproportionately excluding persons based on race, colour, religion, sex and national origin. This would involve the use of psychometric tests which have such an effect and are not job related and inconsistent with business necessity.[965] The disparate impact model of discrimination recognises that although certain employment practices and policies are implemented without the

---

[957] Stabile "The Use of Personality Tests as a Hiring Tool: Is the Benefit Worth the Cost?" (2002) 4 *University of Pennsylvania Journal of Labour & Employment Law* 279 282.

[958] § 2002 (1) – (4).

[959] § 2002 (1) – (4).

[960] Hebert *Employment Privacy Law* (2009) § 7:10.

[961] 42 U.S.C. § 2000e -2(h).

[962] 42 U.S.C. § 2000e -2(l).

[963] SEC. 2000e – 2(a) and (e) and SEC. 2000e – 2(j).

[964] SEC. 2000e – 2(h).http://www.eeoc.gov/policy/docs/factemployment_procedures.html (2009-05-23).

[965] http://www.eeoc.gov/policy/docs/factemployment_procedures.html (2009-05-23).

intention of discriminating against anyone or a group, their effect or impact is to exclude certain individuals or groups "disproportionately in comparison with other privileged groups".[966] It is however important to bear in mind that Title VII expressly excludes all state owned entities from the ambit of the Act.[967]

The Americans with Disabilities Act [968] ("ADA") prohibits the discrimination against employees by both public and private sector employers on the basis of disability. Provisions of the ADA further restrict the medical examination of employees and job applicants.[969] Of particular importance, the ADA's restrictions apply to any employee and job applicant (not just disabled employees and applicants).[970] As such, the ADA may have implications for the use of psychological testing by employers if psychological tests qualify as "medical examinations" in terms of the Act. That said, the Act and its regulations offer no definition for the term "medical examinations". The Act does, however, define the term "disability" to include psychological disorders and as such courts may consider a psychological examination administered, with the purpose of determining the suitability of an individual for a position, to be a medical examination. [971]

On the contrary, it is also possible that courts may not consider psychological testing administered for the sole purpose of identifying individuals with undesirable personality traits to constitute medical examinations covered by the ADA. This is so, particularly in light of The Equal Employment Opportunity Commission ("EEOC") Enforcement Guidance on Pre – Employment Inquiries under Americans with Disability Act of 1995. The EEOC's enforcement guidance excludes these tests from the definition of "medical examination". The enforcement guidance suggests

[966] http://www.eeoc.gov/policy/docs/factemployment_procedures.html (2009-05-23).

[967] 42 U.S.C. § 2000e.

[968] Act of 1990.

[969] Job applicants may be required to submit to medical examinations provided a conditional offer of employment has been made and all the applicants are subjected to the examination (42 U.S.C.A. §12112 (c)(2), 3). Employees may be required to submit to medical examinations provided the examination is related to requirements of the job and is consistent with business needs of the employer (42 U.S.C. A. §12112 (c)(4); 29 C. F. R. §1630.14 (c)). See Hebert *Employment Privacy Law* 2009 § 7: 11.

[970] See The Employment Opportunity Commission Guidance (EEOC) on Disability Related Inquiries and Medical Examinations of Employees Under the Americans With Disabilities Act of 2000 suggesting the ADA restrictions apply to any employee and job applicant. See also US Court of Appeal decision of *Karraker v Rent – A – Center, Inc*., 239 F. Supp. 2d 828, 834 – 836, 13 A.D Cas. (BNA) 1639 (C.D. III. 2003). See also Hebert *Employment Privacy Law* (2009) § 7: 11.

[971] Hebert *Employment Privacy Law* (2009) § 7: 11.

psychological tests administered for the purpose of ascertaining an individual's general psychological health or the presence of a mental disorder or impairment are "medical examinations" within the scope of the ADA, whereas psychological tests administered for the purpose of ascertaining personality traits such as honesty, preferences and habits fall outside the definition of "medical examinations" as defined in the Act[972].[973]

In addition to the abovementioned federal legislation, several states have enacted their own statutes regulating psychological and honesty testing. The majority of state legislation does not prohibit employers entirely from requiring employees to submit to psychological tests. The legislation instead restricts the manner in which employer may use psychological testing.[974] To illustrate, Alaska prohibits state employers from requiring employees to submit to psychological testing that is structured in such a way as to elicit information unrelated to employment requirements, namely, information that is related to an individual's sexuality or an individual's religious beliefs or practices, or political affiliation.[975] California expressly prohibits both public and private sector employers from requiring an applicant to submit to a psychological examination before a conditional offer of employment is made.[976] Other states such as New York and Pennsylvania require the psychological testing of employees in specified positions or occupations. The New York statute, for example, requires that applicants for positions as correctional officers be subjected to at least three psychological instruments.[977] Pennsylvania, on the other hand, requires candidates for

[972] See *Grenier v Cyanamid Plastics, Inc*., 70 F3d 667 (CA 1 1995) where the United States Court of Appeals held psychological examinations do not constitute medical examinations under the ADA and were as such prohibited before a conditional offer of employment was made. The court however held such examinations may be allowed if their purpose was not to ascertain the existence of a disability but to ascertain whether an applicant was able to perform specific job functions.

[973] Psychological tests like the Minnesota Multiphasic Personality Inventory (MMPI) would be considered "medical examinations" in terms of the EEOC guidance given that it assesses personality and psychological abnormalities. Honesty tests like the IFIB Personality Test which reflect an individual's propensity to lie would not be considered "medical examinations". Hebert *Employment Privacy Law* (2009) § 7:12.

[974] Hebert *Employment Privacy Law* (2009) § 7: 13.

[975] Hebert *Employment Privacy Law* (2009) § 7: 14.

[976] Hebert *Employment Privacy Law* (2009) § 7: 13.

[977] Hebert *Employment Privacy Law* (2009) § 7: 13.

lethal weapons training to be subjected to psychological testing for purposes of excluding individuals that are mentally unfit or unstable.[978]

6.3.3.2 Case Law

Griggs v Duke Power Co[979] concerned a group of black employees who brought a class action against an employment practice implemented by their employer, Duke Power Company ("DPC"). The employer required a high school education or the passing of standardised general intelligence tests (i.e. psychometric tests) as a condition of employment in or for the transfer between jobs. The two tests that employees were required to pass were the Wonderlic Personnel Test, which purports to measure general intelligence, as well as the Bennett Mechanical Comprehension Test,[980] which purports to measure mechanical aptitude.[981] The employees in *Griggs v Duke Power Co* alleged that the practice was a violation of Title VII. At issue was whether an employer was prohibited by the Civil Rights Act from requiring a high school education or the passing of general standardised intelligence and aptitude tests as a condition of employment in or transfer to jobs where:

1. neither standard is shown to be significantly related to successful job performance;
2. both requirements operate to disqualify black employees at a substantially higher rate than their white counterparts; and
3. the jobs in question formerly had been filled only by white employees as part of a longstanding practice of giving preferences to whites.[982]

The District Court found that although the employer had, prior to the enactment of the Civil Rights Act, implemented a policy which openly discriminated on the basis of race in the employment and assignment of its employees, the policy had now ceased. The District Court also found that because the Civil Rights Act was forward looking in nature, the impact of prior inequalities was beyond its reproach.[983] The District Court concluded that there was no racial motive or purpose underlying the adoption of the requirements of a high school diploma and the passing of the tests and, in any

[978] Hebert *Employment Privacy Law* (2009) § 7: 13.
[979] 401 US 424.
[980] 428.
[981] http://www.personality-and-aptitude-career-tests.com/bennett-mechanical-test.html (2009 -05-20).
[982] 425 – 426.
[983] 428.

case, these requirements had been applied fairly to both black and white employees alike.[984]

The Court of Appeals agreed with the District Court in finding that in the absence of a discriminatory purpose, the requirement of a high school education or the passing of standardised general intelligence tests as a condition of employment in or transfer of jobs was permitted by the Civil Rights Act. It further rejected the claim that because these requirements operated to exclude a markedly disproportionate number of black employees, they were unlawful under the Civil Rights Act unless it could be shown that they were job related.[985] In other words, the employer had adopted the requirements of a high school diploma and the passing of standard intelligence tests without the intention to discriminate against black people.

Ultimately, the United States Supreme Court pointed out the object of Title VII was to achieve equality in employment opportunities for all races and to remove employment barriers which had the effect, in the past, of favouring white employees over other employees. As such, employment practices and procedures or tests which appear neutral on their face or in terms of their intent had to be eradicated because they perpetuated discriminatory employment practices and policies.[986] The United States Supreme Court agreed that DPC's intent may not have been to discriminate against blacks "but good intent or absence of discriminatory intent does not redeem employment procedures or testing mechanisms that operate as "built – in headwinds" for minority groups and are unrelated to measuring job capability".[987] The Supreme Court held this after it determined that neither requirement was job related because the evidence showed that employees who had not met either requirement continued to perform satisfactorily in their jobs.[988]

In *Mckenna v Fargo*[989] applicants for the position of fire fighter were required, in terms of a New Jersey statute, to undergo psychological testing for the purpose of selecting applicants likely to withstand the psychological pressures of fighting fires

[984] 429.
[985] 429.
[986] 429 – 430.
[987] 432
[988] 431.
[989] 451 F Supp 1355.

and living in close quarters. The applicants led evidence indicating the psychological tests they were required to undergo consisted of questions which inquired into "religious beliefs, political opinions, reading habits, sexual preferences, social beliefs, familial relationships". The applicants argued that the tests violated their constitutional right to privacy. The Court observed that the "degree and character of disclosure" required by the personality tests amounted to an intrusion on the privacy interest in non-disclosure of personal information:

> "The evaluation looks deeply into an applicant's personality …fire fighter candidates are called upon to reveal the essence of their experience of life, the collective stream of thoughts and feelings that arise from the ongoing dialogue which individuals carry on between the world and themselves in the privacy of their being. It involves a loss of the power individuals treasure to reveal or conceal their personality or their emotions as they see fit, from intimacy to solitude".[990]

In balancing the interest of the employer in promoting an efficient fire department and the applicants' interest in preserving aspects of their personality, the Court concluded that the employer not only had a compelling interest in promoting an efficient fire department, but also in its psychological evaluation and hiring procedure:

> "… the psychological evaluation and hiring procedure taken as a whole is useful in identifying applicants whose emotional make – up makes them high risk candidates for the job of fire fighting. Because fire fighting, like police work, involves life – endangering situations, the State interest is of the highest order…a fireman who loses emotional control endangers his own life as well as those of other firemen. While a psychological evaluation intrudes on an applicant's privacy, it may save him from risk of losing his life. The life of a community, as well, depends, at the most basic level, on whose job it is to protect the community from physical forces, like fire, that have escaped from the control that makes them productive. Property, and security of the

[990] 1380 – 1381.

> community, as well as lives, are at stake in improving the fire department".[991]

In *Redmond v City of Overland Park*[992], the plaintiff, a probationary police officer, alleged that the defendants (city, police officials and consulting psychologists and psychiatrists) violated her constitutional right to privacy in discussing and exchanging her personal information with one another. The Court established that because the plaintiff had signed a release permitting the psychiatrists to disclose her records to the police department she had no privacy interest in the psychiatrist's or psychologists records. The Court further reasoned that the police officials had an interest in disclosing and obtaining information concerning the plaintiff as they had to ensure the plaintiff's ability and fitness to serve as a police officer.[993] Finally, the Court found that the city was justified in requiring the plaintiff to undergo psychological testing[994] as it also had an interest in ensuring the plaintiff was fit to serve as a police officer and this interest outweighed her "narrow" privacy interest in preventing the disclosure of the personal information.[995]

The appellants in *Soroka v Hudson*[996] were required to submit to a personality test for the position of store security officer for a large retail chain. The purpose of the test was to screen out emotionally unfit candidates and consisted of over 700 true or false questions, some of which related to religious attitudes and sexual orientation. The applicants argued that the questions posed in the test were not job related and violated their constitutional right to privacy. The court found that although the employer had an interest in employing emotionally stable persons for the position of store security officer, such an interest was not furthered by requiring applicants to respond to questions relating to religious attitudes and sexual orientation.[997]

---

[991] 1381.
[992] 672 F. Supp. 473.
[993] 483.
[994] *Supra*.
[995] 484.
[996] 1 Cal. Rptr. 2d 77.
[997] 86.

6.3.4 Analysis

Employers argue that the use of psychological testing enables them to employ suitable employees. However, the tests infringe the privacy interests of test subjects because they may consist of questions which are highly personal and sensitive in nature. South Africa (as do the other jurisdictions under review) has discrimination legislation (the EEA) regulating the use of these tests in employment. However, the legislation primarily aims to protect applicants and employees against the biased use of these tests. In other words, the legislation does very little to protect the privacy interests of applicants and employees. In addition, South African courts have yet to deal with the issue of the privacy concerns raised by the use of the tests. The United Kingdom's DPA directly restricts the use of the tests in employment and the Employment Practices Code and the Employment Practices Code Supplementary Guidance provide United Kingdom employers with detailed guidelines in using the tests. This, to some extent, addresses concerns about the protection of the privacy interests of applicants and employees. The United States experience shows that privacy in the current context can be protected through use of discrimination legislation or reliance on the constitutional protection of privacy. At the same time, it is clear that United States courts have been willing to uphold (highly invasive) testing of employees in safety sensitive positions.

6.4 POLYGRAPH TESTING

The polygraph relies mainly on a subject's physiological reactions or changes in blood pressure, heart rate, pulse rate, respiration and perspiration to a set of questions to draw an inference on the subject's truthfulness. There has been much debate as to whether the polygraph can produce empirically and scientifically reliable results.[998]

[998] The US in its 1983 Office of Technology Assessment concluded that there was limited evidence for establishing the validity of polygraph testing. The assessment further concluded that polygraph accuracy may be affected by a series of factors including: the training, orientation and experience of the examiner, the examinee's emotional stability and intelligence, the use of countermeasures and the examinee's willingness to be tested. Finkin *Privacy in Employment Law* (2003) 117. Similar concerns regarding the reliability and accuracy of polygraph testing have been expressed by South African legal commentators. See for example Christianson "Polygraph Testing in South Africa Workplaces: Shield and Sword in the Dishonesty Detection versus Compromising Privacy Debate" (2000) 21 *Industrial Law Journal* 17 and Tredoux and Pooley "Polygraph Based Testing of Deception and Truthfulness: An Evaluation and Commentary" (2001) 22 *Industrial Law Journal* 819. Tredoux and Pooley correctly point out that polygraphs do not measure the presence or absence of deception or lying (in fact there is no known instrument that directly records whether a subject is lying or deceptive) but merely measure a subject's physiological activity.

This uncertainty about the validity and reliability of polygraph testing has to some extent filtered through to case law on the admissibility of the results of polygraph testing as evidence.

6.4.1 South Africa

In South Africa, the results of polygraph tests have, on occasion, been used as evidence against employees in disputes about unfair dismissal. Before *Sosibo & Others v Ceramic Tile Market*[999] commissioners and arbitrators treated the issue of the admissibility of the evidence provided by polygraph tests inconsistently. On the one hand, some commissioners showed a reluctance to readily accept the admissibility of polygraph tests[1000] while other commissioners accepted the admissibility of the tests, such as in *SACCAWU obo Sydney Fongo v Pick 'n' Pay Supermarkets*[1001] (where the commissioner was prepared to accept that polygraph tests provide "96% of the truth"). South African tribunals have even gone so far as to construe an employee's oral or written agreement to undergo a polygraph test as a waiver of that employee's right to privacy.[1002] As correctly observed by the commissioner at the time *Sosibo & Others v Ceramic Tile Market*[1003] was decided, there is no clear approach to the admissibility of polygraph test results. There are instead divergent approaches to the admissibility of polygraph test results, summarised as follows:

a) polygraph test evidence is unreliable and inadmissible and no adverse inference is to be drawn if an accused employee refuses to undergo such a test;[1004]

---

[999] (2001) 22 ILJ 811 (CCMA).

[1000] See *Jacob v Unitrans Engineering*(1999) KN21921(the commissioner stated that it would be absurd to assume that a man is guilty simply because he exercises a legitimate right to refuse to submit to a test or answer a questionnaire). See also *Sosibo & Others v Ceramic Tile Market* (2001) 22 ILJ 811 (CCMA), *Stern Jewellers and SACCAWU* (1997) NP144 and *Mahlangu v CIM Deltak* (1986) 7 ILJ 346 (IC).

[1001] (2000) FS 15555.

[1002] In *Mncube* an employee had been dismissed on charges relating to theft, bribery, fraud, dishonesty, forgery and bringing the name of the employer into disrepute. In order to resolve the dispute the employee consented to a polygraph. The commissioner held that the applicant had consented to the polygraph test and consequently concerns about privacy and free will did not feature in the circumstances

[1003] (2001) 22 ILJ 811 (CCMA).

[1004] *Kroutz v Distillers Corporation Ltd* 1999 8 BLLR 912 (CCMA) and *Jacob v Unitrans Engineering* (1999) KN21921.

b) polygraph test evidence is not admissible if there is no evidence on the qualifications of the polygraphist and if the polygraphist is not called to give evidence;[1005]

c) polygraph test evidence is admissible as expert evidence but cannot on its own prove an accused employee's guilt. That is to say, polygraph tests alone cannot prove a person's guilt without corroborative evidence to support the inference of guilt;[1006]

d) polygraph test evidence may be taken into account where there is no other supporting evidence.

6.4.1.1 Legislation

Section 8 EEA prohibits psychological and similar assessments in employment unless the assessments are unbiased, scientifically valid and reliable and can be applied fairly to all employees. For polygraph tests to fall within the ambit of the EEA they have to be classified as psychological or similar assessments. Polygraph tests are clearly not psychological assessments as they measure a subject's physiological reactions to draw an inference of truthfulness. It is further unlikely that a polygraph test can qualify as a "similar assessment", again and in contrast to psychological or psychometric tests, because they do not measure personality traits. Moreover, because the scientific validity and reliability of polygraph testing remains a matter of debate, polygraph testing is likely to fall outside the provisions of the EEA.[1007]

Christianson has argued that the use of polygraph testing in the South African workplace and the inconsistent way in which polygraph testing has been treated, warrant the enactment of legislation similar to that of the United States EPPA, designed to control the use of polygraphs by employers.[1008] Legislation similar to the United States EPPA in South Africa would require that guidelines be created for

[1005] *Kleyhans v Tremac Industries* 2001 5 BALR 469 (CCMA) and *Stern Jewellers v SACCAWU* (1997) NP 144.

[1006] *Metrorail v SATAWU obo Makhubela* 2000 5 BALR 599 (IMSSA) ;*Ndlovu v Chapelat Industries* (Pty) Ltd 1999 8 BALR 996 (IMSSA) and *Smith v Canoa Eastern Cape* (2000) 12 BALR 1436 (CCMA).

[1007] Christianson "Polygraph Testing in South Africa Workplaces: Shield and Sword in the Dishonesty Detection versus Compromising Privacy Debate" (2000) 21 *Industrial Law Journal* 17 36. See also *PETUSA obo Van Schalkwyk v National Trading Company* (2000) 21 ILJ 2323 (CCMA).

[1008] Christianson "Polygraph Testing in South Africa Workplaces: Shield and Sword in the Dishonesty Detection versus Compromising Privacy Debate" (2000) 21 *Industrial Law Journal* 17 36. See also *PETUSA obo Van Schalkwyk v National Trading Company* (2000) 21 ILJ 2323 (CCMA).

adjudicators pertaining to the admissibility, reliability and weight to be given to polygraph test results in an effort to create consistency and uniformity.[1009] Despite a preference for the cautionary approach in *Sosibo*, some decisions have continued to make unequivocal pronouncements on the inadmissibility of polygraph test results and even to question the role of polygraphers as expert witnesses as nothing more than subjective opinion. In *Steen v Wetherlys (Pty) Ltd*[1010] the commissioner held that:

> "[t]o date there is nothing either in the body of research or in the authority of any case law to convincingly suggest that polygraphers are in fact expert witnesses or that they are medically qualified to interpret the physiological responses of witnesses…In addition such evidence is inconclusive, and does no more than to indicate that the subject was in a heightened state of general emotional arousal. It does distinguish anxiety, stress/tension or indignation from guilt…The polygraphist is often a stranger and the test may be given in an unfamiliar environment. This alone may cause increased nervousness and physiological responses in the body. A further factor is the natural fear in the mind of the innocent that the tests results may not correctly reflect his innocence."[1011]

6.4.1.2 Case Law

In *Sosibo* the commissioner found that a number of previous decisions approached the question of the admissibility of polygraph tests with caution and prudence. For

[1009] Tredoux and Pooley "Polygraph Based Testing of Deception and Truthfulness: An Evaluation and Commentary" (2001) 22 *Industrial Law Journal* 819 839. Christianson on the other hand is of the view that legislation such as the EPPA would be unnecessary and undesirable in that it would accord too much significance to a technique that should be utilized as an occasional tool.

Christianson "Truth, Lies and Polygraphs: Detecting dishonesty in the Workplace" (1998) 18 *Contemporary Labour Law* 1 10.

[1010] [2006] 2 BALR 222 (CCMA).

[1011] 227 A - C. The commissioner in *Steen* further questioned the role of polygraphers as expert witnesses: "In essence the research shows that polygraphers are deemed to be expert witnesses…while there is nothing to show that they are in fact expert witnesses. They may very well be self-appointed or self-acclaimed "experts' in an industry that does not have objective standards against which results of the interpretation thereof can be tested…The polygraphist is able to conclude only two things – the results suggest "deception' or "no deception'. The polygrapher thereafter guesses what the result means for he has no medical or pharmaceutical training or knowledge to assist him in his analysis of the result, and is simply not able to determine what effect any medication, mood swing or emotional state may have on the results recorded." See also *MEWUSA obo Mbonambi v S Bruce CC t/a Multi Media Signs* [2005] 8 BALR 809 (MEIBC) where the arbitrator concluded an employee cannot be convicted on the strength of a polygraph test alone and additional circumstantial evidence was needed to justify admission and acceptance of the polygraph test results.

instance, in *Mahlangu v CIM Deltak*[1012] the court concluded that voice analysis tests conducted by persons not registered as psychologists were unscientific, unreliable and illegal. In *Mncube v Cash Paymaster Services (Pty) Ltd*[1013] it was accepted that the polygraphist who conducted the test was qualified but the question was raised whether the evidence was reliable. The commissioner in *Sosibo* further observed that there was no clear approach as to the admissibility of polygraph test results. There were instead divergent approaches to the admissibility of polygraph test results, already referred to above. In *Sosibo* it was also observed that generally tribunals take a cautionary approach to the reliability of polygraph evidence, in that polygraph tests alone cannot prove a person's guilt without corroborative evidence to support the inference of guilt. It was furthermore noted that such a cautionary approach is also followed in foreign jurisdictions such as the United States. In *Sosibo* 3 reasons (as they related to the facts in issue) were identified as justification for such an approach:

a) The person administering the tests, while an expert in the polygraph field, was neither a qualified doctor nor psychologist;
b) The tests were simply an indicator of deception and could not give details on the extent of the misconduct;
c) The sole reliance on the polygraph results was insufficient to discharge the onus on the employer in terms of s192 of the Labour Relations Act of 1995 to prove the dismissal was fair. [1014]

6.4.2 United Kingdom

Polygraph testing in the United Kingdom has been mostly used in criminal investigations and much of the published research on polygraph testing concerns the use of these tests in criminal investigations. The British Psychological Society ("BPS") defines a polygraph as "a set of equipment that accurately measures various sorts of [mental] and bodily activity such as heart rate, blood pressure, respiration, and palmar sweating".[1015] The BPS, in its Working Party Report[1016] strongly questioned the reliability and accuracy of polygraph testing and found that published reports on

[1012] (1986) 7 ILJ 346 (IC).
[1013] (1997) 5 BLLR 639.
[1014] (2001) 22 ILJ 811 (CCMA) 522 - 523.
[1015] The British Psychological Society *A Review of the Current Scientific Status and Fields of Application of Polygraphic Detection* Working Party Final Report (6 October 2004).
[1016] The British Psychological Society *A Review of the Current Scientific Status and Fields of Application of Polygraphic Detection* Working Party Final Report (6 October 2004).

the use of polygraph testing in the employment context pointed to its ineffectiveness in identifying employees who are likely to engage in counter - productive behaviour or criminal activity in the workplace.[1017] As such, polygraph testing may not meet the DPA requirement that data be processed fairly and lawfully, because its scientific validity and reliability is questionable.[1018]

6.4.2.1 Legislation

As indicated in the earlier discussion of both background checks and psychometric testing, the DPA regulates the processing of personal and sensitive data.[1019] It was also pointed out that the DPA does not prevent employers from processing sensitive data, but limits the circumstances under which such data can be processed. The use of polygraph tests entails the processing of personal and sensitive data by an employer, because these tests give information to employers about the commission of an offence by an employee or information that is to form part and parcel of the proceedings to determine whether any offence has been committed. This of course, is said on the assumption that the polygraph test is used to determine whether an employee committed a specific offence against the employer. United Kingdom employers making use of polygraph testing will have to observe the DPA requirements in relation to the processing of personal and sensitive data. In this regard, the DPA requires an employer to obtain the explicit and unequivocal consent of an employee before subjecting an employee to a polygraph test, failing which the use of the polygraph in such an instance will be unfair and unlawful. The DPA would also require the employer to notify an employee of all intended purposes of the results which the polygraph test will produce, even where the intended purpose appears obvious. Notably, the Employment Practices Code does not provide employers with detailed guidelines on using polygraph tests in the workplace. This could be due, as

---

[1017] According to the authors Grubin and Madsen the report came about after the BPS assembled a working group to investigate the reliability, validity and ethical concerns associated with the use of the polygraph in the employment vetting process and in criminal investigations. Grubin and Madsen "Lie Detection and the Polygraph: A Historical Review" 2005 16 (2) *The Journal of Forensic Psychiatry & Psychology* 357 – 369, 365.

[1018] *Supra*.

[1019] Notably, the Court of Appeal in *Durant v Financial Services Authority* [2003] EWCA Civ 1746 clarified what was meant by "personal information". The court explained that personal data was not merely information bearing or mentioning an individual's name but information that has affected the data subject's privacy. The Court further explained the question of whether information is personal data depends on the ambit of such information in a "continuum of relevance and proximity to the data subject".

already mentioned, to reigning doubt about the reliability and accuracy of polygraph testing in the employment context.

6.4.2.2 Case Law

According to Grubin and Madsen, and unlike the position in the United States, the use of polygraph tests in the United Kingdom has generally not been pronounced. This is evidenced by the fact that there exists very little case law concerning the use of polygraph testing by United Kingdom employers.[1020]

That being said, and although there is little case law on the use of the polygraph in the United Kingdom employment context, the issue of polygraph testing in the context of Article 8 (regulating privacy) of the European Convention on Human Rights[1021]("ECHR") was considered in the decision of *R. (on the application of C) v Ministry of Justice*[1022]. The complainant in this matter sought to quash a condition imposed on him on his release from prison, namely, that he submit to polygraph testing. The complainant had been convicted of two counts of rape and indecent assault (one of his victims was his minor daughter). The condition provided that the complainant had "[t]o comply with any instructions given by [his] supervising officer requiring [him] to attend for a polygraph session, to participate in polygraph sessions and examinations as instructed by or under the authority of [his] supervising officer and to comply with any instructions given to [him] during a polygraph session by the person conducting the polygraph session…". The condition was imposed in terms of the Offender Management Act[1023], which provides that an offender manager may in appropriate circumstances impose the polygraph condition. In this case, the offender manager had considered the seriousness of the offences and the unreliability of the complainant in initially admitting the offences and later denying them, as well as a general concern that the complainant will be loathe to voluntarily disclosing information during his supervision. The complainant argued that the polygraph condition was contrary to his rights in Article 8 of the ECHR. The complaint was dismissed by the Court. First, the Court agreed that the imposition of the condition engaged Article 8 and involved a serious intrusion upon the complainant's private life,

[1020] Grubin and Madsen "Lie Detection and the Polygraph: A Historical Review" 2005 16 (2) *The Journal of Forensic Psychiatry & Psychology* 357 – 369, 365.

[1021] Drafted by the Council of Europe in 1950 and came into force on 3 September 1953.

[1022] [2010] H.R.L.R 3, [2009] EWHC 2671 (Admin).

[1023] Act of 2007.

but found the intrusion to be justified as part of a comprehensive arrangement for the supervision and rehabilitation of offenders who had committed very serious sexual offences. The Court further found that, given the seriousness of the original offences committed by the complainant, his conduct and his attitude towards his convictions, it was not disproportionate for him to be subjected to the polygraph condition. This decision shows that there is a close link between polygraph testing and privacy concerns, but that, under appropriate circumstances; justification for testing outweighs these privacy concerns.

6.4.3 United States

Polygraph testing in the United States is regulated by the Employee Polygraph Testing Act[1024] ("EPPA") and varied state legislation. The EPPA was enacted in response to concerns about the abuse of polygraph tests in private sector employment and the validity and reliability of the tests. The Act prohibits most private employers from using polygraph tests before or during employment but allows for employers to request an employee to take a polygraph in connection with an on-going investigation if there is reasonable suspicion that the employee was involved in the incident; and then only if an employer provides the employee with a written statement describing the basis of the reasonable suspicion.[1025] It is important to bear in mind that the EPPA regulates the use of polygraph testing in the private sector and not the public sector.[1026]

6.4.3.1 Legislation

The EEPA prohibits private sector employers from "directly or indirectly" "requiring, suggesting, or causing" an employee or applicant to submit to a polygraph test.[1027] Courts have chosen to construe this aspect of the prohibition strictly to mean that an employer may not request or even suggest an employee voluntarily submit to a polygraph test.[1028] In addition, courts have noted that an employee's request to take a polygraph test in an effort to exonerate himself or herself, for example, does not constitute a waiver of the employee's rights.[1029] Furthermore, an employer may not "indirectly" require an employee to submit to a polygraph test by using other entities

[1024] Act of 1998.
[1025] § 2002 (1) – (4).
[1026] § 2006.
[1027] § 2002 (1) – (4).
[1028] *Polkey v Transtecs* 404 F. 3d 1264 (2005).
[1029] *Blackwell v 53rd – Ellis Currency Exchange* 852 F. Supp. 646.

to make the request or suggestion. The EPPA further prohibits an employer from "using or asking about the results of polygraph tests taken by individuals" and "from discharging, disciplining, discriminating or taking adverse action" against an employee or applicant on the basis of polygraph test results.[1030] This prohibition has been read to mean that an employer may not take or threaten to take adverse action against an employee or applicant based on the results of the test[1031].[1032]

Courts have, despite the EPPA's prohibitions, upheld a private sector employer's decision to submit its employees to polygraph testing, particularly those employees in safety and security sensitive positions. In *Stehney v Perry*[1033], for example, the court upheld the polygraph testing of an employee in the private sector because she performed safety sensitive research for a federal agency charged with national security. The matter concerned an employee of a private non-profit body who performed sensitive research in cryptography for the federal National Security Agency ("NSA"). The employee was dismissed after losing her security clearance and declining to submit to a periodic polygraph test authorised by the NSA. The court found that the NSA's interest in using polygraphs to conduct national security background checks outweighed the employee's privacy interests.

The EEPA does not disallow government, state and local government entities from requiring the polygraph testing of individuals.[1034] For this reason, public employers may require or suggest that employees and applicants submit to polygraph testing. Nonetheless, courts may afford protection to public sector employees required to undergo polygraph testing, if the employee can establish the questions he or she was expected to respond to not only fell within the protected zone of privacy, but were also unrelated to an applicant's ability to perform in a particular position. The applicant in *Thorne v City of El Segundo*[1035], for example, was required to undergo polygraph testing on application for the position of police officer. The Court found the testing had violated her constitutional right to privacy because the employee had been

[1030] § 2002 (1) – (4).
[1031] *Lyles v Flagship Resort Development* 371 F. Supp 2d 597 (2005).
[1032] Hebert *Employment Privacy Law* (2009) § 6: 12.
[1033] 101 F. 3d 925 (3d Cir. 1996).
[1034] § 2006.
[1035] 726 F. 2d 459 (1983).

asked a large number of questions regarding her sexual life and past sexual relationships.

The EPPA further permits federal government to require polygraph testing of experts, consultants, or employees of contractors with government agencies concerned with national security, intelligence and counter intelligence such as the National Security Agency, Federal Bureau of Investigation, Central Intelligence Agency and the Departments of Energy and Defence.[1036]

The Act provides private sector employers with the "ongoing investigation" exemption from its requirements. The exemption allows employers to require employees to submit to polygraph tests "in connection with an ongoing investigation involving economic loss or injury to the employer's business such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage".[1037] The EPPA further exempts certain private employers, namely employers offering security services and drug security (that is manufacturing, distributing or dispensing controlled substances) except where the results of the polygraph or the refusal to take a polygraph test constitutes the sole basis for acting against an employee or applicant.[1038]

The use of polygraph testing in employment is further regulated by state legislation. Broadly, state legislation may directly or indirectly regulate the use of polygraphs in employment.[1039] States such as Connecticut directly regulate the use of polygraphs in employment by prohibiting both private and public sector employers from requesting or requiring an employee or applicant to submit to polygraph testing. The Connecticut statute further prohibits employers from relying on the results of a polygraph test or an employee's refusal to take a polygraph tests in taking adverse employment action. The statute only permits the use of polygraph testing with respect to the employment of non-civilian employees of the police and correctional department.[1040] Iowa's statute does not prohibit all polygraph testing in employment but merely prohibits private and public sector employers from requesting or requiring an employee or applicant to

[1036] Hebert *Employment Privacy Law* (2009) § 6: 12.
[1037] § 2002 (1) – (4).
[1038] Hebert *Employment Privacy Law* (2009) § 6:21.
[1039] *Supra*.
[1040]Hebert *Employment Privacy Law* (2009) § 6:27.

submit to a polygraph test as a condition of continuing employment or of employment.[1041] Other states, like Alabama, only regulate the licensing of polygraph examiners and the instrument used in conducting a polygraph test, but do not regulate or circumscribe the circumstances under which the polygraph testing can be conducted.[1042] States indirectly regulating the use of polygraph testing in employment place a restriction on the nature of questions an employee or applicant may be asked during the testing by for instance, prohibiting questions on an individual's private life which are in no way related to the position sought by the individual.[1043]

Title VII may be violated under the disparate treatment theory if an employer uses polygraph tests in a discriminatory manner or to discriminate against minority employee or applicants.[1044] The issue of whether being required to undergo polygraph testing amounts to "materially adverse" employment action under Title VII came before the Court in *Alford v South Carolina Department of Corrections*.[1045] The employee in *Alford* contended the employer had required him to undergo polygraph testing in retaliation for a racial discrimination claim he had made. The Court held that the requirement did not constitute a materially adverse employment action because it was unlikely to affect a reasonable person's decision to make a racial discrimination claim.[1046]

Even though the Americans with Disabilities Act of 1990 do not directly regulate the use of polygraphs, the Act does restrict employers from enquiring about physical disabilities. According to the Equal Employment Opportunity Commission's Enforcement ("EEOC") on Pre – employment Inquiries Under the American with Disabilities Act, polygraph tests are excluded from the Act's definition of "medical examinations".[1047] The enforcement guidance prohibits employers from making enquiries (prior to administering a polygraph test) related to the existence of factors that might adversely affect the results of the test[1048] By, for example, enquiring about

[1041]Hebert *Employment Privacy Law* (2009) § 6:35.
[1042]Hebert *Employment Privacy Law* (2009) § 6:22.
[1043] Hebert *Employment Privacy Law* (2009) § 6:21
[1044]*Smith v American Service Co. of Atlanta* 611 F. Supp 321 (1984).
[1045]2006 WL 1997434 (D.S.C. 2006).
[1046]Hebert *Employment Privacy Law* (2009) § 6: 12 6:19.
[1047] Section 12102.
[1048] Hebert *Employment Privacy Law* (2009) § 6:20.

an applicant's physical condition or any medication an applicant may be taking. The EEOC's Enforcement Guidance on Disability Related Inquiries and Medical Examinations also excludes polygraph tests from the Act's definition of "medical examination". However, the guidance prohibits employers from making enquiries related to disability during the polygraph test.[1049]

6.4.3.2 Case law

In *Hester v City of Milledgeville*[1050] a group of fire fighters challenged the constitutionality of the city's requirement that fire fighters undergo polygraph tests consisting of control questions. The city argued that the use of control questions improved the accuracy of the polygraph test results and was aimed at promoting public safety by ferreting out drug abuse in the department. The Court stated that, generally, the use of "control questions" tailored to "evoke a deceptive or nervous response from everyone tested" violated the constitutional right to privacy. However, the nature of questions concerned did not implicate the constitution because they avoided personal issues related to "marriage, family and sexual relations".[1051]

The appellant in *Thorne v City of El Segundo* left her employment as a clerk – typist and applied for a promotion to city police officer. As part of the application process the appellant was required to undergo a polygraph test. The evidence before the Court indicated her employment was conditioned on her answering questions about her sex life because, prior to polygraph test, the appellant was given information indicating questions about her sexual behaviour would constitute a significant part of the overall test.[1052] The Court observed that the off – duty personal activities of an individual had no relationship to his or her job performance and are protected by the constitutional guarantee of privacy.[1053] The Court held that the questioning of the appellant regarding her sex life and reliance on the information obtained about her sex life violated her privacy.[1054]

[1049] Hebert *Employment Privacy Law* (2009) § 6:20.
[1050] 777 F. 2d 1492 (11th Cir. 1985).
[1051] 1497.
[1052] 469.
[1053] 471.
[1054] 471.

Moreover, in *Polsky v Radio Shack*[1055] and *State v Community Distributors Inc*[1056], the courts recognised that an employee's willingness to sign a waiver for taking a polygraph test should not be seen as voluntary consent, since the employee may be driven by an economic compulsion to sign the form, leaving him or her little choice.[1057] The Court in *Chesna v United States Department of Defense*[1058], however, found that the employee had "knowingly waived his right to privacy" because the evidence showed he had signed a consent form to undergo polygraph testing. Further, the employee did not argue that he was explicitly deceived, ordered, harassed or intimidated against his will to waive his rights.[1059]

6.4.4 Analysis

Polygraph tests may infringe the privacy of employees because they essentially attempt to penetrate the private inner domain of an individual "by compelling communication of thoughts, sentiments, and emotions which the examinee may have chosen not to communicate".[1060] There is no legislation in South Africa regulating the use of polygraph tests in employment and South African courts have yet to address the privacy implications raised by the use of these tests. Polygraph testing in the United Kingdom appears to be conducted primarily in the criminal context. As such, there seems be little or no need for legislation regulating the use of these tests in employment and, to the extent that regulation is necessary, the DPA seems to offer some protection. The use of polygraph tests in United States employment is regulated by the EPPA. However, the EPPA only restricts the use of these tests in private sector employment. As such, public sector employers are largely unregulated with respect to the use of the tests in employment (barring reliance on constitutional protection of privacy). Moreover, United States courts are likely to uphold the use of the tests for employees in safety sensitive positions and questions are work-related. Discrimination

[1055] 666 F. 2d 824. In *Polsky v Radio Shack*, Polsky brought a claim after she was discharged because of the results of a polygraph test . Polsky argued that the results of the test were obtained in violation of a Pennsylvania statute prohibiting an employer from requiring an employee to submit to a polygraph examination as a condition for employment or continuation of employment.

[1056] 123 NJ Super.589, 304 A.2d, 213 N.J. Co. 1973.

[1057] Christianson "Polygraph Testing in South African Workplaces: Shield and Dishonesty versus Compromising Privacy Debate" (2000) 21 *ILJ* 16 30.

[1058] 850 F. Supp 110 (D. Conn. 1994)

[1059] 116.

[1060] *Long Beach City Employees Association v City of Long Beach* 41 Cal.3d 937, 227 Cal.Rptr. 90 Cal. 198 , 944.

legislation offers only roundabout protection and its application very much depends on the questions asked during testing. Generally speaking, it also seems as if privacy concerns raised by polygraph testing is, to some extent at least, balanced by courts' continued reluctance to rely on the results of polygraph testing as evidence of employees' wrongdoing.

6.5 DRUG AND ALCOHOL TESTING

The previous chapter discussed how employers engage in drug testing in order to identify users of illicit drugs or substances in the workplace and to deter individuals in the workplace from using drugs. This, of course, serves to reduce the incidence of drug related problems such as accidents and illnesses.[1061] The chapter also indicated that some forms of blood testing, such as urinalysis, were more intrusive than others because urinalysis, for example, requires an employee to perform the act of urination which has been described by courts as highly personal and private. Moreover, some commentators observe that urinalysis tends to reveal more than the mere presence of illegal drugs such as the types of medication an employee is taking and whether an employee is epileptic, pregnant or diabetic. The manner in which urine samples are collected also has the potential to intrude on the privacy of employees, especially where the samples are to be provided under direct observation to prevent adulteration or substitution of the sample.

6.5.1 South Africa

South African employers engage in routine and random drug and alcohol testing of employees. It appears from published research that breath alcohol testing is more common than drug testing or blood alcohol testing. Recent research into the management of intoxication in the construction sector revealed that sectors such as construction, private transport and government lacked clear and comprehensive policies on drug and alcohol and engaged in minimal alcohol testing.[1062] The study further found that where such policies exist, their implementation is inconsistent and ineffective.[1063]

[1061] Hebert *Employment Privacy Law* (2009) § 2:5.

[1062] Evans "How to Manage Intoxication Compliance" *Transport World Africa: Multiple Transport Solutions* (2006) Supplement March 26 - 27.

[1063] *Supra*.

6.5.1.1 Legislation

Medical testing is defined in section 1 of the EEA as including "any test, question, inquiry or other means designed to ascertain or which has the effect of enabling the employer to ascertain any medical condition". For drug testing to qualify as "medical testing" in terms of the EEA the drug or alcohol dependency of the test subject has to constitute a "medical condition". It is unclear if drug or alcohol dependency constitutes a medical condition because the EEA does not define the term "medical condition" and the issue has yet to be addressed by our courts. One argument in favour of such an interpretation is that alcohol and drug addiction, as far as dismissal is concerned, is regarded as medical incapacity. Furthermore, the Code of Good Practice: Key Aspects on the Employment of people with Disabilities seems to make it clear that drug and alcohol dependence, which is not based on current use of illegal substances or alcohol and where the employee is in rehabilitation, may qualify as a disability. At the same time, foreign jurisdictions, such as the United States, have excluded drug testing from the definition of medical testing in the context of disability legislation.[1064] While drug addiction is not a protected condition under the Americans with Disabilities Act, a person who uses alcohol is protected if he or she qualified to perform the essential functions of the job.[1065]

Mention must be made that medical testing is regulated by section 7 of the EEA. The section prohibits medical testing unless legislation requires or permits such testing or the testing is justifiable in the light of medical facts, employment conditions, social policy, the fair distribution of employee benefits or the inherent requirements of a job.

Section 8 of the Occupational Health and Safety Act[1066] ("OSHA") places a duty on employers to provide and maintain a safe and healthy working environment. In terms of this duty, employers have to take steps to eliminate and mitigate threats to the safety and health of employees. The regulations issued in terms of OSHA deal expressly with the issue of intoxication in the workplace. The regulations require employers to prevent persons who are or seem to be under the influence of drugs and alcohol access to the workplace and to prevent persons on prescribed medicines from perform their duties if the side effects of such medication pose a threat to health and

[1064] American With Disabilities Act of 1990 as Amended

[1065] http://www.ada.gov/copsq7ag.htm (2009 - 05 - 16).

[1066] Act 85 of 1993.

safety in the workplace. This means that employers may prevent persons under the influence of drugs, alcohol and prescribed medication from performing work that threatens the safety and health of themselves and others. It is difficult to see how employers can meet the requirements of these regulations without infringing on the privacy of their employees by requiring employees to disclose medical conditions (such as AIDS and depression) which they would otherwise prefer to remain undisclosed.[1067]

6.5.1.2 Case Law

South African arbitrators have relied on signs of mental and physical impairment to establish that an employee in under the influence of drugs. Similarly, employers place reliance on:

> "visual evidence regarding the employee's gait, manner of speech and other physical characteristics' in proving an employee's degree of intoxication. The breathalyser test may be used to add weight to evidence or support other evidence led pointing to an employee's state of intoxication".[1068]

Arbitrators appear divided about the evidentiary weight to be placed on breathalyser tests.[1069] However, it is apparent from the cases that the results of a breathalyser test are not conclusive and need to be supported by other relevant physical characteristics.[1070]

The Labour Appeal Court stated the following with regard to determining an employee's state of intoxication:

> "intoxication is a matter of degree…[an employee] would only be 'under the influence of alcohol' if he was no longer able to perform the

[1067] Nell "The Employer's Dilemma: Intoxication and Legislation" (2005) Vol 1 *Risk Management* 13.

[1068] *Cane Carriers (Pty) Ltd and Govender* (1989) ARB 8.11.10 referred to in Grogan *South African Law of Unfair Dismissal* (2002) 303 footnote 74.

[1069] On one hand some arbitrators have found that the results of breathalyser tests constitute sufficient evidence in the absence of evidence on an individual's physical condition. See for example *NUMSA obo Davids/Bosal Africa (Pty) Ltd* [1999] 10 BALR 1240 (IMSSA) where the court found that an employee could be held liable for his state of intoxication even though he was able to operate a heavy duty crane for three hours with alcohol in his blood without causing an accident. See also *Exactics – Pet (Pty) Ltd v Patelina NO & Others* [2006] 6 BLLR 551 (LC). On the other hand other arbitrators have relied on eye witness accounts of an employee's physical condition as evidence of an employee being under the influence of alcohol.

[1070] Grogan *South African Law of Unfair Dismissal* (2002) 303 footnote 74.

> tasks entrusted to him, and particularly the driving of a heavy vehicle, with the skill expected of a sober person. Whether an employee is, by reason of the consumption of intoxicating liquor, unable to perform a task entrusted to him by an employer must depend on the nature of the task. A farm labourer may still be able to work in the fields although he is too drunk to operate a tractor. Consumption of alcohol would make an airline pilot unfit for his job long before it made him unfit to ride a bicycle. The question…is, therefore, whether the respondent's faculties were shown in all probability to have been impaired to the extent that he could no longer properly perform the ….[tasks he or she is employed to do]."[1071]

In *Chetty and Kaymac Rotomoulders (Pty) Ltd*[1072], an employee in a safety sensitive position, challenged his dismissal after testing positive for drugs after a random drug test. Prior to the testing the employee had confided in his superiors about his drug dependency problem and further sought help for his problem. The employee argued that the testing was not random but aimed at dismissing employees known to have a drug dependency problem. The arbitrator took issue with the manner in which the tests were conducted, particularly with the fact that the employee had not been offered the assistance he had been promised after disclosing his drug problem but had been merely dismissed.

The employer in *Yende and Cobra Watertech*[1073] had a zero tolerance policy with respect to being under the influence of drugs at work, was aware of the applicant's cannabis dependency problem and had attempted to assist the employee with rehabilitation instead of dismissing him. The employee tested positive for cannabis and was dismissed by the employer for being under the influence of drugs while performing his duties. The arbitrator found the employee's dismissal substantively unfair because the purpose of the test was not to see if the employee was performing

[1071] *Tanker Services (Pty) Ltd v Magudulela* [1998] JOL 1786 (D) 2 – 3.
[1072] (2004) 25 ILJ 2391 (BCA).
[1073] (2004) 25 ILJ 2412 (BCA).

his duties under the influence of drugs but rather to see if the employee's dependency had decreased.[1074]

The employee in *Mayer and Mind Pearl*[1075] was dismissed for possession and use of drugs in the workplace after a fellow employee reported observing him consume drugs in his work cubicle. The employee denied consuming drugs while at work and stated that he had volunteered to take a blood drug test, but the employer did not require him to take one. The commissioner upheld the dismissal of the employee after hearing expert evidence on the symptoms associated with the use of drugs and evidence from other employees confirming that the employee's performance and behaviour were consistent with symptoms described by the expert witness. Of importance, the commissioner pointed out that there was no obligation on the employer to require an employee to submit to a drug test particularly where there was sufficient evidence to suggest an employee was using drugs.

6.5.2 United Kingdom

The Employment Practices Code includes good practice recommendations on the collection and handling of information from drug testing, which suggests that drug testing does occur in the United Kingdom workplace. Information obtained from drug testing is considered sensitive data in terms of the DPA and as such invokes the sensitive data rules limiting the circumstances in which the information can be processed.[1076] The processing of sensitive information in terms of the DPA requires that the information be processed for a lawful purpose.[1077] An employer, for example, will have satisfied one of the data protection conditions if it requires employees to submit to drug tests in order to meet its health and safety obligations.[1078] The Employment Practices Code guides employers to consider whether the intrusion on the privacy interests of employees is justified for health and safety reasons.[1079]

[1074] 2414.
[1075] AG 2005 26 ILJ 382 (CCMA).
[1076] First Principle of the DPA.
[1077] Employment Practices Code 74.
[1078] Employment Practices Code 75.
[1079] Employment Practices Code 68.

6.5.2.1 Legislation

The Employment Practices Code Guidance suggests drug testing be used only where less intrusive means such as a cognitive ability test or performance assessment cannot provide real evidence of impairment or potential impairment.[1080]

With respect to the different types of drug tests, the Employment Practices Code Guidance cautions employers that regular or periodic drug testing is unlikely to be justified unless the testing is conducted on employees in safety critical positions or there is a reasonable suspicion of drug or alcohol use. The Employment Practices Code Supplementary Guidance further advises employers to conduct post incident testing only where there is evidence that an employee was responsible for an incident.[1081] The Employment Practices Code further cautions employers that random testing of all employees can rarely be justified because different employees pose different risks depending on the nature of their duties[1082]: "For example, a train driver or signal engineer whose actions are impaired through exposure to alcohol or drugs would generally pose a significantly greater safety risk than would a ticket inspector or rail enquiries clerk".[1083] Employers have to ensure, in conducting random drug tests, that the criteria for the testing is genuinely random.[1084] Employers are further advised to avoid testing employees for the purpose of detecting illegal use except where the illegal use breaches the employment contract and can damage the employer's business.[1085] In other words, employers should ideally conduct drug testing for the purpose of ensuring safety at work rather than for detecting illegal use of drugs. Of particular importance, employers have to inform employees of the type of drugs the tests will detect.[1086] Employers have to further inform employees of their alcohol and drug policy and the consequences of breaching the policy.[1087]

[1080] Employment Practices Code Guidance 68.
[1081] Employment Practices Code Guidance 68.
[1082] Employment Practices Code 87.
[1083] Employment Practices Code Guidance 69.
[1084] Employment Practices Code 87.
[1085] Employment Practices Code 87.
[1086] Employment Practices Code 86.
[1087] Employment Practices Code 87.

6.5.2.2 Case Law

Various decisions involving drugs and alcohol policies in the workplace have been considered by the Employment Appeal Tribunal.[1088]

At issue in *South West Trains Ltd v Mr SA Ireland*[1089] was the dismissal of an employee who was employed as a trainman guard. The respondent's duties were considered as safety critical by the appellant and entailed collecting fares from customers, being responsible for passengers on the train and guard duties. The respondent was informed of the employer's drug policy and he indicated that he understood the purpose of the drug policy (which sought to ensure that no employee reported for duty or carried out their duties under the influence of drugs or alcohol). The policy further informed employees that the punishment for a positive result was an automatic dismissal. After the respondent was randomly sampled for drugs along with other employees, his body sample was found to contain traces of cannabis and benzodiazepines and he was automatically dismissed on the basis of the positive test result. An employment tribunal found dismissal of the respondent to be unfair. The tribunal reasoned that because the aim of the policy was safety concerns and not moral concerns, there was no evidence indicating the traces of drugs in the respondent's body sample affected his ability to carry out his duties satisfactorily. The EAT, without referring to the ECHR and its privacy provisions housed in Article 8, disagreed with the decision of the employment tribunal. The EAT held that the tribunal had ignored evidence from a medical practitioner that the respondent was unfit for duty because of the traces of drugs identified in his body and deemed the employer's conduct reasonable in the circumstances.

Article 8 of the ECHR was briefly considered in *O'Flynn v Airlinks The Airport Coach Co Ltd.*[1090] The employee's duties in *O'Flynn* were considered safety critical as they included driving vehicles and serving hot meals in and around an airport. The employer's drug policy informed employees they could be subjected to random screening and that a positive result was tantamount to gross misconduct punishable by dismissal. O'Flynn was dismissed after she disclosed her drug use before her urine sample could be screened following a random workplace drugs test. The employment

[1088] Delaney "Employee Privacy – Grasping the Nettle" (2003) 56 *Employment Law Bulletin* 4 5.
[1089] Appeal No. EAT/0873/01.
[1090] [2002] Emp. L.R. 1217.

tribunal found her dismissal fair and the EAT confirmed the tribunal's decision on the basis of three factors: first, O'Flynn was aware of the policy and its contents and had not contested its implementation; second, O'Flynn's duties raised safety issues; and third, the policy did not interfere with O'Flynn's Article 8 rights, except in requiring that she report for duty drug free. However, any interference with her Article 8 rights would be justified by the fact that her duties raised safety issues.

An in - depth discussion of the relationship between Article 8 and employer drug and alcohol policies was undertaken by the Privy Council in *Whitefield v General Medical Council*[1091] and the European Court of Human Rights in *Wretlund v Sweden*.[1092] The appellant in Whitefield, a registered medical practitioner, appealed against conditions imposed on his registration by the respondent, the Health Committee of the General Medical Council, after the Committee determined that his fitness to practise was seriously impaired by reason of severe depressive illness. The conditions imposed on the appellant included a total prohibition on his alcohol consumption and compliance with arrangements for random testing of his blood and urine. The appellant contended the condition imposing a total ban on his consumption of alcohol interfered with the right to respect for private life and the effect of the ban was to deprive him of enjoyment of social drinking on family occasions. The appellant further contended his Article 8 rights were infringed by the condition that subjected him to random blood testing of his blood and urine. The Privy Council rejected all of the appellant's contentions based on ECHR rights. In respect of the condition banning his total consumption of alcohol, the Privy Council held:

> '[T]the appellant's claim to private life was reduced to the extent that as a doctor he has brought (and is likely to bring) his private life into contact with public life or into close connection with other potential interests. His "right" to an unrestricted social life must give way to the wider public interest in ensuring that he does not present a risk to his patients.'

The Court further held that even if the condition were found to constitute an interference with Article 8 (1), such interference would be justified under Article 8

[1091] Appeal No. 90 of 2001.

[1092] (Admissibility) (Application No. 46210/99) (Unreported, March 9, 2004) (ECHR).

(2). With regard to the condition subjecting the appellant to random blood testing of his blood and urine, the Court was confident that by virtue of Article 8 (2), the condition in question was imposed pursuant to a legitimate aim and was necessary and proportionate:

> 'The Committee was entitled to provide for testing (including random testing) to establish whether or not he had been drinking and to ensure that the appellant knew he was to be subject to such tests and that he might need help in overcoming his addiction as recommended by his medical supervisor.'

At issue in *Wretlund* was the admissibility of a complaint by the applicant that her employer company's compulsory drug and alcohol testing policy infringed on her right to respect for her private life under Article 8 of the ECHR. The applicant was an office cleaner for a nuclear power plant owned by a company, OKG. Although the applicant's duties placed her in a low risk area for radioactivity and did not oblige her to undergo radiological examinations, she was required to undergo drug and alcohol tests every third year. The applicant contended such tests were not justified in relation to her duties and breached her right to respect for her private life under Article 8. The court *a quo* found that the applicant was obliged to participate in the drug test but not the alcohol test. The court *a quo* further reasoned the effect of Article 8 was not a general prohibition on drug testing, but a balancing of competing interests. Upon balancing the applicant's and the company's interests, the court *a quo* found first, that OKG's interest in having a drug – free plant outweighed those of the applicant, given that the risks specific to running a nuclear plant were far – reaching and, secondly, that it was unrealistic to expect OKG, in implementing its policy, to distinguish between employees working in high risk areas within the plant and employees working in low risk areas. The ECHR declared her application as inadmissible. The ECHR agreed with the decision of the court *a quo* and held the requirement that she undergo the drug tests pursued legitimate aims under Article 8 (2), which included public safety and the protection of the rights and freedoms of others. The ECHR further agreed with the court *a quo* that OKG's compulsory blood testing was a measure necessary in a democratic society, because the running of a nuclear power plant required very high levels of security and the use of drugs among employees could threaten security. Finally, the ECHR found the implementation of the policy to

be reasonable and that due regard was given to the applicant's interest by ensuring that the tests were carried out in private, the tests results were disclosed only to persons involved in the policy and the test results were to detect employee drug use and for no other purpose.[1093]

6.5.3 United States

In an attempt to ensure drug free workplaces, public and private sector employers in the United States employ drug testing. United States courts appear to look favourably on government efforts to regulate workplace drug use by testing employees, particularly in safety or security sensitive positions.[1094] Even before the Supreme Court pronounced on the reasonableness of workplace drug testing under the Fourth Amendment in *Skinner* and *Von Raab*[1095], United States courts had established that certain government employees have a diminished or lowered expectation of privacy in this context.[1096]

6.5.3.1 Legislation

A number of federal statutes indirectly regulate drug testing in the public sector. The Rehabilitation Act[1097]defines an "individual with handicaps" as one with "physical or

[1093] Case Comment – "Employment and Discrimination: Compulsory Drug Testing of Employees" (2004) 4 *European Human Rights Law Review* 454.

[1094] Morin "Balancing Public Safety and The Right to Privacy: The New Jersey Supreme Court Affirms Random Testing for Employees Holding Safety – Sensitive Positions" (2000) 10 *Seton Hall Constitutional Law Journal* 455. See for example, in *The Committee for GI rights v Callaway* 518 F. 2d 466 (2 September 1975) in which decision a group of soldiers challenged the constitutionality of a mandatory drug-testing program in the US army. The drug testing programme had several components to it and in circumstances the programme required the testing of soldiers confirmed to be drug abusers and was undergoing active rehabilitation and/or follow up observation. The programme also included searches of soldiers' rooms, property and person (in the form of non-penetrative skin inspections). The court considered whether these searches violated the soldiers' right to privacy and concluded the searches including the drug testing did not violate the soldiers" right to privacy first for a number of reasons. First, the evidence before the Court indicated that the increased abuse of drugs in the Armed Forces posed a material threat to the readiness and effectiveness of the US Army. Second, a soldiers' expectation of privacy in relation to their rooms and personal belongings in army barracks were different to that of a civilian in his home and as such a soldier cannot reasonably expect the army barracks to be a sanctuary like his civilian home. Third, the army implemented the programme in an effort to maintain and preserve the physical and mental capacity of its soldiers for service. Fourth, given the nature of drugs unannounced searches appeared to be the most effective means of identifying drug users to enable them to receive treatment and in eliminating the illegal drugs from the unit. Lastly, the army in permitting the drug inspections had done all that was reasonably practicable to guard the dignity and privacy of the concerned soldiers. Remy "The Constitutionality of Drug Testing of Employees In Government Regulated Private Industries" (1991) 34 *Howard University Law Journal* 633 635.

[1095] 489 US 602 (1989).

[1096] *Supra.*

[1097] Act of 1973.

mental impairment which substantially limits one or more of such a person's major life activities".[1098] Alcoholism and drug addiction have been included in the Act's definition of "physical or mental impairment" and working constitutes a "major life activity".[1099] Consequently, alcoholics and drug addicts would qualify as "individual[s] with handicaps" to the extent that their impairments prevents or limits their ability to carry out employment.[1100]

The Americans with Disabilities Act of 1990 ("ADA") prohibits the discrimination against qualified persons with disabilities. The Act defines qualified persons with disabilities as persons "with a physical or mental impairment that substantially limits a major life activity, but who is able, with reasonable accommodation, to perform the essential functions of the position in question".[1101] On the basis of the ADA's definition of a person with disabilities, an employee whose drug addiction has an adverse effect on his or her ability to work can qualify as disabled. It is however important to note that the ADA excludes employees or applicants currently engaging in the use of illegal drugs from its coverage.[1102]

The Drug –Free Workplace Act[1103] also indirectly regulates drug testing by public employers. The Act in essence places an obligation on federal contractors and recipients of federal grants to make "a good faith effort to provide a drug - free workplace", failing which their contracts and grants can be suspended or terminated. The Act does not require an employer to engage in drug testing in order to provide a drug free workplace, but the Act "encourages" federal contractors and grant recipients to resort to drug testing in an effort to meet the requirements of the Act and in so doing secure their federal contracts and grants.[1104]

A number of states in the United States have enacted legislation directly or indirectly regulating drug testing in employment. Oklahoma's Standards for Workplace Drug

[1098] Section 7(6).
[1099] Section 7(6).
[1100] Hebert *Employment Privacy Law* (2009) § 3:23.
[1101] Section 12102.
[1102] Hebert *Employment Privacy Law* (2009) § 3:24.
[1103] Act of 1988.
[1104] Hebert *Employment Privacy Law* (2009) § 3: 25.

and Alcohol Testing Act[1105] directly regulates the circumstances under which and the manner in which drug testing in employment can be conducted by both private and public sector employers.[1106] The statute permits employers to require applicants to submit to pre – employment testing provided a conditional offer of employment has been made and the testing is required for the position.[1107] Of particular importance, the statute prohibits testing in the absence of a detailed written policy including specifics such as testing procedures, sample handling and purpose of the test.[1108] Moreover, some of the statute's provisions protect the privacy interests of employees and applicants. For example, the statute prohibits direct observation of the act of urination in the process of urine collection and requires an employer to keep information collected in relation to the testing confidential.[1109] Rhode Island has adopted a similar statute regulating the circumstances under which and the manner in which drug testing may be conducted in employment. The Rhode Island statute permits public sector employers to conduct pre – employment testing on applicants for positions in law enforcement, correctional services and fire fighting. Private sector employers may also conduct pre – employment testing to the extent that it is consistent with the requirements of the statute. The statute generally prohibits the testing of employees unless reasonable grounds exist to suggest the employee's ability to perform his or duties is impaired by the use of drugs. Further protection for employees is found in the requirement that employers refer employees who test positive for drugs to professional assistance. An employer may only dismiss an employer who tests positive if further tests reveal the employee is still engaging in illegal drug use.[1110]

The South Carolina statute does not directly regulate testing but instead encourages employers to implement drug prevention programmes and an employer may, as part of the programme, require that employees submit to drug testing.[1111] Pennsylvania's statute concerning unemployment benefits compensation also indirectly regulates testing. The statute provides that an employee who fails to submit to or pass a drug

[1105] Act of 1993.
[1106] Section 2 of the Act.
[1107] Section 2 of the Act.
[1108] Section 2 of the Act.
[1109] Hebert *Employment Privacy Law* (2009) § 4:20.50.
[1110] Hebert *Employment Privacy Law* (2009) § 4:22.50 .
[1111] *Supra*.

test is not eligible to receive benefits to the extent that his or her unemployment is a result of his or her refusal to take a test or failure of the test.[1112]

6.5.3.2 Case Law

Public sector drug testing infringes employees' Fourth Amendment rights to be free from unreasonable search and seizure by the government.[1113]

The Supreme Court in *Skinner v Railway Labour Executives Association*[1114] and *National Treasury Employees Union v Von Raab*[1115] determined that drug testing was a search a seizure under the Fourth Amendment because the collection and analysis of urine samples intrudes upon the privacy expectations of the individuals tested.

Certain public sector employers have argued that there is a distinction between the drug testing of applicants and employees in the same position. This was the argument made by the employer in *Wilner v Thornburgh*[1116] on the basis of the following three reasons: first, the drug testing of an applicant is less intrusive because applicants are often notified of the testing and as such are able to refuse to submit to the testing by withdrawing their job application; second, job applicants have lesser reasonable privacy expectation than employees; third, employers do not have opportunities to observe applicants outside of the pre – employment stage.

The District Court refused to recognise that there was a distinction between the drug testing of applicants and employees. The Court found that the exhaustive background investigation that applicants for the position underwent could serve the government's interest as opposed to drug testing.

The Court of Appeals reversed the District Court's decision and found that applicants had lesser privacy expectations than employees, because they were informed of the requirement for testing and given notice of the testing and as such had control over whether or not they would submit to the testing. The Court of Appeals further found that the fact that applicants underwent an exhaustive background investigation and

---

[1112] Hebert *Employment Privacy Law* (2009) § 4:21.50.

[1113] Marculewicz "Some Tough Questions for Challenges to Pre – employment Drug Testing" (1994) 10 *Journal of Contemporary Health Law & Policy* 243 251.

[1114] 489 US 602 (1989).

[1115] 489 US 656 (1989).

[1116] 738 F Supp 1 (D DC1990), reversed 928 F2d 1185 (CA DC 1991).

were required to provide information of any drug use further diminished their privacy expectations.

Some United States courts have also upheld the testing of public sector employees regardless of whether their duties entail safety sensitive work. In *Loder v Glendale*[1117] the California Supreme Court upheld the pre – employment drug testing of applicants for city positions regardless of the nature of the positions. The Court upheld the testing on the basis of the government's interest in, amongst others, avoiding absenteeism and diminished productivity.

The Fourth Amendment rights to be free from unreasonable search and seizure by government do not however extend to drug testing in the private sector. The constitutional claim by public sector employees and job applicants that drug testing violates their right to privacy does not also extend to private sector employees. However some state courts have extended the reasoning in *Skinner* and *Von Raab* to justify the testing of private sector employees in safety sensitive positions.[1118]

This means that private sector employers can require their employees to undergo drug testing even as a condition of an offer of employment as was the case in *Wilkinson v Times Mirror Corporation*.[1119] In *Wilkinson* the California Court of Appeal found a requirement by a private publishing company that prospective employees submit to a pre – employment drug test did not violate the California state constitution right to privacy provision. The Court held that although the testing infringed on the privacy of the applicants, its intrusiveness was lessened by the following factors: first, applicants for employment in a private business should have reasonably expected to take a pre – employment medical examination which included a drug test; second, the publishing company's policy informed prospective employees the job offer was conditioned on consent to a drug test; and third, the medical examination was designed in such a way that it minimised intrusions into individual privacy.

[1117] 14 Cal 4th 846 (1997).

[1118] For example a New Jersey Supreme Court in *Hennessey v Morin Coastal Eagle Point Oil Company* 129 N.J. 81 (1992) 475 found the discharge of an "at will employee" (employed as a lead plumber whose responsibilities included managing the flow of gasoline) lawful after the employee tested positive after a random drug lawful. The Court held that the public's interest in ensuring that employees in safety sensitive positions are drug free trumped the rights of the "at – will employee".

[1119] 215 Cal. App. 3d 1034 1990.

The Supreme Court in *Skinner* and *Von Raab* determined that drug testing was a search a seizure under the Fourth Amendment because the collection and analysis of urine samples intrudes upon the expectation of privacy. The Court further affirmed that 'where a Fourth Amendment intrusion serves a special governmental need, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectation against the Government's interest to determine whether it is impractical to require a warrant or some level of individualised suspicion in a particular context'.[1120] At issue in *Skinner* was the blood and urine sample testing (authorised by the Federal Railroad Administration regulations) of railroad crews involved in certain accidents and employees violating certain safety rules.[1121] Justice Kennedy reasoned as follows: first, the taking of a blood or urine sample might be characterized as a Fourth Amendment seizure, since it may be viewed as a meaningful interference with the employee's interest in his bodily fluids, therefore intruding upon expectations of privacy that society recognises as reasonable; second, the Government's interest in regulating the conduct of railroad employees to ensure safety, like its supervision of probationers or regulated industries, or its operation of a government office, school, or prison, 'likewise presents 'special needs' beyond normal law enforcement that may justify departures from the usual warrant and probable-cause requirements[1122]; third, the privacy expectation of the concerned employees were diminished by reason of their participation in an industry that is rigorously regulated to ensure safety, a goal which is linked to the health and fitness of its employees; fourth, the compelling Government interests served by the testing regulations would be significantly hindered if railroads were required to point to

[1120] *Von Raab supra* 665. See also *Skinner supra* 619.

[1121] In *Von Raab* the union and union president brought action against United States Customs Service to obtain injunction and to challenge constitutionality of drug-testing program that analyzed urine specimens of employees who applied for promotion to positions involving interdiction of illegal drugs, requiring them to carry firearms or handle classified materials. Justice Kennedy found: first, Custom Service's drug-testing program was subject to reasonableness requirement of Fourth Amendment; second, the a warrant was not required by the Customs Service in order for it to conduct a drug testing program and; lastly, requiring suspicion less drug testing of employees involved in handling illegal drugs or carrying firearms was reasonable under Fourth Amendment.

[1122] This particular reasoning in *Skinner* is sometimes known as the "special needs doctrine" given the court found established the existence of special needs which rendered the drug testing of railroad crews permissible. Wefing "Employer Drug Testing: Disparate Judicial and Legislative Responses" (2000) 63 *Albany Law Review* 799 807.

specific facts giving rise to a reasonable suspicion of impairment prior to testing an employee.[1123]

On the contrary, the United States Supreme Court in *Chandler v Miller*[1124] found that the government had failed to show there were 'special needs' justifying the testing of candidates for state office. At issue was a Georgia statute that required candidates for designated state offices to certify that they have taken a urinalysis drug test within 30 days prior to qualifying for nomination or election and that the test result was negative. Candidates for high office in Georgia brought an action before the Supreme Court challenging the constitutionality of the statute requiring candidates to submit to and pass the drug test to qualify for state office. The Supreme Court in *Chandler* confirmed that the requirement of drug testing infringed the candidate's reasonable expectation of privacy. As to whether this infringement could be justified by a compelling state interest the court held: "…the proffered special need for drug testing must be substantial – important enough to override that individual's acknowledged privacy interest, sufficiently vital to suppress the…normal requirement of the individualized suspicion". The Court found the testing programme to be unconstitutional for several reasons:

a) The state of Georgia failed to demonstrate that there was a real problem with illegal drug use among candidates for state office;
b) The program failed to identify candidates who violated anti-drug laws;
c) The program was not a credible means to deter users of illicit drugs from seeking election;

[1123] After the articulation of the "special needs doctrine" in *Skinner* and *Von Raab* some courts extended the doctrine to cover the drug testing of employees in security – sensitive positions. See *Harmon v Thornburg* 878 F.2d 484 (D.C. Cir. 1989) and *National Federation of Federal Employees v Cheney* 884 F.2d 603 (D.C. Circ. 1989) where the court upheld the testing of Department of Justice employees and of civilian employees in the Department of Defence respectively. The courts in both decisions upheld the testing on the basis of the nature of employment. In *Harmon* the court upheld the random testing of employees with top secret national security clearances and in *Cheney* the court upheld the testing of persons in positions which are most critical in times of safety, integrity or sensitivity of information. Remy "The Constitutionality of Drug Testing of Employees In Government Regulated Private Industries" (1991) 34 *Howard University Law* Journal 633 649.

[1124] 520 US 305 (15 April 1997).

d) The state further offered no reason as to why ordinary law enforcement methods were insufficient for the apprehension of candidates addicted to illicit drugs.[1125]

6.5.4 Analysis

Drug testing in the workplace appears to be an accepted policy or practice. Drug testing, particularly urinalysis, has raised privacy concerns because the act of urination is by its very nature considered to be private. Urinalysis may also reveal more than just the presence of illicit drugs in a test subject's body given that it can reveal medical conditions such as depression. Employers have been known to require that employees give urine samples under observation so as to prevent adulteration of the sample and this also raises privacy concerns. At the same time, as intrusive and evasive as drug testing particularly urinalysis is, employers have found them to be a useful and necessary precaution particularly for those employers in safety sensitive positions.

It is unclear whether the EEA regulates drug testing in South African employment and South African courts have addressed the issue of drug testing in employment, but only to address the question of whether the results of the testing justified the dismissal of an employee.

It is unclear to what extent drug testing is carried out by United Kingdom employers. However, it is clear that it is an accepted practice and is regulated by the DPA and the Employment Practices Code. The Employment Practices Code's Guidance provides employers with comprehensive guidelines on how to go about testing employees for drugs in the least intrusive manner.

United States courts have dealt extensively with the issue of drug testing and it appears United States courts are likely to uphold the testing for employees in the public sector regardless of whether their positions implicate safety concerns. The United States has both federal and state legislation regulating the use of drug tests.

[1125] See also *Baron v Hollywood* 93 F Supp 2d 1137 (SD Fla 2000) and *Robinson v City of Seattle* 102 Wash. App. 795, 10 P 3d 452, 16 E.R. Cas. (BNA) 1405 (2000).

6.6 HIV/AIDS TESTING

The previous chapter discussed how the arguments advanced by employers to justify the HIV/AIDS testing of employees were increasingly making way for a growing need to protect and preserve, amongst other rights, the rights to privacy and dignity of persons suffering from the HIV/AIDS pandemic in light of the fear, antagonism and misconceptions surrounding HIV/AIDS. The South African decision of *Hoffmann v SAA* emphasised this when it alluded to the fact that negative and misguided conceptions of HIV/AIDS had caused deep anxiety and considerable hysteria against those infected and, as such, ill – informed public perceptions and the policies of others should not be allowed to detract from the constitutional rights of employees not to be discriminated against and their rights to privacy and dignity.[1126]

6.6.1 South Africa

South Africa has one of the highest HIV/AIDS rates on the globe. At the end of 2005, an estimated 5,5 million South Africans were living with HIV according to UNAIDS/WHO, 2 million of whom were unaware of their HIV positive status.[1127] UNAIDS/WHO further estimates that 1000 HIV related deaths occur daily in South Africa.[1128] This means total HIV/AIDS deaths in South Africa have increased by 79% from 1997 to 2004. The rising AIDS deaths in South Africa have decreased the average life expectancy to less than 50 years in three South African provinces – namely the Eastern Cape, Kwazulu – Natal and Free State.[1129]

The South African Law Commission, in its discussion paper on "Aspects of the Law Related to AIDS: Pre-employment Testing", stated that although HIV/AIDS cannot be transmitted casually and transmission in the workplace was unlikely, the virus would nevertheless have a dramatic effect on the workplace and the economy given that many of those who were affected by the virus constitute the economically active population. The virus has had a marked impact on investment in training, cost of labour and productivity of workplaces and on sero - negative individuals (as their time

[1126] 1374 – 1376.
[1127] UNAIDS/WHO 2006 AIDS Epidemic Update.
[1128] http://www.avert.org/aidssouthafrica.htm (2007-01-25).
[1129] UNAIDS/WHO 2006 AIDS Epidemic Update.

is spent caring for and supporting sick spouses, dependents and other family members).[1130]

As previously mentioned, the common law right to privacy in South African law derives from the right to dignity which is inextricably linked with the right to bodily and psychological integrity.[1131] Hence, in terms of South African common law, a prospective employee or employee who is HIV positive enjoys the right to privacy like any other person under the common law. The common law right to privacy serves to protect the individual's dignity and personality by forbidding unjustifiable intrusions into the private sphere of either business or social life. The significance of this right in the workplace translates into the following:

1. an employer may not lawfully coerce the prospective employee or employee to take an HIV test and;
2. the employer may not disclose the HIV status of a prospective employee or employee without the concerned person's consent.[1132]

6.6.1.1 Legislation

Section 14 of the Constitution[1133] explicitly recognises the right to privacy and for this reason affords individuals protection against unwarranted HIV testing/disclosures in the workplace. The constitutional right to privacy ensures that privacy is not given a narrow meaning, but a broad meaning adopted by constitutional jurisprudence, subject to international human rights norms. South Africa has legislation shielding the employee from unwarranted HIV/AIDS testing in the workplace in the form of the Employment Equity Act[1134] and the South African Code of Good Practice and Key Aspects of HIV/AIDS.[1135]

The EEA constitutes the first piece of legislation in South Africa that offers protection specifically to employees living with HIV against unfair discrimination and

[1130] South African Law Commission *Aspects of the Law Related to AIDS: Pre-employment HIV Testing* Project 85 Discussion Paper 72 http://www.doj.gov.za/salrc/dpapers.htm (2005-02-05).

[1131] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2791.

[1132] Ngwena "HIV in The Workplace: Protecting the Rights to Equality and Privacy (1999) 15 *South African Journal of Human Rights* 513 533.

[1133] Constitution of the Republic of South Africa Act 108 of 1996.

[1134] Act 55 of 1998.

[1135] Code of Good Practice on Key Aspects of HIV/AIDS and Employment (2001) 22 *Industrial Law Journal* 62 -75.

unauthorised testing. The scope of the definition given to medical testing is wide enough to include any test question, inquiry or other means designed to ascertain or which has the effect of aiding an employer to ascertain whether an employee has any medical condition. The scope of the definition given to "testing" is commendable in that it goes beyond physical testing to extend to indirect means of ascertaining an employee's HIV status. Section 7(2) of the Act prohibits the testing of an employee or prospective employee unless the Labour Court deems such testing justifiable.[1136]

The South African Code of Good Practice on Key Aspects of HIV/AIDS,[1137] borne out of the recommendations of the Southern African Development Community HIV/AIDS Code on Employment,[1138] provides there should be no compulsory testing of employees. Of importance, the code recognises that protection of the human rights and dignity of people with HIV/AIDS is essential to the prevention and control of the epidemic. The code further reinforces the role of the Labour Court to police HIV/AIDS testing in the workplace. Under the heading of confidentiality and disclosure, the code further provides that all persons with HIV/AIDS have the legal right to privacy and an employer therefore must not disclose the HIV status of its employees.

South Africa, like the United States and Australia, excludes members of the National Defence Force, Secret Service and National Intelligence[1139] from benefiting from blanket prohibitions on HIV/AIDS testing, whereas countries like Canada[1140] and

---

[1136] Heywood and Hassan "The Employment Equity Act and HIV/AIDS: A Step in The Right Direction" (1999) *Industrial Law Journal* 845 851.

[1137] Code of Good Practice on Key Aspects of HIV/AIDS and Employment (2001) 22 *Industrial Law Journal* 62 -75.

[1138] The Code of Good Practice on Key Aspects of HIV/AIDS and Employment recommends that SADC member's states (Zimbabwe, Zambia, Botswana, Swaziland, Namibia, Mauritius, Angola, Lesotho, Malawi, Tanzania and South Africa) should develop tripartite national codes on HIV/AIDS and Employment that shall be reflected in the law.

[1139] Other organs of state such the Department of Correctional Service and the South African Police stopped pre-employment HIV/AIDS testing in 1997. Heywood and Hassan "The Employment Equity Act and HIV/AIDS: A Step in The Right Direction" (1999) *Industrial Law Journal* 845 852.

[1140] See *Thwaites v Canada* (Canadian Armed Forces) [1993] C.H.R.D. No. 9 (7 June 1993); affirmed *Canada (Attorney General) v Thwaites*, [1994] 3 F.C. 38 (F.C.T.D.). At issue in Thwaites was the discharge of an enlisted classified and trained in the military trade of naval sensor operator on the grounds that his HIV disease had progressed from an asymptomatic stage to a symptomatic stage. The Canadian Human Rights Tribunal held the following: Thwaites perceived fitness for duty was discriminatory since the ability of an individual with HIV varies from individual to individual. As such appropriate and individualised consultation with Thwaites with a physician was required so that a decision could be made on his real condition and not perceived condition; and the increased risk to himself or to others at sea and away from specialist care was not sufficient to warrant his

Belgium have extended such benefits to military and armed forces personnel.[1141] Nonetheless, in the South African context and prior to the decision in *South African Security Forces Union and Others v Surgeon General and Others*[1142] members of the South African National Defence ("SANDF") could have recourse based on an infringement of their constitutional rights to equality, privacy and dignity and the provisions of the Promotion of Equality and Prevention of Unfair Discrimination Act[1143] ("PEPUDA") (which is aimed at giving effect to the right to equality in section 9 of the Constitution and promoting equality and preventing the unfair treatment of persons).

6.6.1.2 Case Law

The South African Labour Court has handed down two important decisions on HIV/AIDS testing in the employment sphere and in so doing shed light on the provisions of the EEA in this respect.[1144] In *Joy v Mining Machinery (A Division of Harnischfeger SA (Pty) Ltd) v NUMSA and Others*[1145] the Court reaffirmed its role of "policeman" with regard to HIV/AIDS testing in employment. The applicant, after

---

exclusion.The Canadian Armed Forces had failed to explore alternatives to Thwaites discharge such as a change in the nature and scope of his duties or a re-muster to some other occupation. Canadian HIV/AIDS Legal Network "HIV Testing of UN Peacekeeping Forces: Legal and Human Rights Issues" 9 September 2001 17. http://www.aidslaw.ca/Maincontent/issues/testing/peacekeepingforces.pdf (2005-02-05).

[1141] Heywood and Hassan "The Employment Equity Act and HIV/AIDS: A Step in the Right Direction" (1999) *Industrial Law Journal* 845 852.

[1142] High Court of South Africa (Transvaal Provincial Division) Pretoria, Case No 18683/07.

[1143] Act 4 of 2000.

[1144] It is important to note that the leading cases with regard to the common law right to privacy and its application to an individual's HIV status are: *C v Minister of Correctional Services* 1996 4 282 (T) *and Jansen van Vuuren v Kruger* 1993 4 SA 842 (A). *C v Minister of Correctional Services* concerned the testing of prisoners for HIV. The decision is credited with determining the doctrine of informed consent to be a prerequisite in testing for HIV. The findings of the court in *C v Minister of Correctional Services* in the employment context require the employer to not only obtain the consent of the person to be tested but further require the employer, prior to administering the test, to explain the purpose of the test, procedure to be followed and the implications of a positive test to the applicant or employee. In *Jansen van Vuuren v Kruger* the then Appellate Division of South Africa looked to the common law right to privacy in finding that a doctor had unjustifiably disclosed his patient's HIV status to a third party. The Appellate Division held that the disclosure of a patient's HIV positive status to a third party amounted to a breach of privacy and that a doctor's respect for his patient's confidentiality was not only an ethical duty but a legal duty. See McLean "HIV Infection and a Limit to Confidentiality" (1996) 12 *South African Journal of Human Rights* 452. According to Radipati the case placed South Africa alongside other jurisdictions in recognising that HIV, although contactable and infectious, is neither contagious nor hereditary (See Radipati "HIV and Employment Law: A Comparative Synopsis" (1993) *CILSA XXVI* 396). The case further confirmed the fact that a person's HIV positive status is an extremely private and personal condition, which an individual may wish to keep to himself and selected individuals. See Ngwena "HIV in The Workplace: Protecting the Rights to Equality and Privacy (1999) 15 *South African Journal of Human Rights* 513 533 – 534.

[1145] 2002 4 BLLR 37 (LC).

consultation with recognised unions representing its employees, sought an order permitting it to conduct voluntary testing on its employees in order to determine the incidence of HIV amongst its staff to enable it to deal with the epidemic better. The court emphasized that before it would authorise an employer to conduct HIV/AIDS tests on employees, it must be satisfied that the tests furthered the objectives of the EEA. The court granted the order in light of the fact the employer had already instituted an education and awareness campaign amongst its workforce, established onsite clinics to treat sexually transmitted diseases, the applicant desired to formulate and implement a strategy to deal with the virus amongst its employees. The employer had assured its employees that they would not be forced to take the test. In other words, the applicant wished to conduct voluntary (and not mandatory) HIV tests on its employees and the employer guaranteed its employees confidentiality in respect of the test results.

It was not necessary for the employer in *Joy* to obtain an order from the Labour Court for the testing, since such testing was to be voluntary and the decision to test its employees was taken in consultation with unions representing its employees.

At issue in *PFG Building Glass v CEPPAWU & Others*[1146] was whether anonymous and voluntary testing of employees for HIV/AIDS fell within the ambit of section 7(2) of the EEA. The Court reasoned that HIV testing infringes the right to bodily and psychological integrity (which includes the right to security in and control over one's body in section 12 (2)(b) of the Constitution and the right not to be subjected to medical or scientific experiments without consent in section 12 (2) (c) of the Constitution) and the right to privacy. The Labour Court reasoned that these rights were not absolute and had to be balanced against the competing fundamental rights of employers, shareholders and regulators, such as the right to access to information and the right to trade. For the Court, even though the objective of the protection against HIV testing is to prevent discrimination and promote equality, the test for justifiability of HIV testing goes beyond determining whether such testing is equitable or not. The test for the justifiability of HIV testing is also a constitutional enquiry and as such has to meet the requirements of the limitations analysis in section 36 of the Constitution. The Court found that because HIV is a medical condition, the testing for

[1146] (2003) 24 ILJ 974 (LC).

it must be medical and this meant that: the data sought must be relevant to the purpose of the testing, the tests must be confidential, and the subjects of the tests should give their voluntary and informed consent to the testing. The Court pointed out that the Code of Good Practice on Key Aspects of HIV/AIDS erred in requiring employers to obtain permission from courts even where employees have given their voluntary and informed consent and exercised their constitutional right in terms of section 12 (2)(b). Pillay J further interpreted section 7(2) so as not to impose a limitation on employees in the exercise of their constitutional rights in section 12 (2)(b) and section 12 (2) (c) of the Constitution. For this reason, Pillay J concluded that anonymous and voluntary testing in the workplace did not fall within the ambit of section 7(2).

The Labour Court recently confirmed that the dismissal of an employee on the basis of his or her HIV status amounted to an automatically unfair dismissal. In *Botes v Eagle Ink Systems KZ Natal (Pty) Ltd*[1147], the employer alleged that it had dismissed the employee for misconduct. However, the Court found that the employer had tried to "camouflage discrimination under the cloak of misconduct"[1148] and had failed to lead evidence showing that misconduct was the real reason for dismissing the employee The Court observed that three measures in South African employment context placed an onerous burden on employers discriminating against HIV positive employees:

> "[r]elative to people living in many other jurisdictions, people in South Africa have the advantage of a constitutionally entrenched right not to be discriminated on the grounds of their HIV positive status. Furthermore, legislation facilitates proof of discrimination, firstly by defining discrimination to include HIV as a prohibited ground of differentiation. Secondly, dismissal of an employee on account of his HIV status is, by definition, an automatically unfair labour practice…[Thus] justifying discrimination on the grounds of an employee's HIV status is a hard row to hoe. Not surprisingly,

[1147] [2007] JOL 20651 (LC).
[1148] 31.

> employers try to avoid basing a dismissal on an employee's HIV status."[1149]

Although *Hoffman v South African Airways*[1150] ("*Hoffmann*") was decided in terms of the general right to equality in the Constitution and not in terms of the EEA, the judgment has been followed in cases decided in terms of the EEA.[1151] The applicant in *Hoffmann* was HIV positive and was considered unsuitable for the position of flight attendant despite having successfully undergone a pre – screening interview, a psychometric test and a formal interview. SA Airways argued that its operational requirements and employment policies and practices excluded the applicant from the position of flight attendant. The applicant contended that he had been discriminated against solely on the grounds of his HIV positive status, resulting in the violation of his inherent right to dignity. The Constitutional Court in *Hoffmann* held that an employer may not exclude an applicant from employment on the basis of their HIV positive status, particularly if such applicants are fit for duty.

The decision in *IMATU & Another v City of Cape Town*[1152] did not pertain to the HIV/AIDS testing of an employee by an employer but it nonetheless concerned the medical testing of an employee to determine his suitability for employment. The decision also echoed the principle laid down in *Hoffmann*, namely that if an employer wants to exclude an applicant from employment on the basis of the condition of their health, the employer must show that the employee is incapable of meeting the requirements of the job.[1153] The applicant in claimed that he was a victim of unfair discrimination after being denied employment as a firefighter by the metropolitan municipality of the City of Cape Town. The Labour Court, after hearing medical evidence that modern drugs had considerably reduced the risks associated with "Type 1" diabetes, held that the applicant could not rely on the ground that he had been discriminated against because of disability, but could assert that he had been unfairly discriminated against in a manner which impaired his dignity.[1154] The Court further found that the blanket ban to which the applicant had been subjected did not fulfil a

[1149] 30.
[1150] 2000 21 ILJ 2357 (CC).
[1151] Grogan *Dismissal: The South African Law of Unfair Dismissal* (2002) 135.
[1152] 2005 26 ILJ 404 (LC).
[1153] *Supra*.
[1154] Grogan *Dismissal: The South African Law of Unfair Dismissal* (2002) 134.

legitimate purpose and accordingly the City could not rely on the defence that the ban was related to "an inherent requirement of the job".[1155]

The matter of *South African Security Forces Union and Others v Surgeon General and Others*[1156] ("SANDF decision") is also worth mentioning notwithstanding that the matter was settled between the parties.[1157] At issue in this matter was the constitutionality of a policy which excluded persons with HIV/AIDS from being recruited, promoted or deployed on international missions if they tested HIV positive. Privacy was of central concern. The applicant in the matter argued that the policy of the South African National Defence Force ("SANDF"), as reflected in its' various policy documents dealing with recruitment, promotion and deployment discriminated against people who are HIV irrespective of their job, post, classification or mustering solely on the basis of their HIV status and the policy was for this reason unconstitutional in that it unreasonably unjustifiably infringed on a spectrum of constitutional the rights of affected persons including the right not to be unfairly discriminated against in terms of section 9(3) of the Constitution and the right to privacy in terms of section 14 of the Constitution and the right to dignity in terms of section 10 of the Constitution.[1158]

In response the SANDF argued, amongst other things, the following:

a) the policy was not directed at people living with HIV but was aimed at excluding persons who are not healthy and in so doing it ensured that the SANDF is at all times ready to do combat and is able to provide respond immediately to threats of national security;
b) the policy of excluding persons with chronic diseases including HIV is not inconsistent with the Constitution on the contrary it is aimed at meeting the Constitutional imperative of the SANDF to preserve and protect national security;
c) in post-apartheid South Africa, the SANDF is under a constitutional and statutory obligation to ensure that it maintains a core force that maintains a streamlined structure and design in order to be efficient and effective,

[1155] Grogan *Dismissal: The South African Law of Unfair Dismissal* (2002) 135.
[1156] High Court of South Africa (Transvaal Provincial Division) Pretoria, Case No 18683/07.
[1157] The matter was settled on 16 May 2008.
[1158] http://www.section27.org/files/2008/05/ApplicantsHeads.pdf (2010-05-17).

something which is militated against by the recruitment of persons who cannot meet the optimal fitness standards;

d) the conditions of deployment are such that deployed members are exposed to significant stress and environmental challenges and these conditions require (amongst other things) that the SANDF conduct pre – deployment testing in order to conduct a medical risk analysis which will dictate the medical services to be provided in deployed areas and that SANDF members who are deployed are of an adequate standard of health in order to withstand hostile employment conditions;

e) in excluding members who do not meet the health standards for deployment the SANDF does not act inconsistently with the Constitution but seeks to discharge its duty to protect employees with chronic illnesses by not exposing them to conditions which may result in a deterioration of their conditions and further seeks to not compromise the safety and integrity of collective units of troops by deploying people who may, once exposed to the harsh conditions characteristic of deployment, become unwell and unfit to discharge their functions as soldiers.[1159]

f) In settling the matter, the parties agreed that the SANDF policy was unconstitutional in that it infringed a spectrum of constitutional rights. The Court gave the SANDF 6 months within which to review its regulations and policies. The settlement put to rest the issue of the constitutionality of the HIV testing policy of the SANDF, a policy which had been repeatedly questioned and challenged (without much success) since 1994 by various concerned and affected persons.

6.6.2 United Kingdom

At the end of 2005 an estimated 63,500 adults aged between 15 and 59 were living with HIV/AIDS in the United Kingdom. In 2005, the United Kingdom reported 730 AIDS cases and 503 deaths.[1160] The United Kingdom has reported the largest increases in HIV cases in Western Europe since 1998, as the number of new HIV diagnoses

[1159] http://www.section27.org/files/2008/05/RespondentsHeads.pdf (2010-05-17).

[1160] http://www.statistics.gov.uk (2007-01-22).

have doubled since 2000. In 2004, the United Kingdom recorded more than 7200 new diagnoses of HIV and a year later (in 2005) this number had increased to 7700.[1161]

6.6.2.1 Legislation

In April 2005 the English parliament passed the Disability Discrimination[1162] Act ("DDA of 2005") thereby amending and extending certain provisions of the Disability Discrimination Act[1163] ("DDA of 1995"). Of particular importance, the DDA of 2005 extended the definition of "disability" in section 1 of the DDA of 1995. The DDA of 1995 defined "disability" as "a physical or mental impairment which has a substantial and long - term adverse effect on [a person's] ability to carry out normal day – to – day activities." [1164] The DDA of 2005 supplemented this definition of "disability" to include persons with cancer, HIV infection and multiple sclerosis.[1165] In terms of the extension, persons living with HIV were included within the disability definition already at the stage of diagnosis. Before 2005, persons living with HIV only fell within the ambit of the DDA from the stage when their HIV seropositivity began to have a long – term adverse effect on their ability to carry out normal day – to – day activities.[1166]

The extension protects people living with HIV from discrimination by making it unlawful for employers to discriminate against an HIV positive employee or potential employee.[1167] For employers, the extension means they have a duty to make reasonable adjustments for HIV positive employees. The DDA places a duty on an employer to make reasonable adjustments to any physical feature, provision or policy in the workplace that places a disabled person at a substantial disadvantage. This includes recruitment policies and conditions relating to the employment, promotion, transfer or training of employees.[1168] In the case of HIV positive employees,

[1161] UNAIDS/WHO 2006 AIDS Epidemic Update.
[1162] Act of 2005.
[1163] Act of 1995.
[1164] Section 1 of the DDA of 1995.
[1165] Section 18 of the DDA of 2005.
[1166] http://www.dwp.gov.uk/aboutus/data_2005.asp (2007-01-23).
[1167] http://www.dwp.gov.uk/aboutus/data_2005.asp (2007-01-23).
[1168] Section 6 of the DDA of 2005.

employers may be required to allow such employee time off for medical appointments and access to an area where they can take their medication.[1169]

At the European level, the Council of Member States has issued guidelines about the treatment of HIV/AIDS in employment. The Council has also recognised the importance of protecting privacy in individual's medical information in general and, in particular, an individual's HIV status. In 1988, the Council and the Ministers for Health of the Member States adopted "Conclusions on AIDS and the Workplace". The Conclusions are only recommendations and not legally binding legislation. The Conclusions recommend that "because people infected with the HIV virus or suffering from AIDS pose no danger to their colleagues at work, there are…no grounds for screening potential recruits for antibodies". The Conclusions further state that there is no risk of HIV infection in medical procedures, if appropriate hygiene guidelines are followed. Employees who are asymptomatic should be regarded as fit for work and should not be under any obligation to disclose their status to their employer. They further recommend that if knowledge of HIV status is obtained, the employer should make every effort to protect the person from stigmatisation, discrimination and maintain medical confidentiality. The Conclusions also dictate that employees suffering from HIV should be treated as other employees with serious illnesses that affect their performance and, where the employee's fitness is impaired, duties or working hours should be adjusted so that such employees may continue working as long as possible.[1170]

Of particular significance are the main provisions of the Equality Act[1171], which is expected to come into force in October 2010. The Equality Act consolidates the grounds of discrimination (sex, race and other grounds of discrimination) into one piece of legislation resulting in one single objective "justification" test to replace the various tests formulated under the varying grounds of discrimination.[1172]The justification test under the Equality Act will result in employers having to meet higher thresholds in justifying their actions if they for instance dismiss an employee for a

[1169] http://www.ukcoalition.org/epf/employers/adjustments.htm (2007-01-23).

[1170] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775.

[1171] Act of 2010.

[1172] http://www.stammeringlaw.org.uk/changes/chan.htm (2010-06-13).

disability related reason. In terms of section 15 (discrimination arising from disability) and 19 (indirect discrimination) of the Equality Act, the employer will have to show that its conduct is a proportionate means to achieve a legitimate aim.[1173] The Equality Act's definition of a person with a disability is wide enough to include HIV positive persons, seeing as the condition may have a substantial and long term adverse impact on a person's ability to carry out normal day to day activities.[1174] That being said, Schedule 1 of the Equality Act unequivocally states that HIV is a disability along with the medical conditions of cancer and multiple sclerosis.

Also of importance is section 60 of the Equality Act, which restricts employers from asking about an applicant's health, including whether an applicant has a disability. Exceptions to this general principle are where the enquiry is aimed at establishing whether an employee has the ability to carry out a function that is intrinsic to the nature of the job concerned or where it is done for purpose of monitoring diversity in the workplace.[1175]

6.6.2.2 Case Law

In *Commission v Germany*[1176] the European Court of Justice included the protection of medical information within the right to privacy. At issue was a German law prohibiting imports of medicinal products prescribed by a doctor in another member state, unless ordered through a German pharmacy. Germany admitted that the statute constituted a restriction on free movement of goods, but argued that this restriction was essential in order to guarantee the protection of the health and life of humans. The European Court of Justice ("ECJ") agreed that the rights to privacy and the right to protection of medical secrets were fundamental rights in the Community, but held they were not absolute rights. The court held that a limitation of these rights may be justified by the objective of protection of public health, provided the restriction actually promotes the objectives of the general interest and is not disproportionate to the extent that it would interfere with the very substance of those rights. The ECJ then found the German law illegal and concluded that Germany had failed to show that it would be impossible to implement controls which would protect public health

[1173] *Supra*.

[1174] Section 6 of the Equality Act.

[1175] http://www.stammeringlaw.org.uk/changes/employment.htm#justification (2010-06-13).

[1176] 1992 E.C.R I – 2575, [1992] 2 C.M.L.R. 549 (1992).

without also excessively interfering in the privacy of medical secrets.[1177] Privacy protection in the European Community is found in Article 8 of the ECHR encompassing the right to oneself, to live as oneself and the balancing of considerations under Article 8(2). Included in this far–reaching protection of personal privacy is the protection of an individual's medical information (even in the workplace).

The fact that the "Conclusions on AIDS and the Workplace" (disseminated at European level and referred to above) are only recommendations (intended to influence Member State laws) and not legally binding legislation in terms of the Community hierarchy of legal norms, was emphasised by the Court of First Instance in *A v Commission*.[1178] In *A v Commission*, A applied for an administrative post in the African, Caribbean and Pacific region with the Commission. A was required to undergo a pre-recruitment medical test which he willingly submitted to and voluntarily informed the testing medical officer that he was HIV positive. The testing medical officer concluded that A was fit for the post. In the Court of First Instance, A made two arguments against the pre-recruitment medical exam, namely that:

1. The purported objective of the Commission's pre-recruitment exam (that is to avoid major future costs) was economic in nature and therefore unjustified under any of the objectives listed in Article 8 of the ECHR.
2. The test violated his right to privacy since his voluntary consent made the test unnecessary or useless in the circumstances.

The Commission on the other hand argued that A was unfit for the post because he had gone beyond mere seropositivity to a condition of active illness. That is to say, because A had gone beyond being merely HIV positive to having full-blown AIDS and, in turn, his full-blown condition rendered his projected duties a risk to his health, since they required placement in "high-risk countries" which would expose A to the danger of infections in the absence of appropriate health care infrastructure.[1179] A objected to this medical determination by the Commission, by stating that he had previously worked in Mexico, "a developing country with only limited

[1177] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States"(1997) 65 *Fordham Law Review* 2775 2785.

[1178] 1994 E.C.R. II-179 (Ct. First Instance).

[1179] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2790.

infrastructures". A further asserted that because he was not asymptomatic, the Commission had violated the Conclusions that an asymptomatic employee should be treated as fit to work.[1180]

The Court of First Instance[1181], in applying the proportionality test formulated in *Commission v Germany*, determined that the objective of pre-recruitment testing required by the Commission was either to avoid the Commission hiring an unsuitable candidate for duties linked to the post, or to assign duties compatible with an assigned candidate's physical condition. The court found such objectives to be lawful within member state traditions and therefore concluded that the test could not be regarded as violating the principle of respect for a person's private life. With regard to A's contention that the nature of the HIV test was useless or unnecessary, the court found that it was beyond its review since it constituted an entirely medical assessment. The court, however, added that the medical officer might base his medical assessment of the candidate's fitness "on a medically justified prognosis of future orders capable of jeopardizing in the foreseeable future the normal performance of the duties in question." As to whether A's seropositivity rendered him unfit for the post, the Court noted that the Conclusions A sought to rely on were not provisions of Staff Regulations or Community legislation and therefore not legally binding on the Commission. The Court did add that the Conclusions nonetheless functioned as rules of practice that could be deviated from without full explanation. The Court concluded that because the medical exam revealed certain symptoms that could be described as symptomatic of associated infections, there existed a link between the medical findings and the conclusion drawn on A's fitness for the duties related to the post, especially considering the fact that those duties were to be carried out in developing countries in which the risks of infection were greater than in Europe. Hence, A was unfit for duties related to the post.[1182]

In *X v Commission*[1183], X a Portuguese freelance typist who had worked for the Commission applied for a temporary post as a typist in the Commission's Portuguese

[1180] *Supra*.

[1181] 1992 E.C.R I – 2575, [1992] 2 C.M.L.R. 549 (1992).

[1182] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2790.

[1183] 1994 E.C.R. I-4737.

Translation Division. The application procedure required X to undergo a medical test, which X refused to undergo. The medical officer ordered supplementary blood tests (T4/T8 blood tests) and concluded that X was suffering from a significant immune deficiency which rendered him unable to perform duties as a temporary typist. X argued that the performance of an HIV test without his informed consent constituted interference with his physical integrity and hence violated his right to privacy. The Court of First Instance accepted X's argument, but refused to accept that the T4/T8 blood tests conducted on X were in fact HIV tests that could determine seropositivity. The Court of First Instance therefore concluded that X's right to privacy had not been violated. On appeal to the European Court of Justice, the court asked the following questions based on the balancing test formulated in *Commission v Germany*[1184]:

1. Whether the tests carried out in the pre-recruitment exam constituted an interference with X's private life. The Court found the medical officer, by ordering supplementary tests in order to indirectly reach the same result as an HIV test, had violated X's right to privacy.
2. Whether such interference was justified by the public interest under Article 8 (2) of the ECHR. The Court found that while the pre-recruitment exam served a legitimate purpose (the protection of health), X's refusal mandated the Commission to respect his refusal to submit to an HIV test in whatever form. The Court stated the following in this respect: "since the candidate expressly refused to undergo an AIDS screening test that right precluded the administration from carrying out any test liable to point to…that illness, in respect of which he refused disclosure."[1185]

To summarise, European Community case law indicates that employers may subject candidates to medical tests with the consent of the concerned person, but should simultaneously consider the implications the results might have on the candidate's recruitment. In the event that a candidate should refuse to submit to a medical test, the

[1184] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2790.

[1185] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2787 – 2788.

medical officer may not perform related tests wherein an employer would be free to reject a candidate based on his refusal.[1186]

6.6.3 United States

The Centre for Disease Control and Prevention ("CDC") describes HIV data collection in the United States as "patchy and incomplete" because not all 50 states of the United States record their HIV infections. According to the CDC only 35 of the 50 states record their HIV infections.[1187] This makes it difficult to give an exact indication of how many people are living with HIV/AIDS in the United States. The UNAIDS/WHO 2006 report estimates "only seven countries…have more people living with HIV than the United States." The United States, according to the report, estimates that the concerned states had 1,2 million people living with HIV in 2005.[1188] Estimates further indicate that 40,000 new HIV infections occur every year.[1189]

6.6.3.1 Legislation

The United State's scheme of statutory legislation protects the disabled from discrimination by both private and public employers in the workplace. HIV seropositivity and AIDS are regarded as disabilities and both conditions find protection under the American with Disabilities Act of 1990 ("ADA") and the Rehabilitation Act[1190].[1191] The ADA prohibits any private or public employer employing 15 or more employees from discriminating against a qualified individual on the basis of their disability.[1192] The Act further prohibits all pre-employment testing medical exams that determine whether an applicant has a disability or the nature of the severity of the disability. The ADA only permits inquiries into a candidate's

[1186] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2791.

[1187] http://www.avert.org/america.htm (2007-02-24).

[1188] UNAIDS/WHO 2006 AIDS Epidemic Update.

[1189] http://www.avert.org/america.htm (2007-02-24).

[1190] Act of 1973.

[1191] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2798. According to Crandall prior to the enactment of ADA the Rehabilitation Act covered the federal government, federal government contractors and subcontractors and recipients of federal financial assistance but left loopholes for employers in the private sector and some state and locals agencies. Hence to remedy the loopholes Congress enacted the ADA, which requires equal treatment of disables persons in the private sector and state and local agencies. Crandall "Confusion in the Courts: What To Do With HIV-Positive and AIDS- Infected Public Employees" (1995/1996) 10 *Cleveland University Journal of Law and Health* 157.

[1192] Section 12112(a).

ability to perform job related functions.[1193] Testing during employment akin to pre-employment testing is also prohibited under the ADA unless the test is job related and consistent with business necessity.[1194] Nevertheless, the ADA permits an employer to reject a disabled applicant who poses a direct threat to the safety and health of others in the workplace.[1195] The employer can also impose a provision that no employee pose a direct threat to the safety and health of others in the workplace after being employed.[1196]

The Rehabilitation Act covers federal employers as well as those benefiting financially from federal government. Equally, the Rehabilitation Act prohibits the discrimination of individuals solely on the basis of their disability and prohibits pre-employment medical exams and inquiries into an applicant's disability. The two Acts differ in that the ADA includes medical exams and inquiries under "discrimination" and the Rehabilitation permits inquiries into an applicant's ability to perform job related functions.[1197] The Rehabilitation Act does not explicitly state that persons with infectious diseases fall within its scope, but the Supreme Court has held that the Act does benefit such persons.[1198] As a result, people infected with HIV/AIDS benefit from the protection offered by the Rehabilitation Act as long as they do not pose a direct threat that cannot be remedied by reasonable accommodation.[1199]

[1193]Section 12112(d).

[1194] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2800.

[1195] Section 12112(d)(3).

[1196] Crandall "Confusion in the Courts: What To Do With HIV-Positive and AIDS- Infected Public Employees" (1995/1996)10 *Cleveland University Journal of Law and Health* 157 159.

[1197] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2798.

[1198]See *School Board of Nassau County v Arline* 480 U.S. 273 (1987). A teacher was fired from her job because of her susceptibility to tuberculosis, brought an action alleging that her dismissal violated the Rehabilitation Act. The court found that the fact that some persons who have contagious diseases may pose serious health threat to others under certain circumstances does not justify excluding all persons with actual or perceived contagious diseases from coverage under the same Act. The court added that "a person poses a significant risk of communicating an infectious disease to others in the workplace will not be otherwise qualified for his or her job if reasonable accommodation will not eliminate that risk". The court further outlined the factors to be taken into account in determining whether a person handicapped by a contagious disease is "otherwise qualified" under Rehabilitation Act are nature of risk, duration of risk, severity of risk, and probability disease will be transmitted and will cause varying degrees of harm.

[1199] The US Congress in 1988 according to Stanley amended the definition of a handicapped individual to exclude an individual "who has a currently contagious disease or infection and who, by reason of such disease or infection would constitute a direct threat to the health or safety of other individuals or who, by reason of the currently contagious disease or infection, is unable to perform the duties of the

Only thirteen American states (including Texas and Florida) have specific legislative restrictions on pre-employment HIV/AIDS testing. The restrictions prohibit pre-employment testing unless the test can establish that HIV negative status is a bona fide job qualification or that there is a material risk of HIV transmission in the workplace, impossible to eliminate through less intrusive means.[1200] Moreover, the implicit right to privacy in the United States constitution provides a measure of protection for unwarranted employee HIV testing, since the United States Supreme Court has held mandatory blood testing is a search and seizure that must comply with the standards of reasonableness imposed by the Fourth amendment.[1201] The search's reasonableness is measured by balancing the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.[1202]

6.6.3.2 Case Law

In *Anonymous Fireman v City of Willoughby*[1203] city fire fighters and paramedics challenged the city's policy of requiring mandatory testing of fire fighters and paramedics for HIV/AIDS as part of its annual physical examination for fitness to serve. The court held:

> "Fire fighters and paramedics are in a high-risk group for the contracting and transmission of the HIV virus since their duties include a significant risk of being exposed to blood, bodily secretions and bodily fluids. This line of work exposes the employees to [the] high risk of bodily injury, lacerations, exposure to bleeding victims, puncture wounds and the like."

The court added:

> "Fire fighters and paramedics are at a higher risk than persons in hospitals for contracting or transmitting the HIV virus, because they work in a non-controlled setting. The universal precautions for fire

---

job". Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2800.

[1200] South African Law Commission *Aspects of the Law Related to AIDS: Pre-employment HIV Testing* Project 85 Discussion Paper 72 http://www.doj.gov.za/salrc/dpapers.htm (2005-02-05).

[1201] *Schmerber v California* 384 U.S. 757, 107 S.Ct. 1492 (1966).

[1202] *O'Connor v Ortega* 480 U.S. 709, 107 S.Ct. 1492 (1987).

[1203] 779 F.Supp. 402N.D.Ohio,1991.

> fighters such as gloves, masks, and protective clothing, may not be practical in this setting."[1204]

The court's reasoning about the effectiveness of fire fighting protective wear against HIV/AIDS transmission was influenced by the evidence given by a medical doctors who testified that "[t]he universal precautions for fire fighters, such as a space suit, boots, masks, gloves, etc., are not very practical because it is difficult to function wearing all of these garments; it is too much paraphernalia to work efficiently" and "…fire fighters who are HIV positive are dangerous because they can transmit diseases".[1205] The court further found on the evidence that the inclusion of a mandatory HIV test in the annual physical examination of city fire fighters and paramedics was rational (therefore not an unreasonable search and seizure in violation of the Fourth amendment) and closely related to fitness for duty. It was furthermore justified by a compelling governmental interest (that is, protecting the public from the contraction and transmission of HIV/AIDS by fire fighters and paramedics and stopping the spread of the deadly AIDS epidemic), in light of the high-risk nature of the job involving the possibility of exposure to blood and bodily fluids in a non-controlled setting. The court concluded that the testing at issue did not violate the plaintiff's right to privacy as protected by the Fourth, Ninth and Fourteenth Amendments and fitness for duty was a compelling governmental interest for safety forces, including fire fighters and paramedics.[1206]

The plaintiff in *Doe v District of Columbia*[1207]contended that the District of Columbia had denied him a position as a fire fighter because of HIV- positive status. The court found the following:

[1204] 412.

[1205] 407.

[1206] The same reasoning has been applied in justifying the HIV/AIDS testing of other government employees. See also *Local 1812, American Federation of Government Employees v Department of State* 662 F. Supp. 50 (1987) HIV/AIDS testing for Foreign Service employees was upheld. At issue was the Department of State's decision to expand its employee medical fitness program for Foreign Service employees seeking to qualify or who have qualified for worldwide service abroad, by including mandatory blood testing for the presence of HIV and related diseases, was contested by a union representing some of Foreign Service employees. The Court held stated that the testing program challenged was not primarily aimed at stopping the spread of the HIV infection but focussed on fitness for duty in a specialized government agency. The Court therefore concluded that on the evidence before it the inclusion of the test for HIV infection appears rational and closely related to fitness for duty.

a) An HIV-positive fire fighter was an "individual with handicaps" within the meaning of the Rehabilitation Act because of physical impairment that substantially limited his major life activities, such as procreation, sexual contact, and normal social relationships.
b) Employment of an individual with HIV-positive status as fire fighter did not pose a "direct threat" to the health or safety of others, within the meaning of the Rehabilitation Act, since the risk of transmission was so small that it vitiated any concern that HIV status would present a "direct threat" to other fire fighters or members of the public.
c) A fire fighter applicant was "otherwise qualified" for his position, within the meaning of the Rehabilitation Act, despite his HIV-positive status, where that fire fighter continued to pass the fire department's own physical examinations throughout the period of litigation and was asymptomatic.
d) The District of Columbia's withdrawal of its offer of employment to applicant for the fire fighter position on the basis of the applicant's HIV-positive status was an act of discrimination in violation of the Rehabilitation Act in light of the fact that the District failed to show that the applicant was not an otherwise qualified individual with handicaps or that he was denied the fire fighter position for reasons other than his HIV status.

The medical experts in *Doe* testified that an HIV-positive asymptomatic status does not impair a person's strength, agility, or ability to breathe and an asymptomatic HIV-infected person should be able to perform all of the functions of a fire fighter as stipulated by the District. In addition, the experts testified that the fire fighting equipment and protective gear required for fire fighters and emergency medical personnel by the Occupational Health and Safety Administration and the National Fire Protection Association and the use of this equipment and protective gear eliminate the risk of blood-to-blood contact in the performance of fire fighting functions. One of the health experts further pointed out that her research revealed that several fire departments throughout the United States employ HIV-positive fire fighters in active-duty status and none of those departments require any special precautions to be undertaken by these HIV-positive personnel. The court emphasised the risky nature

of fire fighting and the uncontrollable rate at which the disease was spreading and infecting new groups of people.[1208] The court said the following in this regard:

> "Much has been written and said about the subject of Acquired Immune Deficiency Syndrome, or AIDS. It has now reached epidemic proportions, both in the United States and throughout the world. At the present time, there is no known cure for AIDS. The only way to stop its spread is by education and prevention until some cure is found. Billions of dollars are now being spent to find a cure for AIDS but, so far, these efforts have not been successful."

The reverse was held four years earlier in the matter of *Glover v Eastern Nebraska Community Office of Retardation.*[1209] Glover concerned the validity of a Nebraska administrative agency's personnel policy requiring certain employees (serving the needs of mentally retarded persons) to submit to blood testing for the HIV virus and hepatitis B. In addition to testing, the policy required employees to inform a personnel officer when they knew or suspected they had HIV or Hepatitis B and to disclose medical records relating to the treatment they received for those diseases. The employer argued that it had a strong and compelling interest in protecting its mentally retarded clients and the rationale for testing these employees was that clients who engage in violent or aggressive behaviour associated with their conditions, such as biting and scratching, risked contracting one of the diseases from an infected employee.[1210] The employer further argued its employees had only a diminished expectation of privacy. The court found both arguments missed the mark. The court concluded that the risk of clients contracting HIV or Hepatitis B from employees was miniscule or negligible and therefore held that the policy constituted an unreasonable search and seizure under the Fourth Amendment.[1211]

[1208] 405. It is interesting to note that AIDS was initially classified in certain countries (such as the US) as a disease of homosexuals and drug users and as such society at that point in time remained unconcerned that the disease would infect the majority of society. Crandall "Confusion in the Courts: What To Do With HIV-Positive and AIDS- Infected Public Employees" (1995/1996)10 *Cleveland University Journal of Law and Health* 157 159.

[1209] 867 F.2d 461 (1989).

[1210] 463.

[1211] *Supra*.

United States Courts have also held that the disclosure of an employee's HIV status by an employer violated the employee's right to privacy.[1212]

6.6.4 Analysis

It has been suggested that the United States safeguards the right to privacy in the context of HIV/ AIDS better than the European community because of its legislative scheme and that protection of the right to privacy in the European Community would be better guaranteed if it were to adopt legislation similar to that of the United States.[1213] This suggestion seems to overlook that there is legislation with similar objectives to the United States's ADA and Rehabilitation Act in the European Community - the ECHR and the Conclusions on HIV/AIDS in the workplace. While it may be true that the Conclusions on HIV/AIDS in the workplace are not binding on member states, they have positively influenced decisions of l the ECJ. Protection of the employee can be achieved indirectly through other means. While, for example, the United States Constitution does not explicitly provide for the protection of the right to privacy, this right has been implied by the courts.[1214] Note that the ADA and the Rehabilitation Act also do not explicitly refer to HIV/AIDS in any of their provisions. Nonetheless, based on judicial interpretation and EEOC guidelines implementing the ADA, HIV is considered a handicap under both pieces of legislation. Lastly, the balancing or proportionality tests used by the European Community and the United States are similar. Perhaps the clearest conclusion to be drawn from the three jurisdictions is that discrimination law remains, in practice (and controlling for the limited possibility of direct reliance on the right to privacy in Constitutions and supranational instruments) the primary vehicle for protection of the privacy in this context (as is also the case with the policies and practices discussed earlier in the chapter).

[1212] *William S v Lassen County* 18 AD Cas.(BNA) 303 (2006) and *Doe v Southeastern Pennyslvannia Transport Authority* 101 IER Cas. (BNA) (1995).

[1213] Stanley "Note: May I Ask You a Personal Question?" The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775 2776.

[1214] In *Griswold v Connecticut*, 381 U.S. 479 (1965) the US Supreme Court first introduced the right to privacy even though it was not expressly provided for in the US constitution.

6.7 CONCLUSION

This chapter sought to provide an overview, on a comparative basis, of a number of policies and practices which typically threaten or put pressure on privacy in the employment sphere and to evaluate to what extent privacy was protected.

With respect to background checks, the chapter revealed that the selected countries have no legislation directly regulating the practice in general. However, various pieces of legislation could be used to protect the employee's rights in relation to such checks. It further emerged from the discussion that, because employers could be held liable for negligent and wrongful acts committed by their employees, the risk exists that employers will conduct background checks on all employees regardless of their position. In some instances, background checks were conducted by employers because legislation (justifiably) compels them to do so. At the same time, legislation such as the United Kingdom's Rehabilitation of Offenders Act is commendable for attempting to protect the privacy of individuals in relation to "spent convictions" and in its attempt to balance privacy interests and the interest in unprejudiced access to employment with concerns employers may have.

The discussion on psychological and psychometric testing showed that South Africa had (discrimination) legislation explicitly prohibiting the use of psychometric testing unless the tests were shown to be scientifically valid and reliable, apply fairly to all employees and are not biased against any employee of group. A popular theme in the discussion on the use of these tests in the United Kingdom and South Africa is that certain duties are placed on employers to ensure that the tests are valid and do not discriminate against any group. The United Kingdom and South Africa have yet to aggressively wrestle with the issue of the use of the tests and their discriminatory impact. Notably, the United States courts have confronted this issue in a number of cases and in so doing established the notion of indirect discrimination. It further appeared from the United States case law discussed that the use of the tests may be justified particularly in safety sensitive positions such as that of fire fighter and probationary police officer.

It also emerged from the chapter that the use of polygraph tests remains controversial because of continued doubt about their scientific validity and reliability.

Notwithstanding this controversy, these tests continue to be used in South African and United States workplaces. Case law points to the fact that in the South African workplace, the tests are used after the commission of an offence to determine if an employee is responsible for the alleged offence. In the United States employment context, employers seem to employ the tests primarily in the pre – employment stage in relation to safety sensitive positions.

The discussion on drug and alcohol testing revealed that employers in the selected countries carry out drug and alcohol testing on employees, especially those employees in safety sensitive positions. The discussion further revealed that legislation (again, primarily discrimination legislation) not only regulated the use of such testing in the different jurisdictions but also in certain instances compelled employers to carry out such testing on employees especially (again, primarily in safety sensitive positions.

South African has made great strides in ensuring that individuals who are HIV positive are protected from discrimination in the workplace. The recent SANDF decision bears testimony to the strides taken by South Africa in ensuring that persons are not negatively treated because of their HIV status. The developments in the protection of HIV positive persons from discrimination has also made it more difficult for South African employers to justify subjecting individuals to the HIV tests in the workplace. These developments are much needed in South Africa (in comparison to other jurisdictions), simply because of the prevalence of HIV/AIDS in South Africa.

The policies and practices identified in this chapter are by no means the only policies and practices employers use in the workplace that impact on privacy. Modern technology has enabled and continues to enable sophisticated forms of testing or monitoring of employees and in the two chapters to follow detailed attention will be given to the most recent and challenging (in the sense of the advanced technology underlying it) of these practices – internet and e-mail monitoring and genetic testing. The technology underlying the policies and practices discussed in this and subsequent chapters implicate employee privacy interests which have to be balanced against competing employer interests. Perhaps the lasting impression of the overview provided in this chapter is that the law is perhaps lagging behind, at least to the extent that it endeavours to use existing legal principles to combat these developments. What this chapter shows, is that privacy protection, for the most part, remains primarily to

be dealt with through a combination of broad constitutional principle (where available) and a perhaps inordinate and curious reliance on discrimination law.

CHAPTER 7:
SELECTED FOCUS AREAS: E-MAIL AND INTERNET

7.1 INTRODUCTION

In Chapter 5 the first steps were taken in consideration of the focus of this research, namely to consider how developments in technology has impacted on privacy protection in the workplace and whether these challenges call for a fundamental reconsideration of such protection. That chapter gave brief consideration to the "privacy in the workplace", examined the arguments for and against the need for privacy protection in the workplace, identified a number of policies and practices in the workplace that threaten privacy in the workplace and discussed how these policies and practices impacted on privacy. It was found that these policies and practices did indeed impact on privacy, and that the extent of this impact depended on the manner and circumstances in which they are used. That chapter also put forward the argument that, in light of technological advancements, there is a continued need for privacy protection in the workplace, but that such protection should consist, in the first instance, not so much on a fundamental re-evaluation of privacy as a protectable interest, but on a contextual balancing of the interests of employers and employees.

Chapter 6 expanded on the discussion in chapter 5 by evaluating how selected countries have approached or dealt with the use of these policies and practices identified by employers in the workplace, with specific emphasis on the availability of statutory protection and the approach of the courts in the different jurisdictions. One interesting insight gained from the discussion in chapter 6 is that apart from common law principles (identified and discussed in earlier chapters) and the odd application of relatively focused legislation (such as the Data Protection Act[1215] in the United Kingdom), discrimination legislation remains one of the main available lines of defence of privacy in the workplace. This situation arguably is already at odds with the importance of privacy as a value and the need for its protection. At the same time, and viewed from a different angle, this is perhaps already a clear indication of the fact that the protection of privacy as such in the workplace may not be of paramount

[1215] Act of 1998.

importance, and that such protection is only deemed worthy where other, related, values (such as equality) are the primary values infringed through conduct by the employer.

This chapter, along with Chapter 8, is one of two chapters that focus in depth on two workplace policies and practices also mentioned in chapter 5 (although not discussed in chapters 5 and 6) as constituting a threat to the protection of privacy in the workplace. What perhaps makes these practices and policies - e – mail/internet monitoring and genetic testing – different to those considered in chapters 5 and 6 – is that e – mail/internet monitoring and genetic testing arguably represent policies and practices based on the most recent and advanced technology available. As such, they represent both the essence of, and the latest in, the ongoing technological challenge to privacy in the workplace. In this chapter, e – mail/internet monitoring will be considered in some detail, while chapter 8 will focus on genetic testing.

7.2 A BRIEF SURVEY OF INTERNET AND E-MAIL

7.2.1 Internet

There is no official definition of the Internet. The Internet is commonly referred to as the "network of all networks"[1216]. United States courts have described the Internet as "an international network of interconnected computers"[1217] and a "vast collection of interconnected computer networks"[1218]. The United States Federal Networking Council passed a resolution in 1995 defining the term Internet as follows: "*…the global information system that (i) is globally linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and other IP compatible protocols; and (iii) provides, uses or makes accessible either publicly or privately, high level services layered on the communications and related infrastructure herein*." The definition is very technical and uses information technology terms such as "TCP/IP" and "protocol". However, the definition was

[1216] Edwards and Waelde *The Law and Internet: Regulating Cyberspace* (1997) 13.

[1217] *Reno v American Civil Liberties Union* 521 US 844 (1997).

[1218] *In re DoubleClick Inc Privacy Litigation* 154 F Supp 2d 497 (2001).

developed in consultation with individuals in the internet and intellectual property fields, hence its use of information technology terms.[1219]

There is much debate surrounding the precise origins and history of the Internet.[1220] What is clear is that the Advanced Research Projects Agency Network ("APARNET") was a major contributor to the birth of Internet in 1969.[1221] APARNET was a United States defence related academic research initiative connected to four computers and aimed at enabling defence researchers across the country to communicate and collaborate. The general view among writers on the Internet is that APARNET was a purely defence related initiative[1222] and the network was designed to withstand a missile attack.[1223] However, some writers believe that although the APARNET network was intended for defence related research[1224] the academics and students who had access to it were using its features (including e-mail, discussion groups, databases and file transfer protocol) to communicate about non- defence issues.[1225]

Whatever the intention behind APARNET may have been, the network developed various technologies that resulted in the Internet[1226]; these technologies include e-

[1219] http://www.nitrd.gov/fnc/Internet_res.html (2006-05-24).

[1220] Peter lists five theories possible theories that have been advanced towards the origins of the Internet: packet switching represents the origins of Internet; TCP/IP protocol represents the origins of the Internet; origins of Internet are represented by the birth of applications and not protocols; inventions and activities of Xerox Palo Alto Laboratories and Ethernet represent the origins of Internet. Peter "The Beginnings of Internet" http://www.nethistory.info/History%20of%20the%20Internet/origins.html (2006-05-24).

[1221] APARNET was funded by the Advanced Research Projects Agency (ARPA). ARPA later changed its name to Defense Advanced Research Projects Agency (DARPA) in 1971 and 1996. Leiner, Cerf, Clark et al "A Brief History of the Internet" http://www.isoc.org/internet/history/brief.shtml (2006-05-24).

[1222] See for example Hiller and Cohen *Internet Law and Policy* (2002) 6 and Edwards and Waelde *The Law and Internet: Regulating Cyberspace* (1997) 15. ARPA was a branch of the military that was responsible for the development of covet systems and weapons during the Cold War and APARNET was accordingly designed to protect between military installations. Bellis "Internet" http://inventors.about.com/library/weekly/aa09598.htm (2006-05-24).

[1223] Edwards and Waelde *The Law and Internet: Regulating Cyberspace* (1997) 15.

[1224] See Peter who writes that what amounted to Internet then (that is APARNET) was not intended to link people or enable people to communicate or be informed but rather to enable time sharing amongst research institutions. Time sharing enabled research institutions to share the research load by using the processing power of each other's computers especially where large calculations were concerned. Peter http://www.nethistory.info/History%20of%20the%20Internet/beginnings.html (2006-05-24)

[1225] Ferrera, Lichstein, Reder, August and Schiano *Cyberlaw: Text and Cases* (2001) 3.

[1226] Pioneers of the Internet existed before 1969, the date usually stated for the invention of the Internet. Leonard Kleinrock of Massachusetts Institute of Technology published the first paper and on packet switching, in 1961 and 1964 respectively. http://www.isoc.org/internet/history/brief.shtml

mail,[1227] telnet[1228] and TCP/IP.[1229] In 1973, APARNET extended its connection beyond the academic community to other networks and to other countries.[1230] Moreover, in the 1980's the power of the Internet was realised and the National Science Foundation joined APARNET to form NSFNET, in order to connect academic and scientific communities. The commercialisation of the Internet started in 1987 when the number of hosts increased from 23 on APARNET to 28,000 on NSFNET.[1231] The growth and expansion of Internet continued after this. The commercialisation of the Internet flourished with its most significant development – the WWW (World Wide Web). The WWW[1232] was developed by Tim Berners–Lee in 1991 and is often mistakenly referred to as the Internet. The court in *In re DoubleClick Inc Privacy Litigation*[1233] differentiated between the WWW and Internet:

> "The Internet is the physical infrastructure of the online world: the servers, computers, fiber – optic cables and routers through which data is shared online. The Web is data: a vast collection of documents

(2006-05-24). Peter agrees that there were others who conceived the idea of the Internet before 1969 and adds that the idea of Internet contrary to popular belief was not conceived solely in the United States. For instance Louis Pouzin, a French national introduced the idea of data grams and Donald Davies, an English National in 1969 also pioneered the packet switching technique. Peter "The Beginnings of Internet" http://www.nethistory.info/History%20of%20the%20Internet/origins.html (2006-05-23).

[1227] See the discussion of what e-mail is and how it works.

[1228] Telnet was developed by APARNET in 1972.Bellis http://inventors.about.com/library/weekly/aa09598.htm (2006-05-24).

Telnet is a program for TCP/IP networks such as the Internet that connects a computer to a network server. http://www.webopedia.com/TERM/T/Telnet.html (2006-05-24).

[1229] TCP/IP is a "set of standard operating and transmission protocols that structure the Web's operation". *In re DoubleClick Inc Privacy Litigation* 154 F Supp 2d 497, 501 (2001) 501.

[1230] The first International connections to APARNET were with the England (University College of London) and Norway (The Royal Radar Establishment of Norway) in 1973. http://www.internetvalley.com/archives/mirrors/davemarsh-timeline-1.htm (2006-05-23).

[1231] http://www.internetvalley.com/archives/mirrors/davemarsh-timeline-1.htm (2006-05-23).The timeline of Internet history is dotted with numerous and significant events however for purposes of this chapter only a few of these events will be discussed.

[1232] The WWW "allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites…the Web consists of a vast number of documents stored in different computers all over the world". *Reno v American Civil Liberties Union* 852. Prior to the WWW there was the Gopher system developed at the University of Minnesota; the Gopher system was not as colourful and interactive as the Internet but simply organised and displayed files on Internet servers. Edwards and Waelde *The Law and Internet: Regulating Cyberspace* (1997) 22.

[1233] 154 F Supp 2d 497, 501 (2001).

> containing text, visual images, audio clips and other information media that is accessed through the Internet". [1234]

Today, in addition to e-mail, the following facilities are available over the Internet: IRC (Internet Chat Relay)[1235], Usenet[1236] and FTP (File Transfer Protocol)[1237]. Internet users connect to the Internet through their Internet Service Providers. Their ISP's in turn connect them to the Internet through network interfaces, telephone lines, satellite dishes and cable television lines.[1238] More so, each Internet enabled computer has an IP (Internet Protocol) address and a DNS (domain name system). The IP address consists of sets of numbers separated by a dot. The DNS was implemented in 1984 to ease the burden of dealing with the digits in the IP address. The DNS identifies the IP address with text names and each domain name is associated with a unique IP number.[1239] The DNS divides addresses into top-level domain names such as .org for organizations and .gov for governments. There are also geographical top-level domain names for countries, such as .za for South Africa and .uk for the United Kingdom.[1240]

The Internet as a computer network operates with digital transmissions represented by the digits one and zero.[1241] Information on the Internet is transmitted in packets (with headers displaying the address information) by routers and servers depending on the address system, that is, the TCP/IP.[1242] The routers and servers would then examine the packets of data to determine the best route the packets should take in reaching the addressee. Hence, the various packets can take different routes in traveling to an

---

[1234] TCP/IP is a "set of standard operating and transmission protocols that structure the Web's operation". *In re DoubleClick Inc Privacy Litigation* 154 F Supp 2d 497, 501 (2001) 501.

[1235] IRC was developed in Finland in the late 1980's and enables people to connect and join live discussions with multiple users on the Internet. http://www.webopedia.com/TERM/I/IRC.html. (2006-05-25).

[1236] Usenet is a worldwide discussion system consisting of forums called newsgroups. Internet users can post messages and articles on the system which are then broadcast to other computer systems. Edwards and Waelde *The Law and Internet: Regulating Cyberspace* (1997)22.

[1237] FTP enables computer users to exchange files over the Internet through TCP/IP protocols. FTP works in the same as HTTP, a language of the Internet that is used to transfer web pages from a server to a user's browser. http://www.webopedia.com/TERM/F/FTP.html (2006-05-25).

[1238] Ferrera, Lichstein, Reder, August and Schiano *Cyberlaw: Text and Cases* (2001) 44.

[1239] Ferrera, Lichstein, Reder, August and Schiano *Cyberlaw: Text and Cases* (2001) 4.

[1240] Edwards and Waelde *The Law and Internet: Regulating Cyberspace* (1997) 16.

[1241] Ferrera, Lichstein, Reder, August and Schiano *Cyberlaw: Text and Cases* (2001) 6.

[1242] *Supra*.

addressee. Once the packets of data have reached their destination, the addressee's computer unpacks the packets for its user to read.[1243]

7.2.2 E-mail

E-mail has been defined as "a plain- language file that is sent by the sender, from computer to computer, via one or more mail servers, until it is delivered to the addressee's inbox"[1244] or a "small file which is sent to its destination through a series of linked computers, called e-mail servers."[1245] The court in *Reno v American Civil Liberties Union*[1246] stated that e-mail "enables an individual to send an electronic message – generally akin to a note or letter to another individual or a group of addresses".[1247]

It is generally accepted that e-mail predates the origins of the Internet.[1248] The creation of e-mail at APARNET was fortuitous. Hardy argues that because of APARNET's functions,[1249] the creation of e-mail as a tool for human communication was not planned and anticipated. After the creation of e-mail in 1971, however, the function of APARNET included human communication.[1250] The first person to send an e-mail message was Ray Tomlinson through The Send Message Command ("SNDMSG") network mail program, a program written by Tomlinson himself. Tomlinson sent this message across APARNET. The second message sent across APARNET announced the availability of e-mail and instructed users on addressing mail.[1251] Initially, the use

---

[1243] *Supra*.

[1244] Blanpain and Van Gestel *Use and Monitoring of E-mail, Intranet and Internet Facilities at Work: Law and Practice* (2004) 227.

[1245] Van Gestel *Forwarding Confidential Information on the Internet: Technological Possibilities of Monitoring and Control* in Blanpain *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 17 – 28.

[1246] 521 US 844 (1997).

[1247] *Reno v American Civil Liberties Union* 521 US 844 (1997) 851.

[1248] Hardy "The Evolution of APARNET Email" (1996) History Thesis submitted at the University of California at Berkeley http://www.ifla,org/documents/internet/hari1.txt (2006-05-25).

[1249] Hardy believed that APARNET arose out of military prerogatives and the need of a computer science research community. Hardy "The Evolution of APARNET Email" (1996) History Thesis submitted at the University of California at Berkeley http://www.ifla,org/documents/internet/hari1.txt (2006-05-25).

[1250] Hardy "The Evolution of APARNET Email" (1996) History Thesis submitted at the University of California at Berkeley http://www.ifla,org/documents/internet/hari1.txt (2006-05-25).

[1251] Dixon *Email Security Policy Implementation in Multinational Organisations with Special Reference to Privacy Law* (2003) 8.

of e-mail was restricted to the ARPANET community.[1252] In fact, the ARPANET community was the first to use e-mail as a substitute for paper correspondence.[1253]

E-mail is today one of the best forms of human communication because it combines two traditional forms of communication, namely speaking and letter writing. E-mail evolved to where it is today after undergoing various modifications to its original SNDMSG program. After SNDMSG there was READMAIL, which enabled users to read messages.[1254] READMAIL, was later modified to offer users a comprehensive list of available messages indexed by a subject and date. E-mail was also developed to selectively delete messages, forward messages, automatically address fields in message replies and handle messages. [1255]

E-mail revolves around client/server technology. In essence, client/server technology allows a computer to access and use the services of another computer.[1256] An e-mail client indicates the list of messages in a user's inbox and allows the user to select a message header and read the text of the message. The client further creates new messages, sends messages, allows attachments to the message and connects to the server.[1257] Two servers are responsible for transferring messages - the Simple Mail Transfer Protocol handles outgoing mail by transferring mails across the Internet and a Post Office Protocol which handles incoming mail.[1258]

7.3 E-MAIL AND INTERNET IN THE WORKPLACE

7.3.1 Introduction

Modern employers and employees not only communicate through letters, office memos and the spoken word, but also through electronic tools like the Internet,

[1252] Hardy "The Evolution of APARNET Email" (1996) History Thesis submitted at the University of California at Berkeley http://www.ifla,org/documents/internet/hari1.txt (2006-05-25).

[1253] Hardy "The Evolution of APARNET Email" (1996) History Thesis submitted at the University of California at Berkeley http://www.ifla,org/documents/internet/hari1.txt (2006-05-25).

[1254] Hardy "The Evolution of APARNET Email" (1996) History Thesis submitted at the University of California at Berkeley http://www.ifla,org/documents/internet/hari1.txt (2006-05-25).

[1255] Hardy "The Evolution of APARNET Email" (1996) History Thesis submitted at the University of California at Berkeley http://www.ifla,org/documents/internet/hari1.txt (2006-05-25).

[1256] Edwards and Waelde *The Law and Internet: Regulating Cyberspace* (1997) 14.

[1257] Edwards and Waelde *The Law and Internet: Regulating Cyberspace* (1997) 14.

[1258] Dixon *Email Security Policy Implementation in Multinational Organisations with Special Reference to Privacy Law* (2003) 10.

intranet and e-mail.[1259] Internet and e-mail are replacing the traditional modes of communication and exchanges such as the letter, fax, telephone and telex. E-mail has enabled instantaneous and inexpensive communications between individuals and it therefore comes as no surprise that e-mail is the preferred medium of communications between individuals in the workplace and further saves on the use and cost of paper and postage stamps. E-mail also enables its users to edit and store documents. In effect, certain e-mail messages and attachments constitute records of business transactions that may be used stored and used later for company business.[1260]

Internet and e-mail have not only altered the face of communication, but have also altered the business and workplace landscape. For instance, before the Internet individuals involved in team work had to be physically situated in the same place to be able to have team meetings or hold briefings. Today, Internet and e-mail usage have introduced the concept of global or virtual teams. Global or virtual teams are able to convene and hold meetings and briefings and in due course carry out their tasks without ever meeting one another and without being in the same office space, let alone the same city or country.[1261] Internet and e-mail have also redefined what constitutes a workday or workspace. Employees are accessible at any time and any place and have access to the workplace and work related data outside the workplace. Employees do not need to come into the workplace to effectively carry out their duties, nor do they need not be physically present in the workplace to be able to communicate and interact with the employer and other employees.[1262]

Insomuch as Internet and e-mail are the preferred medium of communications in today's workplace, employers feel the need to closely regulate or monitor their use by employees to avoid the threats associated with their use. The monitoring of employee Internet and e-mail use involves two competing interests in the employment context: namely, the employer's right to conduct his or her business as he or she deems fit and

[1259] Blanpain *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) xi.

[1260] Dixon *Email Security Policy Implementation in Multinational Organisations with Special Reference to Privacy Law* (2003) 12 – 13.

[1261] Wallace *The Internet in the Workplace: How New Technology is Transforming Work* (2004) 2 – 3.

[1262] See Cohen *Employee Perceptions of Invasions of Privacy Whilst Surfing the World Wide Web at Work* (2001) 2. Cohen points out that "…advances in technology have literally removed the face of the employer and replaced him/her with silent apparatuses". Cohen *Employee Perceptions of Invasions of Privacy Whilst Surfing the World Wide Web at Work* (2001) 2.

the employee's right to privacy. On the one hand, employers are concerned about the abuse and unrestricted use of these tools by employees and the harm that could result from this unrestricted use. On the other hand, employees are concerned about their right to privacy and the use of Internet and e-mail in the workplace. The monitoring of employee Internet and e-mail use can, for example, result in the employer having knowledge of an employee's personal and private information.[1263]

That said, it is important to bear in mind that the monitoring of employee communications by employers is not a new phenomenon. The monitoring of employees by employers certainly occurred before the introduction of electronic communications. In the past (as is still the case today), employers monitored use of company resources by using onsite managers and supervisors whose job was to physically observe and monitor employees at work, to ensure that employees were being productive and efficient. Nonetheless, in the information age employers prefer other, perhaps more efficient, methods to monitor their business operations in the interest of productivity.[1264] In short, electronic communications have enabled employers to monitor employees on a larger scale, without time and space constraints, and with a certain element of immediacy.

7.3.2 Arguments in favour of Monitoring Internet and E-mail Use in the Workplace

A number of reasons have been advanced to justify the monitoring of workplace tools such as Internet and e-mail. Some of these arguments are discussed below.

First, employers argue that as the owners of the Internet and e-mail system in the workplace, they have the right to specify how employees will use the Internet and e-mail provided by them.[1265] The employer as the owner of Internet and e-mail tools in

[1263] Hebert *Employment Privacy Law* (2009) § 8A: 2.

[1264] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 258.

[1265] Blanpain *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) xii. Individuals using company resources do not own these resources. Employees do not own the computers they use to surf the Internet or to send and receive e-mail messages. The company owns the computers, the network and even the e-mail address an employee is given to use during employment. For this reason, an employee often loses his or her e-mail address upon leaving the employer's employment. Moreover, when an employee receives an e-mail via the company e-mail address the e-mail is not delivered on the individual's private computer, it is delivered to the company's e-mail server. Furthermore, the company system administrator usually

the workplace also has a duty to ensure its employees use these tools appropriately and responsibly.[1266] An employer's failure to meet this duty may result in it being held liable for any misconduct by an employee through the use of Internet and e-mail.[1267] This argument may be referred to as the ownership argument and is premised on the idea that because the employer is the owner of the Internet and e-mail resources in the workplace, the employer has every right to determine when and how these resources shall be used by employees.

Secondly, employees may conduct a number of illegal activities via the employer's computer system. Employees may, for example, enter chat rooms while at work, use anonymous screen names and discuss confidential company information or post false information over the Internet about the company's financial performance. Furthermore, employees may appropriate the employer's trade secrets stored on the employer's computer system for the benefit of a competitor.[1268] Inappropriate use of Internet and e-mail in the workplace has also resulted in employers being held liable for copyright infringement,[1269] defamation[1270] and sexual and racial

---

backups employee files, e-mails etc… on the company computers and this information remains on the company's system even where the employee deletes the messages from his or her inbox and recycle bin. These files and e-mails ultimately are never really private instead they are in the very least personal. Sheehy *Monitoring and Control of Use of E-mail and the Internet by the Employee. Managements Point of View* in Blanpain *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 30.

[1266] Sheehy *Monitoring and Control of Use of E-mail and the Internet by the Employee. Managements Point of View* in Blanpain *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 30.

[1267] *Supra*.

[1268] *Shurgard Storage Centers Inc. v Safeguard Self Storage Inc* 119 F. Supp.2d 1121, 174 A.L.E. Fed. 655.

[1269] The Internet can facilitate and exacerbate employees infringing copyright laws particularly when downloading software programs with registered patents via the company's system. In addition to facing liability for the copyright infringements of their employees, employers may find themselves liable for the copyright infringements of third parties such as subscribers of a bulletin board. In *Playboy Enterprises Inc. v Russ Hardenburgh Inc* 982 F. Supp. 503, 1998 Copr.L.Dec. P 27,771 a magazine publisher brought an action against the operator of an electronic bulletin system board distributing and displaying copies of the magazine publisher's adult photographs. The operators of the bulletin board encouraged subscribers to upload files including adult photographs onto the system and employees (of corporation operating the bulletin board) viewed all uploaded files before moving them to the general files which were available to all subscribers.

[1270] Employers may have claims of defamatory e-mail communications made against them by various individuals including their employees. For example in *Meloff v New York Life Insurance Co*51 F.3d 372 an employee M, brought an employment defamation action against her former employer after she was dismissed and the reason given for her dismissal was "credit card fraud". The reason for her dismissal was communicated to a number of individuals in the company via electronic mail. The electronic mail was entitled "Subject: Fraud" and alleged that M had used her corporate credit card in

harassment[1271].[1272]Employers may also attract negative publicity where an employee, for example, visits a website displaying sexually graphic images and the website captures and stores the employer's IP address and domain name.[1273] This argument may be referred to as the illegal activity argument and in sum holds that an employer is entitled to monitor an employee's e-mail and Internet activity in order to ensure that the employee is not engaging in any illegal activities in the name of the employer or through the use of the employer's resources.

Thirdly, employers sometimes take the view that Internet and e-mail can lure employees away from company business and that unrestricted e-mail and Internet usage by employees will encourage employees to spend time on personal business, which, in turn results in time wasting, poor customer service, lost business and profits and high overheads.[1274] Furthermore, a company's mail server and Internet may become congested or its transmission bandwidth may be strained by employees sending and receiving voluminous e-mails (containing short films, photos or power point presentations) that are not work related, thereby slowing down the networks' response.[1275]

Employers also argue that the monitoring of employee and Internet usage enables them to measure employee work performance and to provide feedback on such performance.[1276]

Fourthly, employers argue that absolute computer security is problematic in the workplace and that electronic communications are created with ease but can be difficult or sometimes impossible to retrieve. Consequently, the restricted use of

---

an inappropriate manner after M charged her commuter train ticket for traveling to and from her workplace to her company credit card

[1271] The court in *Autoli ASP Inc. v Department of Workforce Services* 29 P.3d 7 12 – 13 86 FEP Cases 228 (Utah App. Ct. 2001) reinforced the fact that "e-mail transmission of sexually explicit and offensive material such as jokes, pictures, and videos, exposes the employer to sexual harassment and sex discrimination lawsuits…".

[1272] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 253.

[1273] *Supra*.

[1274] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 252 – 253.

[1275] *Supra*.

[1276] Hebert *Employment Privacy Law* (2009) § 8A:2.

Internet and e-mail by employees is necessary in light of the risks associated with the use of Internet and e-mail, such as the loss of confidential information.[1277] For example, a Trojan Horse program, which is capable of sending information to undisclosed third parties without a user's knowledge, can be sent with an e-mail that appears harmless to a user.[1278] Sensitive information sent over e-mail, unless encoded, may be intercepted or its contents forged or altered. Furthermore, viruses can be transmitted via an e-mail sent to a recipient.[1279]

7.3.3 Arguments against the Monitoring of Internet and E-mail Use in the Workplace

A number of arguments against the monitoring of Internet and e-mail usage in the workplace have been advanced. Below, a selection of the more important of these arguments is considered. The essence of all of these arguments is primarily a theme that resonates throughout this dissertation, namely that employees have a right to privacy even in the workplace. Because employees take the view that their fundamental right to privacy does not cease to exist once they enter the employment relationship, it is not surprising that they further expect employers to respect their right to privacy in the workplace. This is so especially because "the once clearly demarcated boundaries between work and private life have become more and more blurred and in many cases eroded through new ways of working and technological developments"[1280]. In addition, new forms and patterns of work such as teleworking, homeworking and location independent working, as well as the growth of electronic communications via Internet, computers and mobile phones have all served to blur the line between an individual's workplace and home.[1281]As a consequence, it is argued that employees should be permitted some personal use of an employer's information technology resources for appropriate online activities.

[1277] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 253.

[1278] Blanpain and Van Gestel *Use and Monitoring of E-mail, Intranet and Internet Facilities at Work: Law and Practice* (2004) 228-229.

[1279] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 252.

[1280] Skyte *The Protection of Privacy at Work* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 1- 8.

[1281] *Supra*.

Moreover, as is the case with ordinary mail, e-mail is a private means of communication in which the recipient is chosen by the author and its content usually intended solely for the recipient. For this reason, it is argued that e-mail often is intended to be private[1282] and a reasonable expectation of privacy should be attached to personal e-mails employees send on or over the company system.[1283] For instance, in the United States the Third Circuit Court held in *Vernars v Young*[1284] that because individuals had a reasonable expectation of privacy that their mail will not be opened and read by unauthorised persons, the same reasoning could be extended to the treatment by employers of their employee's personal mail.

At the same time, security measures applied with respect to workplace computers and networks (such as confidential passwords and unique usernames) give the impression that computers are akin to personal desks or lockers in which employees have been held to have a reasonable expectation of privacy.[1285] In this regard it was held by the Texas Court of Appeal in *K-Mart v Trotti*[1286] that, as general rule, employees have a right to privacy in items locked in a desk, file cabinet, or locker if their employer does not require them to provide the supervisor with a key or a combination to open a lock.

It is also argued that the use of e-mail and Internet enhances employees' computer skills which may be applied in their workplaces.[1287] In the same vein, the personal use of company resources may lead to an increase in productivity and may improve employee morale and cement loyalty. It may further allow employees to experience a sense of ownership in the company's resources. It is also contended that it is unrealistic for employers to expect their employees to cease contact with family and friends upon entering the workplace and that employers should primarily be

[1282] See *Vernars v Young* 539 F.2d 966 (3d Cir. 1976).

[1283] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.*) On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 257.

[1284] 539 F.2d 966 (3d Cir. 1976).

[1285] *Kesan First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251257.

[1286] 677 S.W.2d 632 (Tex. Ct. App.1984).

[1287] *Kesan First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 257.

concerned with whether or not an employee is doing his or her job and not with whether the employee is spending significant time on the Internet.[1288]

Lastly, the restriction of on-line activities may increase stress levels of employees. Studies have indicated that electronic monitoring is a source of stress as it can take a physical and emotional toll on employees and ironically result in decreased productivity in the workplace.[1289]

In summary, communications in the workplace take place not only through the spoken word but also through use of electronic tools like the Internet, intranet and e-mail. Internet and e-mail are replacing the traditional modes of communication and exchanges such as the letter, fax, telephone and telex. Internet and e-mail have not only altered the face of communication, but have also altered the business and workplace landscape. The use of Internet and e-mail at work has also redefined what constitutes a work day or workspace. Employees are accessible at any time and any place and have access to the workplace and work related data outside the workplace. Because Internet and e-mail are the preferred and most prevalent medium of communications in today's workplace, employers feel the need to closely regulate or monitor the use of these communications by their employees in order to avoid the risks associated with their use. As such, the monitoring of employee use of workplace e-mail and Internet brings into play two competing interests, namely the employer's right to conduct his or her business as he or she deems fit and the employee's right to privacy.

Employers advance a number of reasons to justify the monitoring of employer workplace tools such as Internet and e-mail. These reasons are formulated on the basis of economic and social reasons and are primarily aimed at ensuring a productive and efficient workplace.

At the same time, a number of arguments against the monitoring of Internet and e-mail usage in the workplace have also been advanced. The basis of these arguments

---

[1288] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 255.

[1289] Kesan *First Principle' Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 251 258.

remains the existence of the right to privacy as a fundamental right, which also deserves recognition and protection in the workplace. Related arguments against monitoring of Internet and e-mail usage in the workplace are based on the realities and flexible nature work in the modern sense and the modern workplace, that these information systems encourage and should protect private use and that this may actually serve to increase economic performance. Viewed negatively, restrictions on privacy in the workplace through monitoring of Internet and e-mail usage may serve to increase anxiety and stress in the workplace, while such a restriction also runs the constant danger of suppressing creativity and innovation, generally recognised as positive side-effects of environments where privacy is allowed to flourish.

The further discussion in this chapter will focus on how the selected jurisdictions have chosen legally to respond to the challenges raised by monitoring of Internet and e-mail usage.

7.4 SOUTH AFRICA

7.4.1 Introduction

Section 14(d) of the South African Constitution provides that everyone has a right not to have the privacy of their communications infringed. This aspect of the South African general right to privacy is known as informational privacy.[1290] Privacy in this sense means control over information about oneself, a conception of privacy that was discussed in chapter 4. Furthermore, as also indicated in chapter 4, this form of control is "control over when and by whom parts of us can be seen or heard, touched, smelled or tasted by others"[1291] and further "control over acquaintance with one's personal affairs".[1292]

Informational privacy, according to De Waal and Currie should be construed as safeguarding the interest of an individual to restrict the collection, storage and use of personal information concerning him or her. The individual's expectation of informational privacy must be reasonable.[1293] The Constitutional Court in *Mistry*

[1290] De Waal and Currie *Bills of Rights Handbook* 5th ed (2005) 323.

[1291] Parker "A Definition of Privacy" (1974) 27 *Rutgers Law Review* 238.

[1292] Gross "The Concept of Privacy" (1977) 42 *New York University Law Review* 172-174.

[1293] De Waal and Currie *Bills of Rights Handbook* 5th ed (2005) 324.

considered the following factors to determine whether an individual's expectation of informational privacy was reasonable in the circumstances: whether the information was obtained in an intrusive manner; whether it was about intimate aspects of an individual's life; whether it involved data provided by the individual for one purpose which was then used for another purpose; and whether it was disseminated to persons from whom the individual could reasonably expect such information would be withheld.[1294] In *Mistry* the Constitutional Court found that there had been no violation of the individual's informational right to privacy, because the information concerned a possible violation of a law by the individual and was communicated to the relevant official in the Medical Council by a member of the public. [1295]

7.4.2 Legislation

Apart from Constitutional provisions, and in contrast to most of the policies and practices discussed in chapter 6, there are a number of pieces of legislation which protect (and protected) the individual right to privacy in their communications by regulating the monitoring of Internet and E-mail communications in a direct or indirect fashion.

7.4.2.1 Interception and Monitoring Prohibition Act (IMPA)

The Interception and Monitoring Prohibition Act[1296] ("IMPA") came into effect on 1 February 1993, before the interim Constitution of 1993 and arguably was the first piece of legislation applicable to monitoring of Internet and E-mail communications. Its purpose was to prohibit the interception and monitoring of certain communications and conversations and to provide for authorisation to do so in certain circumstances. IMPA repealed section 118A of the Post Office Act[1297], which had earlier prohibited the wiretapping of a landline. For this reason, the purpose of IMPA placed emphasis on the fact that it aimed at the prohibition of the interception and monitoring of telephone conversations or the interception of postal articles communications. In actual fact, no mention was made of the regulation of the interception and monitoring

[1294] De Waal and Currie *Bills of Rights Handbook* 5th ed (2005) 325.
[1295] De Waal and Currie *Bills of Rights Handbook* 5th ed (2005) 324.
[1296] Act 127 of 1992.
[1297] Act of 1958.

of Internet and e-mail communications.[1298] In contrast to section 118A, which was widely criticised for being "largely toothless" and limited, IMPA introduced harsh penalties for its contravention and signified a strong stance against illegal interception and monitoring.[1299]

Despite the fact that the Act primarily focused on telecommunications, there appeared to be room for the argument that the provisions of the Act were broad enough to include Internet and e-mail communications. First, section 1 of the Act defined a "telecommunications line" to include "any apparatus, instrument, pole, mast, wire, pipe, pneumatic or other tube, thing or means which is or may be used for or in connection with sending, conveying, transmitting or receiving of signs, signals, sounds, communications or other information". Secondly, a "monitoring device" was defined in the section 1 as "any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any conversation or communication". Thirdly, section 2 of the Act which contained the prohibition on interception and monitoring provided as follows:

"(1) No person shall –

a) intentionally and without knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line or;

b) intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning any person, body or organisation".

Because the word "person" was not defined it arguably included an employer. Section 2(1)(a) required the interception to be intentional and without consent or knowledge of the dispatcher (the party sending the communication). Section 2 further related to the interception of a communication that has been sent, is being sent and is intended to be sent. As such, in the employment context, an employer would have been able to intercept an employees' Internet or e-mail communication at any point in time. With reference to the transmission of communications, the phrase "transmitted by telephone

[1298] Mischke "The Monitoring and Interception of Electronic Communications: Obtaining and Using E-mail and Other Electronic Evidence" (2001) Vol 10 *CLL* 91 92.

[1299] *Protea Technology Ltd & Another v Wainer and Others* 1997 (3) All SA 594 (W) 604.

or in any other manner over a telecommunications line" also appeared to cover Internet and e-mail communications, seeing as Internet and e-mail communications are to a large extent transmitted over a telecommunications line.[1300] Section 2(1)(b) stated that no one may intentionally monitor a conversation or communication through the use of a monitoring device for the purpose of gathering confidential information on a person, body or organisation. This meant, with regard to Internet and e-mail communications in the workplace that employers were not permitted to monitor such communications for the purpose of gathering confidential information on their employees. IMPA did not define the phrase "confidential information". However, courts have defined "confidential information" to mean "information [the communicator] does not intend to disclose to any person other than the person to whom he is speaking and any other person to whom the disclosure of such information is necessarily or impliedly intended to be restricted"[1301] and "information upon which the law confers the attribute of confidentiality"[1302]. In *Protea Technology Ltd & Another v Wainer and Others* it was further held with regard to the provisions of section 2 (1)(b), that the purpose of monitoring could be determined by examining the contents of the communication concerned.[1303]

7.4.3 Case Law

Mention has to be made of *Moonsamy v The Mailhouse*[1304] where a different view of IMPA and its applicability in the private sphere was taken. It was held that IMPA was not concerned with interception and monitoring in the private sphere and therefore could not be applied to private sector employers and employees. Rather, it was held that IMPA was intended for use by public agencies such as the police, military and intelligence services in gathering evidence during the investigation of a crime.[1305]

7.4.3.1 Case Law before RICPCIA

Courts also addressed IMPA's application with regard to interception and monitoring of telephone conversations and the admissibility of the evidence of such recordings.

[1300] Mischke "The Monitoring and Interception of Electronic Communications: Obtaining and Using E-mail and Other Electronic Evidence" (2001) Vol 10 *CLL* 91 93.

[1301] *Protea Technology Ltd & Another v Wainer and Others* 1997 (9) BCLR 1255 (W) 1234.

[1302] *S v Kidson* 1999 (1) SACR 338 347.

[1303] 1997 (9) BCLR 1255 (W) 1234.

[1304] 1999 20 ILJ 464 (CCMA).

[1305] 467-468.

The admissibility of telephone conversation recordings obtained in contravention of IMPA was at issue in *Tap Wine Trading CC v Cape Classic Wines (Western Cape)*[1306]. The Court in *Tap Wine Trading* found that participant electronic monitoring does not breach the provisions of the Act and the constitutional right to privacy. In this regard, the Court drew a distinction between participant surveillance and third party surveillance. Participant surveillance, according to the Court, concerns the surveillance by one of the parties to the communication without the knowledge of the other party. Third party surveillance, on the other hand, concerns surveillance by a person or body other than the participants to the communication. The distinction between third party and participant surveillance was accepted by J Cameron in *S v Kidson*[1307]. Cameron J held that the intention of the legislature was for section 2 (1)(b) to apply to third party surveillance and not participant surveillance[1308].[1309]

In *Protea Technology Ltd & Another v Wainer & Others*[1310] (decided under the Final Constitution), the employer had recorded phone calls made by the employee in the workplace without his consent. These phone calls were used in court to prove that the employee was acting in breach of a restraint of trade agreement. The employee argued that the recording invaded his right to privacy and contravened IMPA and that the court had no discretion to admit the evidence. The Court considered two issues: first, whether the employer's conduct amounted to a breach of privacy and, secondly, whether the common law power of a court to admit evidence irrespective of the means by which it is obtained (that is the relevance test in *Goosen v Caroline's Frozen Yoghurt Parlour*[1311]) remained valid under the new Constitutional dispensation. With

[1306] 1999 (4) SA 194 (CC).

[1307] 1999 (1) SACR 338.

[1308] 348.

[1309] See also *S v Dube* 2000 (2) SA 583 (NPD). Mischke "The Monitoring and Interception of Electronic Communications: Obtaining and Using E-mail and Other Electronic Evidence" (2001) Vol 10 *CLL* 91 96.

[1310] [1997] 9 BCLR 1255 (W).

[1311] 1995 16 ILJ 396 (IC). *Goosen* was decided under the Interim Constitution and concerned the dismissal of an employee who after a disciplinary hearing sought to rely on telephone transcripts that he obtained without the consent of the employer to show that the chairperson of the disciplinary hearing was biased. At issue was the admissibility of the recordings. The Industrial Court found the recordings admissible and reasoned in this regard that the test to be applied when determining the admissibility of the evidence is whether the evidence is relevant to the matters in issue. (This test is commonly referred to as the relevance test). The Court further held that it had no need to concern itself with the manner in which the evidence was obtained as long as the evidence was not obtained under duress and the 'accused' was not obliged to give self incriminating evidence. The Industrial Court in considering the privacy provision in section 13 Constitution and the limitations clause in

respect to the first issue, the Court held that the right to privacy requires a subjective expectation of privacy which society recognizes as objectively reasonable. More importantly, the Court also held the employee's subjective expectation of privacy not to be objectively reasonable in light of the fact that the employee was in a position of trust and the telephone calls were made from the employer's premises within business hours. The Court concluded that, because the parties were in an employment relationship, the conversations relating to the employer's affairs were not private and therefore not protected by the Constitution. With respect to the second issue, the Court found that the discretion to admit illegally obtained evidence had to be exercised with reference to the substance of section 36(1) of the Constitution, meaning that the competing interests had to be balanced. The Court accordingly concluded the relevance test in *Goosen* was inconsistent with the Constitution, but still recognised discretion to be exercised on a case-by-case basis to admit illegally obtained evidence.

At issue in *Moonsamy v The Mailhouse*[1312] was whether the employer was entitled to use evidence at a disciplinary hearing which it had obtained by intercepting and recording the employee's telephone calls in his office and which subsequently contributed to the employee's dismissal. The employee argued that the evidence contravened IMPA and the Constitution. As mentioned above, the arbitrator established that IMPA applied only to interception or monitoring carried out by the police and the Defence Force. The tribunal based this on the fact that section 3(2) of IMPA provides that any application to a judge for a directive shall be made by a police officer, or an army officer, or a member of the intelligence services: "This would seem to be a clear indication that [IMPA] was intended to be used by only the police or military, including intelligence services, and is not concerned with interception or monitoring in the private sphere but is rather concerned with gathering of evidence by public agencies during the investigation of a crime"[1313]. The arbitrator also confirmed that the relevance test formulated in *Goosen* was contrary to the right to privacy contained in the Constitution. The arbitrator concluded that the recording

section 33 of the Constitution stated that although the concept of human rights emanated from the relationship between individuals and the state it could foresee circumstances in which the concept could be extended to relations between individuals. Collier "Workplace Privacy in the Cyber Age" (2002) 23 *ILJ* 1743 1745.

[1312] 1999 20 ILJ 464 (CCMA).

[1313] 467.

was in violation of section 14(d) of the Constitution and proceeded to consider whether the infringement was justified in terms of the limitations clause contained in the Constitution.

In considering whether the infringement was justified,[1314] the tribunal considered the following issues: the nature of right the court; the importance of the purpose of the limitation; the extent and nature of the limitation; the relation between the limitation and its purpose; and whether less restrictive means to achieve the purpose were available. In respect of the nature of the right, the tribunal held that the employee had a reasonable expectation of privacy in respect of calls made at his employer's premises.[1315] With reference to the importance of the purpose of the limitation, the tribunal reasoned that the employer considered its actions necessary for financial preservation and therefore the employee's right to privacy had to be qualified. The arbitrator observed that the court in *Protea Technology* identified the competing interests to be the employee's right to privacy versus the employer's right to economic activity. The right to economic activity is no longer guaranteed in terms of the Final Constitution and has been replaced by section 22 of Constitution guaranteeing freedom of trade, occupation and profession. The introduction of section 22, according to the tribunal, seemed to indicate that the framers of the Constitution preferred "the employee's personal right to the more amorphous (consequently controversial) right to economic activity".[1316] In considering the nature and extent of the limitation, the arbitrator opined that an employer might have a right to ask an employee to disclose the number of personal calls he or she made during working hours.[1317] With regard to the relationship between the limitation and its purpose, the tribunal reasoned that if an employer showed that telephone tapping was the only method through which it could secure essential evidence against an employee, its use may be justified. As regards less restrictive measures to achieve the purpose, the tribunal reasoned that if the only method to obtain evidence was telephone tapping, the employer should have sought prior authorization.[1318]

[1314] See section 36 of the Constitution.

[1315] 470.

[1316] 470 – 471.

[1317] 472.

[1318] Supra.

In sum, and prior to IMPA coming into effect, "all relevant evidence which was not rendered inadmissible by an exclusionary rule was admissible in a civil court irrespective of how it was obtained".[1319] This unrestricted use of evidence resulted in abuse and violations of privacy. IMPA restricted the manner in which evidence was obtained and further introduced penalties for obtaining evidence in a manner contrary to the Act's requirements. The language of IMPA further points to the fact that the legislation was intended to apply to state agencies which were in the business of intelligence gathering for purposes of investigating and ultimately combating criminal activities.

Up until the tribunal's reasoning in *Moonsamy v The Mailhouse*, it appears as if courts were quite willing to find that the application of IMPA was wide and that the Act applied to interception and monitoring in the private sphere. One reasons for this is that certain of terms in IMPA and its general prohibition were couched widely enough for the argument to be made that the Act could well regulate the interception and monitoring in places such as the workplace.

The decision of *Moonsamy v The Mailhouse* altered this view when it cast doubt over the application of the Act in relation to interception or monitoring in the employment context. It is submitted that the arbitrator in *Moonsamy v The Mailhouse* was correct in finding that the Act aimed to regulate the interception and monitoring of communications by state institutions such the police, the military and other public agencies during the course of criminal investigations. Section 3(2) of IMPA is indicative of this fact because it provides that only a judge may issue a directive on application by a police officer, or an army officer, or a member of the intelligence services enabling such persons to intercept and monitor communications: The fact that the Act was intended to apply in the private sphere was later confirmed by the promulgation of Regulation of Interception of Communications and Provision of Communication – Related Information Act[1320] ("RICPCIA"), IMPA's successor. It is, however, important to bear in mind that it was only a matter of time before IMPA was replaced by legislation more attuned to advancements in technology. As pointed out in

[1319] *Protea Technology Ltd & Another v Wainer and Others* [1997] 3 All SA 594 (W), 605.

[1320] Act 70 of 2002.

Protea Technology[1321] the language of IMPA concerned modes of communication, such as telegrams and telefaxes, that people in this day and age make little or no use of.

7.4.3.2 The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICPCIA)

The Regulation of Interception of Communications and Provision of Communication – Related Information Act[1322] ("RICPCIA"), IMPA's successor, is concerned with interception in both the private and public spheres and applies to private sector employees and employers. RICPCIA came into force and effect on the 30 September 2005 and provides that no one may directly or indirectly intercept communications (including telephone calls, cell phone calls, e-mail and instant messaging, as well as SMS's). Specifically, the Act prohibits the intentional interception or authorisation of an interception of any communication in the course of its occurrence or transmission.

Section 2 of the Act contains the general prohibition and reads as follows:

> *"Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept*[1323] *or attempt to intercept, at any place in the Republic, any communication*[1324] *in the course of its occurrence of transmission."*

Notwithstanding the general prohibition in section 2 of RICPCIA, the Act recognises 3 instances in which the lawful interception of communications may take place:

a) The Act in section 4(1) permits anyone other than a law enforcement officer to intercept certain communications if that person is a party to the communication. The Act does not define the term party, but within its

---

[1321] 603.

[1322] Act 70 of 2002.

[1323] 'Intercept' is defined as 'the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all the contents of the communication available to a person other than the sender or recipient or intended recipient of that communication, and includes monitoring of any such communication by means of a monitoring device; viewing, examination or inspection of the contents of any indirect communication; and diversion of any indirect communication from its intended destination to any other destination.'

[1324] 'Communication' is defined as including both direct and indirect communications.

ordinary usage and meaning "party" includes the sender, recipient and probably the provider of the communications (i.e. the employer). [1325]

b) If one of the parties to the communication has given their prior consent in writing to such interception (section 5). The Act in section 5(1) again allows any person other than a law enforcement officer to intercept communications where one of the parties to the communication has given prior written consent to the interception. The consent to the communication must be given before the interception occurs and be in writing. The consent of an employee may be included in the terms and conditions of the employee's contract of employment which may include an e-mail and Internet policy.[1326] In the course of the carrying on of any business.[1327]

c) Section 6 permits any person to intercept any direct communication by means of which a transaction is entered into in the course of that business (section 6(1)(a)), or which relates to the business (section 6(1)(b)), or which otherwise takes place in the course of carrying on of that business. The 'business exception' provides the employer with lawful means of intercepting business communication without having to obtain consent from the employee. In terms of the exception, section 6(2) provides certain requirements an employer must meet in order for its interception to be lawful.

These requirements relate to the nature and content of the intercepted communications (it must be communication related to the business or must take place during the course of the business); the purpose for which the interception is effected (it must be for legitimate purposes such as to establish the existence of facts, investigate or detect unauthorized use of the employer's telecommunications system or to secure the effective operation of the employer's telecommunications system); the nature of the telecommunication system involved (the telecommunication system must be provided for use wholly or partly in connection with the business of the employer); and the measure of control exercised over the interception process by the system

[1325] Beech 'The Right of an Employer to Monitor Employees' Electronic Mail, Telephone Calls, Internet Usage and Other Recordings' (2005) 26 *Industrial Law Journal* 650 656.

[1326] Beech 'The Right of an Employer to Monitor Employees' Electronic Mail, Telephone Calls, Internet Usage and Other Recordings' (2005) 26 *Industrial Law Journal* 650 658.

[1327] The term 'business' is defined as 'any business activity conducted by any person, including activities [the] activities of any private or public body.

controller(the system controller has to make all reasonable efforts to inform all individuals using the system in advance that interception of all communications may take place). The business exception only applies to indirect communications. An "indirect communication" is defined in section 1 of the Act as the transfer of information including a message, or any part of a message, whether in the from of speech, music or other sounds, data, text, visual images (animated and non-animated), signals, or radio frequency spectrum, transmitted in whole or in part by means of a postal service or telecommunication system. Hence e-mail and Internet usage (as well as telephone conversations) by employees may be intercepted by the employer within the parameters of this exception. In contrast, section 1 of the Act defines a "direct communication" as an oral communication other than an indirect communication between two or more people that occurs in the immediate presence of all the people participating in that communication, or the utterances of a person participating in an indirect communication, if the utterances are audible to another person who, at the time of the indirect communication, is in the immediate presence of the person participating in the indirect communication. (An employer may not monitor direct communications such as face to face discussions or post, since these are not transmitted over a telecommunications system.) Noteworthy is the fact that the exception ceases to apply once the e-mail has reached it destination, since the Act indicates that the interception must occur during the course of transmission.

7.4.3.3 Case Law after RICPCIA

Bamford & Others/Energizer (SA) Limited[1328] is one of the earliest decisions to put into perspective or effectively address the issue of employee privacy in the workplace, particularly in relation to the use of the employer's e-mail and Internet facilities. In this case Energizer, a leading manufacturer of batteries for electrical appliances, summarily dismissed a group of its female employees for violating the company's e-mail policy. At issue in *Bamford* was the fairness of this summary dismissal. The company justified the dismissal of the applicants on the following charges:

1. The repeated violation of company policies and procedure regarding the use of company e-mail.
2. The repeated receipt and forwarding to colleagues of obscene pornographic, racist and sexist material and jokes.

[1328] [2001] 12 BALR 1251 (P).

3. The violation of company procedures regarding the work environment.[1329]

The applicants did not deny receiving and forwarding the said material and jokes. However, they contended that there was no clear rule against the private use of e-mail, that their right to privacy was invaded, and that there was a discriminatory application of discipline by the respondent.[1330] In respect of last-mentioned claim, the applicants argued that the standard of behaviour required by the respondent as regards company e-mail use was flawed because, were it applied across the board in business and industry, almost every employee would be at risk of losing their jobs.[1331] In other words the applicants were asserting that even if there was a rule in place prohibiting the receipt and forwarding of pornographic, racist and sexist material and jokes, this rule was not consistently applied in the workplace, the more so because they were aware of other employees who received and forwarded such material and jokes without any disciplinary being taken against them.

In considering these arguments the arbitrator found that although the standard policy document did not explicitly state the prohibitions about e-mail use in the workplace, there was enough in the document to suggest such prohibitions. The background of the applicants, which the arbitrator described as 'middleclass…not bereft of education', convinced the arbitrator that the applicants should have known that their conduct was not socially acceptable.[1332] The arbitrator further stated that some of the materials received and forwarded by the applicants were 'contrary to what would circulate amongst self-respecting people.' Lastly, the arbitrator drew on common sense. He stated that even if the policy was silent on prohibitions against e-mail use in the workplace, common sense should have directed the applicants that the grotesqueness of the material they were receiving and forwarding had no place in the workplace.[1333]

The arbitrator proceeded to find that the penalty of dismissal could be reasonably expected in the circumstances and also relied on the traditional arguments employers

[1329] 1252.
[1330] 1257.
[1331] 1257.
[1332] 1257.
[1333] 1257.

advance to justify workplace surveillance of employee e-mail and Internet usage. In particular, the dismissals were found to be fair because of:

1. The risks posed by the trafficking;
2. The grotesqueness of the images.
3. The danger of the outside world becoming aware of the exchanges of these messages and the further risk of the domain name of the respondent being associated with such material and jokes.
4. The respondent's exposure to trademark violations as the applicants resorted to entertaining themselves with trademark parodies.
5. The offence that could be taken to the material and jokes by other staff members.
6. The embarrassment to the employer by the exchange of such material and jokes.[1334]

As far as violation of the applicants' right to privacy was concerned, the arbitrator found this not to be the case. The arbitrator found that the material and jokes concerned could not be described as personal in nature, the personal dignity or personal affairs of the applicants had not been affected in any way, and the material and jokes concerned were stored in the respondent's computers and could not be considered personal communications.[1335] As such, *Bamford* broke new ground in that it made clear that, even where there is no (explicit) policy regulating employee use of e-mail in a workplace, employees cannot argue that they had a reasonable expectation of privacy in respect of all received and forwarded communications in that workplace.

The applicant in *Cronje/Toyota Manufacturing*[1336] had been dismissed for circulating a cartoon he received via company e-mail. The cartoon superimposed President Mugabe of Zimbabwe head's on a gorilla's body. The bigger gorilla depicted in the cartoon was holding a smaller gorilla, also with Mugabe's features, with a caption alongside worded "*Mugabe and his right hand man. We want the farms to grow more bananas*." Although privacy considerations did not play a role in this case, the

[1334] 1269.

[1335] 1271.

[1336] [2001] 3 BALR 213 (CCMA).

respondent argued that it found it necessary to dismiss the applicant based on the following:

1. race and race related issues are familiar and important issues on the shop floor;
2. the employer's factory employed a total of 4500 employees and 77 percent of these employees were black. This means one had to take extra care and display extra sensitivity towards the race issue, specially in light of the country's past;[1337]
3. concern that the incident would cause serious problems such as industrial action on the shop floor;[1338]
4. the employer had dealt harshly with race related incidents in the past;
5. employees knew that racially offensive remarks and the distribution of racially offensive material or sexually explicit material would be dealt with in a very serious light;
6. the employer's internet and e-mail code specifically prohibited the display and/or transmission of any offensive racial, sexual, religious or political images, documents and images on the company system;[1339]
7. the depiction of a black person as an ape is racist and there is still a section of the white population that associated black people with apes; and
8. the respondent's shop stewards and black employees found the cartoon very offensive in that it portrayed black people as apes.[1340]

The employee argued that he did not regard himself or the cartoon as racist, which is why he readily distributed the cartoon to others. The applicant also acknowledged that he was aware of the company's e-mail policy, but was not aware of the fact that the cartoon fell within the policy's prohibitions.[1341]

On analysis of the evidence and argument, the presiding commissioner found that the cartoon was racist and inflammatory:

> "The subject of the crude superimposition is President Mugabe, but the picture and to no lesser extent, the caption, fall square into the crude,

[1337] 216.
[1338] 216.
[1339] 215.
[1340] 218.
[1341] 219.

> offensive, racist stereotype developed over centuries by white people that associate black people with primates, beings of lesser intelligence and lower morality…The fact that the offensive, racist stereotype associating black people with apes exists is not disputed. This is a matter of deep moral, social and cultural sensitivity to black people, and this sort of offensive racial stereotyping is not by any means limited to black people. One recalls the grossly offensive and inflammatory caricatures of Jews which were specifically created by the Nazi party in the 1930's, in order to alienate Jews from other Germans, as a prelude to the horrific social engineering that was to end in the holocaust. Jews were depicted as evil, as thieves, as base money lenders, as killers of German babies and the like. In a less crude form, these caricatures were deployed by anti-Semitic elements amongst Afrikaners prior to the Second World War. These caricatures were and are still are, deeply offensive to Jewish people, and not only to the particular person or leader depicted in the caricature. They offend people's self-image as a cultural racial entity. The depiction of an Islamic leader as a pig would be found to be deeply reprehensible by Muslims in this and in many countries. In the same way the depiction of a black person as an ape is racist, inflammatory and inherently wrong."[1342]

Although the issue of employee privacy in the context of company e-mail systems was not raised in *Dauth/Brown and Weir's Cash and Carry*[1343], the matter deserves discussion since it adds to the general tenor of how South African courts and tribunals have addressed employee privacy with regard to e-mail use. In *Dauth/Brown* the applicant, a marketing manager, was dismissed for sending an e-mail on the internal company e-mail service to over 100 persons including managers and directors.[1344]

The applicant argued that he could not be held responsible for the contents of the e-mail as he was in a state of diminished responsibility because of his prescription drug intake for depression, insomnia and physical pain and emotional stress brought on by

[1342] 222 and 223.

[1343] [2002] 8 BALR 837 (CCMA).

[1344] 838.

his marital problems and the state of anxiety at losing his job.[1345] On analysis of the evidence and arguments, the commissioner found that the applicant was not influenced by his medication when he sent the e-mail. The commissioner further found the dismissal justified since the remarks the applicant made about Jews were 'a gross and sickening example of racism'. The commissioner harshly rebuked the applicant and felt the e-mail would '…offend not only Jewish people, but… [also] offend any enlightened or civilized person of whatever cultural or religious persuasion. The grotesque caricatures which flowed so glibly from the applicant's key board, are strikingly similar to those which found favour with Nazi propagandists of the 1930's, and it is well known that it was the use of that form of profoundly shameful racist stereotyping, that facilitated the complicity of German civilians in ghettos and the transportation of German Jews. Applicant should be deeply ashamed of himself…'.

The employee in *Singh and Island View Storage Ltd*[1346] had been dismissed for sending a sexually explicit e-mail to 3 of his colleagues on the company's intranet. The employee admitted that he was aware that the e-mail he had sent was inappropriate and contained sexually explicit material and also that he was aware of the company's electronic communications policy and that his conduct could result in his dismissal. The employee argued that he had intended no harm in sending out the e-mail but had done so as a joke. The employee further argued that the company's electronic communications policy had not been consistently applied. Although the commissioner agreed that this was probably the case, the commissioner also reasoned that what was of paramount importance was the employee's motive in sending out the e-mail. In this respect, the commissioner found that the employee's motive was to embarrass and cause offence as he had admitted that he had a hostile and less than amicable relationship with his colleagues. The commissioner concluded that the employee was well aware of the consequences of his actions and his intention in sending the e-mail was to offend and insult his colleagues and, as such, found his dismissal to be justified.

[1345] 843.

[1346] (2004) 13 CCMA 8.32.1.

The decision of *Toker Bros (Pty) Ltd and Keyser*[1347] adopted the reasoning in Bamford. In *Toker Bros (Pty) Ltd and Keyser* an employee was charged with dishonesty in that she excessively misused the company computer for personal use during working hours and without permission. The employee was further charged with making defamatory remarks about her employer in an e-mail to a friend she sent from the company computer. The employee argued that her employer was aware that she was accessing the Internet to arrange a 20th school reunion, that her access to the Internet was mostly work related and that she was not told by her employer about a policy or rule against personal use of the Internet. The employee further admitted the defamatory remarks about her employer in her e-mail to a friend, but challenged the manner in which the e-mail was retrieved by her employer. The employer argued that it had advised the employee not to download from the Internet and denied giving her permission to use the Internet to arrange her school reunion. The arbitrator found that at issue was whether, in the absence of a written and clear policy against personal use of Internet, the employee could be reasonably expected to know or be aware of the rule. The arbitrator further found that "not all rules and policies have to be made known to employees as some common sense...[has] to be weighed against reasonableness". As such, the employee "could reasonably have been expected to know the rules as she was cautioned at the start of her employment and due to her experience as an employee." More importantly, the arbitrator pointed out that the charge was not for using Internet for personal use, but for using the Internet excessively for personal use. This implies that employers can reasonably expect their employees to make personal use of company Internet facilities, but the employee has to ensure that such use is within reasonable limits and not excessive.

With regard to the employee's challenge to the manner in which her defamatory e-mail was accessed, the employer had argued that the manner in which the e-mail was obtained was not illegal in that the e-mail was obtained during an investigation into the employee's excessive Internet usage. The arbitrator stated that the right to privacy in the Constitution particularly section 14 (d) prohibiting the monitoring and interception of employee communications, can be limited where consent has been given or a clear policy on monitoring and intercepting of communications in the workplace is implemented. The arbitrator found that the e-mail was not obtained with

[1347] (2005) 26 ILJ 1366 (CCMA).

malicious intent but its discovery was incidental to the investigation into the employee's abuse of the company's Internet facility. The arbitrator also considered the fact that the employee's e-mail to her friend could have resulted in her employer being held vicariously liable in civil law, given that the e-mail could be regarded as offensive and insensitive by some of its recipients.

In *Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others*[1348] the Labour Court reinforced the principle that personal e-mails sent from a company's e-mail system are not private as they can be read by other recipients, especially where the intended recipients also use the company e-mail system. The applicant had been employed as chief sub-editor by a newspaper when she had a heated argument with her editor and two other employees while on night duty. The next day the applicant addressed an e-mail to the managing director of the newspaper and six members of management to set out her frustrations at work, problems in the workplace and criticised the managing director and other senior management members. The employee sent an e-mail to her superior a day later in which she vented her feelings and frustrations about work and further referred to her editor and his deputy as that 'arse hole' and 'his overbearing cohort'. This second e-mail landed on her editor's desk in an unmarked envelope, even though the employee and her superior had not forwarded the e-mail to anyone else. The employee argued that the second e-mail to her superior should not be admitted by the arbitrator because of its private nature. The arbitrator found the employee should have been reasonably aware that the second e-mail would be read by people other than its intended recipient given that:

a) when her superior received her e-mail, two of her colleagues were standing behind her superior;
b) the first and second e-mail were sent within a short time of each other and both dealt wholly or partly with work related issues;
c) the second e-mail was not marked private or confidential;
d) the company's e-mail policy stipulated that all information stored on the company system belongs to the company and cautions employees not to assume that their e-mails will not be read by others; and
e) the e-mail had been sent to a communal computer which belonged to the company.

[1348] (2005) 26 ILJ 2433 (LC).

Recent case law relating to staff abuse of company e-mail and Internet suggests that courts and commissioners are unlikely to accept the argument that the employee was unaware of a policy regulating such abuse, particularly where the concerned employee held a managerial or leadership role in a company and, of course, where the abuse is of an excessive nature.

The employer in *Kalam and Bevcap (Nampak)*[1349] established that over a period of 5 months the employee had visited thousands of Internet sites, most of which contained pornographic material. The employer found that the employee had spent approximately 285 hours per week visiting 14802 non - work related sites. The employer further ascertained that the employee had visited and downloaded sexually explicit images using the company's Internet access. The employee was for this reason dismissed. The employee contended that his actions could not be considered unacceptable because he was aware of the company's IT policy document, but had not read it because it was bulky document. The commissioner found the latter argument to be unacceptable and also found that the employee knew of the policy and its content because he ignored the popup messages that warned that the sites he was accessing were prohibited. The commissioner added that even if the employee was unaware of the policy and its contents, his common sense should have prevailed. The commissioner found the employee's dismissal to have been both substantively and procedurally fair.

The employee in *Latchmiah and Billiton Aliminium SA (Pty) Ltd t/a Bayside Aliminium*[1350] was also dismissed for repeatedly accessing pornographic websites via the employer's Internet. However, unlike the employee in *Kalam,* the employee argued that he had a "dependency problem", which employer had failed to explore. The employee, who had been employed as a process superintendent, further argued that his accessing of pornographic websites did not interfere with his work and that the rules in place restricting the accessing of pornographic sites, was not consistently applied. The employee further disputed the employer's argument that his repeated access interfered with the company's information systems as he did not access the sites with malicious intent.

[1349] (2006) 15 MEIBC 8.32.1.
[1350] (2006) 13 MEIBC 8.32.2.

The arbitrator found, in turn, the existence of a well-established rule in the employer's workplace; the employee admitted to being aware of the rule; the rule was lawful and reasonable because it was aimed at dissuading unethical conduct, keeping the company information systems free from viruses and outside intrusion, preventing the slowing down of the system due to traffic, as well as preventing sexual harassment claims; the rule had been breached by the employee's conduct and the "dependency problem" defence could not be considered because the employee failed to take steps to bring the problem to the attention of the employer; the rule was consistently applied; the company's Internet and access policies had evolved because of the increase in Internet access in the workplace; and dismissal was an appropriate sanction because of the excessive nature of the employee's conduct.[1351]

From the preceding discussion of case law decided since the enactment of RICPCIA, it appears as if South African courts take the following view towards employee privacy in the workplace:

a) The employer is justified in protecting its business interests by regulating the use of e-mail and Internet in the workplace, because it owns the e-mail and Internet facilities in the workplace.
b) The absence of an explicit policy or no policy is no excuse for forwarding racist or offensive e-mails using the employer's Internet facilities. This is probably the most consistent theme throughout the case law, which also shows reliance, in cases like *Toker Bros (Pty) Ltd* and *Kalam and Bevcap (Nampak)*, on the common sense to be expected of employees.
c) A tribunal will consider a number of facts in deciding whether or not the employer was justified in dismissing an employer because of abuse of a company's e-mail facilities. Of particular importance in this regard is the reliance on our country's new democratic and constitutional dispensation to address racial abuse (as evidenced by *Cronje* and *Dauth/Brown*).
d) Tribunals in certain circumstances examine the intention of the employee in sending out an e-mail which later became the subject of his or her dismissal

[1351] See also *Masinga & Another & Kraft Food SA* (2006) 15 CCMA 8.32.1. The applicants in *Masinga & Another & Kraft Food SA* admitted that they had receiving and disseminating offensive emails but argued that their employer had not only acted inconsistently in dismissing them but had dismissed them because it had made a loss in the past four years and wanted to save costs by shedding some of its senior management.

and in some instances the intention of the employer in retrieving an employee's e-mail in deciding whether dismissal is appropriate (see *Singh and Island Storage Ltd* and *Toker Bros (Pty) Ltd*).

e) The Labour Court in *Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others* held that personal e-mails sent from a company's e-mail system are not private as they can be read by other recipients especially the intended recipients who are also using the company e-mail system.

f) South African tribunals also tend to draw on comparing what would have been acceptable before the constitutional dispensation as opposed to what is considered acceptable in the new constitutional democracy. This is often the case when faced with the dismissal of an employee for use of the employer's e-mail system to receive or forward racially offensive material to third parties Take for instance, the decisions of *Cronje* and *Dauth/Brown*.

Ironically, the right to privacy has only been considered in a handful of cases. From these cases it seems clear that in those instances where the right to privacy clashes with the interests of the employer in the context of e-mail and Internet use, the way in which the employer gathers information may well mean that the right to privacy has not been infringed upon (because of circumstances which eliminate a reasonable expectation of privacy), or, to the extent that there does exist an infringement of privacy, those (employer interests) may well constitute a justifiable and acceptable limitation on that right. South African tribunals have yet to apply the provisions of RICPCIA.

7.4.4 Analysis

In summary of the review of the South African approach to interception and monitoring of employee e-mail and Internet communications, it is immediately apparent (in contrast to the policies and practices discussed in Chapters 5 and 6) that South Africa now has legislation – RICPCIA - directly regulating this policy and practice. This was not always the case, as IMPA did not specifically provide for such interception and monitoring, although it arguable was broad enough to include Internet and e-mail communications in its scope of application. This, in itself, is a clear indication of the challenges technological developments create for the law in general, and privacy in particular At the same time, case law decided under IMPA did

address the issue of privacy in the context of the interception of communications. In particular, it was decided that telephone calls in the workplace were not protected by the Act by virtue of the nature of the relationship between the employee and employer (*Protea Technology*). Furthermore, case law drew a distinction between participant surveillance and third party surveillance and concluded that the latter did not contravene the provisions of IMPA and infringe on the constitutional right to privacy (*Tap Wine Trading*). Furthermore, it was also decided that IMPA was not concerned with interception and monitoring in the private sphere because it was intended for use by public agencies in gathering evidence during criminal investigations and therefore could not be applied to private sector employers and employees (*Moonsamy*). What can be said about these decisions is that they already started to send out a clear message that the clash of interests surrounding privacy has to be evaluated in the context of the workplace and that employers may have legitimate interests which trump any reliance on the right to privacy in the workplace.

IMPA's successor, RICPCIA, regulates the interception of communications in both the private and public spheres. RICPCIA, in general, prohibits the interception of communications, but also recognises 3 instances in which the interception of communications may be lawful – where a party to the communication is involved in the interception; if one of the parties to the communication has given their consent to the interception; and if the interception is carried out in the ordinary course of business. The latter exception provides the employer with a lawful means of intercepting business communications without the consent of the employee and applies to indirect communications such as e-mail and Internet connections intercepted within the parameters of RICPCIA. As such, legislation now also sends out a clear message that, in the circumstances defined by the Act, employees either do not have a reasonable expectation of privacy in the workplace, or, to the extent that they do, there are employer interests that outweigh privacy.

Case law decided after the enactment of RICPCIA has not really dealt with the application of that Act, nor in much detail with the balancing required where employer policies relating to e-mail and Internet clash with the privacy concerns of employees. Even so, and even though most cases have dealt with the fairness of dismissal of employees who abused e-mail and Internet systems, these cases already

make it clear that an employer has an important interest in the integrity of its information systems and that these interests typically will trump those of the employee. In general, these cases show a fourfold approach – that use of the systems provided by the employer already means that information stored and disseminated on those systems cannot be said to be private; by accepting that flagrant abuse (especially the dissemination of racial or sexually explicit material) of an employer's information system (e-mail and Internet) does not raise privacy issues (even in the absence of a policy, there is no reasonable expectation of privacy, especially where the employee in question disseminates e-mail widely); that an employer may validly limit privacy through a clear policy in the workplace; and, to the extent that an employee may validly raise privacy issues, the interests of the employer are regarded as more important.

7.5 UNITED KINGDOM

7.5.1 Introduction

In 2006, the United Kingdom's Department of Trade and Industry ("DTI") reported in its Information Security Breach Survey that 97 percent of United Kingdom businesses had Internet connection and 88 percent of this Internet connection is broadband.[1352] Furthermore, scanning of incoming e-mail and Web downloads was commonplace – 70 percent of businesses scanned e-mail for viruses, 36 percent for inappropriate content, 15 percent for confidential information and 11 percent for unencrypted information that should ideally be encrypted. 62 percent of businesses reported having suffered a security incident in the previous year, 52 percent reported having suffered a malicious security breach and 68 percent of businesses attributed the cause of their worst security breach to an external threat. With regard to the type of breach businesses had suffered, 35 percent pointed to infection by viruses or other malicious software, 29 percent to systems failure or data corruption, 22 percent to staff misuse of information systems, 17 percent to attacks by an unauthorized outsider and 8 percent to theft and fraud involving computers. With specific regard to staff abuse of company information systems, 21 percent of companies indicated they had been affected and, as far as the type of abuse is concerned, 17 percent of companies pointed to abuse of Web access, 11 percent to abuse of e-mail access, 4 percent to

[1352] Information Security Breaches Survey of 2006.

unauthorized access to data systems, 2 percent to breaches of data protection laws or regulations and the abuse of confidential information.[1353]

The 2008 Information Security Breaches Survey further showed that 24 percent of employers restricted Internet access to some staff only and 46 percent logged and monitored Web access in the workplace. Furthermore, 38 percent of employers blocked access to inappropriate websites and 94 percent of employers quarantined suspicious e-mail attachments. The 2008 survey also showed that most employers scanned outgoing e-mails for viruses, 26 percent of them for inappropriate content, such as the profane use of language and 16 percent of employers scanned outgoing e-mail for confidential information. With respect to security breaches, 45 percent of companies reported having suffered a security breach in the previous, 35 percent of those being malicious. Most companies attributed the worst security breach they had suffered in the previous year to internal threats such as insider abuse of Internet access, viruses and laptop and mobile theft. A significant 62 percent of businesses claimed the cause of their worst incident was internal. Furthermore, 23 percent of businesses suffered a breach in the form of a systems failure or data corruption, 16 percent suffered staff abuse of information systems and attacks by unauthorised outsiders (including hacking attempts) and, lastly, 14 percent of businesses suffered a breach in the form of an infection by viruses or malicious software.[1354] Levels of staff abuse of company information systems dropped after 2006, but visiting inappropriate websites, excessive browsing and sending inappropriate e-mail remain commonplace. Lastly, the 2008 results show that security breaches that become known outside the company and receive adverse media coverage generally speaking remain somewhat of a rarity. Only 3 percent of United Kingdom employers attributed some damage to their reputation to the worst security incident they had suffered.

7.5.2 Legislation

7.5.2.1 Article 8 of the ECHR and the Human Rights Act

The European Convention on Human Rights[1355](“ECHR”) guarantees a number of political and civil rights, including the right to privacy. Article 8 of the ECHR

[1353] Information Security Breaches Survey of 2006.

[1354] Information Security Breaches Survey of 2008.

[1355]Drafted by the Council of Europe in 1950 and came into force on 3 September 1953.

provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence." This right can only be limited by a public authority in accordance with domestic legislation and as far as it is necessary in a democratic society for the protection of legitimate claims.

The Human Rights Act[1356] contains the absorption of Article 8 of the ECHR into United Kingdom law. Article 8 of the Human Rights Act generally protects a person's private and family life, home and correspondence from arbitrary interference by the state, except where that interference is in accordance with the law (such as legislation or rules of a professional body); in the interests of legitimate objectives set out in the Act (the interests of national security, the prevention of disorder or crime; the protection of health or morals and the protection of rights and freedoms of others); and necessary in a democratic society (the nature and extent of the interference must be weighed against the end it is set to achieve). By affirming the right to respect of one's private life and correspondence, Article 8 of the Human Rights Act has implications for the online and e-mail privacy of employees.

The ECHR provides no definition of what it means by privacy, but case law has shed light on the meaning of privacy in light of the ECHR.[1357] Case law defines privacy as a wider than the inner sanctum of life and can encompass professional of business activities. Employees cannot rely on the ECHR for effective protection of their online rights, for a number of reasons, including uncertainty about the protection, if any, of an employee who uses e-mail without the employers permission and whether an employee who is informed monitoring will take place for legitimate purposes will have a reasonable expectation of privacy.[1358]

The European Court of Human Rights imposes a duty on member states to ensure that measures are in place to afford individuals respect for their privacy and correspondence. In this regard, it was established in *Niemetz v Germany*[1359] that an additional duty be placed on the state to put in place mechanisms which protect privacy between individuals, such as employee and employer. Hence, in *Klass v*

[1356] Act of 1988.

[1357] *Niemetz v Germany* [1992] EHRR 97.

[1358] See decision of *Halford v United Kingdom* (1997) 24 EHRR 523.

[1359] [1992] EHRR 97.

Federal Republic of Germany[1360] and in *Malone v United Kingdom*[1361] this duty was held to apply to the relationship between the employee and employer.

7.5.2.2 Data Protection Act

The Data Protection Act[1362] ("DPA") is incorporates aspects of the EC Directive 95/46 – Data Protection Directive ("Data Protection Directive") on personal data and governs the processing of personal data. The Data Protection Directive, , which aims to protect the data privacy of individuals provides for a number of general principles related to privacy in this context: everyone should have a right of access to personally identifiable data relating to themselves; a right to rectification of data where it is shown to be inaccurate; a right to object to the processing of his or personal data a right to information as to the purpose of processing and identity of the data controller (the person or body that determines the purposes and means of processing data, such as a company in relation to information about its clients and employees) and a right to consent to the processing of the data, especially where the data is sensitive.[1363] The directive further ensures the free flow of data within the European Union by permitting companies and organizations within Europe to transfer data throughout the European Union. However, such transfers may be limited in the employment context and decisions to block transfers are taken on specific individual cases in terms of Article 25.4 of the Directive. Article 26 of the Directive provides for the circumstances under which a transfer of data on employees may take place (for example where the transfer is essential for the protection of the interests of the individual concerned). Finally, the Directive's application is limited in that it does not extend to the processing of data by individuals in the domestic sphere or the areas of public safety, defence or law enforcement.[1364]

The DPA primarily places restrictions on the "processing" of "personal data". Part I of the Act defines "data" to include information which is being processed by means of equipment operating automatically in response to instructions given for that purpose or is recorded with the intention that it should be processed by means of such

[1360] [1978] 2 EHRR 213.

[1361] [1984] 7 EHRR 14.

[1362] Act of 1988.

[1363] Articles 6 – 12 of the Data Protection Directive.

[1364] Article 3 of the Data Protection Directive.

equipment. The definition therefore includes automatic systems that involve the interception of electronic communications such as Internet and e-mail[1365] as well as employment related records. "Personal data" is defined in Part I of the DPA as data which relates to a living individual who can be identified from the data or from data and any other information in the possession of, is likely to come into possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. The "processing" of data or information is defined as obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data including, *inter alia*, dissemination or otherwise making available, disclosure of information or of data by transmission, consultation or use of information or data and retrieval.[1366]

Two preliminary points have to be made about the act. First, the DPA has to be promoted and enforced by a public officer known as the Information Commissioner. The Information Commissioner's functions include promotion of the Data Protection Act, ensuring enforcement of the Act, to give advice on the Act and to decide cases relating to the Act. The Commissioner is also empowered under section 51 of the Act to prepare codes of practice to give guidance. In 2000, a draft Code of Practice on the Use of Personal Data in Employer/Employee Relationships, which discussed and clarified the application of the Act in the employment context, was issued.[1367] Three years later (in 2003) The Employment Practices Data Protection Code ("Employment Practices Data Protection Code"), which includes a section on "Monitoring at Work", was issued. The legal requirement on each employer is to comply with the Act and the Employment Practices Code sets out the Commissioner's "good practice recommendations" as to how the legal requirements of the DPA can be met. The Employment Practices Code is not legally binding, but it can influence the decisions of tribunals and courts, particularly where there is uncertainty and the Employment Practices Code recommends a particular interpretation of a provision of the Act. As

[1365] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 132.

[1366] Part I of the DPA.

[1367] The Commissioner of Information is empowered to prepare code of practice in consultation with trade associations, data subjects or their representative bodies. Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 135.

such, relevant parts of the Employment Practices Code are likely to have persuasive weight in connection with any enforcement action that arises with regard to processing of information in the employment context.[1368] The second preliminary point about the Act is that it requires data controllers to comply with eight data protection principles with respect to personal data. However, only the first, second, third, fifth and sixth data principles are relevant to monitoring of Internet and e-mail use in the workplace. The five relevant data principles, in their numbering assigned by the Act, will be discussed below.

7.5.2.2.1 First Data Principle

The "first principle"[1369] is the duty to process data lawfully and fairly, which happens if at least one of the conditions set out in Schedule 2 of the Act is met. These conditions include the consent of the data subject to the processing. The use of the word "consent" in this context is misleading and should be understood to mean that an employee must be given a real choice whether to accept or decline the processing and be guaranteed that he or she will not be prejudiced as a result of whatever choice is made.[1370] The consent of the sender or the third party or parties will be difficult, if not impossible, to obtain for the purpose of e-mails sent by employees, as they are likely to contain information about the sender or third parties.[1371] The most important condition in Schedule 2 is that processing may be "necessary for the purposes of the legitimate interests pursued by the data controller or parties to whom the data are disclosed, except where processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject." This condition has been criticised for its uncertainty. The condition requires that a balance be struck between the data controller's interests and interests of the data subject and depends wholly on the extent to which the courts accept that legitimate interests may include both economic and human rights interests (such as privacy).[1372]

[1368] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 132.

[1369] Section 1 – 4 of the DPA.

[1370] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 132.

[1371] *Supra*.

[1372] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 132.

The Act provides that "[i]n determining for the purposes of the first principle whether the personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled at to the purpose or purposes for which they are processed."[1373] Schedule 1 goes on to specify that the processing will not be fair unless the data controller ensures as far as it is practical that the data subject has information about, *inter alia*, the identity of the data controller, the purposes for which the data has to be processed and any further information necessary, having regard to the specific circumstances in which the data are or to be processed, to enable the processing to be fair. An additional duty exists to provide such information where the information was obtained from a source other than the data subject, unless, amongst other things, the provision of the information involves a "disproportionate effort". The Information Officer in determining whether the effort is "disproportionate" will take into account *inter alia* the cost to the data controller of providing the information, the difficulty of providing the information and the length of time it will take in each case, balanced against the extent to which withholding the information may be prejudicial to the data subject.[1374]

The requirement of lawfulness is not defined or explained in the Act, but, in borrowing from the definition of "unlawful" in English case law, it is accepted to mean "…something which is contrary to some law or enactment or is done without lawful justification or excuse."[1375] This interpretation means that various forms of data processing would be in breach of the "first principle" requirement of lawfulness.[1376]

7.5.2.2.2 Second Data Principle

The "second principle" of the DPA requires that personal data be obtained only for one or more specified and lawful purpose(s) and shall not be processed in a manner incompatible with that purpose or those purposes. [1377] The purpose or purposes for

[1373] Schedule I of the DPA.

[1374] *Morris English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 132.

[1375] *Morris English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 134.

[1376] The Information Officer cited *R v R* [1993] 3 W.L.R. 767 in *Morris English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 134.

[1377] Section 4 – 5 of the DPA.

which personal data may be obtained may be specified in a notice by the data controller to the data subject or the Information Commissioner (data controllers are required to give the Commissioner notification about specific details of their processing of data). Moreover, in determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data was obtained, regard must be had to the purpose or purposes for which the personal data is intended to be processed by persons to whom such data is disclosed.[1378]

7.5.2.2.3 Third Principle

The "third principle" necessitates that personal data be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.[1379]

7.5.2.2.4 Fifth Data Principle

The "fifth principle" of the DPA requires that personal data processed shall not be kept for longer than is necessary for that purpose or those purposes.[1380] This principle may be breached if an e-mail is deleted from a system but is held as back- up or as archive data.[1381]

7.5.2.2.5 Sixth Data Principle

The "sixth principle" provides that data shall be processed in accordance with the rights of data subjects, which includes the right to notice where a data subject has not consented to the processing.[1382] The "sixth principle" will be breached where the data controller fails to supply the data subject with a copy of information constituting personal data about them. A further breach of the principle will occur where the data controller "…fails to comply with a notice from a data subject requiring the controller to cease processing any personal data on the ground that, for specified reasons, the

[1378] Section 4 – 5 of the DPA. See also Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 134.

[1379] Schedule 2 and section 8 of the DPA.

[1380] Schedule 2 of the DPA.

[1381] Schedule 2 of the DPA.

[1382] Section 8 of the DPA.

processing is causing or is likely to cause substantial damage or substantial distress to the data subject or another and that damage or distress will be unwarranted".[1383]

7.5.2.3 Employment Practices Code and Supplementary Guidance

The Employment Practices Code Supplementary Guidance, which is not binding legislation *per se* but a guide to employers to enable them to meet the requirements of the DPA, encourages employers monitoring electronic communications such as Internet and e-mail to put in place a policy on the use of such communications and to communicate the policy to employees. Moreover, employers have to ensure that the Employment Practices Code reflects data protection principles and integrates data protection features by, for example, specifying in detail the extent to which employees may use electronic communications for private use and the restrictions on material that can be sent or received.[1384] More importantly, employers do not only have to communicate the nature and extent of the monitoring but also the purpose of the monitoring.[1385] The Employment Practices Code Supplementary Guidance further advises employers to consider an impact assessment in determining whether the monitoring can be limited.[1386] An employer may, for example, use a less intrusive method such as automated monitoring and a detection process to protect its system from hackers and viruses.[1387] Employers are also encouraged to request employees to mark e-mails as personal and private so as to confine the monitoring to e-mails that are not marked as such.[1388] The Employment Practices Code stresses the principles of transparency and proportionality. To address the transparency principle, the Supplementary Guidance of the Employment Practices Code recommends that employers notify employees and other parties to the communications of the monitoring. To address the proportionality principle, the Employment Practices Code

[1383] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 134.

[1384] Employment Practices Code Supplementary Guidance 64.

[1385] Employment Practices Code Supplementary Guidance 67.

[1386] Employment Practices Code 50.

[1387] Employment Practices Code Supplementary Guidance 65.

[1388] Employment Practices Code Supplementary Guidance 66.

Supplementary Guidance recommends employers eliminate the collection of personal information that is "irrelevant and excessive" to the employment relationship.[1389]

7.5.2.4 Regulation of Investigatory Powers Act and the Telecommunications (Lawful Business Practice) Regulations

7.5.2.4.1 Regulation of Investigatory Powers Act (RIPA)

Similar to the Data Protection Act, the Regulation of Investigatory Powers Act[1390] ("RIPA") regulates the use of e-mail and Internet usage at work in regulating for amongst other things, the interception of communications and the acquisition of data relating to communications.[1391] RIPA was created to "ensure that the relevant investigatory powers are used in accordance with human rights" by extending the legal regulation of interceptions to cover private networks directly or indirectly attached to a telecommunications system.[1392] RIPA aims to reform national law and to implement the pertinent requirements of European Directive 97/66 on Data Protection Telecommunications.[1393] Prior to RIPA, there was a gap in English law with respect to legislation governing the interception of communications on private telecommunications networks.[1394] "Communications" are defined in the Act to include speech, music, sounds, visual images, and data of any description, e-mail messages, telephone calls, faxes, voice mail and Internet access. The Act provides in section 1(3) that:

> "[a]ny interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication it is without lawful authority and is either –

[1389] Lasprogata, King and Pillay "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada" (2004) 4 *Stanford Technology Law Review* 1 60.

[1390] Act of 2000.

[1391] See the introductory text of the Act.

[1392] McColgan "Do Privacy Rights Disappear in the Workplace" (2003) Special Issue *European Human Rights Law Review* 120 134.

[1393] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 128.

[1394] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 128.

a) an interception of that communication in the course of transmission by means of that private system; or
b) an interception of that communication is the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system."

Section 2(3) further provides that for purposes of the Act, a person intercepts a communication in the course of is transmission by means of a telecommunications system if he modifies or interferes with the system, or its operations; monitors transmissions made by means of the system; or monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, so as to make some or all the contents of the communication available to a person other than the sender or intended recipient of the communication. An employer who intercepts a communication to or from its own telecommunication system could therefore face a suit from the sender or recipient of a communication on the basis that the interception lacks lawful authority.[1395]

The Act accomplishes two purposes. First, it creates the general framework for the interception of all communications on private and public telecommunications systems. Secondly, it establishes the general principle that such interception shall be lawful if parties making and receiving the communications have consented to the interception.

7.5.2.4.2 Telecommunications (Lawful Business Practice) Regulations

The Secretary of State has authority in terms of RIPA to make regulations permitting businesses to lawfully intercept communications to which the parties making and receiving the communications have not consented.[1396] The Secretary of State has exercised this authority through the Telecommunications (Lawful Business Practice) Regulations of 2000 ("the Regulations"). The Regulations give employers considerable powers of interception, especially in the performance of a variety of purposes such as ensuring the effective operation of their systems and in order to comply with external and internal regulations. The Regulations authorise interceptions

[1395] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 130.

[1396] The Secretary of State is authorised in terms of section 4(1)(e) of RIPA to make such regulations.

of telecommunication communications which would otherwise be unlawful in terms of section 1 of RIPA. Interceptions permitted in terms of the Regulations have to meet three conditions to be considered lawful: first, the interception must be done using the business' own telecommunications system;[1397] second, the interception is authorised only if the system controller of the business telecommunications consented to the interception or carried out the interception and further made all reasonable efforts to inform users of the business telecommunications system that interceptions may be carried out;[1398] third, the sole purpose of the interception must be the surveillance of communications relevant to the controller's business.[1399]

Section 3 of the Regulations goes on to list seven purposes which would make non-consensual interception and recording of communications lawful:

a) To establish the existence of facts. This purpose refers to the need for businesses to keep records of communications relating to, for example, orders and purchases;

b) To ascertain compliance with regulatory or self-regulatory practices[1400] or procedures applicable to the system controller in carrying on of his business or applicable to another person in the carrying on of his business, where that person is supervised by the controller in respect of those practices or procedures. This purpose refers to binding and voluntary legislation, codes or standards of any country within the European Economic Area;

c) To ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties. This

[1397] The Regulations in section 2 define the term "business" to include activities of a government department, public authorities, or any body exercising statutory functions.

[1398] A "system controller" in terms of the Regulations means a person with a right to control the operation or use of a particular telecommunication system. According to Morris the UK's Department of Trade and Industry has interpreted this condition to cover only direct users and exclude those users calling from outside and those users who receive a call from outside using another system. Consequently staff and other working at the employer's premises and not third parties must be informed about the interception which is solely for purposes of monitoring and where permissible recording communications relevant to the system controller's business. Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131.

[1399] The Regulations define "a communication relevant to a business" as a communication which involves a business transaction or relates to the business or takes place in the course of carrying on of the business.

[1400] Section 2 of the Regulations define "regulatory or self regulatory practices and procedures" as any law of any state within the European Economic Area or any standard or code of practice published or on behalf of a body established by any state within the European Economic Area.

purpose refers to standards and procedures set by the employer such as quality control and training procedures;

d) To prevent or detect crime;

e) To investigate or detect unauthorised use of any telecommunications system. This is designed to enable employers to intercept their employee's communications in order, for example, to check if employees are not contravening workplace rules on the use of Internet and e-mail;

f) To ensure the effective operation of the system. This purpose is designed to cover interception as an inherent part of a system's effective operation, such as virus checks, traffic routing[1401] and system maintenance (which is still lawful under RIPA);

g) To monitor (not record) communications to determine whether the communication is relevant to the business. This purpose was designed to enable employers to check the communications of a temporarily absent employee in order to determine the existence of business matters that need attention in the absence of that employee.[1402] This purpose strikes a balance between giving businesses access to their own communications and protecting the privacy of non-business communications, but at the same it introduces the risk of intercepting non-business communications in order to establish whether communications are business related.[1403]

The aforementioned purposes are, however, subject to limitation borne out of the uncertainty regarding the correct interpretation of the Regulations and other legislation in the same area, as well as the relationship between the Regulations and other legislation.[1404] The first and most important limitation relates to personal data. Whenever surveillance entails the processing of personal data, the limitations that the DPA imposes on workplace surveillance will apply and so will the provisions of the

[1401] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131.

[1402] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131.

[1403] *Supra*.

[1404] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131.

Regulations in order to comply with the First Data Protection Principle that surveillance should constitute lawful processing.[1405]

The second limitation is imposed by the Human Rights Act[1406] requirement that all legislation be interpreted in accordance with Article 8 of the ECHR, which reinforces the protection of privacy. This requirement will affect the interpretation of RIPA and the Regulations whether or not surveillance is covered by the DPA.[1407]

The third limitation lies in the scope of the power to regulate in RIPA. The Act grants the Secretary of State the power to make Regulations and at the same time impresses binding conditions on the use of that power.[1408] Limitations may also apply to the different purposes identified by the Regulations which would make interception lawful.[1409] The first purpose (which provides that employers may intercept solely to establish the existence of facts) does not furnish employers with the additional permission to intercept in order to establish the identity of those facts. The first purpose thereby appears to preclude employers from keeping commercial records. The third purpose (which allows for compliance with an employer's own standards) makes reference to the employee's "duties", thereby suggesting that the interception may extend only to standards that are included in the employee's contract of employment.[1410]

The fourth limitation is found in the fact that RIPA and the Regulations aim to improve national law and implement Directive 97/66. In effect, the Directive limits some of the lawful purposes identified in the Regulations. Purposes one to five (establishing facts, compliance with external regulations, compliance with internal standards, detecting crime and detecting unauthorised use) fall within the scope of Directive 97/66, though their scope appears to be wider than permitted by the

[1405] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131.

[1406] Act of 1998.

[1407] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131 - 132.

[1408] *Supra*.

[1409] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131 - 132.

[1410] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131 - 132.

Directive.[1411] In terms of Article 5(2) of the Directive, permissible exceptions to the principles of privacy and confidentiality include those "in the course of lawful business practice for the purposes of providing evidence of a commercial transaction or for any other business communication".[1412] On the contrary, the Regulations and section 4 (2) of RIPA refer to the establishments of facts (not evidence) and seem to preclude employers from keeping commercial records, but not requiring that transactions be commercial. Further, the Regulations and RIPA refer to communications related to the business, whereas the Directive refers to business communication.[1413] Moreover, purposes six and seven (ensuring the effective operation of the system and checking to determine whether communication is relevant to the business) appear to fall outside the scope of the Directive, which is primarily concerned with the confidentiality and privacy of communications.[1414]

The Regulations have been criticised for giving employers "sweeping powers to monitor" their employee's e-mail and Internet activities in the workplace. First, the Regulations do not interfere with the employer's unilateral power to determine the manner in which the communications will be used.[1415] Secondly, the Regulations permit the employer to intercept communications in order to determine whether its telecommunications system is being used appropriately.[1416] Thirdly, the Regulations do not require employers to show that they suspect the unauthorised use of their system or that their action is proportionate before monitoring any communications. Lastly, the Regulations permit employers to monitor (not record) communications to determine whether the communication is relevant to the business. This creates the threat of all communications (regardless of whether they are relevant to the business) being intercepted.[1417] The Regulations have further been criticised for contradicting

[1411] *Supra*.

[1412] *Supra*.

[1413] *Supra*.

[1414] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131 - 132.

[1415] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131 - 132.

[1416] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131 - 132.

[1417] *Supra*.

primary legislation like the Data Protection Act.[1418] Notwithstanding this, the Regulations only permit interception to the extent that it is in line with Directive 95/46, Directive 97/66, the Data Protection Act and the Human Rights Act.[1419]

7.5.3 Case law

English law does not explicitly entitle employees to use their employer's Internet and e-mail for personal purposes and the extent of use of an employer's on-line facilities is usually determined by the employer. A number of cases have come before the European Court of Human Rights concerning the interception of workplace communications and these decisions in essence spell out the approach of English and European tribunals to the privacy of employees and their communications in the workplace.

7.5.3.1 Halford v United Kingdom

Halford v United Kingdom[1420] is the first decision in which the European Court of Human Rights considered the application of Article 8 to the workplace. At issue in *Halford* was the interception of workplace communications (more specifically employee phone calls in the workplace). The court found that the employee, an assistant Chief Constable, had a reasonable expectation of privacy because of the presence of the following factors: the employee had not been warned that her calls could be subject to interception by her employer; she had the sole use of the two phones in her office, one of which was solely for private use; and she had been guaranteed a measure of privacy in relation to calls made from her office for purposes of her sex discrimination case. On the face of it, the decision seems to be a positive one for workplace privacy protection. On closer scrutiny, the decision is quite narrow as it rests particularly on Halford's "reasonable expectation of privacy". Ford observes that the "reasonable expectation test" in *Halford* "appears to take as its starting point that privacy at work is a deferential to management prerogative. Provided management tells workers or imposes a contractual "agreement" that for example, their calls are liable to interception, they will be watched by CCTV or they

[1418] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131 – 132.

[1419] Morris *English Law* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 131 – 132.

[1420](1997) 24 EHRR 523.

will be tracked by infrared badges, it is hard to see how private life is engaged at all".[1421]

7.5.3.2 Niemetz v Germany

The ECHR in *Niemetz v Germany*[1422]construed the private life categories in Article 8 and declined to take a narrow approach to the interests protected by Article 8:

> "[t]he Court does not consider it possible or necessary to attempt an exhaustive definition of "private life". However, it would be too restrictive to limit the notion to the "inner circle" in which the individual may live his own personal life as he chooses to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of private life should be taken to exclude activities of a professional or a business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest opportunity of developing relationships with the outside world…especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given time".

The *Niemetz* approach suggests that a key aspect of private life in Article 8(1) is "establishing and developing relationships with others, including with work colleagues during… [working hours] as well as outside [the workplace]…" and further exhibits "…a strong tendency to require stringent objective justification of a wide range of employer practices" in terms of Article 8(2)".[1423]

[1421] Ford "Two Conceptions of Worker Privacy" (2002) 31 *Industrial Law Journal* 135.

[1422] *Niemetz v Germany* [1992] EHRR 97.

[1423] Ford "Two Conceptions of Worker Privacy" (2002) 31 *Industrial Law Journal* 135 143.

7.5.3.3 Copland v United Kingdom

As in *Halford*, the European Court of Human Rights found in *Copland v United Kingdom*[1424] that because the employer had no internal policy in place pertaining to the monitoring of telephone, e-mail and Internet usage by its employees, its employees had a reasonable expectation to privacy with respect to their telephone, e-mail and Internet usage.

The facts were that C was employed by a state college as personal assistant to the college principal and was required to work closely with the deputy principal. C went on leave and whilst on leave, the deputy principal instructed that her telephone, e-mail and Internet usage be monitored. C argued that the monitoring violated her right to respect for her private life and correspondence (protected by Article 8 of the ECHR), because it not only covered her telephone, e-mail and Internet usage but her movements at work and whilst on leave.

The college contended that the monitoring was essentially carried out to determine whether C was making personal use of the colleges' facilities and merely entailed the analysis of automatically generated data. The college further contended that the monitoring was carried out in pursuit of the legitimate aim of ensuring that the facilities of the college, which was publicly funded, were not abused and that it had authority to do so in terms of its' statutory powers.

The Court reasoned that the employee's telephone usage in the workplace was protected by Article 8 and for this reason C had a reasonable expectation of privacy in her telephone, e-mail and Internet usage at work, because she had not been warned that the use of her work telephone would be the subject of monitoring. This expectation extended to her usage of e-mail and Internet at work. The Court found that the collection and storage of personal information relating to C's use of her work telephone, e-mail and Internet interfered with her right to respect for her private life and correspondence protected in Article 8, because such collection and storage was done without her knowledge. Lastly, the Court found that the interference was not in accordance with the law because there was no general domestic law or statutory powers regulating the monitoring in place at that time.

[1424] 2007 45 EHRR 37.

7.5.3.4 Re an Employer's Call – Monitoring System

The employer in the Austrian decision of in *Re an Employer's Call – Monitoring System*[1425] installed a new telephone system, but only gave its employees information about the possibility of installing the system three months after its actual installation. Moreover, the employer installed and used the new telephone system without prior consent from the Work Council. The system, like telephone service companies' systems, was capable of recording data (that is the caller's extension, the number called, the line used, the date, the time, the length of the conversation, the cost and the number of impulses) for both business and personal outgoing calls.

The Works Council argued that the installation of the system was likely to affect the human dignity of the affected employees, because it was tantamount to a monitoring system and its use would involve the collection, analysis and storage of employee data. It argued that the system could identify employees contacting the Works Council and further identify persons making calls to employees. The employer, on the other hand, argued that the system was a business tool which enabled it to determine whether a call from its premises was a business or a private call, which could assist for purposes of reducing prolonged private telephone conversations and avoiding excessive use of telephones. The employer further argued that the system did not involve listening in on calls; hence the privacy of the employees' call was preserved.

The Austrian Supreme Court stated that it was settled law in terms of European Court of Human Rights jurisprudence that telephone conversations taking place at the workplace were envisaged in the concepts of "private life" and "correspondence" expressed in the wording of Article 8 of the ECHR. The Court also pointed out that there were two conflicting fundamental rights at stake– the employers' right to inviolability of property (protected by Article 5 of the ECHR) versus the employees' right to respect for his private and family life (protected by Article 8 of the ECHR). The Court further identified three interests invoked by the employment relationship in this regard: first, the employer's obligation to provide for the welfare of its employees; the employee's duty of trustworthiness; and the general interest in the economic consideration of reducing telephone bills. In weighing up these competing interests, the Court found that the employer, "as the owner of the telephone system

[1425] [2004] E.C.C 4.

and as the person responsible for paying the telephone service provider, cannot be prevented from charging his employees for private calls...Monitoring does not itself infringe any privacy enjoyed by the employees. It is a feature of the employment relationship that the employee is subject to the control of the employer".[1426]

7.5.4 Analysis

The 2006 and 2008 DTI Information Security Breaches Survey indicate that a considerable number of United Kingdom employers do monitor and to some extent intercept employee e-mail and Internet communications in the workplace. It further appears that the United Kingdom employers monitor and intercept employee e-mail and Internet communications for a number of reasons, primarily to prevent viruses and other malicious software from corrupting their information systems and also as a means for ensuring that employees do not send out inappropriate content and confidential employer information using the employers systems.

English law does not explicitly entitle employees to use their employer's Internet and e-mail for personal purposes and the extent of use of an employer's on-line facilities is usually determined by the employer. That being said, United Kingdom employees have recourse to three pieces of legislation to protect their rights, namely Article 8 of the ECHR, the DPA and RIPA (which has similar provisions to our RICPCIA). Article 8 of the Human Rights Act has implications for the online and e-mail privacy of employees by virtue of its affirmation of the right to respect one's private life and correspondence. Article 8 of the ECHR was absorbed into domestic law after the implementation of the Human Rights Act and provides a measure of protection for the right to privacy in employment.

There are different approaches to privacy in the ECHR associated with the judgments in *Niemetz* and *Halford*, Ford describes these as follows: "[t]he conception of privacy endorsed in *Niemetz* is close to a right to individual and perhaps collective autonomy…Conversely, it is clear that a conception based on a "reasonable expectation" test will in practice fail to offer any significant protection against the growing intrusiveness of new techniques of surveillance, or indeed any worker

[1426]Paragraph 31.

interests".[1427] McColgan, expounding on the effect of these differing approaches, states that if the more generous and purposive *Niemetz* approach is preferred, then Article 8 can provide significant protection from workplace surveillance. However, if the restrictive *Halford* approach is applied, Article 8 will be of little use for protection of employees against the interception of workplace communications and surveillance of employees through the use of CCTV, monitoring of key board use, audio recording, vehicle monitoring and internet access monitoring. The *Halford* approach will to some extent, however, prove useful as employees may have "a reasonable expectation of privacy", particularly in the absence of clear and express warning, in relation to e-mails protected by a password and which have been deleted and in relation to telephone calls.[1428]

The DPA primarily places restrictions on the "processing" of "personal data" and does so, among other things, through enforcement of data principles, five of which are relevant in the current context: the "first principle" is the duty to process data lawfully and fairly; the "second principle" requires that personal data be obtained only for one or more specified and lawful purposes; the "third principle" necessitates that personal data be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed; the "fifth principle" requires that personal data processed shall not be kept for longer than is necessary for that purpose or those purposes; and the "sixth principle" provides that data shall be processed in accordance with the rights of data subjects under this the Act and includes *inter alia* the right to give the data subject notice where a data subject has not consented to the processing. The DPA almost always applies to surveillance in the workplace. It further will almost always involve the making of records which identifies an individual and therefore constitutes the processing of personal data as described by the Act.

Similar to the DPA, the RIPA and the Telecommunications (Lawful Business Practice) Regulations of 2000 issued in terms of RIPA, regulate the use of e-mail and Internet usage at work. RIPA was created to "ensure that the relevant investigatory powers are used in accordance with human rights" by extending the legal regulation of interceptions to cover private networks directly or indirectly attached to a

[1427] Ford "Two Conceptions of Worker Privacy" (2002) 31 *Industrial Law Journal* 135 153.

[1428] McColgan "Do Privacy Rights Disappear in the Workplace" (2003) Special Issue *European Human Rights Law Review* 120 128 - 129.

telecommunications system. The Regulations give employers considerable powers of interception, especially in the performance of a variety of purposes such as ensuring the effective operation of their systems and in order to comply with external and internal regulations. The Regulations authorise interceptions of telecommunication communications which would otherwise be unlawful in terms RIPA. Interceptions permitted in terms of the Regulations have to meet three conditions to be considered lawful: first, the interception must be done using the business' own telecommunications system; second, the interception is authorised only if the system controller of the business telecommunications consented to the interception or carried out the interception and further made all reasonable efforts to inform users of the business telecommunications system that interceptions may be carried out; third, the sole purpose of the interception must be the surveillance of communications relevant to the controller's business. The Regulations furthermore set out seven purposes which would make non-consensual interception and recording of communications lawful, but, as discussed, these purposes may themselves be limited. Available case law has not so much dealt with the application and interpretation of legislation regulating e-mail and Internet use in the United Kingdom. Rather, it has dealt with the application of the right to privacy as found in the ECHR and the Human Rights Act. Even so, it is noteworthy that, just as the case is in South Africa (and, again dissimilar to the other policies and practices discussed in Chapter 5 and 6), the United Kingdom has enacted legislation more or less specifically aimed at electronic interception. As such, the legislation itself already recognizes the magnitude of the threat to privacy (given the ease of infringement through technological developments), but also seeks to balance the interests of both employer and employee.

7.6 UNITED STATES

7.6.1 Introduction

United States employers generally argue for the monitoring and regulation of employee e-mail and Internet usage for the following reasons: to ensure that trade secrets and other confidential business information remain so; to ensure that sexual or racial harassment or the creation of a hostile work environment is not occurring through the "transmission and display of sexually or racially suggestive material or the circulation of injurious to or about a co-worker"; to ensure that employees remain

productive; to ensure that the company system is not overloaded with non-work related attachments such as jokes and chain e-mails; to ensure that the company is not held liable for copyright infringement, particularly where an employee copies and disseminates copyright protected material using the company's system; and to monitor the transmission of legally incriminating electronic information sent or received by employees.[1429]

A 2005 American Management Association ("AMA") survey on Electronic Monitoring and Surveillance revealed that United States employers were primarily concerned with inappropriate Web surfing and, consequently, that 76 percent of employers monitor employee Website connections. The survey further revealed that computer monitoring is varied: 36 percent of employers track content, keystrokes and time spent on the keyboard; 50 percent of employers' store and review employee computer files; 55 percent of employers retain and review employee e-mail. Eighty percent of employers engaging in monitoring and surveillance activities inform employees that the company is monitoring content, key strokes and time spent on the keyboard; 86 percent alert employees about e-mail monitoring and 89 percent notify employees that their Web usage is monitored. Lastly, 13 percent of businesses have been engaged in workplace lawsuits arising from employee e-mail use.[1430] In the 2004 survey, 13, 2 percent of respondents confirmed that their organisation had faced a sexual, or racial or hostile work environment lawsuit emanating from e-mail.[1431]

According to the 2007 Electronic Monitoring & Surveillance Survey from the AMA, over 50 percent of employers had dismissed employees for either e-mail or Internet abuse. More specifically, 28 percent of employers had dismissed employees for various forms of e-mail abuse (namely breach of confidentiality rules, violation of company policy, excessive personal use and inappropriate or offensive language) and 30 percent for Internet abuse (namely violation of company policy, viewing, downloading or uploading inappropriate or offensive content and excessive personal use). Web surfing by employees, according to the 2007 survey, remained a primary

[1429] Finkin "Information Technology and Worker's Privacy: The United States Law" (2002) 23 *Comparative Labour Law and Policy Journal* 471 474 – 476.

[1430] 2005 Electronic Monitoring and Surveillance Survey: Many Companies Monitoring, Recording, Videotaping – and Firing - Employees.

[1431] 2004 American Management Association Survey.

concern for employees even though a lesser percentage of employers reported that they monitored Internet connections (in 2007 only 66 percent of employers monitored employee Web activity). A considerable number of employers also monitor e-mail use mostly through technology which automatically monitors e-mail and to a lesser extent by assigning an individual to manually read and review e-mail. The 2007 survey further showed that employers were not only monitoring employee computers by tracking content or keystrokes and by storing and reviewing computer files, but by also monitoring the blogosphere and social networking sites to see what is written by employees.[1432]

7.6.2 Legislation

Even though these surveys indicate that a considerable number of employers in the United States prefer to limit employee use of company e-mail and Internet facilities and may enjoy an almost unfettered discretion in limiting employee use of e-mail and Internet, the privacy interests of employees are protected by legislation.

7.6.2.1 Constitution

The Fourth Amendment of the United States Constitution prohibits unreasonable searches and seizures by government employers.[1433] Employees may argue that employer monitoring of their computer usage constitutes an unreasonable search and seizure and therefore violates their Fourth Amendment rights. In order to succeed in such a challenge, an employee has to establish that he or she had a legitimate privacy expectation in the computer monitored and further has to establish that his or her subjective expectation of privacy is one that society is prepared to accept as objectively reasonable.[1434] Individuals possess reasonable privacy expectation in their privately owned home computers.[1435]United States courts seem reluctant to extend a similar expectation of privacy with respect to the contents of office computers. It is generally accepted that government employees and private sector employees may have a reasonable expectation of privacy in their offices, desks or file cabinet. However it is also accepted that this expectation may be reduced by office procedures,

[1432] 2007 Electronic Monitoring and Surveillance Survey

[1433] *O'Connor v Ortega* 480 US 709 (1987).

[1434] *US v Simons* 206 F3d 392, 398 (2000).

[1435] *Trulock v Freeh* 275 F 3d 391 (4th Cir. 2001).

practices and regulations.[1436] Even where courts have held that employees possess a privacy expectation with respect to the contents of office computers,[1437] it does not follow that courts will hold that the monitoring constitutes an unreasonable search. For example, in *Simons* the court found that although the employee had a reasonable expectation of privacy in his office, this expectation did not extend to the record of his internet usage in the workplace, particularly in light of the employer's computer monitoring policy which stated that the employer would "audit", "inspect" or "monitor" employee internet use including all file transfers, all web sites visited and e-mail messages sent and received.[1438]

7.6.2.2 Electronic Communications Privacy Act

The Federal Wire Tap Act[1439] ("Wire Tap Act") and the Stored Communications Act (Stored Communications Act) were enacted in the Electronic Communications Privacy Act[1440]("ECPA") to address the interception of electronic communications such as e-mail. It is important to note that the ECPA applies to both public and private conduct. The ECPA protects the privacy of the contents of electronic communications. The ECPA limits employer interceptions of employee e-mail messages and although the statute does not specifically mention "electronic mail" (but rather "electronic communications"), Congress[1441] and the courts[1442] take the view that

[1436] *O'Connor v Ortega* 717. See *Williams v Philadelphia Housing Authority* 826 F. Supp. 952 (E.D. Pa. 1993) (where the court held that no reasonable expectation of privacy existed against removal of an employee's computer disk and subsequent search of the desk by the employer because all the documents on the disk were work related and *United States v Simons* 29 F. Supp. 2d 324 (E.D. Va. 1998) (where court found no reasonable expectation of privacy in employees' hard drive because employee had downloaded a vast amount of pornographic material and the downloading of such material was unacceptable in light of his employer's Internet use policy).

[1437] *Leventhal v Knapek* 266 F 3d 64 (2d Cir. 2001).

[1438] *US v Simons* 398 - 399. See also *Leventhal v Knapek*. Even though the court in *Leventhal v Knapek* held the employee had a reasonable expectation of privacy in the contents of his computer, the search of his computer was held not to have violated his Fourth Amendment rights because it was reasonably related to investigations concerning his workplace misconduct.

[1439] The federal Wire Tap Act was formally known as the Omnibus Crime Control and Safe Streets Act of 1968. The Wire Tap Act and Stored Communications Act are derivatives of the Omnibus Crime Control and Safe Streets Act. The Electronic Communications Act was enacted to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technology". *Fraser v Nationwide Mutual Insurance Co* 135 F Supp 2d 623, 632 - 633 (2001).

[1440] Act of 1986.

[1441] The 99th Congress stated that e-mail *inter alia* new technologies such as pagers, mobile phones and digital information is one of the technologies envisaged by the ECPA. S. Rep. No. 99 – 541, 99th Congress 13 – 14 (1986), reprinted in U.S.C.C.A.N. 3555, 3562 – 66.

[1442] For example in *Steve Jackson Games, Inc. v. United States Secret Service* 26 F.3d 457, 461 (5th Cir. 1994) the 5th Circuit stated because e-mails can be intercepted illegally it fell within the ambit of the

the term "electronic communications" includes e-mail. More so, because the ECPA's enactment constituted an effort to update United States law in light of technological advancements.[1443] The ECPA consists of two parts which are relevant to employee e-mail privacy – the Wire Tap Act[1444] (contained in "Title I" of the ECPA) and the Stored Communications Act[1445] (contained in "Title II" of the ECPA). The Wire Tap Act prohibits the interception of electronic communications, whilst the Stored Communications Act prohibits the unauthorised access of stored electronic communications. Title I of the ECPA amended the Federal Wire Tap Act which previously addressed only the interception of wire and oral communications, to also address the interception of electronic communications. Title II of the ECPA, on the other hand, created the Stored Communications Act designed to address the access to stored wire and electronic communications.[1446]

Title I of the ECPA prohibits the unauthorised and intentional interception of electronic communications while such communications are in transit. More precisely, Title I provides a right of action against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication".[1447] Title I defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo-optical system, but does not include any wire or oral communication, any communication through a tone-only paging device, any communication from a tracking device, or electronic funds transfer information stored by a financial institution in a communications system." An "interception" is defined as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or

ECPA. See also in this regard *Wesley College v Pitts* 974 F.Supp. 375, 385 (D.Del. 1997) in which the court explained that the term "electronic communications" in the ECPA included electronic mail.

[1443] Isajiw PJ 'Workplace E-Mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers' 2001 20 *Temple Environmental Law and Technology Journal* 73 81.

[1444] 18. U.S.C. § 2511 – 2521.

[1445] 18. U.S.C. § 2701 – 2711.

[1446] Isajiw "Workplace E-Mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers" (2001) 20 *Temple Environmental Law and Technology Journal* 73 footnote 214.

[1447] Miller "Don't Be Evil": GMail's Relevant Text Advertisements Violate Google's Own Motto and Your E-Mail Privacy Rights" (2005) 33 *Hofstra Law Review* 1607 1616.

other device". As such, the contents of a communication are deemed to have been intercepted where they are acquired "through the use of any electronic, mechanical, or other device". In terms of the Federal Wire Tap Act[1448], the term "intercept" (at least with regard to oral and wire communications) was construed as requiring that the acquisition of the communication be contemporaneous with the transmission of the communication from the sender to the recipient.[1449] Some courts applied this "contemporaneous requirement" of the term "intercept" to electronic communications such as e- mail. That is to say, these courts have construed the term "intercept" to have the same meaning for the different types of communications.[1450] This is problematic, because the different modes of communication rely on different technologies and are transmitted in different ways. The court in *Fraser v Nationwide Mutual Insurance Co*[1451] described the nature of e-mail communications as "indirect" because an e-mail message "passes through intermediate storage or back – up storage in the course of transmission" from the sender to its recipient. The court added that the transmission of e-mail "is completed when the recipient logs on to the system and retrieves the message from intermediate storage"[1452]. Consequently, e-mail may be intercepted before its transmission is complete, or whilst it is stored in intermediate or back – up storage. The narrow interpretation of the term "intercept" (based on contemporaneity) excludes e-mail communications from the Act's interception protection. As such, some courts like the court in *Fraser v Nationwide Mutual Insurance Co* have attempted to give the term "intercept" a broader meaning and found that an e-mail message can be intercepted whilst in storage, before it is received by its recipient.[1453]

Title II of the ECPA protects against the unauthorised acquisition of stored electronic communications. Title II defines "electronic storage" as "(A) any temporary, immediate storage of wire or electronic communications incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic

[1448] Act of 1968.

[1449] *United States v Turk* 526 F2d 654 (5th Cir. 1976).

[1450] *Steve Jackson Games Inc v US Secret Service* 36 F 3d 457 (5th Cir. 1994); *Konop v Hawaiian Airlines Inc* 302 F3d 868 (9th Cir. 1992); *United States v Steiger* 318 F3d 1039, 1048 – 49 (11th Cir. 2003; *Fraser v Nationwide Mutual Insurance Co* 352 F3d 107 C.A. 3 (Pa.) (2003).

[1451] 135 F Supp 2d 623 (2001).

[1452] 633.

[1453] See also *Konop v Hawaiian Airlines Inc* 236 F 3d 1035 C.A. 9 (Cal.) 2001.

communication service for the purposes of backup protection of such communication." Further, the unauthorised access to a facility providing electronic communication services and thereby access to stored electronic communication, constitutes a federal crime in terms of Title II. Moreover, unless the interception or unauthorised access of electronic communication is permitted by a statutory exemption or defence, such interception or unauthorised access constitutes a violation of the ECPA and the commission of a federal crime. Title I houses exceptions for "business use in the ordinary course of business", "providers of communications" and "authorisation by users of communications systems" and Title II houses the exceptions for "providers of communications" and "authorisation by users of communications systems."

It is important to note that theUnited States Patriot Act[1454]repealed the inclusion of "stored wire communications" in the definition of "wire communication". The repeal of this particular aspect of the ECPA has significant implications, given that some courts have based their findings on the textual distinction between "wire communication" and "electronic communication" and have, on the basis of this distinction, held that the definition of "intercept" in Tile I with regard to electronic communications applies only to "acquisition contemporaneous with transmission" and not to communications in electronic storage.[1455]

The ordinary course of business exception permits an employer to intercept an electronic communication 'in the ordinary course of business through use of equipment provided by a communications carrier as part of the communications network.' The term "ordinary course of business" is not defined in the ECPA. However, it requires that the use be for a legitimate business purpose, routine and with notice to persons being monitored.[1456]

[1454]Act of 2001. The Act was enacted in response to the September 11 terrorist attacks on the US and the provisions of the Act afford government greater authority to monitor electronic communications. The Patriot Act further has significant implications for the privacy rights of employees as employers may be required in terms of the Act to assist government in its investigations into terrorism by providing information about their employees.

[1455] Hebert *Employment Privacy Law* (2009) § 8A:18.

[1456] Finkin "Information Technology and Worker's Privacy: The United States Law" (2002) 23 *Comparative Labour Law and Policy Journal* 471 481.

The provider exception allows "an operator of a switchboard, or an officer, employee or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is necessary to the rendition of his service or to the protection of the rights or property of the provider of that service." The provider exception simply allows e-mail providers to intercept and disclose electronic communications necessary to render services or to protect the rights or property of the provider. Therefore, an employer who provides an electronic communications service is free to intercept and disclose electronic communications in protecting its rights and property or in rendering services.[1457]

The consent exception provides that an interception or disclosure of an electronic communication is lawful where the party intercepting or disclosing is a party to the communication and where one of the parties to the communication consents to the interception or disclosure. The courts have accepted that "full knowledge or adequate notice", such as an employee's signature on a company e-mail policy, suffice as implied consent.[1458] However, the mere knowledge that an employer's system may be monitored does not constitute implied consent.[1459]

At first glance the ECPA seems to provide comprehensive protection of privacy in the context of e-mail and Internet, but the Act allows monitoring in the sense that "[o]nce an employer meets an exception, the ECPA place no restrictions on the manner and extent of monitoring…." Moreover, some courts have interpreted the scope of the ECPA and further limited its effectiveness. Specifically, courts have held that an electronic communication is only intercepted when it seized while in the process of transmission.[1460] Other court decisions have narrowed Title II to hold that

[1457] See for example *United States v Mullins* 992 F. 2d 1472 (9th Cir. 1993).

[1458] Isajiw "Workplace E-Mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers" (2001) 20 *Temple Environmental Law and Technology Journal* 73 89.

[1459] See *Deal v Spears* 980 F.2d 1153 (8th Cir. 1994) and *Ali v Douglas Cable Communications* 929 F. Supp. 1362 (D. Kan. 1996). Finkin "Information Technology and Worker's Privacy: The United States Law" (2002) 23 *Comparative Labour Law and Policy Journal* 471 481 – 482.

[1460] Miller ''Don't Be Evil: Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-Mail Privacy Rights' (2005) 33 *Hofstra Law Review* 1607 1610. For example in *Steve Jackson Games, Inc. v. United States Secret Service* 26 F.3d 457, 461 (5th Cir. 1994) the Fifth Circuit held that the seizure of a computer on which is stored private e-mail that has been sent to an

unauthorised access to stored communications is unlawful only when the electronic communication has not been delivered to the recipient.[1461]

That being said, two decisions have interpreted the ECPA broadly and purposively. In the first of these decisions, *Theofel v Farey – Jones*,[1462] the defendants argued that the messages they accessed were not "electronic storage" as defined by Title II and therefore fell outside the ambit of Title II. The court pointed out that several courts have held that the definition of "electronic storage" covers e-mail messages stored pending delivery to the recipient and does not cover post – transmission storage. The court, however, held the following in respect of the definition of "electronic storage": "In contrast to subsection (A), subsection (B) does not does not distinguish between intermediate and post – transmission storage…[b]y its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post – transmission" .[1463]

In the second and probably most important decision, *United States v Councilman*[1464], the Fifth Circuit held that Congress intended that "electronic communication" as defined in the ECPA be interpreted broadly. The court also held that Congress did not intend, by including electronic storage in the definition of wire communications, to exclude electronic storage from the definition of electronic communication. The court

---

electronic but not yet read by recipients was not unlawful under the Federal Wiretap Act. In other words the court found that the seizure of such a computer did not constitute an interception as defined by Title I of the ECPA. The court distinguished between the definitions of "wire communication" and "electronic communication" and observed that although the definition of "wire communication" included the electronic storage of wire communications, the definition of "electronic communication" by contrast did not include the storage of electronic communications. As such, the court concluded that congress did not intend for "intercept" in Title I to apply to "electronic communication" when those communications are in "electronic storage". Similarly in *Konop v Hawaiian Airlines*, the Ninth Circuit adopted a narrow interpretation of the term "intercept" to mean contemporaneous acquisition and as such found that the pilot's website amounted to a stored communication which was not included in the Title I definition of "intercept". The airline pilot in *Konop* maintained a website on which he posted bulletins critical of his employer and others. The website could only be accessed through a password given to eligible individuals mostly employees of the airline and such individuals had to register and consent to a non-disclosure agreement prior to acquiring a password. The vice president of the airline was able to occasionally gain access and view the website by using an eligible employee's password. The airline pilot became aware of the vice president's access and brought an action against the airline, alleging that the airline's unauthorised access to the website violated his Title I right.

[1461] *Fraser v Nationwide Mutual Insurance Co*. 135 F. Supp. 2d 623 (E.D. Pa. 2001).

[1462] 341 F. 3d 978 2004 Daily Journal D.A.R. 2089.

[1463] 2346.

[1464] 418 F.3d 197 (1st Cir. 2005).

concluded in this regard that "electronic communication" included "transient electronic storage that is intrinsic to the communication process"[1465].

A combination of the exceptions created by the ECPA, the narrow interpretation of the ECPA by various courts and the fact that the majority of companies implement detailed e-mail and Internet policies, lessens the chances of success for an employee's claim under the ECPA[1466]. However, in *Fischer v Mount Olive Lutheran Church*,[1467] a youth minister brought an action against the church and some its staff alleging they had violated his Title I right by eavesdropping on personal telephone conversations. The defendants argued that their conduct was not in violation of Title I, because the employee's telephone conversations were intercepted in the "ordinary course of business". The upheld the plaintiff's claim by finding that under Title I the employer is obliged to cease listening as soon as it had ascertained that its employee's calls was personal, regardless of the contents of the conversation.[1468]

7.6.2.3 State Legislation

The weaknesses or shortcomings of the ECPA may be supplemented by state wiretapping legislation.[1469]Florida's Security of Communications Act of 2003, for example, is more protective of electronic communications than the ECPA. The Act prohibits the interception and disclosure of electronic communications, including workplace communications, where the sender and the recipient have not given consent. However, this is not required in certain circumstances, such as where the employer reasonably suspects the employee of breaking the law or of creating a

[1465] Miller argues that the narrow *Konop* and *Steve Jackson Games* interpretation of the ECPA is problematic because it permits service providers such as "Gmail to intercept, process, and utilise e-mail intended for users for advertising and revenue purposes" and suggests as a possible remedy the amendment of the Wiretap Act by creating a definition of "intercept" for both wire and electronic communications. In other words the statute has to be amended to "specifically include unopened, post transmission e-mail messages in temporary storage within the list of communications that may be intercepted." Miller ''Don't Be Evil: Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-Mail Privacy Rights" (2005) 33 *Hofstra Law Review* 1607 1638.

[1466] Lasprogata, King and Pillay "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada" (2004) 4 *Stanford Technology Law Review* 1 74.

[1467] 207 F. Supp. 2d 914 (W.D. Wis. 2002).

[1468] 923.

[1469] Notably 48 US states have adopted legislation fashioned on ECPA provisions and exceptions. Eltis "The Emerging American Approach to E-Mail Privacy in the Workplace: Its Influence on Developing Case Law in Canada and Israel: Should Others Follow Suit" (2003) 24 *Comparative Labour Law and Policy Journal*) 487 501.

hostile work environment.[1470] Colorado requires that state employers have written e-mail monitoring policies and Wisconsin restricts the ability of employers to discipline its employees on the basis of information obtained through surveillance.[1471] Connecticut has further legislated specifically on electronic communication harassment and so have the states of Delaware, Alabama, Indiana and New York.[1472] The state of Nebraska has unique legislation which allows employers to intercept their employee's electronic communications without consent.[1473] States protecting the right to privacy in their constitution, like the state of California in *Soroka v Dayton Hudson Corporation*[1474], have extended this protection to a private employee. Even though California's constitutional privacy provision protects both private and public sector employees, the employees in *Bourke v Nissan Motor Corporation*[1475]could not rely on it to protect their e-mail communications. The employees were dismissed for sending sexually suggestive material through the employer's e-mail system. The employees argued that they had a reasonable expectation of privacy in their e-mail communications in the workplace because they had been given individual passwords. The court found that the employees had no reasonable expectation of privacy because they knew that their e-mail may be monitored.[1476]

7.6.3 Case Law

The general tenor of United States case law is that employees' have no reasonable expectation of privacy in e-mail boxes maintained by an employer or sent over an employer's e-mail system, despite assurances from employers that such communications would not be intercepted and would not constitute the basis of a

[1470]Lasprogata, King and Pillay "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada" (2004) 4 *Stanford Technology Law Review* 1 84.

[1471]*Supra*.

[1472]Lasprogata, King and Pillay "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada" (2004) 4 *Stanford Technology Law Review* 1 84.

[1473]Supra.

[1474] 7 Cal. App. 4th 203, 1 Cal. Rptr. 2d 77, 84-85 (1991), review dismissed, 24 Ca. Rptr. 2d 587 (1993).

[1475] No. B068705 [1 ILR (P&F) 109] (Cal. Ct. App. 26 July 1996).

[1476] Robinson "Big Brother or Modern Management: E-Mail Monitoring in the Private Workplace" (2001) 17 *Labor Lawyer* 311 324.

termination.[1477]Moreover, employees have no reasonable expectation of privacy in their e-mail communications sent over the company's system even where an employer does not have in place an effective e-mail and Internet policy.[1478]

7.6.3.1 Fourth Amendment Case Law

The United States Court for Appeals for the Armed Forces confirmed in *United States v Maxwell*[1479] that an individual had a reasonable expectation of privacy in e-mail messages transmitted through an on - line computer service such as AOL, because the e-mails were stored in a centralized computer until the recipient opened his or her network and retrieved them.[1480] The court also found that the expectation of privacy in e-mail messages was largely dependent upon the type of e-mail and the intended recipient: "[E-mail] [m]essages sent to the public at large in the "chatroom" or e-mail that is forwarded from [one person to another] loses any semblance of privacy"[1481].[1482]On the contrary, in *United States v Slanina*[1483] it was reasoned that public sector employees would have a reasonable expectation of privacy in their offices and in files stored on a computer in the absence of a policy informing employees that their computer and internet usage will be monitored and where an employee's computer is not routinely accessed by other employees. Other courts have suggested that employees have no reasonable expectation of privacy in electronic

[1477] *Smyth v Pilsbury Co* 914 F. Supp. 97 (E.D. Pa. 1996).

[1478] For example in the unreported decision of *Restuccia v Burk Technology* of N.E.2d, 1996 WL 1329386
Mass.Super. 1996 the employer had no policy against chatting on its e-mail system and had not specifically indicated to its employees that management had access to their computer files. As such, the employees in *Restuccia* argued that they had an expectation of privacy in their e-mails messages which included nicknames for the company president and references to his alleged extra marital affair with another company employee. The employees claimed that they did not know that deleted e-mails on the company e-mail system were saved on the company's back up file.

[1479] 45 M.J. 406 (C.A.A.F 1996).

[1480] 417.

[1481] 419.

[1482] Similarly in *United States v Charbonneau* 979 F. Supp. 1177 (S.D. Ohio 1997) the court found there was no reasonable expectation of privacy in e-mail messages sent by an individual in an electronic chat room because the "openness of the chat room" incrementally diminished an individual's reasonable expectation of privacy. The court further stated that an e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that communication is received. The court also noted expectations of privacy in e-mail transmissions depend in large on the type of e-mail sent and the recipient of the e-mail. The court further noted that e-mail messages sent to an addressee who forwards the e-mail to third parties such as the public at large in a chat room did not enjoy some reasonable expectation of privacy. Courts have also held that a user of a computer bulletin board has no legitimate expectation of privacy in e-mail sent to such a board (*Guest v Leis* 255 F.3d 325 (6th Cir. 2001).

[1483] 283 F3d 670, 677 (5th Cir. 2002)

communications sent through an employer's network. The reasoning of the United States Court of Appeals for the Armed Forces in *United States v Munroe*[1484] supports this suggestion. The court in *Munroe* confirmed that an employee of the United States Air Force had no reasonable expectation of privacy from personnel maintaining the system in e-mail messages sent through an electronic host system, because the system resided on a computer owned by the air force. The court found that the expectation of privacy in such e-mails was further diminished by the fact that users had received notice that by logging into the system they are consenting to monitoring.[1485]

7.6.3.3 Common Law Case Law

Private and public sector employees may claim an invasion of their common law right to privacy with respect to e-mail monitoring. The common law of tort relating to the invasion of privacy has been divided into four distinct parts: (1) unreasonable intrusion into one's seclusion, (2) misappropriation of one's name or likeness, (3) public disclosure of private facts, and (4) false light.[1486] In the context of the privacy of electronic communications in the workplace, the relevant tort is 'unreasonable intrusion into one's seclusion'. The Second Restatement of Torts defines the tort as follows: "One, who intentionally intrudes, physically or otherwise, upon the solitude of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person". [1487]

The decision of *Smyth v Pillsbury*[1488]touched on this tort in relation to e-mail monitoring. In Smyth an employee brought an action against his employer for wrongful discharge. The employee was discharged from his position as regional operations manager for transmitting in appropriate and unprofessional comments over his employer's e-mail system. The Pennsylvanian court held that the termination did not violate public policy and the former employee could not maintain a wrongful

[1484]52 M.J. 326 (C.A.A.F. 2000).

[1485] 330.

[1486]Prosser *Privacy: A Legal Analysis* in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 104 - 107.

[1487]The decision of *Nipper v Variety Wholesalers Inc* 638 So. 2d 778 (Ala. 1994) defined the tort as the wrongful intrusion into one's private life activities in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities.

[1488]914 F Supp 97 (E.D. Pa. 1996).

discharge claim under Pennsylvania law. The court reasoned: "…we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communication would not be intercepted by management. Once [the employee] communicated the alleged unprofessional comments to…his supervisor over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost". [1489] The reasoning in *Smyth* was considered instructive in *Garrity v John Hancock Mutual Life Insurance Company*[1490]. In *Garrity*, two employees of an insurance company were dismissed after they transmitted sexually explicit e-mail over the company's intranet system in violation of the company's e-mail policy. The employees admitted that they knew that the company could access and view their e-mails on its intranet system and that they had to exercise caution in sending e-mails, but argued they had a privacy expectation because the company had instructed them on how to create a passwords and personal mail folders. The court held that the employees had no reasonable expectation of privacy where the employees assumed that recipients might forward the messages to others, knew the company had the ability to look at e-mail on the intranet system and knew they had to be careful about sending e-mails. Similarly, in *McLaren v Microsoft Corporation*,[1491] the court found that an employee had no reasonable expectation of privacy over the contents of e-mail messages sent over the company's e-mail system, because, even though the employee stored his e-mail messages in "personal folders" and created a password to access his e-mail messages, all e-mail messages stored in his personal folders were first transmitted over the network and were at some point accessible to a third party.[1492] Courts have also held that employees have no reasonable expectation of privacy in a computer provided by the employer for use in the employee's home, particularly where the employer's computer monitoring policy

[1489] 101.

[1490] 18 IER Cases 981 (D. Mass. 2002).

[1491] 1999 WL 339015 (Tex. App. Dallas 1999).

[1492] See also *Thygeson v US Bancorp*, 34 Employee Benefits Cas. (BNA) 2097, 2004 WL 2066746 (D. Or. 2004). In *Thygeson* the United States District Court for the District of Oregon in held an employee had no reasonable expectation of privacy in files accessed through his personal e-mail account and stored in his personal folder because the employer's policy on monitoring computer use permitted the employer to access to the files.

made it clear that the employer would monitor files and messages on the computer and the employee consents to the policy.[1493]

7.6.4 Analysis

It appears that United States employers, unlike their United Kingdom counterparts, who primarily monitor employee usage of e-mail and Internet to minimize the security risks associated with such usage, mainly monitor employee e-mail and Internet use in the workplace in order to minimize litigation associated with the inappropriate use of these tools by employees and the role that electronic evidence plays in such lawsuits and in regulatory investigations.

Generally, United States legislators have been slow in designing laws that address privacy in the workplace, probably because they know that such laws will not have the support of corporate America and congress. At the same time, legislation that does exist at both Federal (the Constitution and the ECPA) and State level, provides protection that may be more apparent than real. This is not only due to presence of exceptions contained in legislation, but also because courts have added fuel to the fire in failing to extend privacy protection, often through restrictive interpretation of applicable legislation, to newer technologies such as e-mail and Internet. What remains true is that case law, whether called on the interpret legislation or applying the common law, works with the underlying concept of privacy (often predetermined in case of legislation) premised on the reasonableness of the expectation of privacy in the surrounding circumstances. In the context of the workplace, and although case law addressing the issues raised by the increase and growth of e-mail and Internet use in the workplace has to draw a balance between employer property rights, employee privacy, and dignity rights, this simply means that United States courts have often held that employees have no expectation of privacy in the workplace. This is especially true where the employee uses the employer's tools to carry out their employment or where employers restrict and monitor employee use of e-mail and Internet tools and provide employees with notice of monitoring activities. Such a

[1493] *TBG Insurance Services Corp v Superior Court of Los Angeles County* 96 Cal. App. 4th 443 (2002).

notice invariably negates any expectation of privacy the employee may claim to be entitled to.[1494]

7.7 CONCLUSION

This chapter argued that employee monitoring is not necessarily a new trend, but that modern technology has enabled employers to monitor their employees more effectively and more extensively due to widespread use of technology enabled tools like e-mail and Internet. The arguments advanced by employers to justify the monitoring of employee e-mail and Internet usage are primarily aimed at protecting the employer's proprietal interest in the e-mail and Internet facilities, in ensuring that the workplace is efficient and productive and eliminating risks associated with abuse of information systems. On the other hand, arguments against the monitoring and of e-mail and Internet usage in the workplace are aimed at preserving the employee's informational privacy. What has become clear from the discussion in this chapter, is that, from a legal perspective, these balancing of interests invariably involve one (or both) of two issues. First, the underlying approach to the concept 'privacy' may serve to ultimately determine this balance. What is clear from the United Kingdom experience (within the supranational European context) is that a society premised on an acceptance that privacy means no more than a 'reasonable expectation of privacy', will find it easier to limit employee interests in the context of e-mail and internet use. The survey in this chapter shows that this is the case across the three different jurisdictions. Whether the 'reasonableness' of the expectation of privacy' is pre-determined in legislation (typically through a prohibition on interception and, crucially, provision for exceptions to the prohibition), or on a case by case basis through judicial evaluation, it will be easy for an employer to make the argument that there was no infringement of privacy (as there was no reasonable expectation of privacy to begin with). Of course, a notion of privacy which is aimed more at the individual may well alter this fundamentally.

At the same time and even where it is accepted that employer policies and practices relating to e-mail and Internet use may infringe upon privacy, this calls for no more than a balancing act between the interests of the employer and employee. For a variety

[1494] Babson *Monitoring Electronic Mail in the Workplace: Property v Privacy* (2001) 1.

of reasons identified across the different jurisdictions, this balancing act will almost invariably be determined in favour of the employer. The point is that although it is difficult to fault the balancing of competing interests to determine a dispute, the nature of privacy and the nature of the employment relationship, in which the balance of power will more often than not be in favour of the employer, will largely predetermine the issue.

If one evaluates these broad statements on a more country-specific basis, it may be said that despite the fact that South Africa is a country with a comprehensive and generous bill of rights, which includes the right to privacy and in particular the right to informational privacy, it appears courts are loathe to allow this right to exist in the context of the workplace, especially, in the context of e-mail and Internet communications within the workplace. South African courts and tribunals are more likely to protect the employer's interest in not having its e-mail and Internet facilities abused for non – business purposes, even in the absence of policies. Tribunals have even suggested that the question remains to finally be determined by an employee's own common sense. South African tribunals have yet to fully consider the implications of RICPCIA on the interception and monitoring of employee communications in the workplace. It is suggested that this will not make much difference – as mentioned above, as long as the underlying notion of privacy remains the reasonableness of the expectation of privacy (an approach arguably codified in RICPCIA), employers have much leeway to control e-mail and Internet use. Perhaps what South Africa needs is a code similar to the United Kingdom's Employment Practices Code, which at least emphasizes the principles of transparency and proportionality, considerations clearly absent from an examination of the decisions in the current context.

In the United Kingdom, employees have recourse to a number of pieces of legislation. One of these pieces of legislation is Article 8 of the ECHR which was imported into United Kingdom through the Human Rights Act. The other important piece of legislation regulating the interception and monitoring of employee communications in the workplace is the Data Protection Act. The Act has a number of principles, which it is submitted reflect a sound balance between the competing rights at play in relation to the general issue of privacy in the workplace. What also makes the Act

commendable is that it has been supplemented by an Employment Practices Code which guides employers towards observing the requirements of the Act. For instance, the Employment Practices Code recommends that employers communicate the nature and extent of the monitoring and also the purpose for which the monitoring is carried out. Furthermore, as already indicated, the Employment Practices Code places an emphasis on two important principles, namely, transparency and proportionality. These principles ensure that the employee's interests to informational privacy are protected and also that the employee has some control over his or her communications in the workplace. It would seem that the different legislative approach at both the supranational (European) and national (United Kingdom) levels, have already served to inform a somewhat different judicial approach to that of South Africa. For example, decisions such as *Halford* ensure that employers were reminded of the fact that the employee's right to privacy is not left at the front door of the office, but exists even if and while the employee is in the workplace. Another example, contrary to the approach of South African Tribunals who have gone so far as justify employer intrusion even in the absence of internal policies about workplace communication systems, is to be found in a decision like *Copland v United Kingdom*, which show that United Kingdom tribunals are likely to find that the absence of a policy creates a reasonable expectation of privacy in respect of the use of information systems.

The United States experience serves as support of the general statements made earlier in this conclusion – despite legislation regulating the interception and monitoring of employee communications in the workplace by the employer, this legislation has been of little or no benefit to employees as case law appears to favour the employer's proprietary interest in such communications. United States courts, similar to South African Courts, have often held that employees have no expectation of privacy in the workplace arena, seeing as the communication systems in place belong to the employer and not the employee and often simply because the employee has been notified of monitoring.

CHAPTER 8:

SELECTED FOCUS AREAS: GENETIC TESTING

8.1 INTRODUCTION

This chapter is the second of two chapters focussing on workplace policies and practices that not only have the potential to threaten or pressurise the protection of privacy in the workplace, but also illustrate how recent advancements in technology create new challenges for the protection of privacy. The previous chapter concluded that the monitoring of employees is not a new concept but rather one that has developed and become sophisticated due to advancements in technology. This chapter focuses on genetic testing, which perhaps is the most recent example of the way in which scientific advancement may challenge privacy.

As point of departure, this chapter considers, first of all what genetic testing means, an enquiry which requires, in turn, a consideration of genes, genetic testing and genetic information. Thereafter, the legal challenges created by genetic testing will be considered.

8.2 GENETIC TESTING

8.2.1 Genes

DNA (deoxyriboneuclic acid) is often said to be the most important molecule in human genetics because of the fact that it is the "basic bearer of genetic information in the human body"[1495].

The human body is made up of approximately 100 trillion cells. Moreover each cell in the human body (except for egg and sperm cells) carries an estimated 50,000 to 100,000 genes and contains DNA molecules.[1496] Thus DNA is found in all human cells except in mature red blood cells.[1497] The DNA molecule is a ribbon consisting of

[1495] Privacy Commissioner of Canada *Genetic Testing and Privacy* Discussion Paper (1995) 5.
[1496] Privacy Commissioner of Canada *Genetic Testing and Privacy* Discussion Paper (1995) 6.
[1497] Privacy Commissioner of Canada *Genetic Testing and Privacy* Discussion Paper (1995) 6.

2 coiled strands forming a double helix or spiral.[1498] Each double helix DNA strand consists of varying sequences of four chemicals bases – adenine (A), guanine (G), thymine (T) and cytosine (C).[1499]

Genes consist of various base pairs located on chromosomes.[1500] Chromosomes are elongated strings of DNA and protein. Every human being has 46 chromosomes, arranged in two sets of 23 chromosomes. One set of 23 chromosomes is received from each parent.[1501]

An individual's entire genetic constitution or make up is also known as the genome and with the exception of identical twins no two individuals have the same genetic constitution.[1502] Genomes vary widely in size and the smallest genome for a free living organism, bacteria, contains approximately 600,000 DNA base pairs, while mouse genomes, like human genomes, contain approximately 3 billion base pairs.[1503]

DNA in the human body is commonly extracted from white blood cells, sperm cells, cells in saliva, nasal secretion, sweat and cells around the roots of the hair.[1504]

Broadly speaking genes can influence an organism's ability to combat infections, viruses and bacteria and the appearance of an organism and its behaviour.[1505] In human beings, genes not only influence an individual's characteristics and development but also an individual's susceptibility or propensity to develop a disease and the existence of particular conditions.[1506]The individual's susceptibility or propensity to develop a disease is in turn influenced by inherited genes or gene mutation or alteration resulting from environmental exposure. An individual may inherit genes from a parent which make them susceptible to developing a disease. For

---

[1498]Schwartz "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review*1 18. See also Edelson *The Human Genome Project* in Barker (ed.) *Genetics and Society* (1995) 44 - 55.

[1499]Privacy Commissioner of Canada *Genetic Testing and Privacy* Discussion Paper (1995) 6.

[1500] Solove and Rotenburg *Information Privacy Law* (2003) 248 – 249.

[1501]Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 7.

[1502]Schwartz "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review*1 21. See also Solove and Rotenburg *Information Privacy Law* (2003) 249.

[1503]http://www.ornl.gov/sci/techresources/Human_Genome/projects/info.shtml (2006-03-10).

[1504]http://www.ornl.gov/sci/techresources/Human_Genome/project/info.shtml (2006-03-10).

[1505]http://www.ornl.gov/sci/techresources/Human_Genome/project/about.shtml (2006-03-10).

[1506]Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 7.

example, scientists have established that conditions such as cystic fibrosis and prostate cancer are inheritable.[1507] Exposure to environmental factors may also alter or mutate an individual's genetic material in a manner that increases his or her propensity to develop a disease.[1508] For example, scientists have identified approximately 50 genetic anomalies that increase an individual's susceptibility to toxic and carcinogenic effects of elements such as copper, radiation, carbon monoxide and cyanide.[1509] Exposure to carbon monoxide and cyanide, for instance, can increase an individual's risk of developing symptoms of sickle cell anaemia.[1510]

8.2.2 Genetic Testing

Genetic testing has been defined as a "medical diagnostic tool used to detect deleterious genetic and chromosomal variations in order to identify potential future health problems or to confirm a prior diagnosis"[1511] and also as "testing to detect the presence or absence of, or alteration in, a particular gene sequence, chromosome or a gene product, in relation to a genetic disorder"[1512]. The United States' Genetic Information Nondiscrimination Act[1513] ("GINA") defines "a genetic test" to mean "an analysis of human DNA, RNA, chromosomes, proteins or metabolites that detects genotypes, mutations, or chromosomal changes".[1514] A genetic test does not, according to GINA, mean "an analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes".[1515] Simply put, genetic testing is the

[1507] See Pesonen "Genetic Screening: An Employer's Tool to Differentiate or to Discriminate?" (2001) 19 *Journal of Contemporary Health Law and Policy* 187 189.

[1508] Hebert *Employee Privacy Law* (2009) § 12: 1.

[1509] Pesonen "Genetic Screening: An Employer's Tool to Differentiate or to Discriminate?" (2001) 19 *Journal of Contemporary Health Law and Policy* 187 195.

[1510] Pesonen "Genetic Screening: An Employer's Tool to Differentiate or to Discriminate?" (2001) 19 *Journal of Contemporary Health Law and Policy* 187 195.

[1511] Deyerle "Genetic Testing in the Workplace: Employer Dream, Employee Nightmare Legislative Regulation in the United States and the Federal Republic of Germany" (1997) 18 *Comparative Labour Law Journal* 547 554.

[1512] United Kingdom Human Genetics Advisory Commission: Report on *The Implications of Genetic Testing for Employment* (1999). http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_03.htm (2006-03-27).

[1513] Act of 2008.

[1514] Section 201 of GINA.

[1515] *Supra*.

medical examination of an individual's genes or genetic material in order to determine whether the individual has the susceptibility or propensity to develop a disease.[1516]

Genetic testing can reveal an array of existing and probable medical information concerning an individual including "presymptomatic medical information about an individual, including information about an individual's increased risk of future disease, disability, or early death…carrier status, that is, the likelihood of parents passing on to their children a genetic condition and about the health of the individual's family members"[1517]. Before embarking on analysis of why genetic testing is potentially privacy invasive, it is also important to describe the type of information that can be determined or gleaned from one's genetic constitution as this will assist in illustrating how and why genetic testing may invade one's privacy.

8.2.3 Genetic Information

8.2.3.1 Introduction

GINA defines genetic information broadly to mean "with respect to any individual, information about such an individual's genetic tests, the genetic tests of family members of such individual, and the manifestation of a disease or disorder in family members of such individual."[1518] GINA excludes information about the sex or age of any individual from the meaning of genetic information.

There appears to be general consensus amongst legal commentators that genetic information is medical information about an individual.[1519] However, unlike other medical information, genetic information "includes information about…the individual's biological family…the results of tests of genetic material, the results of non-genetic medical tests revealing genetic information, and family medical history".[1520] Genetic information may be obtained from the following sources: genetic test results, medical records such as medical history forms, health insurance claims

[1516] Hebert *Employee Privacy Law* (2009) § 12: 1.

[1517] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal*139 143.

[1518] Section 1 of GINA.

[1519] Lasprogata King and Pillay "Workplace Privacy and Discrimination Issues Related to Genetic Data: A Comparative Law Study of the European Union and United States" (2006) 43 *American Business Law Journal* 79 88.

[1520] *Supra*.

and research on the prevalence of genetic diseases in a particular family.[1521] Broadly speaking, genetic information is therefore medical information ascertained from analysing an individual's genetic material and medical history. This link between medical and genetic information in mind the question then arises whether genetic information is different from other medical information and requires that it be treated differently from other medical information.

8.2.3.2 The Genetic Exceptionalism Debate

"Genetic exceptionalism" is the idea that genetic information is "…qualitatively different from other medical information and therefore raises unique social issues"[1522]. The genetic exceptionalism debate concerns the manner in which genetic information should be treated. On the one hand, proponents of genetic exceptionalism argue that genetic information is exceptional and should therefore be treated differently from other medical information. For instance, the confidentiality presumption in section 206 of GINA suggests that genetic information is somewhat different from other medical information. This presumption requires employers to treat genetic information as a confidential medical report about employees and to keep the information on separate forms and in separate medical files.

On the other hand, critics of genetic exceptionalism are of the view that genetic information should be treated like other medical information because there is nothing extraordinary or different about it.[1523]

8.2.3.3 Proponents of Genetic Exceptionalism

As already indicated above, proponents of "genetic exceptionalism" argue that genetic information is inherently exceptional and unique in comparison to other personal or

---

[1521] Hendricks "Genetics, Data Protection and Non – Discrimination: Some Reflections from an International Human Rights Perspective" (2001) 20 *Medicine and Law* 31 39.

[1522] Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 674. Suter blames various institutions (namely the public, media, scientific community and legislators) for perpetuating and upholding the idea of "genetic exceptionalism".

[1523] See for example Annas "Genetic Privacy: There Ought to Be Law" (1999) 4 *Texas Review of Law & Politics* 9 and Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1988) 11 *Harvard Journal of Law and Technology*. Poste however holds the view that genetic data does warrant special legal protection from other forms of medical information. Poste however submits that genetic testing poses different privacy risks from testing for an existing disease. Poste "Privacy and Confidentiality" (1999) 4 *Texas Law Review of Law and Politics* 25 26.

medical information. Underlying the idea of genetic exceptionalism is what has been described as "genetic determinism".

"Genetic determinism" is the notion that "genes determine and explain everything about us.[1524] For many, genes define our essence, make us human, and explain "our place in the world: our history, our social relationships, our behaviour, our morality, and our fate"[1525].

Proponents of "genetic exceptionalism" such as Annas argue that genetic information is more "powerfully private" than other forms of personal or medical information because it concerns very private information about an individuals' future health and an individuals' family's future health. Genetic information is also more private because it concerns information relating to private decision making (such as whether or not to have a child).[1526]Genetic information is further private because "it is in essence a reverse diary: it informs our younger selves about our aging selves".[1527] At the same time, unlike a written diary, which often contains present information, genetic information contains future information which is in code and probabilistic: "[Genetic information] is coded and probabilistic: we are not necessarily going to get every disease that we are genetically predisposed to develop. But you can think about your DNA molecule as a future diary. It is in code and probabilistic but just as private"[1528]. According to proponents, the fact that genetic information has historically been abused and misused, for example by the Nazis and scientists during the Eugenics movement, is also a pointer to its inherent power and value.[1529]

Green and Thomas assert that genetic information is "qualitatively" and "quantitatively" different from other medical information. In support of this assertion, Green and Thomas provide five distinguishing features of genetic information.[1530] The first feature relates to the risks associated with DNA's informational nature. The

[1524] Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly*669 674.

[1525]*Supra*.

[1526]Annas "Genetic Privacy: There Ought To Be Law" (1999) 4 *Texas Review of Law & Politics* 9 10.

[1527]*Supra*.

[1528]Annas "Genetic Privacy: There Ought To Be Law" (1999) 4*Texas Review of Law & Politics* 9 11.

[1529]Annas "Genetic Privacy: There Ought To Be Law" (1999) 4*Texas Review of Law & Politics* 9 12.

[1530]Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 572-573.

principal risk emanating from the nature of DNA is related to the kind of information genetic information reveals about an individual's genetic inheritance and the effect of the information on the concerned individuals.[1531] The risks include anxiety, distress and other psychological maladies brought on by individuals learning that they carry defective genes that may predispose them to serious conditions. Incidental risks in this regard include unintended disclosures of painful facts about family relationships, such as paternity issues.[1532] The nature of DNA further poses economic risks associated with discrimination in employment, medical insurance and life insurance.[1533] The second feature concerns the longevity of DNA.[1534] The longevity of DNA has the potential to harm individuals and their descendants. For example, the creation of DNA databases storing genetic samples may in some instances outlive the individuals who donated them, thereby not only compromising the concerned individuals' right to withdraw their samples, but also threatening their descendants.[1535] The third distinguishing feature relates to the familial risks implicated by genetic information.[1536]The study of genetics points to the fact that genes are shared among family members. The genetic testing of individuals therefore invariably implicates an individual's family members and exposes those members to physical, psychological and social harms.[1537] The fourth feature concerns DNA's role as an identifier. DNA is information rich and dense.[1538] For this reason, DNA has the ability to identify individuals who donate samples anonymously.[1539] The last distinguishing feature of genetic information is that it can impact members of a broader community group. Genes are not only shared among family members, but among ethnic or racial

[1531] *Supra*.

[1532] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 572-573.

[1533] *Supra*.

[1534] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 577.

[1535] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 577.

[1536] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 580 -581.

[1537] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 580 -581.

[1538] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 579.

[1539] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 579.

communities, and other groups with distinctive genetic inheritances.[1540] For instance, sickle cell anaemia is associated with persons of African American descent, the Tay-Sachs disease is associated with persons of Ashkenazi Jewish inheritance and Mediterranean fever is associated with individuals of Armenian descent. The fact that larger ethnic and racial communities are associated with certain conditions may reinforce prejudice against these communities and create "genetic castes".[1541] Green and Thomas argue that because of the above mentioned features (and associated risks) genetic information merits distinctive legal consideration, particularly in the context of insurance and employment.[1542]

8.2.3.4 Critics of Genetic Exceptionalism

Critics of "genetic exceptionalism" primarily contend that there is nothing unique or exceptional about genetic information in comparison to other forms of personal and medical information. For Ginsburg, the difference between a DNA test and family medical history is one merely of degree.[1543] Ginsburg agrees that a genetic test provides a high degree of specificity and may also provide a measure of predictability in comparison to a person's medical history, but contends that both types of medical information point to the probability of an individual developing a particular disease.[1544]Suter also argues that genetic information is not unique or exceptional as compared to other medical information purely because the issues it raises "…are cloaked in new technological guises".[1545] For Suter, the issues raised by genetic

[1540]Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 584 -585.

[1541]Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 584 -585. See also Schwartz "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review*1 28-30.

[1542]Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 590.

[1543]Ginsburg "Genetics and Privacy" (1999) 4 *Texas Review of Law and Politics* 17.

[1544]Ginsburg "Genetics and Privacy" (1999) 4 *Texas Review of Law and Politics*17 19. Even though Laurie agrees with Ginsburg's assertion that genetic information is not exceptional, Laurie prefers to view family medical history as different from genetic information. Family history for Laurie is abstract and detail flawed knowledge that may depend on poor or imperfect human memory. Further, it cannot determine the precise reason why an individual fell ill and the pattern of an individual's illness whereas genetic information can offer a high degree of specificity in terms of predicting the likelihood of disease or even the mode and manner of an individual's death. Furthermore, the threat posed by family medical history is abstract whereas the threat posed by genetic information is more concrete and is capable of altering an individual's perception in ways that family history cannot. Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 94.

[1545] Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 671.

information are on the contrary old and persisting problems about discrimination and privacy. Suter maintains that genetic information and other forms of medical information are akin and treating the two in a dissimilar manner will create inequities between individuals and classes.[1546] Suter advances a number of reasons in support of the unexceptional nature of genetic information. First, even though genes are an immutable trait, the risk factors that influence the degree to which genes affect our future health can be controlled.[1547] Second, most genetic information does not predict future disease.[1548] Third, although certain genetic diseases are prevalent in a particular racial or ethnic group or sex, most genetic diseases are not.[1549] Fourth, most genetic information is shared and therefore not unique.[1550] Fifth, not all genetic information is highly sensitive and stigmatizing.[1551]

Laurie also observes that genetic information is not exceptional because other forms of medical data can generate information that appears "genetic" in its functions. For example, high cholesterol levels are known predictors of cardiovascular disease. Furthermore, not all genetic information is predictive of future grave ill health. Many forms of genetic information are no more predictive than general health information.[1552]

[1546] *Supra*.

[1547] For example if an individual carries the gene for colon cancer, that individual can reduce the risk of developing colon cancer by undergoing regular endoscopies, a proper diet or surgery. Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 709.

[1548] For example if an individual carries a single copy of a recessive gene, the presence of the gene does increase the risk of future disease in the concerned individual but it does increase the chances of the individual having affected offspring. Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 710.

[1549] Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 710.

[1550] Human beings share 99 percent of their genetic information with other human beings and chimpanzees, resulting in only a fraction of genetic information being unique to each individual. Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 710.

[1551] For example genetic information such as an individual's blood type or eye colour is not sensitive or stigmatizing information. Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 710.

[1552] Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 104. See also Poste "Privacy and Confidentiality in the Age of Genetic Engineering" (1998) 4 *Texas Review of Law and Politics* 25. Poste like Ginsburg, Suter and Laurie contends that genetic information does not deserve separate legal consideration and the distinction between genetic information and other medical information is false.

8.2.3.5 Problems with Genetic Information

Proponents of "genetic exceptionalism" often argue that genetic information is exceptional because of its predictive accuracy in determining who is likely to be affected by a genetic disease.[1553] However, the predictive accuracy of genetic information is compromised by the fact that no two individuals, with the exception of identical twins, have exactly the same genes or gene constitution. Moreover, an individual's sequence tends to be unique and as such no standard DNA sequence exists. The developing nature of genetics further means that the genetic component of one condition will be known while the genetic component of another condition will be unknown. For example, a certain group of women will be labelled as having a propensity or gene for breast cancer, but another group of women will suffer from breast cancer without being labelled as having this propensity or gene. [1554] Consequently, a considerable element of chance is involved in labelling the two groups of women as genetically fit and genetically unfit.[1555]

The predictive accuracy of genetic information is further not assured in dominant monogenic diseases and in polygenic disorders. [1556] Monogenic dominant disorders (such as cystic fibrosis, sickle cell diseases and Huntington's disease) are caused by abnormalities in one gene.[1557] What is more, monogenic dominant disorders such as Huntington's disease may manifest themselves as adult onset conditions, that is, at a later stage in an individual's life. [1558] Monogenic diseases often result in "incomplete penetrance", meaning that the symptoms experienced by individuals may vary.[1559]Polygenic disorders (such as cardiovascular diseases, Alzheimer's and most

[1553] Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 94.

[1554]Schwartz "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review*1 20-22.

[1555]Schwartz "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review*1 20-22.

[1556]Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 8.

[1557]Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 8.

[1558] Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for A Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1504.

[1559] In the majority of monogenetic diseases the link between genetic mutations and their functional effects is direct yet the manifestations of the disease are intricate to determine. For example 300 mutations of the Cystic Fibrosis gene have been identified and some of the mutations according to researchers will produce no effect. Another example is mutations in the BRCA 1 gene strongly linked to susceptibility to breast cancer however research has shown that 10 – 15 percent of women with mutations of this gene will not develop breast cancer. Kim "Genetic Discrimination, Genetic Privacy:

forms of diabetes[1560]) are caused by abnormalities in more than one gene.[1561]The unpredictability of polygenic disorders is further reinforced by the fact that environmental factors play a major part in such disorders. [1562] Polygenic disorders belong to a broader group of multifactorial conditions, the manifestation or progression of which is influenced by genetic defects and non-genetic factors or environmental factors such as diet, stress, exercise, alcohol, exposure to toxic chemicals and radiation and drugs.[1563]

8.3 GENETIC TESTING IN THE WORKPLACE

8.3.1 Genetic Screening and Genetic Monitoring

In the context of the workplace, employers administer genetic testing for pre-symptomatic, susceptibility and carrier testing purposes.[1564] Two types of genetic testing occur in the workplace, namely genetic screening and genetic monitoring. Genetic screening is often conducted on a once- off basis to determine an individual's inherited traits. More specifically, genetic screening determines whether an individual has inherited genes that render him or her susceptible to both occupation – related or non – occupation- related diseases.[1565] Given that the primary purpose of genetic screening is to determine whether the presence of a particular genetic trait exists in an individual, the screening is often conducted on an individual basis.[1566] Genetic

---

Rethinking Employee Protections for A Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1504.

[1560]Report on "The Implications of Genetic Testing for Employment": United Kingdom Human Genetics Advisory Commission July 1999 www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_03.htm (2006-03-27).

[1561]Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 9.

[1562] Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 96. See also Schwartz "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review*1 20-21.

[1563] Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 96. See also Schwartz "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review*1 20-21.

[1564] United Kingdom Human Genetics Advisory Commission: Report on The Implications of Genetic Testing for Employment 1999. http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_03.htm (2006-03-27).

[1565] Hebert *Employee Privacy Law* (2009) § 12: 1.

[1566]Deyerle "Genetic Testing in the Workplace: Employer Dream, Employee Nightmare Legislative Regulation in the United States and the Federal Republic of Germany" (1997) 18 *Comparative Labour Law Journal* 547 554.

screening tests can detect, amongst others, sickle cell anaemia, Huntington's disease, Thalassaemia, cystic fibrosis and Tay – Sachs disease.[1567]

In contrast to genetic screening, genetic monitoring in the workplace occurs over a period of time and is conducted on a group of employees, particularly on employees who have been exposed to workplace hazards. Genetic monitoring determines whether "occupational exposure to hazardous agents has resulted in any chromosomal or genetic damage"[1568]. For example, the genetic monitoring of employees exposed to the agent benzene may reveal a peripheral cell count in the concerned employees, whilst employees exposed to lead may be found to have a concentration of lead in their blood.[1569] The term "genetic monitoring" in GINA means "the periodic examination of employees to evaluate acquired modifications to their genetic material, such as chromosomal damage or evidence of increased occurrence of mutations, that may have developed in the course of employment due to exposure to toxic substances in the workplace in order to identify, evaluate and respond to the effects of or control adverse environmental exposures in the workplace".[1570] Genetic monitoring aids employers in not only identifying hazards in the workplace and the effects of such hazards on employees, but also enables employers to take appropriate action in reducing or eliminating such hazards.[1571]

To summarise: genetic monitoring serves the following functions: first, it monitors workplace exposure to hazardous substances; second, it identifies the risks for an exposed group in order to target workplace areas requiring increased health and safety precautions; and third, it reveals the necessity to reduce exposure levels.[1572]

[1567] Privacy Commissioner of Canada *Genetic Testing and Privacy* Discussion Paper (1995) 11.

[1568] Deyerle "Genetic Testing in the Workplace: Employer Dream, Employee Nightmare Legislative Regulation in the United States and the Federal Republic of Germany" (1997) 18 *Comparative Labour Law Journal* 547 555.

[1569] European Group on Ethics in Science and New Technologies to the European Commission *Genetic Testing in the Workplace* 6 March (2000) 6.

[1570] European Group on Ethics in Science and New Technologies to the European Commission *Genetic Testing in the Workplace* 6 March (2000) 6.

[1571] European Group on Ethics in Science and New Technologies to the European Commission *Genetic Testing in the Workplace* 6 March (2000) 6.

[1572] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 139 146.

Employers may also obtain genetic information from individuals by administering or requiring an individual to submit to genetic testing, particularly where an employer has made an offer of employment conditioned on the individual undergoing a medical examination which includes a genetic test. Employers can further obtain genetic information directly from an individual by enquiring about the individual's family medical history or whether or not an individual has disabilities and the nature and extent of those disabilities. Lastly, employers may also use third parties - such as insurance companies - to obtain genetic information relating to an individual. For instance, an offer of employment may be conditioned upon an individual signing a waiver allowing a potential employer to access his or her medical records supplied by his or her medical insurance provider, which records could include genetic information.[1573]

8.3.2 Employer Interests in Genetic Testing

The employer's primary interests in requiring individuals to undergo genetic testing are to reduce costs and improve workplace efficiency.[1574] Employers argue that genetic testing determines the future employability of individuals prevents increased health care costs and ensures public safety.

As far as future employability is concerned, employers argue that genetic testing identifies individuals at an increased risk of developing an illness which is likely to have an effect on their performance and individuals with susceptibility to workplace

[1573] Rothstein (ed) *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (1997) 112.

[1574] The employer's economic argument for accessing an individual's genetic information is supported by some legal scholars. See for example Posner "The Right to Privacy" (1978) 12 *Georgia Law Review* 393 and Epstein "The Legal Regulation of Genetic Discrimination: Old Responses to New Technology" (1994) 74 *Boston University Law Review* 1. Epstein contends that the genetic testing of employees provides employers with an opportunity to reduce labour costs and improve the efficiency of their operations. Epstein further provides that because the employer is driven by rational concerns of profit and loss in accessing genetic information on its employees, it will make only economically rational and efficient use of the information. Epstein "The Legal Regulation of Genetic Discrimination: Old Responses to New Technology" (1994) 74 *Boston University Law Review* 1 18. Epstein believes further believes that full disclosure by an employee of his or her genetic information is required particularly where an employee knows he or she is at risk of a condition from family history or from a reliable genetic test. It would be immoral for an employee to, for example, conceal that he or she carries the Huntington's disease gene from his or her employer. Epstein "The Legal Regulation of Genetic Discrimination: Old Responses to New Technology" (1994) 74 *Boston University Law Review* 1 11.

exposures.[1575] Genetic testing therefore enables employers to screen out "genetically unsuitable" individuals, that is, individuals at an increased risk of developing an illness or having a predisposition towards developing a work related illness. Such individuals are less attractive employees to an employer since they are likely to work less hours, impose greater health care costs on employers,[1576] increase the costs of hiring temporary replacements and training permanent replacements and require that more precautions be taken in dealing with health and safety risks.[1577]

Second, employers also see genetic testing as a useful measure to prevent increased health care costs. An employer may, for example, not wish to continue employing an individual with a predisposition to cancer or Alzheimer's as these conditions are likely to impose excessive health care costs on the employer, particularly after the employer has spent time and money training the employee.[1578]

Third, employers argue that genetic testing of individuals enables them to protect the employee, other employees and the public.[1579] Employers have various obligations towards their employees and the public. Employers, for example, have a duty to provide acceptable standards of care for their employees and to bear the costs of work related accidents. Employers have the additional obligation of bearing responsibility for the careless conduct of employees who cause harm or injury in the course of their employment. As such, employers are liable to third parties for any harm or damage occurring on the employer's premises or as a result of the employer's operations.[1580] It is for these reasons that genetic testing is perceived as a useful tool in assisting employers to meet these obligations by employing only "genetically suitable" individuals.

[1575]Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 79 – 89.

[1576]Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995)79.

[1577]Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 56.

[1578]Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 82.

[1579] Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 152.

[1580]*Supra*.

On the other hand some employers use genetic testing to accommodate individuals who are not "genetically suitable". For example, where an employee operating heavy machinery is found to be suffering from a condition that makes him or her prone to a sudden heart attack beyond a particular age, then his or her employer can take steps to ensure that the employee is given another, less hazardous, job to perform at that age. Another example is that an employee, who is found to have a propensity for a particular condition that is exacerbated by environmental factors, may be placed in a safer working environment.[1581]

Employers further argue that the genetic testing of individuals in the workplace can reduce the incidences of occupational disease. In the United States, for example, black employees have been screened for the sickle cell trait because of concerns that exposure to nitro or amino compounds could precipitate the sickling of blood.[1582] Male employees have also been screened for sex linked genetic abnormality of glucose-6-phosphate dehydrogenise deficiency because of concerns that exposure to oxidizing chemicals could precipitate haemolytic anaemia.[1583] Workplace genetic testing can also, for example, identify individuals with a high risk of developing a late onset disease - such as Huntington's disease – which would enable the employer to take steps to prevent the concerned individuals from harming themselves and others in the course of their employment.[1584]

It has been argued that individuals also have an interest in undergoing genetic tests in the workplace as it enables them to assess their own susceptibility to occupational disease. This, in turn, enables individuals to make free and informed decisions regarding the suitability of a particular employment and affords them due regard for their health and safety. Testing further enables individuals to avoid employment

[1581]Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 84. See also the US decisions of *Echazabal v Chevron* 226 F.3d 1063 (2000) and *Johnson Controls* 499 U.S. 187 (1991).. In both decisions the employer wanted to exclude employees because they were likely to suffer some form of risk to their person (*Echazabal v Chevron*) or unborn child (*Johnson Controls*) from the toxins present in the workplace.

[1582]Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 84.

[1583]*Supra*. See also the US decisions of *Echazabal v Chevron* 226 F.3d 1063 (2000) and *Johnson Controls* 499 U.S. 187 (1991).

[1584]Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 57.

which is likely to aggravate their risk of ill health, allowing them to safeguard their economic well-being as well as that of their families.[1585]

8.3.3 Arguments Against Workplace Genetic Testing

The argument that genetic testing determines the future employability of individuals assumes that testing provides an adequate basis to determine an individual's employability. In fact, the tests are poor predictors of gene manifestation and even poorer predictors of disabling conditions. [1586] The argument further ignores the fact that genes are often characterised by "incomplete penetrance" i.e. individuals carrying a particular gene may never exhibit manifestations of the gene.[1587] Even in those cases where the gene does manifest itself, the extent of the gene's effects may differ considerably from person to person[1588]. For example, with sickle cell anaemia, certain individuals die within the first 5 years of their lives and others survive into their 50's.[1589] Behavioural modifications have also been shown to limit gene manifestation. For example, patients at risk of diabetes and coronary artery disease can modify their diet and thereby reduce the manifestations of the particular gene.[1590] To provide a further example, in the case of Huntington's disease, the presence of the Huntington's gene has a disabling and debilitating effect, but the manifestation of the gene or onset of the disease may be delayed. For these reasons, the exclusion of individuals from employment on the basis that their genetic profile impacts on their future employability merely discriminates against the concerned individuals regardless of

[1585] Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 56. See also Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 152.

[1586] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 81.

[1587] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 81.

[1588] *Supra*.

[1589] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 81.

[1590] *Supra*.

whether their particular gene has manifested itself and affected the ability of the individual to perform his or her duties.[1591]

The argument that genetic testing is an effective tool for reducing health care costs is flawed because the exclusion of individuals with undesirable genetic constitutions imposes heavy health care costs on society,[1592] especially in societies where healthcare is financed through private and public insurance markets. In the United States, for example, the majority of individuals covered by health care insurance are found in the employment based portion of the private insurance market. Employers purchasing group health care insurance receive public support in that they can deduct the cost of their contributions as a business expense. Employment based insurance is further beneficial to employees because it is considerably cheaper when obtained through the employer. Hence individuals exiled from the private health care insurance market only have recourse to public health care programs and charity organisations and this increases society's health care costs.[1593]

Employers also justify the use of genetic tests with reference to public health and safety. Although employers have an important responsibility in this regard, genetic testing is not an effective tool for discharging this responsibility. As already indicated, genes may be characterised by incomplete penetrance, variable expression and delayed manifestation. A more effective tool in meeting this responsibility would be for employers to require individuals to undergo other types of routine tests or screening (such as routine medical supervision or screening[1594]) to determine their actual capacity to carry out their duties.[1595] For example, an airline can require its pilots to undergo physical examinations every 6 months and a bus company can require its bus drivers to undergo neurobehavioral tests frequently. Such non-genetic

[1591] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed) *Genetics and Society* (1995) 81.

[1592] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed) *Genetics and Society* (1995) 83.

[1593] Schwartz "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review* 1 33-34.

[1594] Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1539.

[1595] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed) *Genetics and Society* (1995) 83.

testing enables the employer to not only meet its public safety responsibilities, but to also identify those individuals whose incapacity cannot be detected by genetic tests.[1596]

Employers further argue that genetic tests enable them to identify applicants with suitable personal traits or cognitive abilities. [1597] However, according to Kim, less intrusive methods of measuring behavior or aptitudes (such as ability testing, job supervision and references) exist. Kim further observes that employers making use of genetic testing in order to identify applicants with suitable personality traits are misguided because research has shown that genetic tests cannot measure behaviour and aptitudes. Genetic tests can merely ascertain the presence of DNA sequences associated with types of behaviour or aptitudes.[1598]

The argument that genetic testing can identify individuals who are at risk of disease brought on by workplace exposures is also flawed.[1599] If employers are to exclude individuals from employment because of their propensity to develop a particular condition they are likely to be lax in their efforts to eliminate potential toxins from the workplace. [1600] Employers can protect individuals from occupational disease or injury by offering individuals the opportunity to be monitored for exposure to toxins (such as lead and radioactive material) and any negative effects from those toxins. In addition, if employees develop excessive exposure to toxins present in the workplace, employers can arrange to transfer the affected employees to a toxin free environment.[1601]

[1596] *Supra*.

[1597] Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1540.

[1598] Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1540.

[1599] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 85.

[1600] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 85.

[1601] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 85.

To conclude, genetic testing compromises the privacy interests of individuals and their families. As previously indicated, genetic information is very confidential and powerful information because it pertains to information about an individuals' future health and the future health of his family. The information affects not only the concerned individual but the individual's family and the individual's personal decisions such as whether or not to have children.[1602] One commentator aptly points out that the information revealed by genetic tests includes "pre-symptomatic medical information about an individual…information about an individual's risk of future disease, disability, or early death… information about an individual's carrier status, that is, the likelihood of parents passing on to their children a genetic condition, and about the health of an individual's family members."[1603] Legal commentators further contend that genetic testing may afford employers the opportunity to discriminate against individuals on the basis of their genetic constitution. Genetic information comprises an irreversible trait of every individual, which an individual did not choose and cannot easily alter or modify.[1604] For this reason, allowing employers to discriminate on the basis of genetic information as an immutable trait is grossly unfair because, more often than not, the individuals concerned have little or no control over their genetic make- up.[1605]

Moreover, research has shown that there are psychological risks (such as anxiety, depression, loss of self esteem[1606]) attached to an individual undergoing genetic testing and learning that he or she is carrying a defective gene that may predispose him or her to a serious condition. As such, genetic information has the potential to not only compromise an individual's privacy and that of his family but also the dignity of the persons the information relates to.[1607] Individuals are further at risk of learning painful

[1602] Annas "Genetic Privacy: There Ought To Be Law" (1999) 4 *Texas Review of Law & Politics* 9 10.

[1603] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v. Employer's Need to Know" (2001) 39 *American Business Law Journal* 139 143.

[1604] Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 706 – 707.

[1605] Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 706 – 707.

[1606] Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for A Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1539.

[1607] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 572 – 573.

facts concerning family relationships.[1608] For example, genetic information can prematurely expose the fact that an individual is not his or her parents' biological child before his or her parents have had a chance to explain this to the concerned individual. [1609] The fact that genetic information may not be as precise in predicting whether an individual is likely to be affected by a genetic disease, does not take away from the highly sensitive and personal nature of genetic information and the risks associated with the disclosure of such information. It also does not diminish the impact of genetic information on life changing decisions such as whether or not to have children. [1610]

Laurie sums up the genetic discrimination and privacy implications of genetic information as follows:

> "Information concerning an individual's genetic make-up is of a highly personal and sensitive nature. To discover that one is likely to develop a debilitating condition in later life or that this might be passed to one's children must be an intense and possibly devastating exposure. Exposure to such knowledge can alter the self-perception and challenge notions of identity, and could adversely affect an individual in [his or] her social and professional and familial milieux. The mere availability of genetic information serves to heighten concerns about uses which might in turn compromise the interests of the person who has been tested – the proband. For example the disclosure of information to employers, insurers or other interested parties might lead to judgments being made which adversely affect or discriminate against the individual. Uniquely, genetic tests can also reveal information about blood relatives of the proband, with a corresponding threat to their privacy interests and their privacy".[1611]

[1608] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 572 – 573.

[1609] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 572 – 573.

[1610] Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571 572 – 573.

[1611] Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 90.

8.4 SOUTH AFRICA

8.4.1 Introduction

It is unclear to what extent South African employers engage in systematic genetic testing in employment. However, selected employers are required in terms of legislation to implement some biological monitoring or surveillance of their employees. For example, the Occupational Health and Safety Act[1612] ("OSHA") protects persons other than persons at work against hazards to health and safety arising out of or in connection with activities of persons at work. OSHA places a number of duties on employers with respect to the safety and health of employees. OSHA further authorises the Minister of Manpower to declare any work as listed work.[1613] Once work is declared as listed, employers whose employees undertake listed work or are liable to exposure to hazards emanating from listed work must identify the risks associated with the listed work and the steps to be taken to comply with the provisions of OSHA: to evaluate the risks associated with the listed work constituting a hazard to the health of employees; as far as reasonably practicable, to prevent the exposure of such employees to hazards concerned (only where such prevention is not reasonably practicable can the employer minimise the exposure); and, having regard to the nature of the risks associated with such work and the level of exposure of such employees to the hazards, to carry out an occupational hygiene programme and biological monitoring and subject employees to medical surveillance.[1614] As such, the type of programme introduced and type of biological monitoring and surveillance the employees are subjected to, will depend largely on the nature of the risks attached to the work and the level of exposure of affected employees.[1615] Employers are required to keep designated workplace health and safety representatives informed of any action taken with respect to listed work and the results of such action. More importantly, OSHA recognises the private nature of the medical information and the privacy of individuals undergoing biological and medical surveillance in terms of the listed work requirements. OHSA restricts the availability of the test results to persons other than the Chief Inspector, the employee concerned or

[1612] Act 85 of 1993.

[1613] Section 11 of OSHA.

[1614] Section 12(b) of OSHA.

[1615] Section 12(1) (a) - (c) of OSHA.

the employer by providing that individual test results of biological monitoring and medical surveillance relating to the work of an employee shall not, without the written consent of the relevant employee, be made available to any other person (except the Chief Inspector, employee concerned or the employer).[1616]

8.4.2 Legislation

There is no legislation directly regulating the use of genetic testing in South Africa. That being said, there exists legislation that has implications for the use of genetic testing in employment, namely the Constitution and the Employment Equity Act[1617] ("EEA").

8.4.2.1 Constitution

In *Harksen v Lane*[1618] the Constitutional Court developed a two stage approach for determining whether conduct by an employer amounts to unfair discrimination. The first raises the question whether discrimination exists more particularly whether the differentiation is based on a listed or unlisted ground of discrimination. If the differentiation is based on a listed ground such as disability, discrimination is established. If the differentiation is not based on a listed ground, discrimination is established by considering whether the differentiation is based on attributes and characteristics which have the ability to impair the fundamental dignity of persons as human beings or to affect them adversely in a comparably serious manner. The second stage asks if the discrimination is unfair. If the differentiation is found to be on a listed ground, unfairness is presumed and if found to be on an unlisted ground, then the complainant will have to establish the unfairness. This in mind, the question arises whether negative decisions by an employer about a(n) (prospective) employee on the basis of a genetic disposition amount to unfair discrimination. In light of the test in *Harksen v Lane* and the fact that disability is a listed ground in both the Constitution[1619] and EEA[1620], the exclusion from employment of an individual on the basis of a genetic predisposition to certain diseases may amount to unfair discrimination. This, however, will only be the case if courts define disability in a

[1616] Section 12(2) of OSHA.

[1617] Act 55 of 1998.

[1618] 1998 (1) SA 300 (CC).

[1619] Section 9(3) of the Constitution of the Republic of South Africa Act 108 of 1996.

[1620] Section 6(1) of the EEA.

generous and broad manner that includes immutable traits such as one's genetic make-up or constitution. It is important to note in this regard that the EEA does provide a definition of 'people with disabilities'. To the extent that this definition applies to the meaning of 'disability' in section 6(1) of the EEA, the apparent problem seems to be that it requires a pre-existing mental or physical impairment (not the potential thereof).[1621] This limitation (i.e. an existing definition of "disability") does not exist in the context of the Constitution.

Perhaps more promising is the possibility that courts will, based on the reasoning in *Hoffmann v South African Airways*,[1622] determine that discrimination on the basis of a genetic predisposition amounts to discrimination on an unlisted ground. The applicant in *Hoffman* argued that his HIV status constituted a disability and, as such, South African Airways - in denying him employment as a cabin attendant - had discriminated against him on a listed ground. The Court established that it was unnecessary to consider discrimination on a listed ground (disability) "because the denial of employment to the appellant because he was living with HIV impaired his dignity and constituted unfair discrimination [on an unlisted ground]"[1623].[1624]

8.4.2.2 The Employment Equity Act

The chief purpose of the EEA is to achieve equity in the workplace. The EEA seeks to reach this goal by promoting equal opportunity and fair treatment through the elimination of unfair discrimination and the implementation of affirmative action measures to redress the disadvantages in employment experienced by designated groups.[1625] Section 1 of the Employment Equity Act defines medical testing broadly as including:

> *"Any test, question, inquiry or other means designed to ascertain, or which has the effect of enabling the employer to ascertain, whether an employee has any medical condition".*

The above definition recognises that medical information is not obtained through medical tests only but can also be obtained through, for example, inquiries into an

[1621] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 748.
[1622] 2000 11 BCLR 1211 (C).
[1623] Paragraph 40.
[1624] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 748.
[1625] Section 2 of the EEA.

individual's family medical history. Furthermore, use of the term "condition" in the definition of medical testing denotes something broader than a disease, illness or injury and arguably includes early diagnosis of HIV/AIDS as well as predispositions to conditions such as various cancers and coronary heart disease.[1626] This would mean that genetic testing is included in the definition of medical testing in the EEA. The significance hereof is that genetic testing would be permitted in terms of section 7 of the EEA, provided the testing is justifiable in light of medical facts, employment conditions, social policy, and fair distribution of employee benefits or the inherent requirements of the job.[1627].

Included in the EEA's definition of the term "designated groups" (for purposes of affirmative action) are 'people with disabilities'.[1628] The EEA proceeds to define "people with disabilities" as "people who have a long term or recurring physical or mental impairment which substantially limits their prospects of entry into, or advancement in, employment".[1629]It appears that individuals with genetic predispositions to certain diseases or conditions fall outside this definition, because the definition seems to require a pre-exisiting physical or mental impairment. The disability provisions of the Act are supplemented by the Code of Good Practice: Key Aspects on the Employment of People with Disabilities ("the Code"). The Code and the EEA share a similar definition of the term "peoples with disabilities". This means both the Code and the EEA seem to exclude persons with a genetic predisposition to a future impairment. The definition of disabled persons, in this sense, further denotes that progressive genetic conditions such as Huntington's disease are only considered disabilities once the impairment becomes substantially limiting of an individual's prospects of entry into, or advancement in employment. This restrictive interpretation of the term disability not only fails to recognise persons with genetic disabilities or impairment as disabled, but also excludes persons with conditions such as HIV from being considered disabled (simply because they suffer from the condition).

[1626]Christianson "The Testing of Employee: The Selective Prohibition of Medical, Psychological and Other Testing in terms of the Employment Equity Act" (1999) vol. 9 *Contemporary Labour Law* 1112.

[1627]*Supra*.

[1628]Section 1 of the EEA.

[1629]Section 1 of the EEA.

The definition of "people with disabilities" in the Code was further criticised by Ngwena and Pretorius[1630] in the context of the *Imatu v City of Cape Town*[1631] decision. The authors argued that the Code is only applicable in case of affirmative action and not in cases of discrimination. This would leave room for a more expansive definition of 'disability' to be applied in discrimination cases, which could, in turn, include a genetic predisposition to future impairment.

At issue in the Labour Court decision *City of Cape Town* was whether the City of Cape Town's imposition of a blanket ban on the employment of diabetics amounted to unfair discrimination in terms of section 6(1) of the EEA. The Labour Court drew on the *Harksen v Lane NO and Others*[1632] approach to unfair differentiation in finding that the City of Cape Town's blanket ban in this regard amounted to differentiation. The Court then proceeded to consider whether the differentiation was based on a listed ground, namely disability, or on an analogous (unlisted) ground.[1633] In this regard, the Court noted, as point of departure, that the term "disability" is not defined in the EEA. Despite this, the Court looked to Item 5 of the Code, which was issued in terms of the EEA, for guidance.

The Court noted the definition of the phrase "people with disabilities" in the Code[1634] and also observed that Item 5 of the Code states that the "the scope of protection for people with disabilities in employment focuses on the effect of a disability on the person in relation to the working environment, and not on the diagnosis or the impairment", an approach indicative of the fact that the Code's approach to disability is not that associated with the medical model of disability, but instead the social model.[1635]

The Court took the view that for the applicant's condition to constitute a disability it had to meet all the elements of Item 5 of the Code, the first being "a .long term or recurring physical or mental impairment" (the "impairment element") and the second being "a substantial limitation on the prospects of entry into, or advancement in,

[1630] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 748.
[1631] (2005) 26 ILJ 1404 (LC).
[1632] 1998 (1) SA 300 (CC).
[1633] 1435.
[1634] 1435.
[1635] 1435.

employment" (the "limitation element"). The Court went on to determine that the applicant's condition met only some of the elements of Item 5 of the Code. In particular, the court felt that the limitation element was not met.[1636] The Court held in this regard that:

> "…that fast acting, analogue insulin controls or corrects the long term physical impairment, diabetes mellitus, so that its adverse effects in relation to the working environment are largely prevented or removed…It must follow that although diabetes mellitus can be accurately described as a long terms impairment, in our law, a sufferer of it is not regarded as person with a disability under the EEA. [The sufferer of diabetes mellitus] lives a normal life apart from his medication regime, and there is no substantial limitation of his abilities to carry out his tasks. He does therefore not fall within the definition of "people with disabilities" in the [Code]. [The City of Cape Town] for that reason did not differentiate on the listed ground of disability within the meaning of that tern in section 6(1) of the EEA."[1637]

The Court then proceeded to consider whether the applicant was discriminated against based on an analogous (unlisted) ground (diabetes) and, based on application of the test for recognition of unlisted grounds in *Harksen v Lane,* came to the conclusion that this was indeed the case. The applicant's medical condition was seen as analogous to the listed grounds of "disability, HIV status and, given its' genetic origins, perhaps even birth".[1638]

Ngwena and Pretorius argue that notwithstanding that diabetes can be said to constitute an analogous ground, the Court in *City of Cape Town* erred in finding that diabetes mellitus did not constitute a disability under section 6(1).[1639] The concept of disability, according to the authors, is a broad concept that has been given multiple and contrasting meanings. Despite this elusiveness and fluidity there have been attempts to achieve a universal meaning of the concept,[1640] which has resulted in two

[1636] 1436.

[1637] 1436.

[1638] 1437.

[1639] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 748.

[1640] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 755.

models of disability, namely the social model and the medical model. The social model, which was referred to by the Court in *City of Cape Town*, takes the view that people are disabled "by a social – cultural environment that is constructed around the norm of "able bodiedness". The medical model conceives of disability as flowing from impairment.[1641] Because disability is such a fluid concept and therefore is capable of taking on different and contested meanings, "the pointer towards deciphering the meaning of disability", according to the authors, is context. In this regard the authors argue that the context for rendering disability a prohibited ground under section 6(1) of the EEA is to eliminate unfair discrimination.[1642]

The authors go on to consider whether the impairment element and limitation element applied in *City of Cape Town* was appropriate. The impairment element for Ngwena and Pretorius was not only proper, but also essential, given that it distinguishes disability from other differential characteristics such as race or sex and further distinguishes disability from temporary impairments brought on by short lived illnesses.[1643] Ngwena and Pretorious contend that the limitation element is "superfluous" and "juridically inappropriate" because it seeks to regulate "disability related discrimination with an under inclusive yardstick",[1644] namely the severity of the impairment or the severity of the effects associated with impairment.[1645] The use of such a yardstick allows an employer who is found to have discriminated against a job applicant on the basis of a disability associated with impairment to argue that he was justified in discriminating against the job applicant because the impairment was not a substantially limiting one.[1646] This approach is inconsistent in the South African constitutional dispensation which advances and holds as paramount human rights such as dignity and equality.[1647]

[1641] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 757.

[1642] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 757.

[1643] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 758.

[1644] *Supra*.

[1645] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 759.

[1646] *Supra*.

[1647] Pretorious, Klinck and Ngwena *Employment Equity Law* (2005) 760.

8.4.3 Case Law

The issue of genetic testing in the employment context has not come before South African courts, but it seems safe to say that it is only a matter of time bearing in mind both the rate at which technology is developing and the increasing affordability of medical testing. As indicated in previous chapters the Labour Court in *Joy Mining Machinery* had to determine the justifiability of HIV/AIDS tests that an employer in the mining sector sought to conduct on its employees. The Court stated that in determining the justifiability of HIV/AIDS testing it will take into account various factors: the prohibition on unfair discrimination; the need for HIV/AIDS testing; the purpose of the test; the medical facts; employment conditions; social policy; the fair distribution of employee benefits; inherent requirements of the job; and the category or categories of jobs or employees concerned. The court further stated that it would consider the following ancillary factors in arriving at its decision : the attitude of the employees; whether the test is intended to be voluntary or compulsory; the financing of the test; preparations of the test; pre-test counselling; the nature of the proposed test and procedure; and post-test counselling. Therefore, South African employers who consider genetic testing of their employees should not only ensure the tests are justifiable in light of section 7(1) (b) of the EEA, but also comply with the primary and ancillary factors listed in *Joy Mining Machinery*.[1648] Alternatively, employers may bring the issue for consideration before the Labour Court, to ensure the justifiability of the genetic testing.

8.4.4 Analysis

South African courts have yet to address the issue of genetic testing in the employment context. There is currently no legislation directly regulating genetic testing. However, both the Constitution and EEA have implications for genetic testing. In terms of the Constitution and decisions like *Hoffmann*, an individual denied employment on the basis of a genetic predisposition may argue that he or she has been unfairly discriminated against on an unlisted ground. In terms of the EEA, it would seem as if genetic testing qualifies as medical testing, even though the Act's definition of disability is not wide enough to include genetic predispositions.

8.5 UNITED KINGDOM

8.5.1 Introduction

Genetic testing is rarely used in the employment context in the United Kingdom because it is still underdeveloped and its predictive value remains an issue of much debate.[1649] In 1993 the Nuffield Council Working Party found evidence of only one compulsory genetic screening programme in use by a United Kingdom employer. This involved the screening of applicants for sickle cell in occupational categories of Her Majesty's Forces (aviation candidates) who were to be exposed to atypical atmospheric conditions. Candidates identified as carriers of this trait were considered unfit for duty because of the risk of sickling (a change in the shape of the red blood cells which can lead to a blockage of the blood vessels) on exposure to reduced atmospheric pressure or hypoxia.[1650] However, by 2002, the Human Genetics Commission ("HGC") had found no evidence of the systematic use of genetic testing in the employment context in the United Kingdom either as a condition of employment or in meeting workplace health and safety obligations.[1651]

It further appears from the results of a 2000 survey by the Institute of Directors that the majority of United Kingdom employers are reluctant to require individuals to undergo genetic testing, particularly where the individuals have not given their consent. The Institute recorded that 0.6 percent of the directors reported they used genetic tests routinely and 1.1 percent indicated they used genetic tests only when they were concerned about particular employees. 34 percent of the directors approved of genetic screening with the employee's consent in determining the likelihood of heart disease and 8 percent indicated they would consider compulsory testing if its use was in the employee's interests. 50 percent approved of genetic testing as an indicator that employees were at risk of occupational related disease due to exposure in the

[1649] Employment Practices Code 88. See also Tottel Publishing "Genetic Testing in the Employment Context – The State of Play" (2006) 13 (9) *Health and Safety at Work* 545 – 547.

[1650] Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 59. See also Opinion of the European Group on Ethics in Science and New Technologies to the European Commission *Ethical Aspects of Genetic Testing in the Workplace* July (2003) 9.

[1651] Human Genetics Commission *Inside Information: Balancing interests in the Use of Personal Genetic Data* (2002) 12.

workplace as long as the employee consented and 16 percent reasoned that this basis of testing should be compulsory.[1652]

The HGC report also recommended that employers not demand that individuals take genetic tests as a condition of employment. The report instead advised employers to monitor the health of its employees or individuals by other means seeing as there exists uncertainty over the reliability of genetic information.[1653]

8.5.2 Legislation

Although the HGC report recommended that government give detailed consideration to legislation aimed at prohibiting genetic discrimination, there is currently no legislation in the United Kingdom directly regulating genetic testing. As such, it has been argued that United Kingdom employers may lawfully require an individual to undergo a genetic test as a condition for employment.[1654] Employers may also refuse an individual employment on the basis of negative genetic test results and employers are not compelled to give reasons for refusing an individual employment[1655].[1656]

The United Kingdom does, however, have a range of other employment related legislation that can have implications for genetic testing in the workplace. This legislation protects the confidentiality of personal information, provides protection against discrimination in general and regulates workplace health and safety issues.[1657]

8.5.2.1 Data Protection Act

The Employment Practices Code provides employers with guidelines on how to meet the requirements of the Data Protection Act[1658] ("DPA") relating to the processing of

[1652]Opinion of the European Group on Ethics in Science and New Technologies to the European Commission *Ethical Aspects of Genetic Testing in the Workplace* July (2003) 9.

[1653]Opinion of the European Group on Ethics in Science and New Technologies to the European Commission *Ethical Aspects of Genetic Testing in the Workplace* July (2003) 9.

[1654] Human Genetics Commission *Inside Information: Balancing interests in the Use of Personal Genetic Data* (2002) 12. See also Tottel Publishing "Genetic Testing in the Employment Context – The State of Play" (2006) 13 (9) *Health and Safety at Work* 545 – 547 http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_04.htm (2006-03-23).

[1655]Nuffield Council on Bioethics Report on Genetic Screening Ethical Issues (1993) 58.

[1656] See also Sweet & Maxwell Limited and Contributors 'Genetic Testing in the Employment Context – The State of Play" 13(9) *Health and Safety at Work* 2006 545 – 547.

[1657]Human Genetics Commission "Inside Information: Balancing interests in the Use of Personal Genetic Data" 2002.http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_04.htm (2006-03-26).

[1658]Act of 1998.

employee data, which includes genetic information. First and foremost, the Employment Practices Code discourages employers from using genetic testing as a means of obtaining information about the future employability of an individual, because the procedure is too intrusive and the predictive value of such information is uncertain.[1659] The Employment Practices Code Supplementary Guidance of the DPA ("Employment Practices Code Supplementary Guidance") states that genetic tests cannot form the basis of an employment decision: "[a]t present, very few genetic tests are available that give information to either an employer or employee which could validly be used in the context of decisions concerning employment"[1660]. In fact, the Employment Practices Code recommends genetic testing in two scenarios only: first, where it is evident the employee with a genetic condition is likely to pose a risk to the safety of others and, secondly, where the workplace environment is likely to pose a risk to employees with particular genetic conditions.[1661] The Employment Practices Code further requires that where genetic testing is used for a valid purpose (that is for health and safety concerns), it has to be subject to levels of accuracy and reliability.[1662]The Employment Practices Code Supplementary Guidance also provides that for genetic testing to be valid, it should not only be geared towards protecting the health and safety of others, but also should be reliable and reproducible and hold levels of predictive value.[1663] This requirement is based on the sensitive nature of genetic information and the sometimes far reaching consequences of the information.[1664] Perhaps the most important guideline provided for in the Employment Practices Code is that the results of the tests be communicated to the test subject and professional persons should be on hand to advise the subject.[1665]

The Employment Practices Code Supplementary Guidance also explains the meaning of and difference between monogenic and polygenic diseases to illustrate why the predictive value of genetic testing remains uncertain.[1666] Both the Employment

[1659]Employment Practices Code 88.
[1660]Employment Practices Code Guidance 71.
[1661]Employment Practices Code 89.
[1662]*Supra*.
[1663]Employment Practices Code Guidance 71.
[1664]Employment Practices Code Guidance 71.
[1665] Employment Practices Code 89.
[1666] Employment Practices Code Guidance 70.

Practices Code and Employment Practices Code Supplementary Guidance point employers to the fact that the Human Genetics Commission is the statutory body responsible for monitoring and advising on genetic issues.[1667] The Employment Practices Code endorses the Commission's recommendation to employers to not require individuals to undergo genetic testing as a condition of employment.[1668]

8.5.2.2 Sex Discrimination Act and Race Relations Act

Inadvertent protection against discrimination by employers on the basis of genetic test results exists under the Sex Discrimination Act of 1975 and the Race Relations Act of 1976. Discrimination is defined in both acts to encompass direct and indirect discrimination.[1669] Furthermore, protection against unlawful direct discrimination (on grounds of conduct which appears prima facie discriminatory) and unlawful indirect discrimination (conduct which appears prima facie non-discriminatory but which is discriminatory in effect)[1670] exists especially for those conditions associated with sex (such as haemophilia associated with males) or particular races (such as thalassaemia associated with persons of Mediterranean descent).[1671] The screening of aviation candidates by Her Majesty's Forces referred to earlier has been criticised, not only for being based on unsound evidence, but also for being discriminatory against members of the African Caribbean population who comprise the greater number of sickle cell carriers.[1672]

8.5.2.3 Disability Discrimination Act

The Disability Discrimination Act[1673] (the "DDA") requires that employers reasonably accommodate disabled employees in the workplace. The DDA may protect employees with adverse genetic test results from discrimination by employers if they have an existing "physical or mental impairment which has a substantial and long-term adverse effect on [their] ability to carry out normal day-to-day activities". The

[1667] Employment Practices Code 88 and Employment Practices Code Guidance 70.

[1668] Employment Practices Code 88.

[1669] Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 58.

[1670] Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 58.

[1671] Human Genetics Commission *Inside Information: Balancing interests in the Use of Personal Genetic Data 2002*. http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_04.htm (2006-03-23).

[1672] Opinion of the European Group on Ethics in Science and New Technologies to the European Commission *Ethical Aspects of Genetic Testing in the Workplace* July (2003) 9.

[1673] Act of 1995.

definition of "disabled person" and "disability" in part 1 of the DDA does not include individuals who are genetically predisposed to a potential disability, but arguments have been made for their inclusion. Some legal commentators have argued that the DDA's definition of "disabled" should not be extended because the DDA's framework is not limited to the employment context, but includes other areas such as the provision of services, goods and facilities.[1674] Others suggest the better approach is for parliament to legislate separately in protecting against the direct or indirect discrimination of individuals on the basis of genetic test results.[1675]

8.5.2.4 Equality Act

Although the United Kingdom's Equality Act will be implemented in phases, the main provisions of the Equality Act are expected to come into force in October 2010.[1676]As already mentioned, the Equality Act subsumes most of the United Kingdom's discrimination legislation (including the aforementioned Sex Discrimination Act, Race Relations Act and the Disability Discrimination Act) into a single piece of legislation. The Equality Act seeks to harmonise and consolidate disability, sex, race discrimination and other discrimination laws under a single piece of legislation.[1677] According to the impact assessment compiled in respect of the Equality Act, this consolidation and harmonisation process was necessary because previous discrimination laws tended to be complex and opaque and tended to provide more protection for certain characteristics, namely disability, race and sex, to the detriment of other characteristics.[1678]

Of particular importance, the Equality Act not only brings various types of discrimination legislation under one piece of legislation but also brings with it a number of changes to discrimination law. One of these changes is the introduction of one objective justification test to the discrimination landscape. The justification test would require, for example, that where an employer treats an employee unfavourably because of the employee's disability, the employer will have to show "that the

---

[1674] See part 19 of the Act.

[1675] Human Genetics Commission *Inside Information: Balancing interests in the Use of Personal Genetic Data* (2002). http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_04.htm (2006-03-23).

[1676] http://www.legislation.gov.uk/ukpga/2010/15/pdfs/ukpgaen_20100015_en.pdf (2010-08-21).

[1677] http://www.stammeringlaw.org.uk/changes/sea.htm (2010-08-21).

[1678] Equality Act Impact Assessment Final Version (Royal Assent) April 2010 7.

treatment is a proportionate means of achieving a legitimate aim".[1679] This results in employers having to meet a higher threshold of justification in case of disability discrimination. This test is not, strictly speaking, a new one as it is currently in use to justify indirect discrimination in the context of sexual or racial discrimination.[1680] The Equality Act does not, however, broaden the definition disability and this effectively means that persons with asymptomatic disabilities are still excluded from the definition.

The Equality Act may also limit the employer's ability to make enquiries into an individual's health and perhaps that of an individuals' family. This, in turn, may limit employers from having access to an individual's genetic information, at the very least before the individual is made an offer of employment, whether that offer is conditional of unconditional.[1681] In this regard, the Equality Act prevents employers, subject to exceptions, from making enquiries into an individual's health. The Equality Act, for instance, permits such enquiries for purposes of establishing whether the applicant will be able to carry out a function that is intrinsic to the type of work concerned and for purposes of monitoring diversity in the workplace.[1682]

8.5.2.5 Health and Safety at Work Act

The Health and Safety at Work Act[1683] places a burden on the employer to ensure the health of employees in the workplace. The Act requires employers to either prevent exposure to risks or to reduce the risks to the health of employees. Where residual risks remain, the Act requires the employer to introduce preventative measures (such as the provision of preventative equipment and health surveillance).[1684] Health surveillance encompasses a range of methods designed to detect adverse effects on those persons exposed to health hazards. It is possible, as the use of genetic tests

[1679] Section 19 of the EA.

[1680] http://www.stammeringlaw.org.uk/changes/sea.htm (2010-08-21). See also *Equality Act Impact Assessment* Final Version (Royal Assent) April (2010) 88 - 89.

[1681] Section 60 of the EA.

[1682] Section 60 (6)(a) and (b) of the EA.

[1683] Act of 1974.

[1684] http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_04.htm (2010-08-22).

becomes more widespread, that these tests will be considered as one of the required methods to detect adverse health effects amongst those exposed to health hazards.[1685]

8.5.2.6 Statutory Bodies

Even though the United Kingdom does not have legislation regulating the use of genetic tests in the workplace, the privacy implications of employer requests for genetic information have been discussed by certain bodies - namely the Nuffield Council on Bioethics[1686] and the Human Genetics Advisory Commission.[1687]

It is interesting to note that the Nuffield Council expressed a reluctance to recommend any initiative to introduce legislation regulating the use of genetic testing and information because of the then lack of evidence regarding the systematic use of genetic testing by employers.[1688] The Council concluded that the use of genetic testing by United Kingdom employers was not a cause for concern. The Council did recommend that the Department of Employment keep under review the potential use of genetic testing by employers.[1689]

The Commission, on the other hand, suggested that legislation be introduced to prevent employers testing individuals for genetic conditions other than those that might substantially compromise the public's safety. The Commission further suggested that genetic testing in the employment sphere be restricted to specific conditions relevant to the particular employment. Samples collected for such testing should not be examined for other conditions and the general principle that the individual's right to privacy should prevail should underlie the genetic testing of individuals in the employment sphere. In sum, the Commission found that access to genetic information is only justified if the knowledge of that information has a direct bearing on the effective performance of the job. The Commission recommended 3 scenarios in which genetic tests might be justified:

[1685] http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_04.htm (2010-08-22).

[1686] Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 63.

[1687] Report on *The Implications of Genetic Testing for Employment* United Kingdom Human Genetics Advisory Commission (1999).

[1688] Nuffield Council on Bioethics Report on Genetic Screening Ethical Issues (1993) 63.

[1689] Nuffield Council on Bioethics Report on Genetic Screening Ethical Issues (1993) 64.

a) where there is a strong evidence of a clear connection between the working environment and the development of the condition for which genetic testing can be conducted;
b) where the condition in question is one which seriously endangers the health of the employee or is one in which an affected employee is likely to present a serious danger to third parties;
c) where the condition is one for which the dangers cannot be eliminated or significantly reduced by reasonable measures taken by the employer to modify or respond to the environmental risks.[1690]

The Commission emphasised that employees should have the freedom to decide whether to undergo the testing. [1691] The Council's recommendations on this particular point are unclear. The Council simply states that genetic testing in employment should be accompanied by safeguards for the employee, while it remains unclear whether this particular recommendation applies to both current and prospective employees. [1692] However, the Nuffield Council did articulate the need to protect the interest of both the current and prospective employee in not knowing their genetic constitution. This particular recommendation of the Nuffield Council, according to Laurie, fails to highlight an important distinction between individuals being tested for conditions which they are likely to contract based on their family medical history and the comprehensive testing of individuals. [1693] The distinction is an important one given that employers should not be allowed to widely test individuals, in which case it may be assumed that the reasons for testing are purely financial and not for the individual's or the public's benefit.

The Human Genetics Advisory Commission found that there were sound reasons for administering genetic tests where a condition may put the employer and others at risk in the workplace, provided that condition can be accurately predicted by a genetic test. As such, the Commission recommended that it would not be in anyone's best interest

[1690]Human Genetics Commission *Inside Information: Balancing interests in the Use of Personal Genetic Data* (2002). http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_05.htm (2006-03-23).

[1691]Human Genetics Commission *Inside Information: Balancing interests in the Use of Personal Genetic Data* (2002). http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_05.htm (2006-03-23).

[1692]Nuffield Council on Bioethics Report on Genetic Screening Ethical Issues (1993) 63.

[1693] Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 152.

to ban the use of genetic test results in employment completely. The Commission further concluded that if and when the systematic use of genetic testing increased, the following principles should be observed:

a) an individual should not be required to take a genetic test for employment purposes – an individual's "right to know" their genetic constitution should be upheld;

b) an individual should not be required to disclose the results of a previous genetic test unless there is clear evidence that the information it provides is needed to assess either current ability to perform a job safely or susceptibility to harm from doing a certain job;

c) employers should offer a genetic test (where available) if it is shown that a specific working environment or practice, while meeting health and safety requirements, might pose specific risks to individuals with particular genetic variations. For certain jobs where issues of public safety arise, an employer should be able to refuse to employ a person who refuses to take a relevant genetic test;

d) any genetic tests used for employment purposes must be subject to assured levels of accuracy and reliability, reflecting best practice. Any use of genetic testing should be evidence-based and consensual. Results of any tests undertaken should always be communicated to the person tested and professional advice should be available. Information about and resulting from the taking of the test should be treated in accordance with Data Protection Principles. Furthermore tests results should be carefully interpreted, in light of how these may impact on and be affected by working conditions;

e) if multiple genetic tests were to be performed simultaneously, then each test should meet the standards set out in b, c and d[1694].

8.5.3 Case Law

It remains to be seen how United Kingdom tribunals will approach the issue of genetic testing in the workplace, particularly the effect of such testing on the privacy interests of the individuals concerned. In this regard United Kingdom tribunals are

[1694]Human Genetics Commission *Inside Information: Balancing interests in the Use of Personal Genetic Data* (2002). http://www.advisorybodies.doh.gov.uk/hgac/papers/papers_g/g_05.htm (2006-03-23).

likely to look to Article 8 of the ECHR to determine whether there has been an infringement of an individual's right to privacy as protected by the ECHR. An important decision in this regard is that of the Grand Chamber of the European Court of Human Rights in *S and Marper v United Kingdom*,[1695] which provided a comprehensive assessment of genetic information.

The applicants in S *and Marper* argued that the retention by authorities of their fingerprints, cellular samples and DNA profiles ("personal data") in terms of section 64 of the United Kingdom's Police and Criminal Evidence Act[1696] ("PACE") interfered with their right to respect for private life, as this information was linked to their identity and concerned a type of information that they were entitled to keep within their control. The applicants further argued that the retention of such personal data interfered with their physical and psychological integrity and breached their right to personal development and self-determination and to establish relationships with other persons.

The Government accepted that the information constituted "personal data" within the meaning of the DPA, but argued that the mere retention of the information in terms of PACE did not fall within the ambit of Article 8 of the ECHR because it did not constitute interference with the integrity or relationships of the applicants.[1697]

The court was of the view that the retention of the personal data amounted to an infringement of Article 8(1). The point of departure was that the concept of "private life" under Article 8 was a broad concept and not capable of an exhaustive definition. The concept of "private life" covers the physical and psychological integrity of a person as well as aspects of a person's physical and social identity. The court then went on to consider whether the personal data concerned involved aspects of "private life" as envisioned by Article 8. In this regard, the court considered fingerprints to be different to cellular samples and DNA profiles, because cellular samples and DNA profiles contained substantial amounts of personal and sensitive data and had a stronger potential for future use. The court expressed particular concern with the fact that DNA profiles could be used for familial searches in order to identify genetic

[1695] 30562/04 [2008] ECHR 1581 (4 December 2008).

[1696] Act of 1984.

[1697] http://www.libertysecurity.org/article2332.html - forum (2010-08-22).

relationships between individuals and could be used to assess the ethnic origin of the donor of such data. The court concluded that the retention of cellular samples and DNA profiles interfered with the applicants' right to private life and further concluded that the retention of fingerprints may give rise to fundamental life concerns.[1698]

After establishing that there was an interference with the applicants' right to private life, the court went on to consider whether the interference was justified under Article 8(2). The applicants had argued that the retention of the personal data was not justified under Article 8(2) for a number of reasons, namely: first, the authorities were given the power to use the cellular samples and DNA profiles for purposes which were widely worded and vague and open to abuse; secondly, the indefinite retention of the personal data of suspected offenders could not be regarded as necessary in a democratic society; and, thirdly, the retention was disproportionate as its application was blanket in nature and disregarded, amongst other things, the type of offence involved. The Government submitted that the interference was justified as the measures were in accordance with the law (i.e. section 64 of PACE) and was necessary and proportionate for the legitimate purpose of preventing crime.[1699]

The court agreed with the applicants that the purposes of retention provided for in section 64 of PACE were so widely and generally worded that they were likely to give rise to an extensive interpretation. The context required that there are clear and detailed rules relating to the scope of the retention measures; detailed safeguards concerning the retention and usage of the personal data; and the procedures preserving the integrity and confidentiality of the personal data.[1700]The court did, however, agree with the Government that the retention of personal data pursued the legitimate aim of detecting and preventing crime. The court found that there was a margin of appreciation given to competent local authorities in making the assessment of whether the interference is necessary in a democratic society, final evaluation of whether remains subject to review by courts to determine conformity with the ECHR principles. The court further noted that the margin tended to be narrower when the right involved is crucial to an individual's enjoyment of fundamental ECHR rights and where the general consensus amongst Contracting States was contrary to the law

[1698] http://www.libertysecurity.org/article2332.html - forum (2010-08-22).

[1699] http://www.libertysecurity.org/article2332.html - forum (2010-08-22).

[1700] http://www.libertysecurity.org/article2332.html - forum (2010-08-22).

concerned. In this regard, the court observed that the United Kingdom was the only Contracting State that had chosen not to set limits on the retention and use of such personal data in an effort to achieve a balance with the competing interest of preserving respect for private life. The court concluded that the blanket and indiscriminate retention of personal data of suspected offenders, (irrespective of the gravity of the offence or the age of the offender) but not convicted offenders, constituted a disproportionate interference with the applicant's right to respect for private life and cannot be regarded as necessary in a democratic society.[1701]

8.5.4 Analysis

There is no legislation directly regulating the use of genetic testing in United Kingdom. There is no legislation preventing employers from using these tests in making employment decisions or restricting employers from making use of such tests[1702]however, legislation such as the Data Protection Act, Sex Discrimination Act, Race Relations Act, Disability Discrimination Act, the soon to be implemented Equality Act, as well as Health and Safety legislation provide some protection. Certain commentators have argued for the enactment of legislation directly regulating the use of genetic testing the in the United Kingdom workplace. This is perhaps a little premature as there is little evidence to suggest that genetic tests are being used by United Kingdom employers. Part 4 of the Employment Practices Code discourages employers from using genetic testing as a condition of employment, because such testing is still under development and because the predictive value of such testing in still largely uncertain. The Employment Practices Code does, however, approve of such testing to obtain genetic information to ensure the safety of employees in the work environment. That said, the Employment Practices Code advises that genetic testing be used as a measure of last resort and requires employers to inform the Human Genetics Commission of the proposed use of genetic testing.[1703] More importantly though, the soon to be implemented Equality Act should deal with any case of genetic discrimination that may arise, particularly those concerning individuals with symptomatic genetic conditions.

[1701] http://www.libertysecurity.org/article2332.html - forum (2010-08-22).

[1702] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_4-information_about_workers_health_2.html (2010-08-22).

[1703] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_4-information_about_workers_health_2.html (2010-08-22).

8.6 UNITED STATES

8.6.1 Introduction

American employers have been conducting genetic testing since the 1960's when Dow Chemical first conducted genetic monitoring of their employees to detect possible mutagenic effects from their workplace environment.[1704] By the 1970's, the United States Air Force Academy refused sickle cell gene carriers to train as pilots. Courts have, however, found that testing for the sickle cell trait has a disproportional impact on African Americans and for this reason several states prohibit employers to conduct such tests.[1705]

The use of genetic testing has increased with the creation of DNA and genetic databases. Moreover, the success of the Human Genome Project has increased the prevalence of this kind of testing in the employment sphere.[1706]

In 1982, the National Opinion Research Centre ("NORC") conducted a survey for the United States Congressional Office of Technology Assessment ("OTA") on the Use of Genetic Testing in the Workplace. NORC sent confidential questionnaires to 500 of the largest industrial companies, chief executive officers of 50 of the largest private utility companies, and presidents of the 11 major unions representing the largest numbers of employees in those companies.[1707] At that time, of the 366 responding companies, 1.6 percent reported that they were currently conducting genetic testing, 4.6 percent indicated that they had used some of these tests in the past 12 years, a further 1.1 percent anticipated using the tests in the next 5 years and 15 percent stated that they would possibly be using the tests in the next 5 years.[1708]

[1704] http://www.privacyinternational.org/survey/phr2003/threats.htm (2004-07-09).

[1705] Opinion of the European Group on Ethics in Science and New Technologies to the European Commission "Ethical Aspects of Genetic Testing in the Workplace" July 2003 10.

[1706] http://www.privacyinternational.org/survey/phr2003/threats.htm (2004-07-09).

[1707] United States Office of Technology Assessment 1982 Survey of the *Use of Genetic Testing in the Workplace*. In 1989 conducted a follow-up survey which demonstrated that the 1982 results indicating that the use of genetic testing by employers was bound to increase. The 1989 survey found that 2 % of the responding companies reported use of genetic screening. Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 60.

[1708] United States Office of Technology Assessment 1982 Survey of the *Use of Genetic Testing in the Workplace*. In 1989 conducted a follow-up survey which demonstrated that the 1982 results indicating that the use of genetic testing by employers was bound to increase. The 1989 survey found

In 1991, the OTA undertook another survey on Genetic Screening and Monitoring in the Workplace of 1,500 United States companies, 50 of the largest utilities and 33 of the largest unions. The survey considered the scientific, legal, ethical and social aspects of such testing in the workplace by these entities.[1709] The survey revealed that 1 percent of companies reported to have used genetic screening to identify persons with increased health risks and a further 12 percent of the companies reported genetic screening or monitoring of their employees. The survey further revealed that 1 percent of company health officers reported that they had a formal policy in place on either pre-employment genetic testing or genetic monitoring.[1710] The American Management Association (AMA) conducted a survey in 1998, which suggested that 10 percent of United States employers routinely test employees for genetic predispositions to diseases. A more recent (2004) AMA survey revealed that this figure may have increased. The survey found that 62.6 percent of employers conduct medical testing on their employees for various categories: sickle cell anaemia (1 percent); Huntington's disease (0.2 percent); family medical history (8 percent) and susceptibility to workplace hazards (10.5 percent).[1711]

8.6.2 Legislation

8.6.2.1 Americans with Disabilities Act

The American with Disabilities Act ("the ADA") specifically prohibits discrimination against "an individual with a disability who, with, or without reasonable accommodation can perform the essential functions of the employment position that such an individual holds or desires."[1712] The ADA defines a disability as: "(A) a physical or mental impairment that substantially limits one or more of the major life activities of such an individual; (B) a record of such impairment; (C) being regarded as having such an impairment."[1713] The ADA does not recognise "genetic disability or impairment"; therefore persons with predispositions to genetic conditions fall outside

---

that 2 % of the responding companies reported use of genetic screening. Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* (1993) 60.

[1709] United States Office of Technology Assessment *Medical Monitoring and Screening in the Workplace: Results of Survey* (1991).

[1710] Opinion of the European Group on Ethics in Science and New Technologies to the European Commission *Ethical Aspects of Genetic Testing in the Workplace* July (2003) 10.

[1711] American Management Association (2004) *Workplace Testing Survey: Medical Testing*.

[1712] Section 12112(a) of the ADA.

[1713] Section 12111(1). (2) and (3) of the ADA.

the ambit of the Act's definition of "disability". Some experts and state legislatures have expressed concern with this state of affairs, a concern based on the view that the ADA is designed to protect individuals who have a genetically related illness or a disability once it manifests and substantially limits a major life activity"[1714]. Other writers have argued that symptomatic individuals with disease linked genetic conditions can also be protected by the ADA under the third prong of its "disability definition" - "being regarded as having such impairment"[1715]. According to Pagnattaro, asymptomatic individuals may be protected by the ADA if an employer covered by the ADA (1) mistakenly believes that a person has a physical impairment that substantially limits one or more major life activities, or (2) mistakenly believes that actual, non-limiting impairment substantially limits one or more major life activities.[1716] The Equal Employment Opportunity Commission ("EEOC") also prefers to extend protection to persons with predispositions to genetic conditions under the third prong of the definition. The EEOC Compliance Manual on the Definition of the Term "Disability" (Order No. 915.002 902 issued in 1995)[1717], provides that "regarded as" in the third prong of the definition is applicable to discrimination based on "genetic information relating to illness, disease, or other disorders"[1718].

[1714] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 139 159. Pagnattaro proposes that a determination into whether an individual with a genetic condition is disabled should be an individualised enquiry based on the individual's actual condition. Pagnattaro adds that therefore a person with Parkinson's whose illness does not impair a major life activity is not necessarily disabled. Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 139 160.

[1715] This argument is usually made under the Supreme Court's finding in *Bragdon v Abbott* 524 U.S. 614 (1998). In *Bragdon v Abbott* the US Supreme Court held that an HIV infection or an asymptomatic HIV infection is protected under the first prong of the definition, that is to say, it constitutes a "physical impairment" that "substantially limits the major life activity" of reproduction. Kim asserts that the Court's holding in *Bragdon v Abbott* cannot be extended to individuals with genetic anomalies because genetic anomalies in contrast to HIV vary in their physical manifestations. The Court in *Bragdon v Abbott* based its decisions on the immediacy with which HIV produces anomalies in the blood and on the predictable course and effect of the disease. Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for A Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1529.

[1716] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 139 161.

[1717] EEOC Compliance Manual Section on the Definition of the Term "Disability" http://www.eeoc.gov/policy/docs/902cm.html (2006-05-03).

[1718] Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for A Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1529 1514.

However, the ADA has shortcomings despite its apparent protection against genetic discrimination in the workplace. Even though the EEOC Compliance Manual presents an important move towards protecting asymptomatic individuals with genetic conditions from discrimination, the manual and its guidelines do not bind courts. In addition, the EEOC interpretation does not consider "unaffected recessive carriers of recessive genes" and fails to prevent employers from requiring a waiver from an individual once they have been made an offer of employment by an employer. Finally, the ADA only prevents use of genetic information. [1719] The ADA does not prevent an employer from acquiring genetic information.[1720]

On the other hand, other legal commentators[1721] have suggested that the ADA should not be expanded to provide protection for asymptomatic individuals with genetic disorders and maladies. One such commentator asserts that the ADA cannot be expanded without violating its legislative intent:

> "…expanding the definition of disability beyond its practical limits would eviscerate the original purpose of the ADA, which was to protect the disabled minority from discrimination by the majority…the current language of the ADA cannot be reasonably be interpreted to include such persons when they only have a probability, rather than a certainty, of contracting a genetic disease in the future…Expanding the definition of disability…to include genetic disorders would substantially dilute the purpose behind the ADA and impair the strength of its protections…the definition of disability is crafted narrowly, and to sustain a claim for discrimination the plaintiff must show that (1) he has a physical or mental impairment that (2) substantially limits (3) one or more major life activities. The most difficult element to overcome "substantial limitation" in a major life

[1719] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 161.

[1720] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 161.

[1721] Steinforth "Bringing Your DNA to Work: Employer's Use of Genetic Testing under the Americans with Disabilities Act" (2001) 43 *Arizona Law Review* 965 989 – 991 and Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for A Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1529.

> activity has been interpreted to mean that a person must show he is "presently-not potentially or hypothetically-substantially limited."[1722]

The ADA further permits employers to conduct medical examinations of current employees if these examinations are "job related and consistent with business necessity".[1723] Thus where the use of genetic testing is motivated by non-discriminatory purposes, the testing can be protected by the ADA as job related and consistent with business necessity.[1724]

The ADA Amendment Act of 2008 came into effect on 1 January 2009 and was enacted to address the result of certain Supreme Court decisions,[1725] which excluded individuals with a range of substantially limiting impairments from falling within the narrowly construed meaning of disability in the 1990 Act.[1726] The 2008 Act provides that the meaning of "disability" in the Act "shall be construed in favour of broad coverage of individuals under the [Act], to the maximum extent permitted by the terms of [the] Act."[1727]

8.6.2.2 Fourth Amendment Constitutional Prohibitions

The constitutionally protected privacy interest in avoiding disclosure of personal matters encompasses medical information and its confidentiality.[1728] In *Whalen v Roe*[1729], the United States Supreme Court recognised a right to privacy in medical

[1722]Steinforth "Bringing Your DNA to Work: Employer's Use of Genetic Testing under the Americans with Disabilities Act" (2001) 43 *Arizona Law Review* 965 989 – 991. See also Kim who argues protection of individuals with genetic anomalies would result in definitional problems as individuals with genetic anomalies would bear a double burden of showing the employer based its decision on genetic characteristics and the employer regards him or her as disabled. Kim "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for A Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497 1529.

[1723]Section 12112(2) of the ADA.

[1724]French "Genetic Testing in the Workplace: The Employer's Coin Toss" (2002) 15 *Duke Law and Technology Review* 9.

[1725] See for instance, the decision of *Toyota Motor Manufacturing, Kentucky, Inc. v Williams* 534 US 184 (2002).

[1726] See section 2 of the ADA Amendment Act.

[1727]Supra.

[1728] Norman –*Bloodsaw v Lawrence Berkeley Laboratory* 135 F.3d 126 1269.

[1729]429 U.S. 589 (1977).

information. Later, in *Doe v Attorney General of the United States*[1730], the Ninth Circuit confirmed that there were inherent privacy interests in medical information.[1731]

8.6.2.3 Title VII of the Civil Rights Act

Under Title VII of the Civil Rights Act[1732] ("Title VII"), genetic tests constitute an adverse effect or an injury when employees or applicants are singled out on the basis of their sex or race. An example of this is to be found in *Norman-Bloodsaw v Lawrence Berkeley Laboratory*[1733] where genetic tests were performed on female employees for purposes of detecting pregnancy, a condition that only women can experience and on black employees for purposes of testing for the sickle cell trait, a condition present mostly in African Americans.[1734] The EEOC, as the enforcement agency of Title VII has established guidelines for the use of employment selection criteria - "EEOC's Uniform Guidelines on Employee Selection Procedures".[1735] These guidelines have been held to constitute "the administrative interpretation of [Title VII] by the enforcing agency and consequently they are entitled to great deference."[1736] The guidelines apply to pre-employment tests and other selection procedures. In terms of the guidelines employers are encouraged to use the least discriminatory selection procedure in serving their interest and in selecting an efficient and trustworthy workforce. Further, the selection process must have a valid purpose, be closely related to the job and be subject to periodic review.[1737]

8.6.2.4 State Constitutions and Legislation

Several states in the United States have enacted statutes directly regulating the use of genetic tests in the employment context. States such as Alaska, New Mexico and Utah have statutes regulating genetic testing and genetic privacy. Alaska's 2004 statute[1738]

[1730] 15 F. 3d 1260, 1270 (N.D. Cal. 1998).

[1731] See also *Doe v City of New York* 15 F.3d 264, 267

[1732] Act of 1964.

[1733] 135 F.3d 126.

[1734] French "Genetic Testing in the Workplace: The Employer's Coin Toss" (2002) 15 *Duke Law and Technology Review* 9 12.

[1735] Pesonen "Genetic Screening: An Employer's Tool to Differentiate or to Discriminate?" (2001) 19 *Journal of Contemporary Health Law and* Policy 187 198.

[1736] *Griggs v Duke Power Co*. 433-434.

[1737] Pesonen "Genetic Screening: An Employer's Tool to Differentiate or to Discriminate?" (2001) 19 *Journal of Contemporary Health Law and* Policy 187 198.

[1738] 2004 Alaska Sess. Laws 176(approved October 24, 2004).

prohibits employers from conducting genetic tests and dealing with the results of genetic tests without "informed and written consent" from the test subject.[1739] The state of New Mexico (Genetic Information Privacy Act of 2005)[1740] prohibits the use of genetic information in relation to employment. The statute further requires the "written and informed consent" of the test subject before genetic information can be obtained or analysed. Utah's Genetic Privacy Act[1741] regulates the use of genetic testing and genetic information by employers. The statute prohibits genetic testing and the use of genetic information for purposes of making an employment decision. On the other hand, some states such as Florida[1742] and New Jersey[1743] initially regulated the use of genetic testing for a particular trait or traits only.[1744] For example, Florida regulated the use of genetic screening for the sickle cell trait. However, in 1992 Florida enacted a broader statute to regulate the use of genetic testing.[1745] The 1992 statute protects applicants and employees from genetic testing without consent and requires that they receive notice in the event that an employment decision is based on the results of genetic testing.[1746] Similarly, New Jersey now also has a broader statute prohibiting the use of genetic testing and discrimination in the employment context.[1747] The Act basically prohibits employers from discriminating against applicants or employees on the basis of acquired or inherited genetic traits or on the basis of a refusal to submit to genetic testing.[1748] Also in this regard, New Jersey's Privacy Act of 2000[1749] offers employees an expansive degree of protection by explicitly acknowledging that the improper collection, retention or disclosure of genetic information can lead to significant harm to the individual, including stigmatization in areas such as employment.[1750] The Act further restricts the disclosure

[1739] Hebert *Employee Privacy Law* (2009) §12:16.50.

[1740] 2005 N.M. Laws 204(approved April 6, 2005).

[1741] 2002 Ut. Laws ch. 120, 2002 Ut. HB 56 (approved March 18, 2002; effective January 1, 2003).

[1742] Fla Stat § 448.076 and Fla Stat 448.075.

[1743] NJ Stat Ann § 10:5 – 12(a).

[1744] Hebert *Employee Privacy Law* (2009) §12:16.50.

[1745] Fla Stat Ann § 760.40.

[1746] Hebert *Employee Privacy Law* (2009) §12:22.

[1747] 1996 NJ Laws ch 126 (effective Nov. 19, 1996).

[1748] Hebert *Employee Privacy Law* (2009) §12:34.

[1749] NJ Stat Ann § 10:5 – 44 (c).

[1750] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal*139 174.

of genetic information by requiring the informed consent of the test subject to obtain, retain or disclose the genetic information concerned. In addition, the Act requires that notice be given to the test subject that the test was performed and the results were received.[1751]

8.6.2.5 Occupational Safety and Health Act

Similar to the United Kingdom Health and Safety at Work Act, the United States Occupational Safety and Health[1752] ("the United States OSHA") charges employers with the safety of its employees. The United States OSHA imposes a dual duty on employers: first, the "general duty clause" of the Act requires employers to provide employees with a workplace "free from recognised hazards that are likely to cause death or serious physical harm"; secondly, the "compliance clause" of the Act requires the employer to comply with the United States OSHA safety regulations and standards.[1753] The Act further requires employers to biologically monitor employees through "periodic analysis of body fluids, tissues and excreta in order to measure the impact of the body's exposure to chemical agents and to evaluate the health risks these chemicals pose".[1754] Moreover, United States OSHA regulations with regard to cancer causing agents require an employee to undergo a physical exam (which includes the personal history of the employee and family and occupational background) before entering a regulated area.[1755] Given that the Act is primarily aimed at protecting the safety of employees, it requires the use of the most precise testing to ensure the safety of employees.[1756]

8.6.2.6 Genetic Information Nondiscrimination Act of 2008

The Genetic Information Nondiscrimination Act [1757] ("GINA") was signed into law in May 2008. The Act provides protection against the misuse of genetic information and

---

[1751] *Supra*.

[1752] Act of 1970.

[1753] Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 139 170.

[1754] This requirement applies especially to those employers dealing with the presence of toxins in their respective workplaces. Pagnattaro "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 139 170.

[1755] Pagnattaro MA 'Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know' 2001 39 *American Business Law Journal* 139,170.

[1756] French "Genetic Testing in the Workplace: The Employer's Coin Toss" (2002) 15 *Duke Law and Technology Review* 9 22.

[1757] Act of 2008.

against discrimination on the basis of genetic information by restricting the collection and use of such information.[1758]

GINA provides protection to individuals with respect to their genetic information in two ways: first, it restricts the collection, storage and use of genetic information and, secondly, it prohibits the discrimination against individuals on the basis of genetic information.[1759] GINA encompasses two broad contexts, namely employment and medical insurance coverage.

GINA defines genetic information broadly to mean "with respect to any individual, information about such an individual's genetic tests, the genetic tests of family members of such individual, and the manifestation of a disease or disorder in family members of such individual."[1760] Information about the sex or age of any individual is excluded from the meaning of genetic information. GINA further defines a "genetic test" to mean "an analysis of human DNA, RNA, chromosomes, proteins or metabolites that detects genotypes, mutations, or chromosomal changes."[1761] A genetic test does not include "an analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes."[1762]

The employment provisions of GINA, specifically section 202(a)(1) and (2), prohibit private and public sector employers, labour organisations or employment agencies from failing to hire or discharging an employee or discriminating against employees on the basis of genetic information with respect to compensation, terms, conditions, or privileges of employment.[1763] The section further prohibits employers from limiting, segregating or classifying employees on the basis of genetic information, in a manner that would deprive or tend to deprive an employee of opportunities in employment or

[1758] Jones "The GINA is Out of The Bottle: The Genetic Information Non – Discrimination Act of 2008" (2009) 52 *Boston Bar Journal* 9.

[1759] Jones "The GINA is Out of The Bottle: The Genetic Information Non – Discrimination Act of 2008" (2009) 52 *Boston Bar Journal* 9.

[1760] Section 201(7) of GINA.

[1761] Section 201(4).

[1762] Section 201(4).

[1763] Section 202(a)(1) of GINA.

adversely affect the status of an employee as such. GINA affords this protection to state and federal employees as well as private sector employees and applicants.[1764]

Of particular significance, GINA incorporates two fundamental presumptions in the employment context – a presumption of confidentiality and a presumption of unlawfulness.

Section 202(b) establishes a general presumption of unlawfulness in respect of an employer who requests, requires or purchases genetic information of an employee or an employee's family member. However, the section incorporates several statutory exceptions to this general presumption. For example, the presumption falls away where an employer inadvertently requests or requires the family medical history of an employee or a family member of an employee through the health and genetic services it offers its employees as part of a wellness programme, or where an employer comes across genetic information after purchasing commercially and publicly available newspapers, magazines, periodicals and books that include family medical history.[1765]

Section 206(a) establishes a further presumption of confidentiality in relation to the treatment and maintenance of genetic information. The section requires that employers, employment agencies and labour organisations treat genetic information in their possession in the same manner as it maintains and treats confidential medical records under Section 102(d)(3)(B) of the ADA.[1766] There are several statutory exceptions to this presumption. For instance, an employer may disclose genetic information to an employee at his or her written request and to a government official investigating compliance with Title II of GINA if such information is relevant to the investigation.[1767]

A number of commentators have identified weaknesses in GINA's employment provisions, particularly its practicality and effectiveness as a discrimination

[1764] Section 202(a)(2) of GINA. Schlein "New Frontiers for Genetic Privacy Law: The Genetic Information Non-discrimination Act of 2008" (2009) 19 *George Mason University Civil Rights Law Journal* 311.

[1765] Section 202(b).

[1766] Section 102(d)(3)(B) of the ADA requires that medical information obtained regarding an individual's medical condition or history be collected and maintained on separate forms and in separate medical files and is treated as a confidential medical record.

[1767] Section 206(b).

deterrent.[1768] It remains to be seen if these criticisms are warranted. GINA's employment provisions are expected to affect the way in which United States employers require or request sensitive genetic information pertaining to their employees and further deter the use of genetic screening and monitoring by employers as a means of curbing employee health care and compensation costs.[1769]

8.6.3 Case Law

8.6.3.1 The Americans with Disabilities Act and Case Law

At issue in *Echazabal v Chevron United States Inc.*[1770] was the decision by Chevron not to hire Echazabal on the ground that it would pose a direct threat to Echazabal's health if he worked at their oil refinery. The question before the court was whether the direct threat defence provided by Title I of the ADA included a threat to one's own health or safety. (The "direct threat" defence permits employers to impose a "requirement that an individual shall not pose a direct threat to the health or safety of other individuals in the workplace",[1771] but this was expanded by an EEOC regulation to include a threat to the employee's own health and safety[1772]) Justice Reinhardt concluded that the ADA's direct threat defence permits employers to impose a requirement that their employees not pose a significant risk to the health or safety of other individuals in the workplace, but does not permit employers to exclude the disabled from jobs on the ground that they may put their own health or safety at

[1768] Schlein "New Frontiers for Genetic Privacy Law: The Genetic Information Non-discrimination Act of 2008" (2009) 19 *George Mason University Civil Rights Law Journal* 311 364 – 367. See also Rothstein (ed) *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (1997) 837.

[1769] Schlein "New Frontiers for Genetic Privacy Law: The Genetic Information Non-discrimination Act of 2008" (2009) 19 *George Mason University Civil Rights Law Journal* 311 362.

[1770] 226 F.3d 1063 (2000). Echazabal had been employed by various maintenance contractors at Chevron's oil refinery. Echazabal subsequently applied to work directly for Chevron and was extended an offer of employment by Chevron at the refinery, primarily in the coker unit. This offer was however contingent on Echazabal passing a physical examination. A pre-employment physical examination conducted by Chevron's regional physician revealed that Echazabal's liver was releasing certain enzymes at an abnormal rate and based on these results, Chevron concluded that Echazabal's liver might be damaged by exposure to the solvents and chemicals in the coker unit and rescinded its job offer to Echazabal. Echazabal after consulting several physicians was diagnosed with asymptomatic, chronic active hepatitis C but none of the physicians advised him to stop working at the refinery because of his medical condition. Echazabal reapplied for the job at Chevron and was again told that his offer of employment was contingent on his passing a medical examination. Chevron again proceeded to rescind its offer of employment. Echazabal filed a compliant with the EEOC that Chevron had discriminated against him on the basis of the disability.

[1771] Section 12111(3) of the ADA.

[1772] EEOC Regulations for the ADA Amendments Act.

risk.[1773] Justice Reinhardt further held that Congress purposely omitted threats to one's own health or safety in the ADA's direct threat defence as it was conscious of the history of paternalistic employment practices often resulting in the exclusion of disabled individuals from employment. The Ninth Circuit concluded that the EEOC regulation exceeded the scope of permissible rule making under the ADA.[1774]

The Supreme Court (in *Chevron v Echazabal*[1775]) reversed the decision of the Ninth Circuit and accepted the EEOC regulation authorising the refusal to hire an individual because his performance on the job would endanger his own health owing to a disability. Justice Souter, in delivering the opinion of the Court, found that the EEOC regulation extended the "direct threat" defence by allowing the employer to screen out a potential worker with a disability for risks on the job to his own health.[1776] It is interesting to note that the Supreme Court equated Echazabal's condition to a "disability" In a nutshell, the Supreme Court reinforced an employer's discretion to decline to hire applicants whose health and safety may be directly threatened by exposure to chemicals present in the workplace.[1777]

In 2001, the EEOC settled the first lawsuit alleging genetic discrimination in employment, namely *EEOC v Burlington Northern Santa Fe Railway*[1778]. The EEOC filed a suit against the Burlington Northern Santa Fe ("BNSF") Railroad for secretly testing its employees for a rare genetic condition that causes carpal tunnel syndrome as one of its many symptoms. The EEOC sought a preliminary injunction against BNSF to end genetic testing of employees who claimed for work related injuries based on carpal tunnel syndrome. BNSF argued that the testing would enable it to determine whether the high incidence of work related injuries among its employees based on carpal tunnel syndrome were work-related. BNSF doctors were not only instructed to test for the rare genetic condition, but were also instructed to screen for several other medical conditions such as diabetes and alcoholism. BNSF doctors conducted the genetic testing without the knowledge or consent of BNSF employees

[1773] 1072.

[1774] *Chevron v Echazabal* supra 73.

[1775] 536 U.S. 73 (2002).

[1776] 81.

[1777] Pesonen "Genetic Screening: An Employer's Tool to Differentiate or to Discriminate?" (2001) 19 *Journal of Contemporary Health Law and* Policy 187 189.

[1778] Civ. No. CO1-4013 MWB (N.D. Iowa 2001).

and at least one employee was threatened with termination of employment for failing to submit a blood sample for a genetic test. The EEOC argued that the tests were unlawful under the ADA because they were not job-related, and any condition of employment based on such tests amounted to discrimination on the basis of disability. The lawsuit was settled by BNSF, which agreed with everything sought by EEOC.[1779]

In *Norman-Bloodsaw v Lawrence Berkeley Laboratory*[1780] employees of a research facility operated by state and federal agencies had their blood and urine samples tested for syphilis, sickle cell trait, and pregnancy without their knowledge or consent and without any notification that the tests were being conducted. Moreover, only black employees were tested for sickle cell trait and only female employees were tested for pregnancy. The employees brought an action against the research facility and contended: first, the defendants violated the ADA by requiring, encouraging or assisting in medical testing that was not job related or consistent with business necessity; secondly, the defendants violated the federal constitutional right to privacy by conducting the testing, collecting and maintaining the results of the testing, and failing to provide adequate safeguards against disclosure of the results; thirdly, the testing violated their right to privacy under the California constitution; and fourthly, the defendants violated Title VII by singling out black employees for sickle cell trait testing and performing pregnancy tests on female employees generally.

As point of departure, the court noted that, although most cases articulating the privacy interest in medical information involved its disclosure to third parties, the most basic violation of this interest involved the performance of unauthorised tests. Such tests were also regarded as searches in violation of Fourth Amendment constitutional rights. The court further noted that there were few subjects more personal and more likely to implicate privacy interests than that of one's health or genetic make-up and the facts revealed by the tests are highly sensitive, even relative to other medical information. The court found that by testing the plaintiffs for syphilis

[1779] http://www.ornl.gov/sci/techresources/Human_Genome/elsi/legislat.shtml (2006-05-03). The EEOC sought an order which included the following terms: "BNSF shall not directly or indirectly require its employees to submit blood for genetic tests; BNSF shall not analyse any blood previously obtained; BNSF shall not evaluate, analyse or consider any gene test analysis previously performed on nay of its employees; and BNSF shall not retaliate or threaten to take any adverse action against any who opposed the genetic testing or who participated in EEOC's proceedings." http://www.eeoc.gov/press/4-18-01.html (2006-05-04).

[1780] 135 F.3d 126.

and pregnancy the defendants had violated the Constitution, because the Constitution prohibited unregulated and unrestrained enquiries into personal sexual matters that have no bearing on job performance. As regards testing the plaintiffs for pregnancy, the court found the defendants had violated the Constitution because pregnancy is also private matter which pertains to one's sexual history and can invoke social stigma. With regard to testing the plaintiffs for the sickle cell trait, the court found that the defendants had again violated the Constitutional privacy provisions as the testing concerned sensitive information about family history and reproductive decisions.[1781] The court reasoned that even where an individual has consented to a general medical examination, this particular consent does not abolish one's privacy right no to be tested for intimate, personal matters involving one's health, nor does consenting to giving blood or urine samples or filling out a questionnaire.[1782] The court concluded that the conditions tested for were aspects of one's health, in which an individual enjoyed the highest expectation of privacy.[1783] The court further found that the same privacy interests implicated under the Federal Constitution were recognised in the Californian Constitution. [1784]

8.6.3.2 Title VII Case Law

The issue of employment testing pursuant to Title VII was examined by the Supreme Court in two decisions, *Griggs v Duke Power Co.*[1785]and *Albemarle Paper Co. v Moody*[1786]. In *Griggs v Duke Power* the Supreme Court erected the parameters for employment testing. The court held that Title VII proscribes not only overt discrimination but also covert discrimination, that is, acts that are facially fair but are discriminatory in their operation. [1787] The court stated that following in this regard:

> "…good intent or absence of discriminatory intent does not redeem employment procedures or testing mechanisms that operate as "built-

[1781] 1269 – 1270.
[1782] 1270.
[1783]1270.
[1784]1270.
[1785]401 U.S. 424 (1971).
[1786]422 U.S. 405 (1975).
[1787] 432.

> in-headwinds" for minority groups and unrelated to measuring capability"[1788].

Consequently, the court observed that if an employment practice which operates to exclude blacks cannot be shown to be related to job performance, the practice is prohibited. The court concluded that an employer was prohibited by Title VII from requiring a high school education or the passing of a standardised general intelligence test as a condition of employment, particularly where neither standard was shown to be significantly related to successful job performance, both requirements operated to disqualify blacks at a substantially higher rate than white applicants and the jobs concerned had formerly been occupied only by white employees as part of a long standing practice of giving preference to whites.[1789]

In *Albemarle Paper Co. v Moody* a group of black employees brought an action against their employer, a paper mill. At issue was the plant's seniority program of employment testing which required applicants to pass two standardised tests (to test non-verbal intelligence, the Beta examination and the Wonderlic test, to measure general verbal facility). The Court found that the job relatedness standard for use of pre-employment testing in *Griggs v Duke Power Co.* and EEOC Guidelines required that discriminatory tests are impermissible unless shown by professionally acceptable methods to be, "predictive of or significantly correlated with important elements of work behaviour which comprise or are relevant to the job or jobs for which candidates are being evaluated".[1790] The Court further found the validation study for pre-employment tests used at the paper mill defective because of the odd patchwork of results from the study, the fact that the study compared test scores with subjective supervisorial rankings, the study dealt only with job-experienced, white workers even though the tests were given to new job applicants, who are younger, largely inexperienced and in many instances non-white and the study was conducted by plant

[1788] 432.

[1789] 426.

[1790] *Albemarle v Moody supra* 431.

officials who could not be considered neutral. The Court concluded that Albemarle's test failed to meet the job relatedness test.[1791]

In *International Union v Johnson Controls*[1792] the Court considered whether an employer may discriminate against its female employees on the basis of their ability to conceive or fall pregnant, in order to protect the unborn foetuses of the concerned women. The Supreme Court found Johnson Control's (a battery manufacturer) policy biased in that it did not apply to the reproductive capacity of the company's male employees in the same way as it applies to its female employees. More specifically, the court established the company's sex-specific-foetal protection policy was not facially neutral since the policy classified on the basis of gender and childbearing capacity rather than fertility alone, despite evidence about the debilitating effect of lead exposure on the male reproductive system.[1793] The court added "…the absence of malevolent motive does not convert a facially discriminatory policy into a neutral policy with a discriminatory effect."[1794] In sum, the Court found that a danger to a woman herself does not justify discrimination[1795] and further found Johnson Control "does not pass the simple test of whether the evidence shows "treatment of a person in a manner which but for that person's sex would be different."[1796] The policy barred all women, except those whose infertility was medically documented, from jobs involving actual or potential lead exposure exceeding OSHA standards in light of the fact that documented evidence indicated that occupational exposure to lead entailed health risks which included harm to an unborn foetus.[1797] Johnson Controls argued its foetal protection policy fell within the safety exception of the bona fide occupational qualification defence ("BFOQ") and professed moral and ethical concerns about the welfare of the unborn foetuses of pregnant women working in the battery

[1791] Pesonen "Genetic Screening: An Employer's Tool to Differentiate or to Discriminate?" (2001) 19 *Journal of Contemporary Health Law and* Policy 187 204.

[1792] 499 U.S. 187 (1991).

[1793] 198.

[1794] 199.

[1795] See also *Dothard v Rawlinson* 433 U.S. 321 (1977) where the Supreme Court permitted an employer to hire only males prisoners in contact areas of maximum security male prisons but the Court only permitted this because more than the individual's woman's decision to weigh and accept the risk of employment was at stake. The Court in *Dothard v Rawlinson* 433 U.S. 321 (1977) 366 concluded sex was a bona fide occupational qualification because the employment of a female guard would due to the guard's sex create a real threat to the safety to others if violence broke out.

[1796] 200.

[1797] 188.

manufacturing business. The Court noted that on the basis of the language and legislative history, the BFOQ defence has to be read narrowly.[1798] More specifically, discrimination on the basis of sex because of safety concerns is limited to circumstances in which sex or pregnancy actually interferes with an employee's ability to perform the job.[1799] The Court found that the language of the BFOQ legislative history and case law prohibit an employer from discriminating against a woman because of her capacity to become pregnant unless her reproductive potential prevents her from performing the duties of her job. The Court reiterated that "…an employer must direct its concerns about a woman's ability to perform a job safely and efficiently to those aspects of the woman's job-related activities that fall within the "essence" of the particular business." The Court concluded that Johnson Controls had failed to establish a BFOQ, given that fertile women were able to perform their duties as efficiently as anyone else. The Court further concluded that Johnson Controls' professed moral and ethical concerns about the welfare of unborn foetuses of their fertile female employees do not establish a BFOQ of female sterility. In this regard, the court observed that "decisions of the welfare of future children should be left to the parents who conceive, bear, support and raise them rather than to the employers who hire those parents".[1800]

8.6.4 Analysis

The United States currently has no comprehensive law protecting the privacy of medical information or genetic information. An employee whose rights have been violated by genetic testing in the workplace has recourse to various pieces of legislation: the Americans with Disabilities; the Fourth Amendment's constitutional prohibition on illegal searches and seizures; Title VII and state legislation.[1801] It remains to be seen what the effect of GINA will be, especially with respect to protecting employees against genetic discrimination. The United States should be commended in enacting legislation that explicitly bans genetic discrimination. The United States should also be commended for having addressed the issue of genetic discrimination and laying down guiding principles even prior to GINA, notably in the

[1798] 201.

[1799] 204.

[1800] 204.

[1801] French "Genetic Testing in the Workplace: The Employer's Coin Toss" (2002) 15 *Duke Law and Technology Review* 9 16.

decisions of *EEOC v Burlington Northern Santa Fe Railway* and *Norman-Bloodsaw v Lawrence Berkeley Laboratory*,[1802]. It appears from these decisions that unless an employee has consented to the testing it will be considered a search in term of the United States Constitution. It further appears that such testing must be job related and aimed at ensuring the safety of employees in the workplace. As to whether such testing violates the right to privacy, United States courts are likely to determine that it does, but it may be justified provided the testing is administered in furtherance of a compelling governmental interest, particularly where the testing involves public sector employees employed in safety sensitive positions.

8.7 CONCLUSION

This chapter focussed on genetic testing, which perhaps is the most recent example of the way in which scientific advancement may challenge privacy. The analysis on genetic testing revealed that genetic information was medical information. The debate further revealed the existence of a debate concerning whether or not genetic information is different from other forms of medical and personal information, which debate is known as the genetical exceptionalism debate. Proponents of "genetic exceptionalism" argue that genetic information is inherently exceptional and unique in comparison to other personal or medical information because it concerns very private information about an individuals' future health, an individuals' family's future health and relating to certain personal decisions (such as whether or not to have a child). Proponents of "genetic exceptionalism" further contend that this type of medical information is more private than other forms of medical information because "it is in essence "a reverse diary" which is not only privacy but also in code and probabilistic. On the contrary, critics of "genetic exceptionalism" argue there is nothing unique or exceptional about genetic information in comparison to other forms of personal and medical information for a number of reasons. One of the reasons put forward by critics of "genetic exceptionalism" is that the majority of genetic information, contrary to popular belief, does not predict future diseases.

The arguments advanced by employers to justify the genetic testing are primarily aimed at safeguarding the health and safety of employees in the workplace. Employers argue that genetic testing allows them to not only identify existing hazards

[1802] 135 F.3d 126.

in the workplace and the effects of such hazards on employees, but also enables them to take appropriate action in reducing or eliminating such hazards. The arguments advanced by employers to justify genetic testing are also based on economics and in this regard employers argue that genetic testing determines the future employability of individuals prevents increased health care costs and ensures public safety. On the other hand, arguments against the genetic testing in the workplace are aimed at preserving the employee's informational privacy and integrity. More importantly, the arguments are aimed at preventing the exclusion of individuals from employment and the discrimination of individuals irrespective of whether a particular gene has manifested itself and affected the ability of the concerned individuals to perform his or her duties. The discussion on the South African experience showed OSHA obligated selected employers to carry out biological monitoring or surveillance in the workplace. That having been said, the South African survey observed there is no legislation directly regulating the use of genetic testing in South Africa however the Constitution and the EEA may have implications for the use of genetic testing in employment as well as the recently enacted the Protection of Personal Information Bill of 2009 ("POPI"). POPI will also have direct implications for genetic testing in employment because the Bill specifically includes and makes mention of biometric information in it's' definition of "personal information". The South African experience in addition showed South African courts had yet to deal with genetic testing in the employment context but noted that it was only a matter of time before they did so bearing in mind both the rate at which technology is developing and the increasing affordability of medical testing. Perhaps the enactment of POPI is indicative of the fact that the time for South courts to consider the issue of genetic testing in the employment context is near. The United Kingdom experience showed genetic testing is rarely used in the employment context (except in the context that it is required by Health and Safety at Work Act) because it is still largely underdeveloped and its predictive value remains a bone of serious contention. That having been said, the DPA's Employment Practices Code discourages employers from using genetic testing as a means of obtaining information concerning the future employability of an individual and recommends the use of genetic testing for health and safety concerns only it because of its' intrusive nature and uncertainty surrounding its' predictive value. The South African and United Kingdom experiences impress that even in those jurisdictions where genetic testing is rarely used in the

workplace law makers are not blind to the rate at which technology is developing and the increasing affordability of medical testing and realise that it is only a matter of time that a larger number of employers (other than those compelled by legislation to carry out genetic testing) carry out genetic testing and this perhaps why they provide for that eventuality in their existing informational privacy legislation. The United States discussion showed that genetic testing is regulated by various pieces of legislation including GINA, the genetic non - discrimination legislation which provides protection against the misuse of genetic information and against discrimination on the basis of genetic information by restricting the collection and use of such information even in the workplace. However these pieces of legislation only effectively address the discriminatory implications of genetic testing as opposed to the informational privacy implications of such testing and perhaps what the United States needs is legislation similar to that of the DPA and POPI.

CHAPTER 9:
CONCLUSION

This dissertation set out to examine the extent to which privacy is protected in the South African workplace in light of advancements in technology and what the implications (if any) are for the right to privacy as such. In the first substantive chapter (Chapter 2), the issue of the protection of privacy is placed in its historical context. To this end, chapter 2 of the dissertation broadly traced the development of the legal protection of privacy. Four specific stages were identified and subjected to critical analysis. The stages are (i) the early conceptions stage; (ii) the gradual and specific protection stage; (iii) the international recognition stage; and(iv) the domestic and constitutional protection stage.

The discussion of the "early conceptions of privacy stage" revealed that early conceptions of privacy existed, but that these conceptions were often obscured by the communal and paternalistic traditions prevailing in these societies. For instance, aspects of human life which contemporary society considers private (such as marriage and sexual relations) were not treated as private concerns but rather as public concerns.[1803] What is more, factors such as the character and structure of the societies (particularly with respect to Greek, Roman and Hebrew societies) and the absence of words or concepts equivalent to the contemporary meaning of "private" and "public" excluded the development of the legal protection of privacy.[1804] This stage further brought to light the fact that conceptions of privacy formulated during the Renaissance period have found their way into contemporary notions of privacy – for example the notion that "a man's home is his castle".[1805] In the "gradual and specific protection stage", privacy was protected on an *ad hoc* basis using existing laws.[1806] This period saw the emergence of a growing awareness that privacy had to be more than just a principle or value, but instead should be a protected right. The "international recognition stage" ushered in a series of international and regional legal

[1803] See Moore *Privacy: Studies in Social and Cultural History* (1984) 135.

[1804] See *Moore Privacy: Studies in Social and Cultural History* (1984) 82.

[1805] Flaherty *Privacy in Colonial New England* (1972) 85.

[1806] Michael *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (1994) 15.

instruments which recognised and advocated for the respect and protection of a fundamental right to privacy.[1807] The final stage – the "explicit domestic and constitutional protection stage" - is characterised by the protection of privacy in various national laws and constitutions.

Chapter 3 of the dissertation concentrated on the development of the legal protection of privacy in selected countries, namely South Africa, the United Kingdom and the United States. These countries were selected for the simple reason that they protect the privacy of their citizens in distinct and varying ways. This diversity in the manner of protection is illustrative of the elusive nature of privacy and further illustrative of the fact that there is neither agreement on exactly what privacy entails nor agreement on the extent to which and the manner in which privacy should be protected. The right to privacy in South Africa, although still in its infancy, enjoys rich and generous protection under both the common law and the constitution. In addition, South Africa has also taken great strides towards enacting specific privacy legislation in the form of the Protection of Personal Information Bill of 2009 ("POPI"). One of the primary purposes of POPI is to give effect to the constitutional right to privacy by safeguarding personal information.[1808] POPI came into existence as a result of recommendations made by the South African Law Reform Commission ("SALRC").[1809] POPI will be discussed in more detail later in this chapter.

Chapter 3 also illustrated with reference to the United Kingdom (more specifically England) that despite the fact that it has no constitution and does not recognise that there is a right to privacy – nevertheless protects privacy through other common law principles and an international human rights instrument. Various commissions set up for the purpose of determining whether a common law right to privacy should be recognised in English law concluded that there was no need for an express recognition of the right to privacy in English law because existing legal doctrines or principles are quite capable of achieving the very same aim that a right to privacy set out to do,

[1807] Craig *Privacy and Employment Law* (1999) 5.

[1808] Section 2 of POPI.

[1809] South African Law Reform Commission "Privacy and Data Protection" Project 124 Discussion Paper 109 October 2005.

namely the doctrine of breach of confidence.[1810] One of the reasons advanced for the non- existence of a common law right to privacy is the fear that changes in existing law would result in legal uncertainty.[1811]The debate as to whether or not English law should recognise a common law right to privacy continues to this day. In this regard, several commentators have suggested that breach of confidence cannot effectively protect privacy interests. They argue that although the two actions appear similar, they are in actual fact two different actions which must be allowed to grow distinctly without jeopardising one another. As such, English courts or parliament should look into the creation of an independent right of privacy tort.[1812] It is submitted that the creation of an independent right to privacy is the only manner in which to ensure that individual privacy interests are protected. The right to privacy cannot be effectively protected through another right or action and can only be protected in its' true nature and form. Note however that certain commentators take the view that where privacy is protected through another right or action it is likely to disappear within that right or action or become a hybrid of that right or action and eventually cease to exist in its' truest or purest form. However, this view is not entirely correct because the United States experience has shown that even in the absence of a specific constitutional right to privacy zones of privacy may be through other constitutional rights.

As already mentioned above despite the absence of a right to privacy in the United States constitution, the United States has found a way to protect zones of privacy through other rights in its' Constitution. In addition, common law protection exists for privacy infringements. It is submitted that the United States should be commended for not only recognising but also protecting the right to privacy despite the absence of the right in its Constitution and for not allowing the absence of the right in its constitution to be an impediment towards the protection the right. The United Kingdom can certainly draw certain lessons from the development of privacy protection in the United States. It is ironic that certain English jurists continue to deny despite the existence of a right to privacy in English despite the line of English decisions (such as

[1810] Carnegie "Privacy and the Press: The Impact of Incorporating the European Convention on Human Rights in the United Kingdom" (1998) 9 *Duke Journal of Comparative and International Law* 311 317.

[1811] Krotoszynski "Autonomy, Community, and Traditions of Liberty: The Contrast of British and American Privacy Law" (1990) *Duke Law Journal* 1398 1404.

[1812] Shorts and De Than *Human Rights Law in the United Kingdom* (2001) 550.

Entick v Carrington[1813)], dating back hundred of years, that recognise a right to privacy. In fact, these decisions were relied upon by the American jurists Warren and Brandeis to advocate for the recognition of a common law right to privacy in the United States.[1814] Perhaps the most important insight to be gathered from the discussion in chapter 3, especially from the experience in South Africa (under the new constitutional dispensation) and the United States, is that, for purposes of legal protection, privacy cannot be accurately defined, and that privacy is a context – dependent right, which, upon closer inspection, renders the phrase 'right to privacy' a misnomer. Rather, the existence of the right is made subject to the subjectively held but objectively reasonable expectation of privacy. This seems to imply that the existence of the right (and its infringement) ultimately becomes dependant on a balancing of interests.

In Chapter 4, three noteworthy realities about the concept of the privacy were revealed. The first of these realities is the existence of two schools of thought with respect to the value or usefulness of privacy.[1815] On the one hand, proponents of privacy proclaim privacy as a useful value that is distinct and coherent.[1816] On the other hand, the 'reductionists' assert that privacy is incoherent and contend that there is nothing morally distinctive about privacy claims, because privacy can be protected through other interests, or reduced to some underlying right or interest such as freedom from mental stress, or property.[1817] Despite the divergent view on the usefulness of privacy, the majority of commentators agree that privacy is a value at the core of human existence and well-being but they also lament the fact that privacy is difficult to define. The difficulty to define privacy, some assert, has played a role in undermining its value and usefulness and has further impeded its effective legal protection.[1818] This leads to the second of the three realities, namely that privacy is

[1813]1558-1774 All E.R. Rep. 5.

[1814] Warren and Brandeis "The Right to Privacy" (1890) *Harvard Law Review* 193 196.

[1815] Schoeman *Privacy: Philosophical Dimensions of the Literature in Schoeman ed. Philosophical Dimensions of Privacy: An Anthology* (1984) 6.

[1816] See for example Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 443. Gavison contends privacy serves certain values and aspects of human and as such those values and aspects of human life would be impossible in the absence of privacy.

[1817] Schoeman *Privacy: Philosophical Dimensions of the Literature*in Schoeman ed. *Philosophical Dimensions of Privacy: An Anthology* (1984) 5.

[1818]Wacks *Privacy: Volume I The Concept of Privacy* (1993) xii.

virtually impossible to define[1819].[1820] The concept has a number of meanings and as such cannot be reduced to a single definition or meaning. What is considered private and what not differs from society to society. For this reason it is a concept that is neither eternal nor universal but rather relative and contextual. The third and final reality revealed in Chapter 4 is that there is general disagreement as to what makes privacy distinct and coherent. The value and distinction of privacy lie in the functions of privacy, the values that privacy promote and those aspects of human life that would be impossible or unlikely in the absence of privacy. Privacy serves a number of functions. For example, it creates and maintains social and personal relations and also limits access to an individual.[1821] Moreover, privacy promotes and is grounded on values such as happiness, justice and liberty. In the absence of privacy, ideals like personal relations and morally autonomous persons would cease to exist.[1822] It is submitted that the reality that privacy is virtually impossible to define should guide its' effective legal protection rather than prevent its' effective protection. In protecting the right, the focus should be on how best to protect the right in each context in which it manifests itself because privacy has multiple meanings.

Despite this reality, a number of legal and philosophical commentators have attempted to define privacy. This has resulted in the postulation ofsix dominant approaches or conceptions of privacy, namely the right to be let alone, limited access to the self, secrecy, control over information, personhood and intimacy. In Chapter 4, these approaches or conceptions of privacy are discussed as well as the value of privacy in relation to each conception and the shortcomings of each conception. It is submitted that the "pragmatic approach" is the more realistic and workable approach to privacy because the approach embraces the dynamic and evolving nature of privacy.[1823] Chapter 4 further concluded that privacy is a concept that cannot be placed in a mould to be used in the same manner over and over again, which is why the pragmatic approach is preferable. The approach accepts privacy as an aspect of customs, norms and traditions that may change from time to time and activities that

[1819] Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1 3 and Michael *Privacy and Human Rights* (1994) 1

[1820] *Supra*.

[1821] Gavison "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421 442- 443.

[1822] Benn *Privacy, Freedom and Respect for Persons* in Pennock and Chapman (eds) *Privacy: Nomos XIII* (1984) 24.

[1823] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review* 1087 1095.

we want to protect from disruptions and interferences.[1824] Of all the dominant approaches or conceptions of privacy postulated, the right to be let alone is perhaps the most commonly articulated one and constitutes one of the earliest conceptions of privacy.[1825] The conception locates the value of privacy in its ability to provide the individual with physical space away from others. One of the criticisms levelled at this conception is that it is merely descriptive of an attribute of privacy.[1826] The conception has also been criticised for being antiquated, "archaic"[1827] and a conception that was appropriate during a time in human history when individuals generally lacked physical space, which is no longer the case because the "opportunities for physical privacy are so much greater" and "abundant".[1828] As fundamental as the conception may be, it has a number of other shortcomings: first, it does not indicate how privacy should be valued; secondly, it obscures the fact that not every violation is a violation of privacy; thirdly, it overlooks the fact that not being let alone does not always result in a loss of privacy; and finally, it is out-dated in its sense of privacy as seclusion or solitude.[1829]

The other approaches to or conceptions of privacy postulated in legal and philosophical literature, namely secrecy, control over information, personhood and intimacy also have shortcomings simply because they locate the value of privacy in a single context and fail to embrace the evolving and dynamic nature of privacy. It is worth repeating at this juncture that ultimately, the pragmatic approach is perhaps the more realistic and workable approach to privacy because the approach embraces the dynamic and evolving nature of privacy. In terms of this approach, privacy is seen as a dynamic and evolving concept, it occurs in varied contexts, can be compromised in diverse circumstances and its underlying interests may evolve.[1830] Put differently, privacy is an aspect of customs, norms and traditions that may change from time to time and activities that we want to protect from disruptions and interferences. The different conceptions have all featured at different times, to different degrees and in

[1824] Solove "Conceptualizing Privacy" (2002) 90*California Law Review*1087 1093.
[1825] Godkin "The Rights of the Citizen: IV. To His Own Reputation" (1890) *Scribner's Magazine* 66.
[1826] Solove "Conceptualizing Privacy" (2002) 90 *California Law Review*1087 1102.
[1827]Posner "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1 4.
[1828]Supra.
[1829]Gavison "Privacy and Limits of Law" (1980) 89 *Yale Law Journal* 421 438.
[1830]Gutwirth *Privacy and the Information Age* (2002) 29.

different contexts in case law across the jurisdictions under review. Chapter 4 finally discussed the conceptions of privacy in each of the selected countries. It was found that each of the jurisdictions protected different conceptions of privacy. For example, the South African common law protects privacy as an independent personality right. Further, a person's privacy is breached when there has been an unlawful intrusion on their personal privacy or an unlawful disclosure of private facts concerning such a person. The right protects the privacy of an individual's person or home, their property, possessions and communications.[1831]In addition the South African Constitutional Court has chosen to view privacy as expressed in the South African Constitution as protecting, amongst other elements, personhood[1832] and intimacy[1833].

The goal of chapters 5, 6, 7 and 8 was to consider the issue that constitutes the heart of this research, namely, the extent to which privacy is protected in the workplace given advancements in technology and the implications (if any) for the right to privacy as such. To this end, the aim of chapter 5 was to briefly consider what is meant by the phrase "privacy in the workplace", and to examine the arguments for and against the need for privacy protection in the workplace. A further aim of the chapter was to consider a number of policies and practices in the workplace that typically threaten or pressurise the protection of privacy in the workplace, as well as the implication of these policies and practices for privacy. Chapter 5 begun with the basic premise that the need for privacy is not created by people, but instead inheres in all.

The chapter went on to examine the arguments for and against the protection of privacy in the workplace. Arguments in favour of the protection of privacy were found to emphasise the value of privacy as well as its constituent elements and suggested that privacy protection is essential because it preserves and maintains the autonomy, dignity and well-being of employees in an environment where the employer in general yields more influence and authority than the employee. The arguments in favour of privacy protection further stated that privacy is inherent in the notions of good faith, loyalty, respect and trust which underpin the employment relationship. These notions breed diversity and nurture the development of fresh and

[1831]*Bernstein v Bester NO* 1996 (2) SA 751 (CC).
[1832]*National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6.
[1833]*S v Jordan* 2002 (6) SA 642

different ideas, beliefs and attitudes, which are crucial for innovation and creativity in individuals.[1834]The chapter also identified the policies and practices in the workplace that typically threaten privacy in the workplace and further examined the extent to which they in fact impact on privacy. Perhaps the most important observation made in chapter 5 is that all the policies and practices identified are enabled by and emanate from advancements in science and technology. It is for this reason that the biggest continuous threat to privacy in the workplace remains developments in science and technology. Chapter 5 concluded that these technological and scientific developments demand no more than a continuous balancing of the interests of the employer and the employee in the different contexts created by new policies and practices made possible by technology.

Chapter 6 paid specific attention to how different jurisdictions have responded to what may be termed this 'contextual challenge' to the accommodation of privacy in the workplace. It did this by briefly discussing the use of the policies and practices identified in the previous chapter in the selected countries. The discussion examined legislation and case law indicative of the use and treatment of a relevant practice or policy in the workplace. It is important to bear in mind that the policies and practices identified in this chapter are by no means the only policies and practices utilised by employers that impact on privacy because modern technology has enabled and continues to enable sophisticated forms of testing or monitoring of employees. The discussion on background checks in the chapter made the general observation that the selected countries have no legislation directly regulating the carrying out of background checks by employers and further illustrated how, notwithstanding the absence of legislation directly regulating background checks in employment, there were various pieces of legislation such as the constitution (where applicable) that could be used to protect the employee's rights in relation to the carrying out of such checks. The evaluation on psychological and psychometric testing showed that South Africa had legislation explicitly prohibiting the use of psychometric testing unless the tests were shown to be: scientifically valid and reliable; to apply fairly to all employees and not biased against any employee of group and employers in using the tests have to ensure that the tests are valid and do not discriminate against any

[1834]Craig *Privacy and Employment Law* (1999) 20 -26.

group.[1835] It moreover emerged that South Africa has yet to aggressively wrestle with the issue of the use of the tests and their discriminatory impact.

The discussion on polygraph tests showed the use of polygraph tests is not without controversy because the scientific validity and reliability of the tests are questionable. The discussion further showed that despite the controversy surrounding the scientific validity and reliability of the tests, the tests continue to be used in the South African workplaces.[1836] The drug and alcohol testing evaluation revealed that employers in the selected countries carry out drug and alcohol testing on employees, especially those employees in safety sensitive positions, and that legislation not only regulated the use of such testing in the selected countries but also in certain instances compelled employers to carry out such testing on employees - especially on those employees in safety sensitive positions.[1837] The discussion on HIV/AIDS testing revealed that in general, individuals in the selected countries who are HIV positive are protected from discrimination in the workplace. The overview provided in this chapter was further illustrative of the fact that technology underlying the policies and practices implicate employee privacy interests which have to be balanced against competing employer interests and the law is perhaps lagging behind, at least to the extent that it endeavours to use existing legal principles to combat these developments. Moreover, what all the identified policies and practices have in common is that all of them are based on recent and continued technological advances. As such, it seems clear that the biggest continuous threat to privacy in the workplace remains developments in science and technology. It may also be said that it does not appear as if the challenge lies in a changed conception of privacy and the values it seeks to protect. Rather, it would seem that technological developments demand no more than a continuous balancing of the interests of employer and employee in the different contexts created by new policies and practices made possible by technology. In sum, chapter 6 sought to provide an overview, on a comparative basis, of a number of policies and practices which typically threaten or put pressure on privacy in the employment sphere and to evaluate to what extent privacy was protected. The main conclusion drawn is that

[1835]Section 8 of Employment Equity Act 55 of 1998.

[1836]Christianson "Polygraph Testing in South Africa Workplaces: Shield and Sword in the Dishonesty Detection versus Compromising Privacy Debate" (2000) 21 *Industrial Law Journal* 17 36. See also *PETUSA obo Van Schalkwyk v National Trading Company* (2000) 21 ILJ 2323 (CCMA).

[1837]Legislation such as South Africa's Occupational Health and Safety Act 85 of 1993.

privacy protection, for the most part, remains primarily to be dealt with through a combination of broad constitutional principle (where available) and a perhaps inordinate and curious reliance on discrimination law.

Chapter 7 of the dissertation provided an in depth view of one the policies and practices identified in chapter 5, namely e-mail and internet monitoring. The chapter departed from the notion the employee monitoring has always been carried out by employers and is not necessarily a new trend. However, what modern technology has simply done is to enable employers to monitor their employees more effectively and more extensively due to widespread use of technologically-enabled tools like e-mail and Internet.[1838] Chapter 7 considered the arguments for and against the monitoring of employees in the workplace, which arguments the chapter reasoned were representative of the two competing interests that would ultimately have to be balanced to determine whether the monitoring is justifiable. In this regard, the chapter revealed that the main arguments advanced by employers to justify the monitoring of employee e-mail and Internet usage are primarily aimed at protecting and preserving the employer's proprietal interest in its' e-mail and Internet facilities[1839] and in ensuring that the workplace is efficient and productive[1840], whereas the chief arguments advanced by employees against the monitoring and of e-mail and Internet usage in the workplace are aimed at preserving the employee's informational privacy. The chapter concluded that a balancing act was necessary to weigh these competing rights or interests to determine whether the monitoring of employee e-mail and Internet usage by the employer is justified. The chapter also pointed out that although the balancing of the competing interests is well-suited to determining whether an employee has an expectation to privacy in the workplace with respect to his or her use of the employer's e-mail and facilities, this approach was perhaps not ideal in a relationship such as the employment relationship, in which the balance of power will more often than not be weighted in the employer's favour. This means that while in

[1838] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 258.

[1839]Sheehy *Monitoring and Control of Use of E-mail and the Internet by the Employee. Managements Point of View* in Blanpain *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002)30.

[1840] Kesan *First Principle Examination of Electronic Privacy in the Workplace* in Blanpain (ed.) *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work* (2002) 252 – 253.

theory a careful balancing of interests should take place, this balancing act will almost invariably be determined in favour of the employer because the nature of privacy and the nature of the employment relationship, in which the balance of power will more often than not be in favour of the employer.

The discussion of the position in the United Kingdom indicated United Kingdom employees have recourse to a number of pieces of legislation including the Data Protection Act[1841] ("DPA") which contain a number of data protection principles and which reflects a sound balance between the competing rights at play. In addition, the DPA is representative of an appropriate means of elucidating the concepts of information privacy rights into practicable and effective terms.The country-specific evaluation also showed that, despite the fact that South Africa is a country with a comprehensive and generous bill of rights, which includes the right to privacy and in particular the right to informational privacy, it appears that courts are generally loathe to allow this right to exist in the context of the workplace, especially in respect of e-mail and Internet communications within the workplace. In fact, it seems that South African courts and tribunals are more likely to protect the employer's interest in not having its e-mail and Internet facilities abused for non–business purposes, even in the absence of express workplace policies. It appears that South African tribunals have yet to fully consider the implications of The Regulation of Interception of Communications and Provision of Communication – Related Information Act[1842] ("RICPCIA") on the interception and monitoring of employee communications in the workplace. Perhaps what South Africa needs and which at least emphasizes the principles of transparency and proportionality has recently presented itself in the form the Protection of Personal Information Bill of 2009 ("POPI"). POPI aims to give practical effect to the constitutional right to privacy and further aims to create a balance between the right to privacy and other important rights such as the right of access of information.[1843]More importantly, the Bill introduces a number of mechanisms aimed at ensuring that personal information concerning an individual is safeguarded when processed by public and private bodies. POPI introduces eight conditions or principles (termed "Information Protection Principles") to ensure the

[1841]Act of 1998.

[1842] Act 70 of 2002.

[1843] See "The Memorandum on the Objects of the Protection of Personal Information Bill of 2009" contained in page 45 of POPI.

lawful processing of personal information. The South African "Information Protection Principles", very much like the data protection principles contained in the United Kingdoms' Data Protection Act, place an emphasis on the pertinent principles of transparency and proportionality. Then again, the United States experience has shown that legislation regulating the interception and monitoring of employee communications in the workplace by the employer is by no means a guarantee that courts would recognize the rights of employees to a reasonable expectation of privacy. The United States experience illustrates that legislation may be of little or no benefit to employees in the workplace. United States courts have often held that employees have no expectation of privacy in the workplace arena because of the nature and character of the employment relationship, which tilts the balance of power will more often than not in favour of the employer.

The second last chapter of this dissertation, namely Chapter 8, focussed on genetic testing, which is perhaps the most recent example of the way in which scientific advancement may challenge privacy. A number of insights were gathered from the discussion on genetic testing. The analysis on how and why genetic testing is potentially invasive of privacy revealed that the type of information that can be determined or gleaned from one's genetic constitution genetic testing, namely medical- and personal information, has profound implications for privacy. The analysis further revealed the existence of two schools of thought as to whether genetic information is different from other forms of medical and personal information. This debate has come to be known as the genetical exceptionalism debate. On the one hand, proponents of "genetic exceptionalism" argue that genetic information is inherently exceptional and unique in comparison to other personal or medical information because it concerns private information about an individuals' future health, an individuals' family's future health and because it contains information that may influence certain personal decisions (such as whether or not to have a child).[1844] Proponents of "genetic exceptionalism" further contend that this type of medical information is more private than other forms of medical information because it is in

[1844] Annas "Genetic Privacy: There Ought To Be Law" (1999) 4 *Texas Review of Law &Politics* 910.

essence "a reverse diary" which is not only privacy but also in code and probabilistic.[1845]

On the other hand, critics of "genetic exceptionalism" argue that, for a number of reasons, there is nothing unique or exceptional about genetic information in comparison to other forms of personal and medical information.[1846] One of the reasons put forward by critics of "genetic exceptionalism" is that the majority of genetic information, contrary to popular perception, does not predict future diseases.[1847]The arguments advanced by employers to justify genetic testing are primarily aimed founded on health and safety concerns. Employers argue that genetic testing allows them to not only identify the hazards in the workplace and the effects of such hazards on employees, but also enables them to take appropriate action in reducing or eliminating such hazards.[1848] The arguments advanced by employers to justify genetic testing are also partially economic. They argue that genetic testing determines the future employability of individuals prevents increased health care costs[1849] and ensures public safety.[1850]On the other hand, arguments against the genetic testing in the workplace are aimed at preserving the employee's informational privacy and integrity. More importantly, the arguments are aimed at preventing the exclusion of individuals from employment and the discrimination of individuals irrespective of whether a particular gene has manifested itself and affected the ability of the concerned individuals to perform his or her duties.[1851] The survey in the chapter on the South African experience showed how the Occupational Health and Safety Act[1852] ("OSHA") obligated selected employers to carry out biological monitoring or

[1845] *Supra*.

[1846] See for example Annas "Genetic Privacy: There Ought To Be Law" (1999) 4 *Texas Review of Law & Politics* 9 and Green and Thomas "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology*.

[1847] Suter "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669 710.

[1848] European Group on Ethics in Science and New Technologies to the European Commission *Genetic Testing in the Workplace* 6 March 2000 6.

[1849] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society*(1995)82.

[1850] Laurie *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) 152.

[1851] Council on Ethical and Judicial Affairs, American Medical Association *Use of Genetic Testing by Employers Journal of the American Medical Association* in Barker (ed.) *Genetics and Society* (1995) 81.

[1852] Act 85 of 1993.

surveillance in the workplace. That having been said, the South African survey illustrated that there is no legislation directly regulating the use of genetic testing in South Africa. Nonetheless, the Constitution and the EEA may have implications for the use of genetic testing in employment. This also holds for the recently enacted POPI. POPI will have direct implications for genetic testing in employment because the Bill specifically includes and makes mention of biometric information in the definition of "personal information".[1853] The discussion of the South African experience further revealed that South African courts have yet to deal with genetic testing in the employment context. However, it is arguable that this it was only a matter of time bearing in mind both the rate at which technology is developing and the increasing affordability of medical testing. Perhaps the enactment of POPI is indicative of the fact that the time for South courts to consider the issue of genetic testing in the employment context is near. The United Kingdom experience pointed to the fact that genetic testing is possibly rarely used in the employment context (except in the context that it is required by Health and Safety at Work Act) because it is still largely underdeveloped and its predictive value remains a bone of contention. The Data Protection Act's[1854] Employment Practices Code ("Code") discourages employers from using genetic testing as a means of obtaining information about the future employability of an individual and recommends the use of genetic testing solely for health and safety concerns because of its' intrusive nature and uncertainty surrounding its' predictive value.[1855] The South African and United Kingdom experiences indicate that even in those jurisdictions where genetic testing is rarely used in the workplace, lawmakers cannot afford to turn a blind eye to the rate at which technology is developing and the increasing affordability of medical testing. It submitted that it is only a matter of time before a larger number of employers (other than those compelled by legislation to carry out genetic testing) begin to carry out genetic testing. The United States experience showed that genetic testing may be regulated by various pieces of legislation including Genetic Information Nondiscrimination Act[1856] ("GINA"), the genetic non - discrimination legislation. GINA provides protection against the misuse of genetic information and against

[1853]Section 1 of POPI.

[18541854]Act of 1998.

[1855] The Employment Practices Code Supplementary Guidance of the DPA 71.

[1856]Act of 2008.

discrimination on the basis of genetic information by restricting the collection and use of such information.The United States' experience further revealed that these pieces of legislation only addressed the discriminatory implications of genetic testing as opposed to the informational privacy implications of such testing. Thus, as it stands, the United States currently has no comprehensive law protecting the privacy of medical information or genetic information. Perhaps what the United States needs is an information privacy act such as the United Kingdom's DPA and South Africa's POPI which can effectively address the information privacy implications of the use of genetic testing.

To some extent, many of the issues discussed in this dissertation and many of the specific recommendations made have been either directly or indirectly incorporated into the recently enacted Protection of Personal Information Bill of 2009 ("POPI"). Given the fact that POPI was enacted after most of the substantive chapters of the dissertation had already been written, it receives scant attention in the dissertation. It is therefore of vital importance to discuss POPI in more detail in order to determine the extent to which it represents an step forward on the road towards the comprehensive protection of privacy in South Africa.

POPI aims to give practical effect to the constitutional right to privacy by introducing mechanisms which ensure that personal information concerning an individual is safeguarded when processed by public and private bodies. The Bill moreover aims to create a balance between the right to privacy and other important rights such as the right of access of information.[1857] Because one of the purposes of POPI is to give effect to the constitutional right to privacy by safeguarding personal information[1858], POPI is in essence the first piece of legislation to expressly deal with the right to privacy in South Africa. More importantly, POPI applies to all public and private entities.[1859] The definitions section of POPI defines a "responsible party" as a public or private body or person which determines the purpose for which and the manner in which personal information is processed.[1860] A "public body" is described as any state,

[1857] See *The Memorandum on the Objects of the Protection of Personal Information Bill of 2009* contained in page 45 of POPI.

[1858]Section 2 of POPI.

[1859]Section 6 of POPI.

[1860]Section 1 of POPI.

administration, functionary or institution of government or exercising or performing a public power, function or duty. A "private body" is defined as a natural person or partnership carrying on or which has carried on a trade, business, trade or profession or a juristic person. The term "processing" is given wide meaning to include the more technologically advanced forms of processing of information such as e-mail monitoring. "Processing" means any automated or non-automated operation or activity concerning personal information including amongst others dissemination by means of transmission, distribution, or making available in any other form or merging, linking, as a well as blocking, degradation, erasure, and destruction of information.[1861] Section 3 of POPI provides that the Bill applies to the processing of personal information entered into by or for a public and/or private entity. The use of the words "by or for" a public or private entity suggests that the Bill applies to the direct processing of personal information and the indirect processing of personal information on behalf of by such public or private entities by a third party. The Bill refers to persons in respect of whom the personal information pertains to as "data subjects". The broad application of POPI to both public and private entities means that the Bill covers both private and public sector employers in so far as they process personal information of their employees. The term "personal information", is defined as information relating to an identifiable individual or juristic person, including but not limited to *inter alia* information relating to an individuals' sexual orientation, well-being, culture, birth of a person and more importantly information related to the education, medical, financial, criminal or employment history of a person. Also included in the definition of "personal information" is information relating to the blood type or any other biometric information of a person. This in effect means that employers carrying out certain of the policies and practices discussed and identified in this dissertation as being potentially privacy invasive (particularly background checks, psychometric testing and genetic testing) will have to observe the obligations placed on them as processors of personal information and further ensure that data subjects are in a position to exercise the rights granted to them in the Bill.

POPI introduces 8 conditions or principles termed "Information Protection Principles" for the lawful processing of personal information. These principles, very much like the principles in the United Kingdoms' DPA, not only place a number of duties and

[1861] Section 1 of POPI.

obligations on responsible parties but also provide data subjects some measure of control over their personal information by according them rights in relation to the processing of personal information relating to them by responsible parties.

Chapter 3 of POPI (which deals with the conditions of lawful processing of personal information) houses these 8 core information protection principles, namely, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. These principles prescribe the minimum requirements for the processing of lawful information.[1862] The SALRC indicated in this regard that it was commonplace for most information privacy legislation to house a set of principles which were considered or regarded as an appropriate means of elucidating the concepts of information privacy rights into practicable and effective terms.[1863]

The "accountability principle" holds a responsible party accountable for complying with complying with the measures and principles enunciated in the Bill.[1864]

In terms of the "processing limitation" principle, a responsible party may only process personal information lawfully and in a manner that does not unreasonably infringe or intrude the privacy of a data subject.[1865] What is more, a responsible party may only process personal information for a warranted, adequate and relevant purpose.[1866] The processing principle further provides that a data subject has to giver or her consent to the processing. A data subject also has the right to object to the processing, at which point the responsible party may no longer process a data subject's personal information.[1867]

The "purpose specification" principle permits the processing of personal information by a responsible party only where the information is collected for a specific, explicitly defined and lawful purpose, which purpose has to be related to a function or activity

[1862] See *The Memorandum on the Objects of the Protection of Personal Information Bill of 2009* contained in page 46 of POPI.

[1863] South African Law Reform Commission *Privacy and Data Protection* Project 124 Discussion Paper 109 October (2005) 13.

[1864] Section 7 of POPI.

[1865] Section 8 of POPI.

[1866] Section 9 of POPI.

[1867] Section 10(3) of POPI.

of the responsible party.[1868] In terms of this principle, a responsible party is required to ensure that the data subject is fully aware of the purpose for which his or her information is processed[1869] and a responsible party is prohibited from keeping records pertaining to personal information which has been processed for any longer than is necessary for meeting the purpose for which it was processed.[1870]

The "further processing limitation" principle prevents a responsible party from processing further personal information unless the purpose for which such further personal information is processed is compatible with the purpose for which it was initially processed.[1871] The principle builds in a number of factors that a responsible party must take into account in determining whether the further processing is compatible with the purpose for the processing such as the nature of the information concerned, the manner in which the information is processed and the consequences of the intended further processing contemplated by the responsible party. The further processing principle stipulates that the further processing of personal information is compatible with the purpose for the processing where, for instance, the data subject has given its' consented to such further processing and the further processing is necessary to prevent or mitigate a serious imminent threat to the public health or safety or the life or health of the data subject.[1872]

The "information quality" principle requires a responsible party to take reasonable steps to ensure that the personal information it processes is not inaccurate, obsolete, incomplete and misleading.[1873]

The "openness" principle provides that personal information may only be processed by a responsible party which has notified the Information Protection Regulator ("IPR")[1874] in terms of chapter 6 of the Bill of its' intended processing of personal information. Perhaps the most important aspect of this principle is the obligation it places on a responsible party to take practicable steps to ensure that the data subject is

[1868]Section 12 of POPI.
[1869]Section 13 of POPI.
[1870]Section 14 of POPI.
[1871]Section 15 of POPI.
[1872]Section 15(3) of POPI.
[1873]Section 16 of POPI.
[1874]The IPR a body to be established in terms of the Bill (see below for a more detailed discussion of the role and functions of the IPR).

aware of, amongst things, that the personal information is being collected; the purpose for which the information is collected; whether or not the supply of the personal information by the data subject is voluntary or mandatory; and the consequences of a failure to provide such personal information.[1875]

The "security safeguards" principle requires the responsible party and anyone processing the personal information on behalf of the responsible party to safeguard the integrity of the personal information by taking the necessary and appropriate technical and organisational measures to safeguard the personal information against loss or damage or destruction or unlawful access.[1876]

The "data participation" principle accords a data subject the right to request a responsible party to provide confirmation, at no cost to the data subject, relating to whether not it holds personal information concerning the data subject and to further request from a responsible party a description of the personal information that the responsible party holds concerning the data subject.[1877] Once a data subject has been provided with this confirmation and is privy to the personal information held by the responsible party, a data subject has the additional right to demand that the responsible correct the information in the event that it is inaccurate, incomplete or out-dated, irrelevant, excessive or unlawfully obtained.[1878]

Provision for the exemptions is made in Chapter 4 of the Bill. Section 33 of the Bill stipulates that the processing of information will not be in breach of the information protection if authorised by the IPR and the IPR may authorise such processing if, for example, the public interest in the processing of the information outweighs any interference with the privacy interests of the data subject.[1879]

The Bill contains a general prohibition on the processing of special or sensitive personal information. Special personal information in terms of the Bill is described as personal information which reveals amongst others certain characteristics of data subject such as their race, ethnicity, health, sexual life, political or religious beliefs

[1875]Section 17 of POPI.
[1876]Section 18 of POPI.
[1877]Section 22 of POPI.
[1878]Section 23 of POPI.
[1879]Section 34 of POPI.

and criminal behaviour.[1880] Exceptions to the processing of special personal information are provided for and these exemptions are possible where for instance the information is required for an essential and legitimate public purpose.[1881]

The Bill establishes an independent and impartial statutory authority known as the Information Protection Regular ("IPR").[1882] POPI charges the IPR with the task of monitoring and enforcing compliance with POPI by public and private bodies.[1883]

In addition, POPI requires public and private bodies to appoint an Information Protection Officer with a number of duties and responsibilities which are mainly aimed at ensuring compliance within such bodies with the information protection principles and also cooperation with the IPR in so far as it is required to conduct investigations into the processing of personal information by the bodies in terms of chapter 6 of the Bill.[1884]

Chapter 6 is concerned with two information protection principles, namely, the principle of purpose specification and openness. The first part of Chapter 6 obliges responsible parties to provide the IPR with notification prior to commencing the processing of personal information[1885] containing particulars such as the purpose of the contemplated processing and a description of the categories of the data subjects. The IPR is required to keep a register of information processing in which it records all notifications received in this regard.[1886]

The second part of Chapter 6 requires the IPR to conduct investigations prior to the commencement of any processing by a responsible party in order to establish whether the contemplated processing complies with the law, for instance, where the processing of the personal information concerned carries a particular risk for the legitimate

[1880]Section 25 of POPI.

[1881] For instance section 27 of POPI allows the processing of special personal information concerning a data subject's race, where that information is used only and is essential for purpose of identifying a data subject or is required by legislation which is aimed at advancing categories of persons disadvantaged by unfair discrimination. This would in fact allow employers to process information regarding the race of their employees for purposes of for example complying with employment equity requirements imposed by the EEA.

[1882]Section 35 of POPI.

[1883]Section 35 of POPI.

[1884]Section48 of POPI.

[1885]Section 51 of POPI.

[1886]Section 53 of POPI.

interests of the data subject.[1887] Section 56 of the Bill prohibits a responsible party from processing any information whilst the IPR is conducting its' investigation.

POPI also makes provision for the IPR to issue codes of conduct incorporating the information protection principles and prescribing compliance with the principles.[1888] The IRP is empowered to issue codes of conduct however it has to do this in conjunction with affected stakeholders or their representative bodies.[1889] The codes of conduct are developed so as to contribute towards the effective implementation of the information protection principles in the divergent sectors and industries.[1890]

POPI has to be much-admired for recognising South Africa's diversity and multiplicity. A respect for this recognition is illustrated in making provision for the various sectors and industries to develop their own codes of conduct which will be sector, activity, industry and profession specific and may even be information specific.[1891]Instead of simply providing for an umbrella code of conduct or practice which attempts to address how best data processors can ensure compliance with the information protection principles in a single code, POPI allows for the existence of tailored or customised codes of conduct which cater for the information protection needs of the various and diverse segments of society.[1892] In taking this flexible and non-rigid approach to the protection of privacy, POPI is taking into account the context specific nature of privacy and the fact that it means different things, to different people in different circumstances. Codes of conduct must developed by the various sectors and industries.[1893] These codes of conduct are required to provide for an expiry period and provide the IRP with the power to review the operation of the Code under certain circumstances.[1894] In this regard, the various sectors and industries that wish to develop codes of conduct can do so under the guidance of the IRP. Provision is made for the IRP to issue written guidelines aimed at assisting the various sectors and industries to develop acceptable and appropriate codes of conduct and on

[1887]Section 55 (1) and (2) of POPI.

[1888]Section 57(1) and (2) of POPI.

[1889]Section 58 of POPI.

[1890] See *The Memorandum on the Objects of the Protection of Personal Information Bill of 2009* contained in page 47 of POPI.

[1891] See section 57(3) of POPI.

[1892]Section 57(1) and (2) of POPI.

[1893] Section 57 of POPI.

[1894]See section 57 (4) of POPI.

how to best address grievances within the codes.[1895] A breach of a code of conduct issued in terms of the Bill is tantamount to a breach of an information protection principle.[1896]

In terms of Chapter 10 of the Bill, a breach of an information principle or for breach of a provision of a code of conduct issued in terms of the Bill by a responsible party is regarded as an "interference with the protection of personal information" of a data subject.[1897] The Bill allows anyone to lodge a complaint alleging an interference with the protection of personal information[1898] and further prescribes the manner in which the complaints may be made.[1899] The IPR has the power to investigate complaints lodged with it and is required to inform a responsible party of an imminent investigation and to allow the responsible party an opportunity to respond to the complaint and possibly assist the parties relating to the complaint to resolve the dispute prior to commencing the investigation.[1900] The IRP also has the authority to refer such complaints to other suitable regulatory bodies.[1901] The IRP is empowered to make an assessment of its' own initiative or by request as to whether a processing practice complies with the provisions of the Bill.[1902]

To summarise, the enactment of POPI is a necessary component in ensuring that informational privacy rights are effectively protected by those processing personal information. The legislation is a much needed addition in South African law because the protection and development of privacy is still in its formative years and the right has yet to find its true expression in our society. Moreover, the legislation accords the individual a measure of active control over whether or not his or her personal information should processed and how it will be handled should he or she consent to the processing of the information.[1903] The South African Law Reform Commission warned that in so much as it is important to learn from the experiences of other

[1895]Section 62 of POPI.
[1896]Section 65 of POPI.
[1897]Section 70 of POPI.
[1898]Section 71 of POPI.
[1899]Section 72 of POPI.
[1900]Section 78 of POPI.
[1901]Section 76(2) of POPI.
[1902]Section 87 of POPI.
[1903]South African Law Reform Commission *Privacy and Data Protection* Discussion Project 124 Paper 109 October 2006 38.

countries, it is also important to not directly import foreign legislation into our law because each country has divergent factors (such as the historical background, public attitudes and population size) which have to be considered in drafting information privacy laws. These factors would ultimately shape the information privacy laws of any country.[1904]

The Bill should also be commended for not being an attempt to directly translate the experiences of other countries into South African law. This comes through in its provision for multiple codes of practices (as opposed to a single code of practice) representing a privacy model that aims to directly empower and involve individuals in the protection of their informational privacy rights and in most cases individuals who were previously deprived the right to exercise some measure of control over the processing of their personal information in the past by public bodies. On the other hand, as much needed as POPI is for the protection of information privacy in South Africa, information privacy laws only protect an aspect of a person's right to privacy. The constitutional right to privacy as expressed in the South African constitution protects other aspects of a person's right to privacy and not only the right not to have the privacy of one's communications or personal information infringed. As such, as important and much need as POPI is in realm of South African privacy protection, there is also a need for other legislation placing an emphasis on the protection of other aspects of the constitutional right to privacy, particularly the substantive privacy right protecting the "personal autonomy" of the individual in areas such as the workplace. As already alluded to in Chapter 3 of this dissertation, substantive privacy rights protect "personal autonomy" whereas informational privacy rights "prevent [disclosure] and access to information".[1905] As such it can be stated that POPI in actual fact aims to give effect to only one (albeit important) aspect of the constitutional right to privacy and not the constitutional right to privacy in its entirety. POPI focuses on the protection of informational privacy rights to the exclusion of substantive privacy rights. There will come a time when South African society requires that privacy be given specific protection as opposed to general protection by the introduction of privacy specific legislation.

[1904] South African Law Reform Commission *Privacy and Data Protection* Discussion Project 124 Paper 109 October 2006 372.

[1905] Devenish *Commentary on the South African Bill of Rights* (1999) 147. See also Woolman et al *Constitutional Law of South Africa 2nd ed* (2005) 38-19.

To conclude, the journey towards the legal protection of privacy has been a long and laboured one. That being said, the journey was one that could possibly not be avoided because privacy is an essential and necessary value, right or claim without which man would cease to flourish, create and function. It was only a matter of time before the legal protection of privacy reached the level of protection that it now enjoys the world over. The value and importance of privacy is emphasised by the fact that the even though it cannot be satisfactorily defined and corralled, it has been found to be worthy of constitutional protection in a number of countries, including South Africa. This dissertation sought to determine the extent of the legal protection of privacy in a specific context in society, namely the workplace. Hence, the issue at the heart of this dissertation was to determine to what extent privacy is protected in the South African workplace given advancements in technology and the implications (if any) for the right to privacy as such. The effective protection of privacy in is still in its infancy in South Africa. In fact, it may be said that the concept of privacy as described in the Constitution is still being developed and nurtured by legal commentators and courts. Advancements in technology have also played a significant contribution towards the legal protection of privacy after Warren and Brandeis first made the observation in 1890 that the biggest continuous threat to privacy is developments in science and technology. That is to say, advancements in technology will invariably determine the extent to which privacy is protected because they remain the biggest threat to privacy in this day and age of significant scientific research and progress.

SELECTED BIBLIOGRAPHY

BOOKS

Shorts E and De Than C *Human Rights Law in the UK* (2001) Sweet and Maxwell, London

Arendt H *The Human Condition* (1958) University of Chicago Press, Chicago

Aries P and Chartier R (eds) *A History of Private Life: From Pagan Rome to Byzantium* (1987) The Belknap Press of Harvard University Press, USA

Aries P and Chartier R (eds) *A History of Private Life: Passions of the Renaissance* (1989) The Belknap Press of Harvard University Press, USA

Aries P and Duby G (eds) *A History of Private Life: Revelations of the Medieval World* (1985) The Belknap Press of Harvard University Press, USA

Arnheim MTW *The Handbook of Human Rights Law: An Accessible Approach to The Issues and Principle*s (2004) Koga Page, London

Babson M *Monitoring Electronic Mail in the Workplace: Property v Privacy* (2001) National Legal Center for the Public Interest, Washington DC

Barendt EM *Privacy* (2001) Dartmouth Publishing Company, England

Barker P (ed) *Genetics and Society* (1995) The HW Wilson Company, New York

Basson A, Christianson M, Garbers C, Le Roux PAK, Mischke C and Strydom EML Essential Labour Law (2003)

Bible JD and McWhirter DA *Privacy in the Workplace: A Guide for Human Resource Managers* (1990) Quorum Books: Connecticut, USA

Blanpain R (ed) and Colucci M *Impact of the Internet and New Technologies on the Workplace: A Legal Analysis from a Comparative Point of View* (2002) Kluwer Law International, Netherlands

Blanpain R (ed) *On Line Rights for Employees in the Information Age: Use and Monitoring of E-mail and Internet at Work* (2002) Kluwer Law International, Netherlands

Blanpain R and Van Gestel M *Use and Monitoring of E-mail, Intranet and Internet Facilities at Work: Law and Practice* (2004) Kluwer Law International, Netherlands

Brownlie I and Goodwin-Gill GS (eds) *Basic Documents on Human Rights* 5th ed (2006) Oxford University Press, Clarendon

Burckhardt J *History of Greek Culture* (1963) Constable Publishers, London

Burns CD *Greek Ideals: A Study of Social Life* 2nd ed (1919) G Bell and Sons Ltd, London

Cohen GS *Employee Perceptions of Invasions of Privacy whilst Surfing the World Wide Web at Work* (2001) Thesis Submitted to Faculty of Arts University of Witwatersrand

Cowell FR *Everyday Life in Ancient Rome* (1961) BT Batsford Ltd, London

Craig JDR *Privacy and Employment* (1999) Hart Publishing: Oxford, England

Davis D, Cheadle H and Haysom N *Fundamental Rights in the Constitution: Commentary and Cases* (1997) Juta and Company Ltd Cape Town

De Waal J and Currie I *Bills of Rights Handbook* 5th ed (2005) Juta and Co, Ltd, Cape Town

Dearman JA *Religion and Culture in Ancient Israel* (1992) Hendrickson Publishers Inc, United States

Devenish GE *A Commentary on the South African Bill of Rights* (1999) Butterworths Publishers Durban

Dickson GL *The Greek View of Life* 19th ed (1945) Metheuen & Co Ltd, London

Dilke OAW *The Ancient Romans: How They Lived and Worked* (1975) David & Charles, Great Britain

Dixon HG *E-mail Security Policy Implementation in Multinational Organisations with Special Reference to Privacy Law* (2003) Thesis Submitted in the Faculty of Computer Studies Port Elizabeth Technikon

Dryness W *Themes in Old Testament Theology* (1979) InterVarsity Press, United States

Edwards L and Waelde C *Law and the Internet: Regulating Cyberspace* (1997) Hart Publishing: Oxford, United Kingdom

Ernst and Schwartz *Privacy: The Right to be Let Alone* (1962)

Etzioni A *The Limits of Privacy* (1999)

Ferrera R, Lichtenstein SD, Reder MEK, August R and Schiano WT *Cyber Law: Text and Cases* (2001) South – Western College Publishing, United States

Finkin M *Privacy in Employment Law* (2003) 117

Flaherty DH *Privacy in Colonial New England* (1972) University Press of Virginia, Charlottesville

Fried C *An Anatomy of Values: Problems of Personal and Social Choice* (1970) Harvard University Press, Cambridge Massachusetts

Grogan J Dismissal: The South African Law of Unfair Dismissal (2002) 175

Gutwirth S *Privacy and the Information Age* (2002) Rowan and Littlefield, Lanham Md

Harris D and Joseph S (eds) *The International Covenant on Civil and Political Rights and United Kingdom Law* (1995) Clarendon Press, Oxford

Hebert LC *Employee Privacy Law* (2009) Thomson Rueters

Hixson RF *Privacy in a Public Society: Human Rights in Conflict* (1987) Oxford University Press, New York

Hoffman H and Rowe J *Human Rights in the UK: A General Introduction to the Human Rights Act 1998* (2003) Pearson Education: Harlow, England

Hubbartt WS *The New Battle Over Workplace Privacy: How Far Can Management Go? What Rights do Employees Have? Safe Practices to Minimise Conflict, Confusion and Litigation* (1998) AMACOM, New York

Laurie G *Genetic Privacy: A Challenge to Medico-Legal Norms* (2002) Cambridge University Press, United Kingdom

Matthews VH and Benjamin DC *Social World of Ancient Israel 1250-587 BCE* (2002) Hendrickson Publishers Inc, Massachusetts 1993

McKechnie WS *Magna Carta: A Commentary on the Great Charter of King John* 2nd ed (1914) James Maclehose and Sons, Glasgow

McQouid – Mason DJ *The Law of Privacy in South Africa* (1978) Juta and Company Ltd Cape Town

Michael J *Privacy and Human Rights* (1994)

Moore B *Privacy: Studies in Social and Cultural History* (1984) ME Sharpe, New York

Neethling J, Potgieter JM and Visser PJ *Neethling's Law of Personality* (1996) Butterworths Publishers (Pty) Ltd Durban

Pennock JR and Chapman JW (eds) *Privacy: Nomos XIII* (1984) Atherton Press, New York

Posner RA *The Economics of Justice* (1981) Harvard University Press, Cambridge: Massachusetts

Repa BK *Your Rights in the Workplace* 6th ed (2002) Nolo Press: Berkeley California

Republic of South Africa *Bill of Rights Compendium* Service Issue 18 June 2006

Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 548 Thesis Submitted at the University of South Africa 2003

Rothstein MA (ed) *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (1997) Yale University Press, New Haven

Salisbury JE (ed) and GS Aldrette (vol ed) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 1The Ancient World* (2004) Greenwood Press: Westport, Connecticut

Salisbury JE (ed) and GS Aldrette (vol ed) *The Greenwood Encyclopaedia of Daily Life: A Tour through History from Ancient Times to the Present Volume 2 The Medieval World* (2004) Greenwood Press: Westport, Connecticut

Salzman *English Life in the Middle Ages* (1926) Oxford University Press, London

Schoeman FD (ed) *Philosophical Dimensions of Privacy: An Anthology* (1984) Cambridge University Press, Cambridge

Solove D and Rotenburg M *Information Privacy Law: Aspen Elective Series* (2003) Aspen Publishers.

Stromholm S *Right of Privacy and the Rights of the Personality: A Comparative Survey* (Working Paper prepared for the Nordic Conference on Privacy organised by the International Commission of Jurists, Stockholm May 1967) (1967) PA Nostedt & Sonersforlag Stockholm

Strum P *Privacy –The Debate in the US since 1945* (1998) Thompson Learning, London

Swanson JA *The Public and Private in Aristotle's Political Philosophy* (1992) Cornell Univeristy Press, Ithaca, New York

Thompson F *Magna Carta: It's Role in the Making of the English Constitution 1300-1629* (1948) University of Minnesota Press, Minneapolis

Thompson JW and Nathan EN *An Introduction to Medieval Europe 300 – 1500* (1965) WW Norton & Company, Inc, New York

Van der Walt JC and Midgely JR *Delict: Principles and Cases* vol 1 2nd ed (1997) Butterworths Publishers, Durban

Van der Walt JC and Midgely JR *Delict: Principles and Cases* vol 2 2nd ed (1997) Butterworths Publishers, Durban

Wagner DeCew J *In Pursuit of Privacy – Law, Ethics and the Rise of Technology* (1997)

Wallace PM *The Internet in the Workplace: How New Technology is Transforming Work* (2004) Cambridge University Press, New York

Westin AF *Privacy and Freedom* (1970) Bodley Head, London

Westin AF *The Origins of Modern Claims to Privacy* in Schoeman FD (ed) *Philosophical Dimensions of Privacy: An Anthology*

Woolman S, Roux T, Klaaren J, Stein A, Chaskalson M and Bishop M *Constitutional Law of South Africa* 2nd ed (2005) Juta and Company Ltd Cape Town

Young J (ed) *Privacy* (1978) Wiley and Sons, Chichester

JOURNAL ARTICLES

Annas GJ "Genetic Privacy: There Ought To Be Law" (1999) 4 *Texas Review of Law & Politics* 9

Benzanson RP "The Right to Privacy Revisited: Privacy, News and Social Change 1890-1990" (1992) 80 *California Law Review* 1133

Bonthuys E "Counting Flying Pigs: Psychometric Testing and the Law" (2002) 23 *Industrial Law Journal* 1175

Botswick "A Taxonomy of Privacy: Repose, Sanctuary and Intimate Decision" (1976) 64 *California Law Review* 1447

Camara WJ and Merenda PF "Using Personality Testing in Pre-Employment Screening: Issues Raised in *Soroka v Dayton Hudson*" (2000) 6 *Psychology, Public Policy and Law* 1164

Carnegie LP "Privacy and the Press: The Impact of Incorporating the European Convention on Human Rights in the United Kingdom" (1998) 9 *Duke Journal of Comparative and International Law* 311

Case Comment - Employment and Discrimination: Compulsory Drug Testing of Employees (2004) 4 *European Human Rights Law Review* 454

Christianson M 'The Testing of Employee: The Selective Prohibition of Medical, Psychological and Other Testing in terms of the Employment Equity Act' 1999 vol 9 No 2 *Contemporary Labour Law* 11

Christianson M "Polygraph Testing in South African Workplaces: Shield and Dishonesty versus Compromising Privacy Debate" (2000) 21 *ILJ* 16

Christianson M "The Testing of Employee: The Selective Prohibition of Medical, Psychological and Other Testing in terms of the Employment Equity Act" (1999) Vol 9 No2 Contemporary Labour Law 11

Christianson M "Truth, Lies and Polygraphs: Detecting dishonesty in the Workplace" (1998) 18 *CLL* 1

Collier D "Workplace Privacy in the Cyber Age" (2002) 23 *ILJ* 1743

Crandall EJ 'Confusion in the Courts: What to Do With HIV-Positive and AIDS-Infected Public Employees' (1995/1996) 10 *Cleveland University Journal of Law and Health* 157

Dekker A "Vices or Devices: Employee Monitoring in the Workplace" (2004) 16 *SA Mercantile Law Journal* 622

Delaney A "Employee Privacy – Grasping the Nettle" (2003) 56 *Employment Law Bulletin* 4

Deyerle KA "Genetic Testing in the Workplace: Employer Dream, Employee Nightmare Legislative Regulation in the United States and the Federal Republic of Germany" (1997) 18 *Comparative Labour Law Journal* 547

Dickler G "The Right to Privacy" (1936) 70 *US Law Review* 435

Ecker RB "To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee" (1994) 63 *University of Missouri at Kansas City Law Review* 251

Eltis K "The Emerging American Approach to E-Mail Privacy in the Workplace: Its Influence on Developing Case Law in Canada and Israel: Should Others Follow Suit" (2003) 24 *Comparative Labour Law and Policy Journal* 487

Epstein RA "The Legal Regulation of Genetic Discrimination: Old Responses to New Technology" (1994) 74 *Boston University Law Review* 1

Evans D "How to Manage Intoxication Compliance" *Transport World Africa: Multiple Transport Solutions* Supplement March 2006 26 – 27

Finkin M "Information Technology and Worker's Privacy: The United States Law" (2002) 23 *Comparative Labour Law and Policy Journal* 471

Finkin M "The Comparative Historical and Philosophical Context: Menschenbild: The Conception of the Employee as a Person in Western Law" (2002) 23 *Comparative Labour Law and Policy Journal* 577

Finkin M "The Kenneth M Piper Lecture: Employee Privacy, American Values, and the Law" (1996) 72 *Chicago Kent Law Review* 261

Fogel SM, Komblut GL and Porter NP "Survey of the Law on Employee Drug Testing" (1998) 42 *University of Miami Law Review* 553

Ford M "Two Conceptions of Worker Privacy" (2002) 31 *Industrial Law Journal* 135

Frayer CE "Employee Privacy and Internet Monitoring: Balancing Worker's Rights and Dignity with Legitimate Management Interests" (2002) 57 *The Business Lawyer* 857

French S "Genetic Testing in the Workplace: The Employer's Coin Toss" (2002) 15 *Duke Law and Technology Review* 6

Fried C "Privacy" (1968) 77 *Yale Law Journal* 475

Gavison R "Privacy and Limits of Law" (1980) 89 No3 *Yale Law Journal* 421

Ginsburg DH "Genetics and Privacy" (1999) 4 *Texas Review of Law and Politics* 17

Green RM and Thomas AM "DNA: Five Distinguishing Features for Policy Analysis" (1998) 11 *Harvard Journal of Law and Technology* 571

Gross H "The Concept of Privacy" (1977) 42 *New York University Law Review* 36

Hendricks AC "Genetics, Data Protection and Non – Discrimination: Some Reflections from an International Human Rights Perspective" (2001) 20 *Medicine and Law* 31

Heywood M and Hassan F "The Employment Equity Act and HIV/AIDS: A Step in The Right Direction" (1999) *Industrial Law Journal* 845

Hoffman S "Pre – placement Examinations and Job Relatedness: How to Enhance Privacy and Diminish Discrimination in the Workplace" (2001) 49 *University of Kansas Law Review* 517

Hustead JL and Goldman J "Genetics and Privacy" (2002) 28 *American Journal of Law and Medicine* 285

Isajiw PJ "Workplace E-Mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers" (2001) 20 *Temple Environmental Law and Technology Journal* 73

Jacques BE "Common Law Right to Privacy in the Employment Context" 2004 *Practising Law Institute* 788

Kim PT "Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace" (2002) 96 *Northwestern University Law Review* 1497

King NJ, Pillay S, Lasprogata GA "Workplace Privacy and Discrimination Issues Related to Genetic Data: A Comparative Law Study of the European Union and United States" (2006) 43 *American Business Law Journal* 79

Lacob Z "HIV Discrimination and Privacy in the Workplace" 1996 Issue 341 *De Rebus* 396

Lasprogata GA, King NJ and Pillay S "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada" (2004) 4 *Stanford Technology Law Review* 1

Marculewicz SJ "Some Tough questions for Challenges to Pre – employment Drug Testing" (1994) 10 *Journal of Contemporary Health Law & Policy* 243

McCloskey HJ "The Political Ideal of Privacy" (1971) 21 *Philosophical Quarterly* 303

McColgan A "Do Privacy Rights Disappear in the Workplace" (2003) Special Issue *European Human Rights Law Review* 120

McGregor M "The Right to Privacy in the Workplace: General Case Law and Guidelines for Using Internet and E-Mail" (2004) 16 *Mercantile Law Journal* 638

Menjoge SS "Testing the Limits of Anti – discrimination Law: How Employers Use of Pre-employment Psychological and Personality Tests Can Circumvent Title VII and the ADA" (2003) 82 *North Carolina Law Review* 326

Middlemiss S "The Truth and Nothing but the Truth? The Legal Liability of Employers for Employee References" (2004) 33 *Industrial Law Journal* 59

Miller JI "'Don't Be Evil': Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-Mail Privacy Rights" (2005) 33 *Hofstra Law Review* 1607

Mischke C "The monitoring and Interception of Electronic Communications: Obtaining and Using E-mail and Other Electronic Evdience" (2001) Vol 10 *Collective Labour Law* 91

Morin MM "Balancing Public Safety and the Right to Privacy: The New Jersey Supreme Court Affirms Random Testing for Employees Holding Safety – Sensitive Positions" (2000) 10 *Seton Hall Constitutional Law Journal* 455

Negley "Philosophical View on the Value of Privacy" (1966) 31 *Law and Contemporary Problem* 319

Nell B "The Employer's Dilemma: In Intoxication and Legislation" (2005) Vol 1 Issue 4 *Risk Management* 13

Ngwena C "HIV in the Workplace: Protecting the Rights to Equality and Privacy" (1999) 15 *SAJHR* 513

Oliver H "E-mail and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out" (2002) 31 *Industrial Law Journal* 321

Pagnattaro MA "Genetic Discrimination and the Workplace: Employee's Right to Privacy v Employer's Need to Know" (2001) 39 *American Business Law Journal* 139

Parent 'A New Definition of Privacy for the Law' 1983 2 *Law and Philosophy* 306

Paterson H and Uys K "Critical Issues in Psychological Test Use in the South African Workplace" (2005) 31 (3) *SA Tydskrif vir Bedrysfsielkunde* 12 – 22

Pellicciotti JM "Construction and application of Employee Polygraph Act of 1998" *American Law Reports*

Pesonen LM "Genetic Screening: An Employer's Tool to Differentiate or to Discriminate?" (2001) 19 *Journal of Contemporary Health Law and* Policy 187

Posner R "The Right to Privacy" (1978) 12 *Georgia Law Review* 393

Posner RA "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1

Post RC "Three Concepts of Privacy" (2001) 89 *Georgetown Law Review* 2087

Poste G "Privacy and Confidentiality in the Age of Genetic Engineering" (1998) 4 *Texas Law Review of Law and Politics* 25

Prosser D "Privacy" (1960) 48 *California Law Review* 383

Rachels J "Why Privacy is Important" (1975) 6 *Philosophy and Public Affairs* 323

Radipati "HIV and Employment Law: A Comparative Synopsis" (1993) XXVI *CILSA* 396

Reiman JH "Privacy, Intimacy and Personhood" (1976) 6 *Philosophy and Public Affairs* 26

Reinhard H "Information Technology and Worker's Privacy: Information Technology and Worker's Privacy: Enforcement" (2002) 23 *Comparative Labour Law & Policy Journal* 527

Remy DM "The Constitutionality of Drug Testing of Employees in Government Regulated Private Industries" (1991) 34 *Howard University Law Journal* 633

Richards HM "Is Employee Privacy an Oxymoron" (1997) 15 *Delaware Lawyer* 20

Robinson EP "Big Brother or Modern Management: E-Mail Monitoring in the Private Workplace" (2001) 17 *Labour Lawyer* 311

Rothstein MA "Workplace Drug Testing: A Case Study in the Misapplication of Technology" (1991) 5 *Harvard Journal of Law and Technology* 65

Rubenfeld J "The Right to Privacy" (1989) 102 *Harvard Law Review* 737

Scales M "Employer Catch – 22: The Paradox between Employer Liability for Employee Criminal Acts and the Prohibition against Ex-Convict Discrimination" (2002) 11 *George Mason Law Review* 419

Schreiber A "Confidence Crisis, Privacy Phobia: Why Invasion of Privacy should be Independently Recognised in English Law" (2006) 2 *Intellectual Property Quarterly* 160

Schwartz PM "Privacy and the Economics of Personal Health Care Information" (1997) 76 *Texas Law Review* 1

Smith JC "The USA Patriot Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment without Advancing National Security" (2003) 82 *North Carolina Law Review* 412

Solove D "Conceptualizing Privacy" *California Law Review* (2002) 90 1087

Stabile SJ "The Use of Personality Tests as a Hiring Tool: Is the Benefit Worth The Cost?"(2002) 4 *University of Pennsylvania Journal of Labour & Employment* 279

Stanley AE "Note: May I Ask You a Personal Question? The Right to Privacy and HIV Testing in the European Community and the United States" (1997) 65 *Fordham Law Review* 2775

Steinforth KA "Bringing Your DNA to Work: Employer's Use of Genetic Testing under the Americans with Disabilities Act" (2001) 43 *Arizona Law Review* 965

Suter SM "The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetic Legislation" (2001) 79 *Washington University Law Quarterly* 669

The British Psychological Society "A Review of the Current Scientific Status and Fields of Application of Polygraphic Detection" Working Party Final Report (6 October 2004)

Thomas T "Employment Screening and the Criminal Records Bureau" (2002) 31 *Industrial Law Journal* 55

Tottel Publishing 'Genetic Testing in the Employment Context – The State of Play" (2006) 13 (9) *Health and Safety at Work* 545 – 547

Tredoux C and Pooley S "Polygraph Based Testing of Deception and Truthfulness: An Evaluation and Commentary" (2001) 22 *Industrial Law Journal* 819

Van Der Merwe RP "Psychometric Testing and Human Resource Management" (2002) 28(2) *South African Journal of Industrial Psychology* 77

Van Niekerk A "The Right to Privacy in Employment" (1994) 3 *Collective Labour Law*105

Warren SD and Brandeis LD "The Right to Privacy" (1890) *Harvard Law Review* 193

Watson "E-mail Surveillance in the UK Workplace: A Management Consulting Case Study" (2002) 54 No 1 23 – 40

Wefig JB "Employer Drug Testing: Disparate Judicial and Legislative Responses" (2000) 63 *Albany Law Review* 799

Whitman JQ "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 *Yale Law Journal* 1151

TABLE OF CASES

SOUTH AFRICA

A

Auret v Eskom Pension and Provident Fund (1996) 7 BLLR 838 (IC)

Auret v Eskom Pensioen & Voorsorgfonds (1995) 16 ILJ 462 (IC)

B

Bailey v Mhlongo 1958 (1) SA 370 (W)

Bamford & Others/Energizer (SA) Limited [2001] 12 BALR 1251 (P)

Beinstein v Bester NO and Others 1996 (4) BCLR 449 (CC)

Black Mountain v CCMA & Others [2005] 1 BLLR 1 (LC)

C

C v Minister of Correctional Services 1996 4 282 (T)

Carolissen/International Brokers & Credit Control (Pty) Ltd (2004) 25 ILJ 2076 (BCA)

Case v Minister of Safety and Security 1996 (3) SA 165 (CC)

Chetty and Kaymac Rotomoulders (Pty) Ltd (2004) 25 ILJ 2391 (BCA)

Cronje/Toyota Manufacturing [2001] 3 BALR 213 (CCMA)

Crown Chicken Ltd t/a Rocklands v Walter Kapp [2002] 6 BLLR 493 (LAC)

D

Dauth/Brown and Weir's Cash and Carry [2002] 8 BALR 837 (CCMA)

De Beers Consolidated Mines Ltd v CCMA & Others (2000) 21 ILJ 1051 (LAC)

Dilks v Postma's Diamond Prospect Ltd 1921 (WLD)

E

Esterhuizen v Administrator, Transvaal 1957 (3) SA 710 (T)

Exactics – Pet (Pty) Ltd v Patelina NO & Others [2006] 6 BLLR 551 (LC)

F

Financial Mail v Sage Holdings 1993 (2) SA 451 (A)

G

Gallant v CIM Deltak (1986) 7 ILJ 346 (IC)

Goosen v Caroline's Frozen Yoghurt Parlour1995 (Pty) Ltd & Another 16 ILJ 396 (IC)

H

Harksen v Lane 1998 (1) SA 300 (CC)

Hoffmann v Monis's Wineries Ltd 1948 (2) SA 163 (C)

Hoffmann v South African Airways 2000 11 BCLR 1211 (C)

Huch v Mustek Electronics [1999] 12 BLLR 1297 (LC)

I

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors 2000 (10) BCLR 1079 (CC)

J

Jacob v Unitrans Engineering (1999) KN21921

Jansen Van Vuuren v Kruger 1993 (4) SA 842 (A)

Joy v Mining Machinery (A Division of Harnischfeger SA (Pty) Ltd) v NUMSA and Others 2002 (4) BLLR 37 (LC)

K

Kidson v SA Associated Newspapers Ltd 1957 (3) SA 461

K v Minister of Safety and Security [2005] 8 BLLR 749 (CC)

L

Lampert v Hefer 1955 (2) SA 507 (A)

Lebowa Platinum Mines Ltd v Hill [1998] 7 BLLR 666 (LAC)

Legolie/Sentrasure Ltd [2001] 7 BALR 769 (CCMA)

M

Mashava v Cuzen & Woods Attorneys [2000] 6 BLLR 691 (LC)

Mayer and Mind Pearl AG 2005 26 ILJ 382 (CCMA)

MEWUSA obo Mbonambi v S Bruce CC t/a Multi Media Signs [2005] 8 BALR 809 (MEIBC)

Mhlongo v Bailey 1958 (1) SA 370 (W)

Mistry v Interim National Medical and Dental Council of South Africa and Others 1998 (7) BCLR 880 (CC)

Mlotshwa/SABC (1) [2002] 12 BALR 1292 (CCMA)

Mncube v Cash Paymaster (Pty) Ltd (1997) 5 BLLR 639

Moonsamy v The Mailhouse1999 20 ILJ 464 (CCMA)

N

National Coalition for Lesbian and Gay Equality v Minister of Justice 1998 (12) BCLR 1517 (CC)

National Media Ltd v Jooste 1996 (3) SA 262 (A)

NUMSA obo Davids/Bosal Africa (Pty) Ltd [1999] 10 BALR 1240 (IMSSA)

NUMSA v Delta Motor Corporation (1998) 7 CCMA 621

O

O'Keefe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244 (C)

Oracle Corporation SA (Pty) Ltd v CCMA & Others [2005] 10 BLLR 982 (LC)

P

PETUSA obo Van Schalkwyk v National Trading Company (2000) 21 ILJ 2323 (CCMA)

PFG Building Glass v CEPPAWU & Others (2003) 24 ILJ 974 (LC)

Protea Technology Ltd & Another v Wainer and Others1997 (9) BCLR 1255 (W)

R

R v S 1955 (3) SA 313 (SWA)

R v Umfaan 1908 TS 62

S

S v A1971 (2) SA 293

S v Dube 2000 (2) SA 583 (NPD)

S v I 1976 (1) SA 781 (RA)

S v Kidson 1999 (1) SACR 338

SACCAWU obo Chauke v Mass Discounters (2004) 13 CCMA [2004] 6 BALR 767 (CCMA)

SACCAWU obo Sydney Fongo v Pick 'n' Pay Supermarkets

SACCAWU OBO Waterson/JDG Trading (Pty) Ltd [1999] 3 BALR 353 (IMSSA)

Sosibo & Others v Ceramic Tile Market (2001) 22 ILJ 811 (CCMA)

Spijkerman v ABSA Bank Ltd (1997) 3 BLLR 287 (IC)

Standard Bank of South Africa Ltd v CCMA & Others [1998] t BLLR 622 (LC)

Steen v Wetherlys (Pty) Ltd [2006] 2 BALR 222 (CCMA)

Stern Jewellers and SACCAWU (1997) NP144

Stoffberg v Elliot 1923 CPD 148

T

Tap Wine Trading CC v Cape Classic Wines (Western Cape) 1999 (4) SA 194

Toker Bros (Pty) Ltd and Keyser (2005) 26 ILJ 1366 (CCMA)

Toyota S Motors (Pty) Ltd v Radebe & Others (2000) ILJ 340 (LAC)

V

Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others (2005) 26 ILJ 2433 (LC)

W

Wium v Zondi & Others [2002] 11 BLLR 1117 (LC)

X

X and SA Breweries Ltd (2006) 27 ILJ 435 (ARB)

Y

Yende and Cobra Watertech (2004) 25 ILJ 2412 (BCA)

FOREIGN CASE LAW

AUSTRALIA

X v Commonwealth of Australia [1999] HCA 63

CANADA

T

Thompson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission) (1990) 47 CRR 1

Thwaites v Canada (Canadian Armed Forces) [1993] CHRD No 9 (7 June 1993); Canada (Attorney General) v Thwaites, [1994] 3 FC 38 (FCTD)

R

R v Dyment [1988] 2 SCR 417, 428

EUROPEAN COURT OF HUMAN RIGHTS

A

A v Commission 1994 ECR II-179 (Ct First Instance)

A v France (1994) 17 EHHR 462

Airey v Ireland (1979-80) 2 EHRR 305, 319

Akzo Chemie v Commission, 1986 ECR 2585, 2603, [1987] 3 CMLR 716 (1987)

Anderson v Sweden (1992) 14 EHRR 615

B

Bruggemann and Scheuten v Germany (1981) 3 EHRR 244

C

Commission v Germany 1992 ECR I – 2575, [1992] 2 CMLR 549 (1992)

D

Dudgeon v United Kingdom (1981) 4 EHRR 149

G

Gaskin v United Kingdom (1989) 11 EHRR CD 402

H

Halford v United Kingdom (1997) 24 EHRR 523

Handyside v United Kingdom (1976) 1 EHRR

Hewitt and Harman v United Kingdom (1992) 14 EHRR 657

Hilton v United Kingdom (1998) 57 DR 108, 117

Hokannen v Finland (1995) 19 EHRR 139

Huvig v France (1990) 12 EHRR 528

I

Internationale Handelsgesellschaft v Einfuhr, 1970 ECR 1125, [1972] CMLR 255 (1972)

K

Klass v Federal Republic of Germany [1978] 2 EHRR 213

Klass v Germany (1979-80) 2 EHRR 214

Kopp v Switzerland (1999) 27 EHRR 91

L

Ludi v Switzerland (1992) 15 EHRR 173

Lustig-Prean v United Kingdom (1997) 7BHRC 65

M

Malone v United Kingdom [1984] 7 EHRR 14

Marckx v Belgium (1979) 2 EHRR 330

Murray v United Kingdom (1994) 19 EHRR 193

N

Niemetz v Germany [1992] EHRR 97

P

Peters v Netherlands (1994) 77-A DR 75, EComm HR

S

Smith and Grady v United Kingdom [1999] ECHR 72

Stauder v Ulm, 1969 ECR 419, 425, [1970] CMLR 112 (1970)

T

Tele Danmark A/S v Handels – og Kontorfunktionaerernes Forbund 2001 ECR I-06993

The Sunday Times v United Kingdom (1979-80) 2 EHRR 245

W

Wretlund v Sweden (Admissibility) (Application No 46210/99) (Unreported, March 9, 2004) (ECHR)

X

X and Y v Netherlands (1985) 8 EHRR 235

X v Austria (1979) 18 DR 154, EComm HR

X v Commission 1994 ECR I-4737

X v Iceland Application No 6825/74

X v Iceland, 5 Eur Commin HR8687 (1976)

Z

Z v Finland (1997) 25 EHRR 371

NAMIBIA

N

N v Minister of Defence (Namibia) Labour Court of Namibia, delivered 2005 05 10, Case No: LC 24/98

UNITED KINGDOM

A

Albert v Strange 1 McN & G25 (1849)

Attorney General v Guardian Newspapers Ltd and Other (No 2) [1998] All ER 545

Attorney-General v Jonathan Cape Ltd [1976] QB 752,769

B

Bernstein v Skyviews Ltd [1978] QB 479

Bartholomew v London Borough of Hackney [1999] IRLR 246

C

Coco v AN Clark (Engineers) Ltd [1969] RPC 41, 47

D

Douglas v Hello! [2001] 3 WLR 992

Durant v Financial Services Authority [2003] EWCA Civ 1746

E

Entick v Carrington 1558-1774 All ER Rep45

H

Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804, 807

J

Jones v Trane (1992, Supp) 153 Misc 2d 822, 830

K

Kaye v Robertson [1991] FSR 62

M

Malone v Metropolitan Police Commissioner [1979] 1 Ch 344

Margaret Duchess of Argyll v Duke of Argyll [1965] 1 All ER 611, [1967] Ch 302

McLorie v Oxford [1982] 1 QB 1290

Morris v Beadmore [1981] AC 446

N

Naomi Campell v Mirror Group Newspapers Ltd [2003] 2 WLR 80

O

O'Flynn v Airlinks The Airport Coach Co Ltd [2002] Emp LR 1217

P

PG and JH v United Kingdom No 44787/98S57 (2001)

Pope v Curl2 ATK 342 (1741)

Prince Albert v Strange and Others1 McN & G 25 (1849)

R

R v Khan (Sultan) [1997] AC 558

S

Saltman Engineering Co Ltd v Campbell Engineering Co Ltd (1948) 65 RPC 203, 215

Seager v Copydex Ltd [1967] 2 All ER 415, [1967] 1 WLR

Seymane's Case [1558-1774] All ER Rep

South West Trains Ltd v Mr SA Ireland Appeal No EAT/0873/01

T

Theakston v Mirror Group [2002] All ER (D) 2

Thompson and Venables v News Group Newspapers [2001] 2 WLR 1038

Truck v Priester 19 QBD 639 (1887)

W

Wainright and Another v Home Office [2003] UKHL 53

Whitefield v General Medical Council Appeal No 90 of 2001

Wigan Borough Council v Davies [1979] IRLR 127 EAT

Wilner v Thornburgh 738 F supp 1 (D DC1990), reversed 928 F2d 1185 (CA DC 1991)

Y

Yovatt v Winyard 1 JAC & W 390

UNITED STATES OF AMERICA

A

Albemarle Paper Co v Moody 422 US 405 (1975)

Alford v South Carolina Department of Corrections 2006 WL 1997434 (DSC 2006)

Ali v Douglas Cable Communications 929 F Supp 1362 (D Kan 1996)

American Federation of Government Employees v Sullivan 744 F Supp 294, 305 (D DC 1990)

American Federation of Government Employees v Thornburgh 720 F Supp 154, 155 n 1 (ND Cal 1989)

American Postal Workers Union v United States Postal Service 871 F 2d 556 (6th Circ 1989)

Anonymous Fireman v City of Willoughby 779 F Supp 402 (1991)

Autoli ASP Inc v Department of Workforce Services 29 P3d 7 12 – 13 86 FEP Cases 228 (Utah App Ct 2001)

B

Baron v Hollywood 93 F Supp 2d 1137 (SD Fla 2000)

Beattie v St Petersburg 733 F Supp 1455 (MD Fla 1990)

Blackwell v 53rd – Ellis Currency Exchange 852 F Supp 646

Bodah v Lakeville Motor Express Inc, 649 NW 2d 859, 862 (Minn App 2002)

Bourke v Nissan Motor Corporation No B068705 [1 ILR (P&F) 109] (Cal Ct App 26 July 1996)

Bowers, Attorney General of Georgia v Hadwick 478 US 186 (1985)

Boyd v United Sates 116 US 616 (1886)

Bragdon v Abbott 524 US 614 (1998)

C

Caruso v Ward 530 NE 2d 850 (NY 1998)

Castillo v California Department of Parks and Recreation 50 F3d 13 1995

Chandler v Miller 520 US 305 (15 April 1997)

Chesna v United States Department of Defense 850 F Supp 110 (D Conn 1994)

Chevron v Echazabal 536 US 73 (2002)

Connecticut Department of Public Safety v Doe 123 SCt 1160 US, (2003)

Curtis v Dimaio 46 F Supp 2d 206, 79 Fair Empl Prac Cas (BNA) 1991

D

De May v Roberts 46 Mich 160 9 NW 146 (1881)

Deal v Spears 980 F2d 1153 (8th Cir 1994)

Doe v District of Columbia 796 FSupp 559DDC 1992

Doe v High – Tech Institute Inc 972 P2d 1060, 132 Ed Law Rep 989, 77 ALR 5th 755 (Colo Ct App 1998)

Doe v University of Maryland Medical System Corporation 50 F 3d 1261 (1995)

Doe v Washington University 780 FSupp 628

Dothard v Rawlinson 433 US 321 (1977)

E

Echazabal v Chevron USA, Inc 226 F3d 1063 (2000)

EEOC v Burlington Northern Santa Fe Railway Civ No CO1-4013 MWB (ND Iowa 2001)

Eisenstadt v Baird, 405 US 453-454, 92 SCt 1038-1039

Ex Parte Jackson 96 US 727 (1877)

F

Fischer v Mount Olive Lutheran Church207 F Supp 2d 914 (WD Wis 2002)

Foster v Loft Inc 26 Mass App 289 (1988)

Fraser v Nationwide Mutual Insurance Co 352 F3d 107 CA 3 (Pa) (2003)

Fraser v Nationwide Mutual Insurance Co 135 F Supp 2d 623 (ED Pa 2001)

G

GM Leasing Corp v United States 429 US 338, 353 (1977)

Garrity v John Hancock Mutual Life Insurance Company 18 IER Cases 981 (D Mass 2002)

Glover v Eastern Nebraska Community Office of Retardation867 F2d 461 (1989)

Goodrich v Waterbury Republican-American, Inc 188 Conn 107, 127-128, 438 A2d 1317, 1329 (1982)

Griggs v Duke Power Co 401 US 424 (1971)

Griswold v Connecticut, 381 US 479 (1965)

Guest v Leis 255 F3d 325 (6th Cir 2001)

H

Harmon v Thornburg 878 F2d 484 (DC Cir 1989)

Hennessey v Morin Coastal Eagle Point Oil Company 129 NJ 81 (1992)

Hester v City of Milledgeville 777 F 2d 1492 (11th Cir 1985)

I

In re DoubleClick Inc Privacy Litigation 154 F Supp 2d 497 (2001)

International Brotherhood of Electrical Workers 856 F 2d 1174 (CA 8 1998)

K

Karraker v Rent – A – Center, Inc, 239 F Supp 2d 828, 834 – 836, 13 AD Cas (BNA) 1639 (CD III 2003)

Katz v United States, 389 US 347 (1967)

K-Mart v Trotti 677 SW2d 632 (Tex Ct App1984)

Konop v Hawaiian Airlines Inc 236 F 3d 1035 CA 9 (Cal) 2001

Konop v Hawaiian Airlines Inc302 F3d 868 (9th Cir 1992)

Kyllo v United States 533 US 27 (2001)

L

Lawrence v Texas 539 US 558 (2003)

Leckelt v Board of Commissioners 909 F 2d 820 (1990)

Leventhal v Knapek 266 F 3d 64 (2d Cir 2001)

Local 1812, American Federation of Government Employees v Department of State 662 F Supp 50 (1987)

Loder v City of Glendale 927 P2d 1200 (Cal1997)

Loder v Glendale14 Cal 4th 846 (1997)

Long Beach City Employees Association v City of Long Beach 41 Cal3d 937, 227 CalRptr 90 Cal 1986

Loving v Virginia 388 US 1 (1967)

Luedtke v Nabors Alaska Drilling Inc 768 P2d 1123 (Alaska 1989)

Lyles v Flagship Resort Development 371 F Supp 2d 597 (2005)

M

Manela v Stevens NY Sup Ct 1890

Marbury v Madison 5 US (1 Cranch) 137 (1803)

McKenna v Fargo 451 FSupp 1355 (DNJ) 1978), affirmed, 601 F2d 575 (3d Cir 1979)

McLaren v Microsoft Corporation 1999 WL 339015 (Tex App Dallas 1999)

Meloff v New York Life Insurance Company 51 F3d 372

Meyer v Nebraska 262 US 390 (1923)

Moore v City of East Cleveland 431 US 494 (1977)

N

National Federation of Federal Employees v Cheney 884 F2d 603 (DC Circ 1989)

National Treasury Employees Union v Von Raab 489 US 656 (1989)

National Treasury Employees Union v Von Raab 816 F2d 170(1987)

Nipper v Variety Wholesalers Inc 638 So 2d 778 (Ala 1994)

Norman-Bloodsaw v Lawrence Berkeley Laboratory 135 F3d 126

O

O'Connor v Ortega 480 US 709, 107 SCt 1492 (1987)

Oliver v United Sates 466 US 170, 177 (1984)

Olmstead v United States 277 US 438 (1928)

Osborn v United States 385 US 323, 87 SCt 439 US (1996)

P

Pavesich v New England Insurance Company 122 Ga 190 (1905)

Pierce v Society of Sisters, 268 US 510 (1925)

Playboy Enterprises Inc v Russ Hardenburgh Inc 982 F Supp 503, 1998 CoprLDec P 27,771

Polkey v Transtecs 404 F 3d 1264 (2005)

Polsky v Radio Shack 666 F 2d 824

Porten v University of San Francisco 134 Cal Rptr 839 (Cal App 1st Dist 1976)

Prince v Massachusetts 321 US 158 (1944)

R

R v Botsford 141 US 250, 251, 11 SCt1000, 1001, 35 LEd 1734 (1891)

Redmond v City of Overland Park 672 F Supp 473, 473 (D Kan 1987)

Reno v American Civil Liberties Union 521 US 844 (1997)

Reno v Condon 528 US 334 (1995)

Restuccia v Burk Technology 1996 WL 1329386 Mass Super,1996 Aug 13, 1996

Robinson v City of Seattle 102 Wash App 795, 10 P 3d 452, 16 ER Cas (BNA) 1405 (2000)

Roe v Quality Transportation Services 838 P2d 128 (Wash 1992)

Roe v Wade 410 US 113 (1973)

S

School Board of Nassau County v Arline 480 US 273 (1987)

Shurgard Storage Centers Inc v Safeguard Self Storage Inc 119 F Supp2d 1121, 174 ALE Fed 655

Skinner v Oklahoma 316 US 535 (1942)

Skinner v Railway Labour Executives' Association 489 US 602 (1989)

Smith v American Service Co of Atlanta 611 F Supp 321 (1984)

Smith v Maryland 442 US 735 (1979)

Smyth v Pilsbury Co 914 F Supp 97 (ED Pa 1996)

Soroka v Dayton Hudson Corporation 7 Cal App 4th 203, 1 Cal Rptr 2d 77, 84-85 (1991), review dismissed, 24 Ca Rptr 2d 587 (1993)

Stanley v Georgia, 394 US 557, 564 89 S Ct 1243, 1247, 22 L Ed 2d 542 (1969)

State v Community Distributors Inc 123 NJ Super 589,304 A2d, 213 NJ Co 1973

Stehney v Perry 101 F 3d 925 (3d Cir 1996)

Stein v Marriott Ownership Resorts Inc 944 P2d 374 (Utah Ct App 1007)

Steve Jackson Games, Inc v United States Secret Service 26 F3d 457, 461 (5th Cir 1994)

T

Tallahassee Furniture Co, Inc, v Harrison 583 So 2d 744, 747 (Fla Dist Ct App 1991)

TBG Insurance Services Corp v Superior Court of Los Angeles County 96 Cal App 4th 443 (2002)

The Committee for GI rights v Callaway 518 F 2d 466 (2 September 1975)

Theofel v Farey – Jones 341 F 3d 978 2004 Daily Journal DAR 2089

Thorne v City of El Segundo726 F 2d 459 (1983)

Thygeson v US Bancorp, 34 Employee Benefits Cas (BNA) 2097, 2004 WL 2066746 (D Or 2004)

Transportation Institute v United States Coast Guard 727 F Supp 648 (D DC 1989)

Trulock v Freeh 275 F 3d 391 (4th Cir 2001)

Trustees of Dartmouth College v Woodward 17 US (4 Wheat) 518 (1819)

Twigg v Hercules Corporation 406 SE 2d 52 (WVa 1990)

U

US v Lifshitz 369 F 3d 173, 4 ALR 6th 697 (2d Cir 2004)

US v Maxwell 45 MJ 406 (CAAF 1996)

US v Munroe 52 MJ 326 (CAAF 2000)

Union Pac Ry Co v Botsford, 141 US 250, 251 (1891)

United States v Charbonneau 979 F Supp 1177 (SD Ohio 1997

United States v Councilman418 F3d 197 (1st Cir 2005)

United States v Drayton 536 US 194 (2002)

United States v Mullins 992 F 2d 1472 (9th Cir 1993)

United States v Simons 29 F Supp 2d 324 (ED Va 1998)

United States v Steiger 318 F3d 1039, 1048 – 49 (11th Cir 2003

United States v Taketa 923 F2d 665 (9th Cir 1991)

United States v Turk 526 F2d 654 (5th Cir 1976)

US v Simons 206 F3d 392, 398 (2000)

V

Valley Bank of Nevada v Superior Court of San Joaquin County 542 P2d 977 (1975)

Vernars v Young 539 F2d 966 (3d Cir 1976)

W

Wal – Mart Stores, Inc v Lee, 348 Ark 707, 74 SW 3d 634 (2002)

Ward v Bartlett, 1 NH 14 (1816)

Watchtower Bible & Tract Society of New York v Village of Stratton 536 US 150 (2002)

Webster v Motorola 637 NE 2d 203 (Mass 1994)

Wesley College v Pitts 974 FSupp 375, 385 (DDel 1997)

Whalen v Roe 429 US 589 (1977)

Wheaton v Peters 33 US 591(1834)

Wilkinson v Times Mirror Corporation 215 Cal App 3d 1034 1990

Williams v Philadelphia Housing Authority 826 F Supp 952 (ED Pa 1993)

Willner v Thornburgh 928 F2d 1185 (DC Cir) cert Denied, Willner v Barr 112 SCt (1991)

Wilner v Thornburgh 738 F supp 1 (D DC1990), reversed 928 F2d 1185 (CA DC 1991)

TABLE OF STATUTES

STATE CONSTITUTIONS AND/OR HUMAN RIGHTS CHARTERS

State Constitutions

Basic Law of the Federal Republic of Germany of 1949

Canadian Charter of Rights and Freedoms, Constitution Act of 1982

Constitution of the Republic of South Africa Act 108 of 1996

The Constitution of the United States of America

International Human Rights Charters

International Covenant on Civil and Political Rights of 1966

International Covenant on Economic, Social and Cultural Rights of 1966

Universal Declaration of Human Rights

Regional Human Rights Charters

American Convention on Human Rights of 1969

American Declaration of the Rights and Duties of Man of 1948

The European Convention of Human Rights of 1950

STATUTES
South Africa

Employment Equity Act 55 of 1998

Health Professions Act 56 of 1974

Interception and Monitoring Prohibition Act 127 of 1992

Interception of Communications and Provision of Communication – Related Information Act 70 of 2002

Occupational Health and Safety Act 85 of 1993

Protection of Personal Information Bill of 2009

Rehabilitation of Offenders Act of 1974, (Exceptions Order 1975)

Interception and Monitoring Prohibition Act 127 of 1992

Interception of Communications and Provision of Communication – Related Information Act 70 of 2002

FOREIGN JURISDICTIONS

United Kingdom

Control of Substances Hazardous to Health Regulations of 1999

Data Protection Act of 1998

Disability Discrimination Act of 1995

Health and Safety at Work Act of 1974

Human Rights Act of 1988

Race Relations Act of 1976

Regulation of Investigatory Powers Act of 2000

Rehabilitation of Offenders Act of 1974, (Exceptions Order 1975)

Sex Discrimination Act of 1975

Telecommunications (Lawful Business Practice) Regulations of 2000

United States of America

Americans with Disabilities Act of 1990

Civil Rights Act of 1964

Electronic Communications Privacy Act of 1986

Genetic Information Non-Discrimination Act of 2009

Occupational Safety and Health Act of 1970

Stored Communications Actof 2003

USA Patriot Act of 2001

Wire Tap Actof 2004

COMMISSION REPORTS

CANADA

Privacy Commissioner of Canada Discussion Paper *Genetic Testing and Privacy* 1995

EUROPEAN UNION

Opinion of the European Group on Ethics in Science and New Technologies to the European Commission *Ethical Aspects of Genetic Testing* in the Workplace July 2003

SOUTH AFRICA

South African Law Reform Commission Project 85 Discussion Paper *Aspects of the Law Related to AIDS: Pre-employment HIV Testing* Project 85 31 July 1997

South African Law Reform Commission *Privacy and Data Protection* Discussion Project 124 Paper 109 October 2006

UNITED KINGDOM

Nuffield Council on Bioethics Report on *Genetic Screening Ethical Issues* 1993

United Kingdom Human Genetics Advisory Commission: Report on *The Implications of Genetic Testing for Employment* 1999

LEGISLATIVE CODES

SOUTH AFRICA

Code of Good Practice on Key Aspects of HIV/AIDS and Employment 2001

Code of Good Practice: Key Aspects on the Employment of People with Disabilities of 2002

UNITED KINGDOM

Draft Code of Practice on the Use of Personal Data in Employer/Employee Relationships of 2000

Employment Practices Data Protection Code of 2003

REPORTS

AIDS Epidemic Update: Special Report on HIV/AIDS: December 2007 Published by Joint United Nations Programme on HIV/AIDS (UNAIDS) and the World Health Organisation (WHO)

PARLIAMENTARY DEBATES

House of Commons Science and Technology Committee *Third Report on Human Genetics*

RESEARCH GROUPS

Fiddick *The Human Rights Bill [HL], Bill 119 of 1997-98: Privacy and the Press* Research Paper 98/25 Home Affairs Section, House of Commons Library 7