Sven Rupert Abrahamse

ABRSVE002

Post Graduate Diploma in Commercial Law

Electronic Communications in the Workplace

Professor Julien Hofman

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the Post Graduate Diploma in Commercial Law in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of the Post Graduate Diploma in Commercial Law dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

Table of Contents.

Chapter One – Introduction

Processing personal data may be an incidental consequence but difficult to avoid in the day to day operations of the employment relationship.

Privacy in the context of the employment relationship is not a precise term but a bundle of not very specifically defined rights and expectations.

Generally the main focus of privacy rights apply to the restraint of power by the state as defined in Section 14[1] of the South African Constitution. It could be applied to the employee and employer relationship.

The existence of other public interest may substantively reduce the scope of such privacy rights.

It is clear that any expectation of privacy of the employee should be balanced against the legitimate and reasonable needs of the employer.

What ever the extent to which privacy is being protected in the workplace, these rights generally are not relied on directly by the employee but rather it works by influencing the judicial interpretation of other laws.

Some of the reasons that are advocated by employers to monitor electronic communications in the employee employer relationship are:

1. The Protection of resources
2. Operational reasons
3. Controlling the flow of information
4. Protection against civil and criminal liability.

However there should simply not be an undirected system if monitoring the electronic communications of the employees. When looking at the

[1] The South African Constitution, Act 108 of 1996

implementation of the RIPA[2] Act in the United Kingdom it becomes clear that we are seeing a paradigm shift away from reactive policing of incidence to proactive policing and management of risk.

1.1. The question of balance.

The ubiquitous nature of computers in our workplace has on the one hand created a situation where cost becomes insignificant to monitor and control employee electronic communication but on the other hand it creates a situation where this technology has the capacity to substantially prejudice the fundamental right to privacy held by employees. It therefore becomes critical to consider the reasons of the employer for the monitoring of the employees electronic communications and question how far they actually need to use these new technologies and how far they merely find it convenient to do so.

Put another way surveillance and data processing has become exponentially more effective and intrusive so it became necessary to look at how the technologies are being used to combat new problems and how far it is being used to deal with problems that already existed and that was already being dealt with, with much less intrusive means.

An example to illustrate this when one looks at the concerns raised around the circulation and display of legal forms of pornography. It should be noted that this has not been difficult to obtain in many workplaces in the form of calendars, magazines and mobile phone content. I am not debating the morals or ethics of having this type of content in the workplace but question how the underlying significance of this problem changed so that the existing methods of dealing with it in the traditional workplace environment needed to be replaced with a much more intrusive system.

New challenges do exist in this paradigm such as the protection of networks against virus attacks and we do not have any historic reference to deal with this.

[2] Regulation of Investigative Powers Act of 2000

1.2. The ILO Code: The standard for workers rights.

In 1996 the International Labour office issued a “code of Practise on the protection of Workers’ Personal Data which protects employees' personal data and fundamental right to privacy in the technological era.[3] These guidelines were published, following three studies on international workers' privacy laws[4].

The general principles of the code are:

- *personal data should be used lawfully and fairly; only for reasons directly relevant to the employment of the worker and only for the purposes for which they were originally collected;*
- *employers should not collect sensitive personal data (e.g., concerning a worker's sex life; political, religious, or other beliefs; or trade union membership or criminal convictions) unless that information is directly relevant to an employment decision and is collected in conformity with national legislation;*
- *polygraphs, truth-verification equipment or any other similar testing procedure should not be used;*
- *medical data should only be collected in conformity with national legislation and principles of medical confidentiality; genetic screening should be prohibited or limited to cases explicitly authorized by national legislation; and drug testing should only be undertaken in conformity with national law and practice or international standards;*
- *workers should be informed in advance of any advance monitoring, and any data collected by such monitoring should not be the only factors in evaluating performance;*
- *employers should ensure the security of personal data against loss, unauthorized access, use, alteration or disclosure; and*

[3] "Protection of workers' personal data," An ILO Code of Practice, Geneva, International Labour Office (1997)

[4] International Labour Office, Conditions of Work Digest: Worker's Privacy Part I: Protection of Personal Data 10 (2) (1991); Worker's Privacy Part II: Monitoring and Surveillance in the Workplace (1993) 12(1); and Worker's Privacy Part III: Testing in the Workplace, 12(2) (1993).

- *employees should be informed regularly of any data held about them and be given access to that data.*

The code does not form international law and is not of binding effect. It was intended to be used "*in the development of legislation, regulations, collective agreements, work rules, policies and practical measures.*"

In order to frame parts of the current debate I include the following questions to try and clarify some of the issues that need further discussion.

1.3. Framing questions.

1. Should employees be guaranteed a certain minimum level of privacy?
2. What does the common law position say about privacy in the work contract?
3. Should employers be required to specifically notify an employee that their emails are being monitored and what their web access or click streams are being monitored?
4. If employers are allowed to read the emails of their employees what right would students and staff at UCT have in this regard?
5. Should the faculty, students and staff have the same privacy concerns and interest?
6. Would the University authorities monitor all the staff and students with the same intensity?
7. Should there be different levels of protection for staff?
8. Should Academic freedom be a consideration?
9. How would the university monitor the staff member's home access without monitoring the non work related parts of the web access and emails?
10. What about the propertization of data stored of the staff member on the computer or network of the university?

Chapter Two – The Current Situation in South African Law

Analysing Employee workplace monitoring from a legislative framework in South Africa requires an analysis of various acts that have an impact in this field and also an analysis on various levels of the constitutional basis to the common law of privacy.

2.1. The South African Labour Relations Act.

The South African Labour Relations Act[5] governs the employment contract and more importantly an employment relationship. This employment relationship has been shown to survive the employment contract[6] The very nature of this employment relationship is not neutral[7] but creates a relationship of subordination.

It also brings into existence a series of rights and duties attributed to each other on an individual and collective basis in relation to each other. In the absence of a series of express or tacit terms most employment contracts default to the common law position and included in this is the employees duty of service, obedience and on the other hand the employers duty to remuneration[8]

2.2. Breakdown of the Employment Relationship

In terms of the LRA then there are three specific reasons that can be used to terminate the employment contract:[9]

1. By virtue of serious misconduct, incapacity or incompetence if it is just and fair to do so;
2. If the conduct of the employee constitutes a material breach of the contract of employment and
3. If the trust relationship between the parties has been broken down irretrievably.

---

[5] National Labour Relations Act
[6] *NAAWU V Borg Warner SA (Pty) Ltd* 1994 ILJ 509 (A)
[7] Davies & Friedland Khan – Freud's labour and the law (1983) 18
[8] See *Golden Cape Fruits (Pty) Ltd v Fotoplate (Pty) Ltd* 1973 (2) SA 642 to 645 for a discussion on what the court would consider a particular custom or trade usage as an implied term of contract
[9] See Jordaan B "Contract of Employment" ,Juta & Co. Ltd 1996

Misconduct implies that the employee did something wrong. The three part test is:[10]

1. Is the rule reasonable and
2. Has it consistently been applied, and
3. Was the employee aware of the rule?

Four requirements must be met before the dismissal of an employee by his employer can be regarded as fair and reasonable

1. The Dismissal must be one in terms of the Labour Relations Act[11]
2. Only employees defined in terms if the labour relations Act is entitled to be protected by the Labour Relations Act
3. The reasons for the dismissal must be substantively fair
4. The dismissal should also be procedurally fair

In terms of this approach the question is: would a dismissal be substantively fair if the employee transgressed the email or internet policy of the employer?

South African employers often also use the issue of avoidance of liability as one of the reasons why they deem themselves the right to monitor the electronic communications of the employee. In terms of South African jurisprudence people that are employed in terms of a contract of "*locatio conductio operarum"* can render their employers liable for unlawful acts conducted in the cause and scope of their employment[12]

But network monitoring tools cannot electronically monitor the employees' intent when for example accessing specific websites. It is therefore critical that employees are afforded some due process right of protection, the right of notice of the violation and some opportunity to be heard. n South Africa the legislative framework that provides for the protection of the rights of employees is found in a number of pieces of legislation.

[10] Schedule 8 7(b)(i) & (iii) of the Labour Relations Act 66 of 1995
[11] Section 186 of the Labour Relations Act of 1995
[12] See PS Atiyah – *Vicarious Liability in the law of Torts,* Butterworths ., London 1967

2.4 A Constitutional approach

On a constitutional level we have section 14[13] of the constitution which states that "*everyone has the right to privacy which includes the right not to have*

1. *Their person or home searched*
2. *Their property searched*
3. *Their possessions searched*
4. *The privacy of their communications infringed"*

For our analysis the right not to have our communications infringed is probably the most important point.

Contrasting this is Section 36(1)[14] of our constitution which allows for the limitation of any right "*only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including*

1. *The nature of the right*
2. *The importance of the purpose of the limitation*
3. *the nature and extent of the limitation*
4. *the relation between the limitation and its purpose, and*
5. *less restrictive means to achieve the purpose "*

This in essence boils down to be free from inclusion and interference from the state and other individuals as defined in the *Bernstein* case.[15]The Constitutional court judgment said "*privacy is acknowledged in the truly personal realm, but as a person moves into communal relations such as business and social interaction, the scope of personal space shrinks accordingly*"[16]

---

[13] Section 14(d) of the South African Constitution , Act 108 of 1996
[14] Section 36 of the South African Constitution , Act 108 of 1996
[15] Ackerman J – *Bernstein & Others v Bester & Others NNO* 1996 2 SA 51 (CC) at ??
[16] In *Investigative Directorate : Serious Economic Affairs v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) the court noted that even if people move away from their "inner core" they still retain the right to privacy and that this right will be limited in so far as it is moves closer or away from the "the intimate personal sphere of the life of human beings"

The *Protea Technology* case[17] illustrates that a constitutional right to privacy should be seen against a backdrop of the limitations clause of the constitution. This involves the balancing of uncovering the truth which is in the public interest against the right to privacy.

Case law seems to be moving in the direction that if a person should have control of the "inner sanctum"[18] he or she should then logically also have control of the "flow of information" about them.

So other than this constitutional framework we also have a whole range of laws that needs to be looked at as they potentially limit the right of privacy in the context of this paper

1. The interception and Monitoring Prohibition Act , Act 27 of 1992
2. The Electronic Communications and Transaction Act, Act 25 of 2002
3. The Regulation of Interception of Communications and Provision of Communication Related Information Act, Act 70 of 2002
4. The National Strategic Intelligence Act as Amended , Act 39 of 1994
5. The National Prosecuting Authority Amendment act, Act 61 of 2000

2.5 The Common law of Privacy:

In South Africa we have a common law right to privacy which is included under the right to privacy which is included under the right to "*dignitas*". This approach in fact is similar to article 12[19] of the universal declaration of human rights, article 17[20] of the international covenant on civil and political rights and of course article 8[21] of the European Convention on human rights.

[17] *Protea Technology Ltd & another v Wainer & others 1997 9 BCLR 1225 (W)*
[18] *Investigative Directorate : Serious Economic Affairs v Hyundai Motor Distributors (Pty) Ltd 2001 1 SA 545 (CC)*
[19] Article 12 of the Universal Declaration on Human Rights – Adopted and Proclaimed by the General Assembly Resolution 217 A(III) of 10 December 1948
[20] The International Covenant on Civil and Political rights – G. A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (NO. 16) at 52, U.N. Doc A/6316 (1996) , 999 U.N.T.S. 171 entered into force March 23, 1976
[21] The European Union Congress No. 108

The original action of"*injuria*" as developed by Roman Jurisprudence is still in use today in South African jurisprudence. It takes a broad view of the action and extends it to cover any situation in which an individual's dignity was unlawfully impaired.

2.6. The Commission for Conciliation Mediation and Arbitration (CCMA) – The Labor Relations Act

Evidence based case analysis of CCMA cases from 1998 to 2005 looking at reported cases that involve computers, internet, email, pornography and computer misuse does not give any reported cases where the CCMA commissioner looked at the issue of the right to privacy of the employee.

As an example in the matter of *Cronje v CCMA*[22] and others and *Dauth v Brown and Weir Cash and Carry*[23] the commissioners only looked at the workplace policies and the norms of our society. To illustrate Mr. Cronje's dismissal was upheld because he distributed racially offensive cartoons on the email network of his employer. The substantive issue of the right to privacy of Mr. Cronje and his expectation of this societal honoring of this right were not discussed at all.

Mr. Dauth's dismissal was upheld after he send anti Semitic comments about management and also attacked management in his emails.

In both these cases the commissioner only dealt with the breach of the workplace policy and in their views this breach was sufficient to be serious misconduct.

In the matter of *Smuts v Back Up Storage Facilities*[24] the dismissal was again upheld as Mr. Smuts downloaded and viewed pornography on the computer using the networks of his employer. Mr. Smuts was the branch manager and as such would have had a higher expectation of privacy of his online actions

[22] *Cronje v CCMA & Others 2002 9 BLLR 855 LC*
[23] *Dauth v Brown & Weir Cash & Carry 2002 8 BALR 837 CCMA*
[24] *Smuts v Back UP Storage Facilities 2003 2 BALR 219 CCMA*

than those of the rest of his staff. In any event again this was found to sufficiently to terminate the employment relationship by virtue of serious misconduct.

In the matter of *Gouws v Score / Price and Pride Furniture*[25] the dismissal of Mr. Gouws was overturned even though it could be proved that he downloaded and viewed pornography on the works computer.
The fact that his employer did not consistently apply the workplace policy to all employees equally was found to be enough to not terminate his employment contract.

2.7. Statutory Issues

2.7.1. The Electronic Communications and Transactions Act, Act 25 of 2002

For the first time in South African Jurisprudence this act creates a doctrine of functional equivalence [26] .This allows for all actions with the exception of two (contracts of sale of property and contracts if marriage) will be equivalent to its real world action. Therefore email which is a fast medium now has the same weight in law as a document and came be used with the same evidentiary value as a document

The employee therefore can contract on behalf of his employer via email and this can lead to a series of fiduciary burdens being imposed on the company. Hence it is important to have a clearly defined email policy publicly available which for example defines who is authorized to contract in behalf if the company.
In terms of the monitoring of employee communications section 25 of the ECT act provides for the protection of personal information collected.

Section 86(2) prohibit the interference with data in *"such a way which causes such data to be modified, destroyed or otherwise rendered ineffective*"

[25] *Gouws v Score/Price and Pride Furniture* 2001 11 BALR 1155 CCMA
[26] Section 22 of the ECT Act 25 of 2002

Section 51 of the ECT act 25 of 2002 provides for a voluntary framework of protection around the collection and storage of personal information.

Section 50 (2) states that the data controller must subscribe to all the principles of the act as a whole as it is not possible to selectively subscribe to some of the principles.

2.7.2. The Interception and Monitoring Prohibition Act, Act 27 of 1992

This act has as one of its general provisions that make it an offense to intercept any communication that will be transmitted over a telephone line or a telecommunications line. It does allow for the direction of the judicatory by way of the application of a warrant based on probable cause, " that a serious offense has been committed or is being or will probably be committed , which cannot be investigated in any other manner and of which the investigation in terms of the act is necessary or that the security of the republic is threatened or the gathering of information concerning a threat to the security of the Republic is necessary

2.7.3. The National Strategic Intelligence Act, Act 39 of 1994.

This Act defines the functions relating to intelligence gathering. The act provided for the "gathering, correlation, evaluation and analysis of domestic, foreign crime and foreign military intelligence by the NIA, SASS, SAPS and SANDF.

These functions are carried out to "identify any threat or potential threat to the security of the Republic or its people"

Section 5 (2) of the act allows for a judge to issue a warrant to collect information that has a bearing on national strategic intelligence.

2.7.4. The National Prosecuting Authority amendment act, Act 61 of 2000

This act authorizes the directorate of special operations to intercept and monitor communications. This is a limited authority in terms of section 28(1) of the national prosecuting authority amendment act 61 of 2000.

The directorate has to be able to show a judge that reasonable ground such as suspicion of an offense and that monitoring is the last resort.

2.7.5. The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

This act regulates the interception of communications, the monitoring of radio signals and radio frequency spectrums and the provision of communication related information. The Act contains a general prohibition [27] against the interception of any communications. Therefore if the employers access the data on the computer of the employee[28] he or she would not be transgressing any provisions of the act. It also regulates the application for interception of communications and provision of communication- related information under certain circumstances. It regulates applications for interception and it regulates law enforcement where interception of communications is involved

Structurally RICA is not limited to the provisions of the act itself but supplemented by a directive, a schedule and four proclamations.
The Directive prescribes the technical and security requirements related to the interception and routing of communications.

Schedule A deals with fixed line telecommunications operators

Schedule B & C deals with mobile cellular providers and internet service providers respectively.

There are a number of classes of exceptions that could be raised against the implementation of this act, namely

[27] Section 2 of the act states "No person may intentionally intercept or attempt to intercept or authorize or procure any other person to intercept or attempt to intercept at any place in the republic any communication in the course of its occurrence or transmission"
[28] As was the case of *Jacqueline Bamford & Four Others v Energizer (SA) limited (CCMA) 2001 – 6-22*

2.7.5.1. General Exception

1. The authorized person who executes an intercept direction or assist with the execution thereof may intercept any communication to which such interception direction relates[29]
2. Any communication may be intercepted by one of the parties of that communication provided such communication is not intercepted for the purpose of committing and offence[30]
3. Any person may intercept any communication if one of the parties to the communication has given their prior consent to such interception in writing[31]
4. Any person may intercept any indirect communication in the course of carrying on a business provided that certain requirements are met[32]

2.7.5.2. Business Exception

The Business exception allows employers to intercept communications of their employees without having to get their permission first. The act defines a number of conditions that needs to be met for the interception to be deemed "lawful"

1. Sec 6(1) of the act allows for indirect communication to be intercepted if:
    a. It relates to transaction being entered into in the normal course of the business
    b. It otherwise relates to the business
    c. It otherwise takes place in the course of that business

2. Section 6(2) makes the interception of the indirect communication "lawful" if
3. The system controller gave his consent or his implied consent[33]

---

[29] Sec 3 (a) and (b) if The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

[30] *S v Kidson 1999 1 SACR 338 (W)*

[31] Section 5(1) of The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

[32] Sec 6(1) and (2) of The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

a. The communication is intercepted for a legitimate purpose with is limited to the
b. Establishing existing facts
c. Investigating the unauthorized uses of the telecommunication system
d. Securing effective operation of the system

4. The use of the telecommunication system concerned is provided for wholly or partly in connection with that business[34]
5. If the system controller made reasonable efforts to inform individuals in advance that their indirect communications may be intercepted or if such indirect communication[35]is intercepted with the express or implied consent of the person who uses the system

[33] Sec 6(2)(a) of the Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002
[34] Sec 6(2)(c) of the Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002
[35] Sec 6(2)(d) of the Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICA), Act 70 of 2002

Chapter Three The Current European Union Position

When considering the protection of the employee's electronic communications and personal information the analysis invariably starts with the right to privacy. Seminal to privacy is the social policy agenda[36] of the European commission which has as its main objective the development and respect of fundamental social rights as a key component of an equitable society and of respect for human dignity, which includes the protection of personal data of individuals in the employment relationship.

3.1. The Right to Privacy in the European Union.

The Right to Privacy is a basic human right under the 1948 Declaration of Human Right[37] and the 1981 EU convention on Human rights.[38] This is the so called Article 8 Right.[39] Since the early eighties member countries have depended on these rights coupled with *"fair information Principals* "to govern the use of personal data.

The Council of Europe Convention for the Protection of human rights and fundamental freedoms (ECHR)[40] was adopted in 1950 shortly after the universal declaration of human rights of the United Nations and it was drafted under the auspices of the Council of Europe. What is important for the protection of the rights to privacy of the employee is primarily Article 8 of this Convention and it is further explained as:

Article 8 – Right to Respect for Private and Family life[41]

1. *Everybody has the right to respect for his private and family life, his home and his correspondence.*

[36] Commission paper (COM2000/379final. 28.06.2000)
2.Article 12 of the Universal Declaration on Human Rights – adopted and proclaimed by the General Assembly Resolution 217 A (III) of 10 December 1948
3. European Union 108 Congress
[39] Article 8 of the European Union 108th Congress in 1981
[40] International Covenant on Civil and Political Rights – G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No.16) at 52, U.N. Doc A/6316 (1996), 999 U.N.T.S. 171 entered into force March 23 1976
[41] Article 8 of the European Union 108th Congress in 1981

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 interest of national security, public safety or the economic wellbeing 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.*

Out of these conventions declarations and recommendations the following three fundamental ideas become self evident and they form the basis of the so called *fair information principles*.

1. Minimalism/Proportionality/Efficiency.
    a. This principle means we collect only minimal data and we keep that data up to date and we maintain data security.
2. Information openness/Disclosure/Awareness.
    a. We will tell you who we are, what we have collected and why. We will do this on a one on one basis or on a one to many basis in the same way as the data is collected.
3. Responsibility/Accountability
    a. We agree to no secondary use of the data unless by authority of law and we will respond to the inquiries of the data subject.

There are three fundamental European Union directives that deal with the protection of personal data.

- Directive of 24 October 1995[42] on the Protection of personal data and on the free movement of such data.
    - This directive has six principals that govern the collection of data
    - It also prohibits the collection of specific types of data such as race, ethnicity, religious beliefs, political opinions and health data. It only allows the collection of this data under very specific conditions and creates a series of obligations to the collectors to have specific security in place.

[42] Directive 95/46/EC

- Directive 97/66/EC[43] concerning the processing of personal data and the protection of privacy in the telecommunications sector
- Directive of 12 July 2002[44] concerning the processing of personal data and the protection of privacy in the electronic communications sector.

How the European Union directives is implemented in the various member states in terms of a constitutional right to privacy , its civil law implementation, its implementation in terms of employment law and data protection law is not always equal between the member states. An example of this is contrasting the "Nikon" case from France and the decision of the Spanish Tribunal Superior de Justicia de Cataluna in case A5/3452. On substantively the same facts the French court upheld the right to privacy of the employees private files stored on the employers computer system whilst the Spanish court decided that employers have the right to read all information stored on their computer system.

3.1.1. The United Kingdom Implementation

The United Kingdom situation is nuanced in that it deals with the issue of work place privacy in much the same manner at the United States but at the same time it also forms part of the European Union and therefore also has the basic safe guards in law that is has to implement as a member state of the European Union. It is also unique in that this is the only country that forms part of the European Union that does not have a fixed written constitution. In point of fact in the United Kingdom parliamentary sovereignty exists in that "a convention right "does not override legislation of the United Kingdom Parliament which cannot be interpreted compatibility with it There is no statutory provisions requiring consultation with workers or worker representatives about monitoring and surveillance other than those that require consultation with safety representatives appointed by a recognized trade union or in their absence employees themselves or elected "representatives" of employee safety. The Draft Code of Practice on the use of personal data in employer/employee relationships recommends that

[43] Directive 97/66/EC
[44] This directive amends the telecommunications directive 97/66/EC

employees should access the impact of the proposed monitoring in consultation with trade unions or other employee representatives.

The Human Rights Act of 1998 [45] implements Article 8 of the EU Convention on Human Rights into law in the United Kingdom and by this implementation for the first time brings the United Kingdom closer to a generic concept of "constitutional rights" by giving effect in a domestic law to the rights and freedoms guaranteed by the European convention on Human Rights.
The United Kingdom implemented EU directive 95/46/EC [46] with the Data Protection Act (DPA)[47]. This Act came into force in 2001. It was amended by the Freedom of information Act of 2000.[48]

The 1998 Data Protection Act (DPA) places obligations on those who collect data and gives rights to those who are the subject if that data. It requires those processing data to comply with enforceable principles[49] of good information handling practice which in turn requires personal data to be collected fairly and lawfully , kept accurately and retained no longer than necessary. The Act requires specific protection measures in place to limit unauthorized access to and the processing of the data and holds the data collector responsible for this by a range of civil and criminal sanctions.
The 1998 Data Protection Act (DPA) also has a comprehensive series of Codes of Practice which deal with the implementation of a number of issues pertaining to workplace monitoring.

[45] The Human Rights Act of 1998
[46] This Directive has become known as the Data Protection Directive
[47] The Data Protection act of 1998. This act came into force in 2001
[48] The Freedom of Information act 2000
[49] A lists of principles include the following

a) Personal data should be processed fairly and lawfully
b) The data should be obtained for only one of more specified lawful purpose
c) The data should be adequate , relevant and not excessive in relation to the purpose for which it is processed
d) Accurate
e) Not kept longer than necessary for a specific purpose
f) processed in accordance with the rights of the data subjects
g) Secure
h) Not transferred to a country where there is not a similar juristic framework to protect the data

As an example the code sets out that monitoring should be proportionate and not unduly intrusive in the individual's privacy. The code for example refers to the employee's right to expect a degree of trust from the employer to be given reasonable freedom in determining his own actions without constantly being monitored. The code also contains a number of benchmarks that can be used to measure monitored activities.

The Benchmarks are divided into:

1. Those apply to all monitoring activities, and
2. Those that apply in relation to each email, internet and telephone monitoring,

The Code includes the following general benchmarks with relates to all monitoring activities

1. *Identify who can authorize monitoring and make sure that they are aware of their responsibilities under the DPA*
2. *Establish a specific business risk for which the monitoring is taking place*
3. *Access the impact of monitoring on pricey , relationship of trust and other legitimate rights of staff and make an assessment of the effectiveness of monitoring in reducing the risk identified and document that assessment;*
4. *Do not introduce monitoring in which any adverse impact to employees is out of proportion to the benefits for the employer;*
5. *If comparable benefits can reasonably be achieved by another method with less adverse impact, adopt the alternative method*
6. *Consider consulting trade unions or other representatives about the need for monitoring;*
7. *Target any monitoring on those areas where it is actually necessary and proportionate to achieve the business purpose as the monitoring of all staff will not be justified if the purpose of the monitoring is to address that risk that is posed by only a few;*
8. *Keep those who have access to personal information obtained through monitoring to a minimum;*

9. *Make all staff aware that monitoring is taking place and of the purpose for which personal information is collected unless in exceptional circumstances including;*
    a. *The monitoring is to check whether employees are complying with the employers rules and standards of conduct; and*
    b. *It is carried out for the purpose of preventing or detecting crime or the apprehension or prosecution of offenders; and*
    c. *Informing staff would be likely to prejudice this purpose; and*
    d. *The standards set out by this code for covert monitoring are complied with*
10. *Do not use personal information collected through monitoring for purposes other than those for which the monitoring was introduced and staff told about it;*
11. *Remember that information collected through monitoring can be misleading, misinterpreted or even deliberately falsified as well as being inaccurate because of equipment malfunction*

The Code also makes the following recommendations in relation to benchmarks that should apply to employers monitoring employees' communications:

1. *Establish a policy on the use of electronic communications which clearly sets out eh circumstances in which employees may or may not use the employers' electronic communication facilities.*
2. *Limit the scope of monitoring to what is strictly required to reduce the intended risk*

The Privacy and Electronic communication (EC Directive) Regulation of 2003 [50]implement European Union directive 2002/58/EC[51] in the United Kingdom. This provides a framework for the protection in law for the use of cookies on websites and to the issue of direct marketing practices.

[50] Privacy and Electronic communication (EC Directive) Regulation of 2003
[51] This directive deals with secure data transmission and electronic commerce.

3.1.2. The interplay between the data protection directive and the telecommunications data protection directive

The Data Protection Directive[52] and the Telecommunications Data Protection Directive[53] seem to diametrically oppose what each of them does.
On the one hand the Data Protection Directive creates a framework for the protection of personal data and on the other hand the Telecommunications Data protection provides a framework under which it is possible to monitor and intercept the electronic communications of the employee. The implementation of the telecommunications data protection directive does not show how the implementation of this is to happen in terms of data privacy and also in terms if the employment contract.

Article 5(1)[54] of the directive requires member states to ensure via national regulations the confidentially of communications by means of a public telecommunications network and publicly available telecommunications services.

The directive permits two exceptions to the principles;

1. Article 5(2) provides that article 5(1) shall not affect any legal authority to record the communication in the course of a lawful business practice for the purpose of providing evidence of a commercial transaction
2. Article 14(1) allows member states to adopt legislative measures to restrict the scope of the obligations and rights provided for in Article 5 when those restrictions constitute a necessary measure to safeguard inter alia
    a. The prevention, investigation, detection and prosecution of criminal offenses or
    b. The Unauthorized use of the telecommunications system

[52] 95/46/EC
[53] 97/66/EC
[54] The Telecommunications Data Protection Directive 97/66/EC of 15 December 1997

3.1.3. The Regulation of Investigatory Powers Act of 2000.

The Regulation of Investigatory Powers Act of 2000 [55]creates a legal framework for workplace monitoring in the United Kingdom. This act implements the European Unions Telecommunications Data Protection Directive.[56]

In the matter of *Halford v United Kingdom*[57], the plaintiff brought suit in the European Court of Human rights that her rights where breached by her employer when he monitored her telephone conversations. The court found that the absence of prior warning about the monitoring had created an expectation of privacy with the plaintiff and accordingly found for her.

Section 1 of the Regulation of Investigatory Powers Act Of 2000 makes it unlawful for a party without lawful authority to intentionally intercept a communication in the course of its transmission.

Section 3 provides for permission of the intercepting party beliefs that both parties consented to the interception.

According to this section the employer would only be able to intercept their employees' communications if they have the consent of both parties.

Section 1(6) of The Regulation Of Investigatory Powers Act Of 2000 gives the owner of a private network the ability to lawfully monitor the network subject to some limits.

So an employer would be indemnified if he /she

1. Has the right to control the use or operation of the system
2. He has the express or implied consent from the operator to conduct interceptions.

[55] The Regulation of Investigatory Powers Act of 2000
[56] EU Directive 97/66/EC
[57] *Halford v United Kingdom 1997 73/1996/692/884*

3.1.4. The Telecommunications (Lawful Business Practice) (Interception of communications) regulations 2000

The Telecommunications (Lawful Business Practice) (Interception of communications) regulations 2000[58] allows for a business to monitor or record all communications transmitted over its network without the employees consent.

The regulations also authorize monitoring without consent for the following [59]

1. *Establishing the existence of facts relevant to the business*
2. *Ascertaining compliance with the regulatory or self regulatory practices or procedures relevant to the business*
3. *Ascertaining or demonstrating standards which are achieved or ought to be achieve by those using the system*
4. *Preventing or detecting crime*
5. *Investigating or detecting unauthorized use of the business telecommunication system*
6. *Ensuring the effective operation of the system*

Section 2(b)[60] says that all monitoring should be shown to be relevant to the employers business

Section 3(1) (b) and (c) [61]authorizes businesses to monitor but not to record the communications transmitted over the system without employees consent for the following purposes

1. *Checking whether or not the communication is relevant to the business*
2. *Monitoring call to confidential counseling or support help lines run free of charge*

---

[58] S(1) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699

[59] S (3) (1) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699

[60] S (2)(b) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699. Relevance in this context is widely defined and includes "any communication relating to the business , which takes place in the course of carrying on that business"

[61] S(3)(1)(b) & (C) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699

Section 3(I) and (ii)[62]authorizes public authorities to monitor and record communications in the interest of national security
These regulations require businesses to *"make all reasonable efforts*" to inform the users of the telecommunications system that interception might occur.

Once the data has been collected it falls under the control of the Data Protection act of 1998[63]. In terms of the provisions of this act employees should be informed before hand about the data collection and in the absence of consent the employer has to as a minimum be able show that the information that has been collected about the employee is:

1. *Necessary for the performance of the employment contract*
2. *It is vital to the interest of the employee*
3. *That the information collected falls within one of the statutory exemptions*

Employers should all have an email, internet use and telephone policy and this should be explained to all employees and training provided on the implementation of this to employees. It should further contain instances under which employees explicit consent to process specific data is required.

Chapters 60 to 61 of the 1998 Data Protection Act (DPA) have a series of sanctions for both parties for non compliance to the provisions of the act.

3.2. The French Approach to Employee Privacy.

Working from home has become common for certain categories of employees in France especially after the reduction of the working week to 35 hours. This type of working relationship creates a whole new spectrum of uncertainty , for example the growing practice of requiring employees to stay home at certain hours of the day so that they are at the disposal of the employer and ready to

[62] S (3)(1)(a)(ii) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699
[63] Data Protection Act of 1998

perform their job if needed (*heures d' astreuntes*). This type of change keeps blurring the definitive lines between the traditional work time and private home time.

There are three seminal laws that frame the issue of workplace monitoring in the French Republic.

1. The Law on Data Processing and Liberty which regulates all automated treatments of data that can identity individuals.
2. The 1970 amendment to article 9 of the French Civil Code[64] protecting the right to respect for private life.
3. The 1992 amendments to the French labor code[65] for the protection of individual liberties in the enterprise.

These three amendments expand the fundamental principles of the 1978 Law [66]and the 1981 Convention 108 of the Council of Europe.

The rights of workers are protected both procedurally and substantively.

Section L432 – 2 – 1[67] of the French labor Code requires that employers should inform and consult with the workers councils and other elective representatives of the workers in advance of any decision to modify any method of monitoring employee activities.

The labor code has also applied the procedural requirements of the law on Data Processing and liberty to the workplace by requiring that employees are informed in advance of any automated treatment of information that can identify an employee and other automated techniques of professional evaluation.

[64] Civil Code Statute 70 – 643, July 17, 1970
[65] Loi no. 78 – 17
[66] Law 78 – 17 of 6 January 1973 "Loi relative 'a L'informatique, aux fichiers et aux liberte's"
[67] Inserted by law 92 – 1446 of December 1992

The employee should be told if the data is being collected is optional or mandatory in terms of other legislation and be given the opportunity to correct any discrepancies with such data.

Section L 121 – 8 of the labor code says that no data concerning the employee or the potential employee may be collected unless the employee is informed in advance of this. The employer should also inform the CNIL about the monitoring if it will result in personal data being collected.

The substantive protection for workers against electronic monitoring stems from the 1992 Law Aubry[68] and implements article 9 of the civil code by the courts. The Penal Code also incorporates some protection of employees against employers monitoring their electronic communications.[69]

Section L 722-35 of the labor Code states that limiting the rights of the employee should be proportionate to the aim pursued and in "*Good Faith*". Similarly Article 226 – 15 of the Criminal Code allows employees to intercept email if they can demonstrate that this is justified for reasons of security.

The Tort of privacy was first recognized in France in 1858[70].
Article 9 of the civil code gives leeway to judicial action of protection of privacy of the individual "*Everyone has a right to respect for his private live* "

Section L 120 – 2 states "*No one may place restrictions on the rights of person and individuals or collective liberties which are not justified by the nature of the task to be accomplished and must be proportional to the importance of a legitimate interest."*

[68] Aubry law 31 December 1992
[69] Penal Code Article 368
[70] *The Rachel Affaire – Judgment June 16th, 1858*

3.2.1. The use of the data that was collected

Under what conditions and to what extend may employers use collected data in order to justify the disciplinary actions and dismissal?

On this point the Cour de Cassation is divided. The Social Chamber's position is that any collection of personal data that did not comply with all the relevant legal requirements is unlawful and may not be used.

This position in French jurisprudence has as a result led to the rejection of the use of hidden video surveillance as grounds for dismissal of an employee.

The Cour de Cassation[71] in one case even rejected the dismissal of an employee where the video surveillance clearly showed the employee stealing from the register[72].

In the matter of *Nikon France and Frederic Onof*[73] the Cour de Cassation rejected the employers accessing the private emails of Frederic and found for him. The court held that workers have the right to respect for his intimacy and privacy even during working hours and at the workplace which also covers the privacy of his correspondence. According to the court this implies that the employer cannot have access to the contents of personal messages, either sent or received by the employee, through an information system made available to the employee for his job even if the employer would have prohibited non- professional use. It is important to note that this case was decided under both Article 8 of the European convention on Human Rights and also Article 9 of the French Civil Code.

The Cour de Cassation showed in its judgment that it considered this case to be a matter of striking a balance between the employer's power to control and the employee's right to privacy

[71] www.courdecassation.fr
[72] *Cas. Soc. Nov 20,1991 Droit Social 1991, No. 28 also see Cas, Soc.May 15,2001 Cahiers sociaux de barreau de Paris 2001 No. 312*
[73] *Onof" v Nikon France Decision No. 4164, October 2, 2001 (99-42-942)*

In contrast the Criminal Chamber takes a different view of the admissibility as evidence of unlawfully collected personal data. In 1994 it ruled that evidence cannot be excluded simply because the manner of collection did not respect the relevant legal requirement. This ruling is similar to the established principle of "*freedom of evidence*" in criminal proceedings.

So it appears that the French Judiciary has taken a position to defend: Human Rights "as opposed to "worker Privacy Rights".

It is important to understand that although the Cour de Cassation forbade the employer from opening private emails, it did not forbid the employer from imposing a disciplinary sanction on employees who breach a prohibition on private use.

French Labor law establishes three types of sanction according to the gravity of the fault committed by the employee

1. A reprimand
2. A temporary suspension and
3. A dismissal[74]

In practice the occasional use of the employers system is tolerated but in terms of French law the regular use of the employers' facilities for private purposes will allow the employer to dismiss the employee[75]

The disciplinary action of dismissing the employee for continues online gambling was proportionate to the extent of the private use made of the internet facilities.

[74] French Labor Law establishes 3 grounds for dismissal
1. True and serious cause (Cause Re elle Et Serieuse)
2. The Serious Fault (Faute Grave)
3. Very Serious Fault (Faute Lourde)

[75] *Cas. Soc. Mar 14 2000 JCP 2001 11 10472*

In order to terminate a fixed term contract before its term the employer must show serous fault but to terminate an open ended employment contract true and serious cause is sufficient.

3.2.2. The National Data Protection Authority

The National Data Protection Authority[76] ('CNIL") has drafted some principles with regard to cyber surveillance

1. Transparency and loyalty: If a copy of a message is made, the duration of conversation should be communicated to employees; if firewall are created , employees should be aware of the significance of the information collected and the duration of conservation thereof; employees should be informed of the specific hierarchical authorities in the company which can perform specific measures of surveillance;
2. Website visiting for private purposes must be allowed; monitoring a posteriori is unlawful; surf control must be performed without individual analysis of consulted websites or of the content thereof; in any case employees should be made aware of the fact that they are subject to monitoring.
3. A prohibition to use email for non professional purposes is unrealistic and disproportionate; Monitoring of use is, however acceptable; but it may not concern content of messages; as far; as incoming messages are concerned (from outside the company) ,every indication of a private nature of the message should render monitoring by the employer illegitimate;
4. Thrust through negotiation; the use of internet for non – professional purposes and the introduction of monitoring systems should be the subject of negotiation between the employer and workers, both on sectoral as well as on enterprise level; at the level of the enterprise, discussions must take place through existing appropriate channels, such as the works council or the health and safety committee.

[76] www.cnil.fr

A 1992 report by influential labor and social lawyer Gerard Lyon – Caen[77] for the ministry of labor advocates greater emphasis on human dignity. The report concluded that the United States approach to workplace monitoring has created a situation where the employee was viewed as an object of measure rather that as a person. Control of the workers was exercised internally to make the worker more transparent thus robbing the worker from his or her rights of human dignity and identity. This was far removed from the traditional and legal notion of subordination implied by the employment contract.

[77] Gerard Lyon-Caen, Les Libertes Publiques Et L'emploi: Rapport Pour Le Ministre du Travail, de L'emploi et de la Formation Professionnelle, 1992

Chapter Four – The United States Approaches, Legislation and Protections.

4.1. Background to employee privacy in the United States

Analysing employee privacy in the United States requires a detailed analysis on various levels from a Constitutional position, Federal position, State position and even the Common law approach to Tort of Privacy.

The basis of employee privacy in modern jurisprudence is found in a report issued by the privacy commission[78] in 1977. This report broadly delineated a series of ideals to be achieved and ways of achieving these standards in the employment context.

4.1.1 Ideals.

The report recognized that employers collect a broad range of information on workers. It also tried to focus on delineating lines of fairness on the collection and the use of employee information. Finally the report also acknowledged that there were a lot of changes since the development of the common law employment norms.

4.1.2 Way to achieve the initial objectives.

The report strived to minimize the intrusiveness of employers in the hiring process by reducing the practice of allowing employers to obtain information about the employee to what it is appropriate. For example it would not be appropriate to collect credit information about an employee if that employee would not be in a position of trusts and works with the employers cash systems whereas it would be appropriate if the employer is in the financial services sector to collect credit information about it employees.

The report also strived to maximize procedural fairness by reducing the use of arrest information to situations where it is required.

[78] The commission was convened pursuant to the Privacy Act of 1974

Over ally the policy group pursued the goal of creating a legitimate and enforceable expectation of confidentiality in employment contracts.

4.3. Constitutional approach to employee privacy.

Perhaps the most pervasive approach to employee privacy in the United States is found in fourth amendment jurisprudence.

The fourth amendment states "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"* [79]

This amendment has throughout American Jurisprudence developed a right to privacy. Of course each application for the protection under this right to privacy needed to be looked at individually.

4.4. The Initial test to privacy protection.

The initial test was called the "*open fields' doctrine*" [80]and essentially it was a framework developed through case law where the courts tried to protect the individual in his home and that got extended to protection in his "curtilage" which was interpreted as the immediate area around the individuals home. There appears to be three broad categories where the courts failed to find a societal recognition of a privacy expectation namely Physicality, Place and Information. In modern work environments of course the privacy of information has become most important.

[79] United States Constitution , Fourth Amendment 1

[80] The open fields' doctrine is a United States legal doctrine created judicially for the purpose of evaluating claims of an unreasonable search by the government in violation of the fourth amendment of the United States Constitution.

4.5. The Current Constitutional approach to evaluating privacy protection claims.

This approach fell away when the Katz doctrine was adopted in 1967. This doctrine simplified fourth amendment jurisprudence tremendously because Potter Steward J in his judgment [81] said that

- The court had an obligation to protect the person and not the place.
- The second important issue that comes from this Judgment is Harlan J whose judgment created a two part test to privacy *"My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable"*.[82]

4.6. The Federal Approach.

On a Federal Level the ECPA (Electronic Communications Privacy Act of 1986) [83] prohibits the intentional interception of any electronic communication. Civil and criminal penalties are provided for in this act. As an example an employer is entitled to monitor his computer networks for business purposes. The employer can therefore view employee emails either in transmission or stored on a server. The employer may not monitor purely personal calls and emails but the system allows the employer to monitor these initially to see if they are personal or business related.

Also an employer may intercept communications where there is actual or implied employee consent. In practice consent has been found where the employer merely gives notice of monitoring[84]. Mere knowledge that the employer has the capacity to monitor was found not to be enough to constitute consent[85].

---

[81] *Katz v United States, 389 U.S. 347 (1967)*
[82] Harlan J Concurring Opinion – *Katz v United States 389 U.S. 347 (1967)*
[83] The Electronic Communications Privacy Act of 1986 U.S.C. 2510 - 2520
[84] *Berry v Fink 146 F 3rd 1003 DC Circuit Court 1998*
[85] *Watkins V L.M. Berry & Co. 04 F 2nd 577 582 11th Circuit Court 1983*

Two sections of this amended act are important to workplace privacy, the Wiretap Act and the Stored Communications Act. The Wiretap Act[86] prohibits the interception of any electronic communication. This applies to the communication during its transmission and not to when it is stored on a server[87] but with the exceptions as discussed above.

The Stored Communications Act[88] prohibits the accessing of electronic communications where it is stored on the server. This section generally exempts the system provider and if as in most cases the systems provider is also the employer it allows the employer to access the stored communications. It is illegal for an employer to access the communications of an employee that is stored on a commercial server as in the case of the *Mt Olive Lutheran Church Inc. v Fischer*[89]

4.7. Employee Privacy Protection of Federal Workers.

The United States Supreme Court in *O'Connor v Ortega*[90] recognized that federal employees may have a legitimate expectation of privacy at their place of employment and that they do not loose their fourth amendment right to privacy just because they work for the United States government

Government employees have a stronger claim to protection against electronic monitoring and surveillance than private sector employees. A key issue in cases of governmental warrants for privacy is whether the employee had a "reasonable expectation of privacy" in relation to the act in question.

This amendment applies only to government action and not to the actions of private employers.

---

[86] 18 U.S.C 2511
[87] *Fraser v Nationwide Mutual Insurance Co. 352 F 3rd 107 (3rd Circuit 2004)*
[88] 18 U.S.C. 2701
[89] *Fisher v Mt. Olive Lutheran Church Inc. 207 F. Supp 2nd 914, 924 (W.D. Wis. 2002)*
[90] *O' Conner v Ortega 1987 107 US 1492*

In the United States Court of Appeals for the 4th district in the matter of *US v Simons*[91] the court dealt with the issue of Internet access. The government agency that Simon worked for notified all employees that it would "Audit, inspect and or monitor" employees use of the Internet including file transfers, all websites visited all "email messages" as deemed appropriate. The court held that the agencies written policy placed on the employees' notice board placed the employee on notice that his Internet activities would not be private and therefore the employee has no reasonable expectation of privacy in any downloaded computer files.

4.8. Other Federal legislation that could have an impact on employee privacy protection.

The National Labour Relations Act (NLRA)[92] is also part of the mosaic that needs to be looked at when considering the issue of electronic monitoring as an employee's communications by email could be construed as a "concerted Activity" and therefore subject to the protects of the act. Disciplining an employee for complaints send using the email system has been found to be a violation of the NLRA.[93] It is also important to apply the electronic monitoring policy and the implementation of disciplinary steps of the company consistently to avoid discrimination claims that could result in the unequal application of computer and email policies[94]

The collection of financial information about applicants and employees is statutorily addressed in the fair Credit reporting act.[95] In *Zamora v Valley Federal Savings and Loan Association*[96] the 10th Circuit court of appeals affirmed a judgment against an employer for obtaining under false pretences credit information on the spouse of an employee in order to make a determination about the trustworthiness of the employee.

---

[91] *US v Simons 206 F 3rd 398 – 401 (4th Circuit 2000)*
[92] National Labour Relations Act 29 U.S.C. 151 - 169
[93] *Timekeeping Systems Inc. 323 NLRB 244 (1997)*
[94] *Logan v Caterpillar Inc. 245 F 3rd 912 (7th Circuit 2001)*
[95] Fair Credit Reporting Act 15 U.S.C. 1681
[96] *Zamora v Valley Federal Savings & Loan Association 55 USCW 2469 (10th Circuit 1987)*

The Americans with Disabilities Act[97] protects the use of medical information of all applicants for a job and employees. It creates a framework around the use of personal information and limits the access and disclosure of this type of information with a range of civil and criminal sanctions.

There is also the dimension that if an employer monitors the employee's emails it could place the business in a position where it is legally required to certain duties. In American Jurisprudence the most obvious obligation on the employer would be the employer's duty to keep the workplace free from harassment as mandated by Title vii of the civil rights act of 1964[98].

The Patriot Act[99] is not discussed in this paper on Workplace communications monitoring as this act was not intended to be used for this purpose even though it creates a framework for electronic monitoring. Secondly also this act is not permanent and when it expires at the end of its current term the situation in jurisprudence reverts back to its current framework in employee privacy rights.

The EEPA Act, The Employee Polygraph Protection Act[100] also is not discussed as it only is pertinent to this debate in so far as it regulates the use of polygraph testing on federal workers.

Even with this framework in place, United States courts have taken widely divergent positions in cases that involve employees and the use of email and internet at work. It appears that government employees enjoy a higher degree of work place privacy than private employees

4.9. Employee privacy protection in state law

On a State level, forty eight states and the District of Columbia have statutes that are similar to the ECPA act. Thirteen states require the consent of both

[97] Americans with Disabilities Act of 1990
[98] Title VII of the Civil Rights Act of 1964
[99] The Uniting and Strengthing America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
[100] 29 U.S.C. 2001 - 2009

parties. Most of these state bills only apply to the monitoring of telephone and wire communications and do not extend to other forms of electronic monitoring and surveillance. Connecticut[101] and Delaware[102] have statutes that require employers to give notice in writing before engaging in electronic monitoring. Employees in Delaware need to acknowledge receipt of notice of monitoring.[103]

The California state law [104] has held that the right to privacy applies to private as well as governmental employees. The employer must show" a compelling intent" to justify any intrusion into the privacy rights of the employee.

However the California Supreme court in *Flanagan v Epson America* [105] refused to apply that right to privacy to the employees email. The court suggested that the extension of a right to constitutional privacy was for the legislature and not for the judiciary.

4.10. The Common Law Tort of Privacy Approach to Employee Privacy rights.

The United States Tort law implementation of privacy in the workplace
The American tort law of invasion of privacy[106] much like a crossing holds four different theories of where liability can reside:

- Placing a person in a false light,
- The misappropriation of a persons name or image,
- The publication of private facts, and
- The unreasonable intrusion into the seclusion of another.

Looking at the four legs of this tort is appears that an employer can avoid liability against the first three positions if he does not disclose private information collected while monitoring the employee. Against this an

[101] Conn. Gen. Stat. 31 – 48d
[102] Del. Code.Ann.tit. 19 705
[103] Del. Code.Ann.tit. 19 705
[104] California Penal Code Section 631 - 632
[105] *Flanagan v Epson America No BC 007036 (Cal.Super. Ct. Mar 12, 1991).*
[106] Restatement of Law, Second. Torts, 652B (1976)

employee would succeed if he could show that the intrusion was highly offensive to a reasonable person.

The Tort of unreasonable intrusion has three elements that need to be looked at, an "*intrusion"* that is "*highly offensive* "to a *"reasonable"* person.

In *Smyth v Pillsbury Co*,[107] the court found that an at will employee[108] has no reasonable expectation of privacy in the contents of an email voluntary sent on an employers email system, In this case the employer had given assurances to its employees that the contents of its email communications would remain confidential and privileged.

The court reasoned that once an employee communicated with a second person over an email system internal to a company any reasonable expectation of privacy is lost and even if such an employee had a reasonable expectation of privacy, the interception of such an email would not be considered "*Highly Offensive*"

What is also interesting in this matter is that the court was not swayed at all by the fact that the employer had represented to the employees that their emails would be held as confidential and that their emails would not be used as grounds for dismissal.

Similarly in *Garrity v. John Hancock Mutual Life insurance Company*[109], the plaintiffs where terminated when their employer found sexually explicit emails in their email folders. The plaintiffs led evidence that their emails where private because the emails where behind a password system and in personal folders. Also that it was part of the security system of the company to have passwords on every access point to the system and finally that the emails were stored in folders marked personal. The court rejected this reasoning

[107] *Smyth v Pillsbury Co. 392 1996 US*
[108] At will employment is an employment relationship in which either party can terminate the relationship with no liability if there was no express contract for a definite term governing the employment relationship
[109] *Garrity v John Hancock Mutual Life Insurance Company 2002 WL 974676 (D Mass)*

because the employer has an email policy that all information on the companies system was the company's property and would be subject to audit.

In the matter of Mac *Claren v Microsoft Corp*[110] the court found that Mac Claren had no reasonable expectation to privacy even though the contents of his "private folder" were protected by two passwords. The court found that the files were stored on a company owned server and send on a company owned network and therefore the emails could have been intercepted at any time.

Other cases reveal that the *Smyth*[111] and *Garrity*[112] cases are not anomalous in American jurisprudence. *Mac Claren v Microsoft Corp.*[113] *Muick v Glenayre Electronics*[114] and *Thygeson v U.S Bancorp*[115] all show that if the employer has an explicit computer and email "no privacy policy" then the employee will not succeed in a invasion of privacy action.

Analyzing cases that survived summary judgment on privacy claims from the plaintiff there is was generally:

- No notice of monitoring given, and or
- That the company had no email and internet policy was in place and or
- That the emails were accessed on systems outside the ownership of the employer as in *Fischer v Mt Olive Lutheran Church*.[116]

[110] *Mac Claren v Microsoft Corp. 1999 WL 339015 (Tx. Ct. App. 5th District May 28, 1999)*
[111] *Smyth v Pillsbury Co. 392 1996 US*
[112] *Garrity v John Hancock Mutual Life Insurance Company 2002 WL 974676 (D Mass)*
[113] *Mac Claren v Microsoft Corp. 1999 WL 339015 (Tx. Ct. App. 5th District May 28, 1999)*
[114] *Muick v Glenayre Electronics 20 F 3rd 741 (7th Cir. 2002)*
[115] *Thygeson v US Bancorp 2004, WL 2066746 (Dr. OR)*
[116] *Fisher v Mt. Olive Lutheran Church Inc. 207 F. Supp 2nd 914, 924 (W.D. Wis. 2002)*

Chapter five – Conclusion

A desirable legal position between employers versus employee rights would allow both parties to achieve some sort of balance in the matter of whether it is possible for an employer to monitor the electronic communications of the employee and how intrusive the monitoring should be. It should also contain guidelines balancing about Quantitative controls and Procedural controls.

5.1.1. Qualitative Controls

The three basic qualitative principles should be expressed as follows:

1. The principle of confidentiality should be expressed in the employment context as a norm requiring that the personal data collection of the employees or job – seekers should be regarded and treated as confidential to them.
2. The principle of proportionality should be used so that the extend of the data collection and analysis should be not more proportional to the need to achieve the purpose for which the data is being collected.
3. The principle of necessity should be articulated as a requirement so that in sensitive situations the collection of data is only in the manner necessary to achieve the end result.

5.1.2. Procedural Controls

Procedural Controls should be expressed as follows:

1. The principle of notification, access and verification should be guaranteed so that work seekers or employees have the opportunity to look at the data that is held about them and are able to fix any problems.
2. The principle of consent, should allow for employees to make meaningful decisions about whether or not to agree to consent to monitoring and if they do not agree to consent that they do not be victimized.

3. The principle of information and consultation, should allow employees to be informed and consulted about the collection of personal data about them

With social justice a strong elements in the South African Constitution perhaps this debate would be better served if we look at the concept such as human dignity and how it is implemented throughout the European Union and get to a normative position in our labour legislation to implement a similar approach. By taking this approach it would be easier to achieve a balance between what an employer would be allowed in terms of monitoring and the conditions under which such monitoring would be allowed versus the dignity of the employee.

Ideally the employment contract would define the issue of employee consent. In terms of the Labour Relations Act and its position on workplace forums, negotiations between employers and existing employees would allow for the issue of consent to be brought into the relationship in a manner that should theoretically allow for both parties to maintain some form of dignity.

Employees should be able to show reasonable effort in providing information to employees about the monitoring of electronic communications.
Some of these efforts would be:

1. Employers providing copies of employee use policies
2. Employees should be informed on a periodical basis about updates and changes to the related policies
3. Online alerts could be used if employees' access prohibited sites
4. The employers' proxy servers could be set so that it excludes specific websites
5. Employers should make workplace policies part of all employment contracts

5.2. Recommendation on Computer Use Policy Guidelines

Some recommended computer use Policy guidelines:
These types of policies should define a series of boundaries on:

1. Types of private use
2. Sending, Handling emails of a dubious nature
3. Managing obscure and unwarranted content
4. Managing discriminatory content
5. Managing employee downloads in terms of licensing and potential virus issues
6. Policy on the use of networks and computers for criminal matters
7. Policy on the use of networks and computers by non employees
8. Policy on private adverts

Monitoring should be well defined to include what will be monitored and when such monitoring will take place. Monitoring should not be targeted to a specific person as that could be viewed as a form of constructive dismissal if the process of monitoring is really intense. It could also be seen as an unfair labour practice.

Intellectual Property Rights should be well defined throughout all sectors of the industry with all options such as licensing and transfer pricing be specifically spelled out in the policy document.

What is also important is that the implementation of this policy should be applied consistently and fairly so that it could be used as a positive device to build team spirit and at the same time also address problems that could occur with potential misuse of the systems.

5.3. Original Framing Questions:

In concluding by addressing the original framing questions:

11. Should employees be guaranteed a certain minimum level of privacy?
    a. From many perspectives having a guaranteed level of minimum privacy is a positive approach. It will allow employees to have a sense of self worth and lead to a higher level of engagement with the company. From a legal perspective having this minimum level of privacy available to all employees would give them some form of protection against unwarranted and unlawful

intrusion into their work and personal data on the system. I think that it would also lead to the CCMA to then deal with the issue of protection of the electronic communications of the employees which is something that they to date have not yet considered in a published case.

12. What does the common law position say about privacy in the work contract?
    a. In the standard work contract it would require either explicit or tacit description about what level of privacy is allowed at work as our common law position does not specifically create a right to privacy at work for the employee nor does it define if such a right did exist how would that be expressed in the work environment.
    b. Our common law position on privacy under the concept of "dignitas" only provides for protection if there was a specific unlawful action of the one party but in most cases since the employer owns the networks and computers monitoring the traffic of the employee would not even be considered "unlawful" under current South African law.

13. Should employers be required to specifically notify an employee that their emails are being monitored and what their web access or click streams are being monitored?
    a. Definitely yes if our approach will be one that enhances the "dignity" of the students and staff at UCT
14. If employers are allowed to read the emails of their employees what right would students and staffs at UCT have in this regard?
    a. UCT as an academic institution which also as one of its core values has the issue of social justice and academic freedom then is should hold itself to a higher standard that just minimums and allow more freedoms to its staff and students. In many departments such as the Graduate School for Business there appears to be an even stricter policy in place to using the networks. I suppose in many ways since it is untested it will in

the end depend on the expectation of privacy that the student or staff member actually exhibits and the level to which that privacy expectation will be honoured by the university. Also what would make this difficult to prosecute is that the policy has never been consistently applied so any action from the university would immediately be seen as discrimination.

15. Should the faculty, students and staff have the same privacy concerns and interest?
    a. Definitely in terms of our constitution we are all equal before the law. However in terms of the wording of this, currently students do not yet have an employment relationship with the university so it would not be possible to take them to the CCMA.

16. Would the University authorities monitor all the staff and student with the same intensity?
    a. Definitely if the university should for example have different intensities of monitoring internet traffic or emails it could be in terms of the LRA be seen as an unfair labour practice because it could constitute victimization and if the intensity of the monitoring is high it could lead to constructive dismissal of the employee.

17. Should there be different levels of protection for staff?
    a. No
18. Should Academic freedom be a consideration?
    a. Definitely because at an institution of higher learning such as UCT students and staff must explore the core ideas of many concepts and by restricting them to specific websites will not allow them to do that. Of course if the system is more “open” it also places a greater responsibility on the end users to not abuse the system and generally in these situations a trust relationship is important.

19. How would the university monitor the staff member's home access without monitoring the non work related parts of the web access and emails?
    a. As computers become more mobile and our economy moves more into a knowledge economy it is becoming more and more frequent that employees are actually connecting to the employers network after regular business hours and as a consequence would increasingly also complete his non work activities on the same system and using the same computer owned by the employer. I believe that a balance is possible in this regard in that the employer should retain the right to monitoring but should also be sensitive to the needs and requirements of the employee in this situation.

20. What about the propertization of data stored of the staff member on the computer or network of the university?
    a. The reality of the situation is that employees spend most of their working lives at the office and as such with the more pervasive nature of computers it becomes difficult to keep personal data separately of the network and computers of the employer. How then would an equitable balance be drawn on what the employer demands and what the employee would like. It would seem that a fair balance would be that the employee be allowed to store data on the computer of the employer and that the employer recognizes that the ownership of that data is vested with the employee but that such data should not lead to any liability to the employer.

Chapter 6 – Bibliography

Following is a review of Academic Articles of research work on the issue of electronic monitoring of employees in the employment context.

6.1. A non exhaustive thesis list – database source Nexus

- Strafregtelike beskerming van inligting by Catharina Wilhelmina Nienaber LLD Unisa 2003
- Cyber crime : A comparative law analysis by Maat, Sandra Mariana LLM Unisa 2002
- The Law of Data (Privacy) Protection : A comparative and Theoretical Study by Anneliese Roos LLD Unisa 2003
- Individual Privacy versus National Security : Accessing Electronic information with specific reference to the South African Situation by Edna Daphne Erasmus- Master of Security Studies University of Pretoria April 2002
- Enforcing Privacy on the internet – F.A. Lategan D Phil in Computer Science Rand Afrikaans University May 2002

6.2. A non exhaustive Literature List.

6.2.1.Articles

- The trouble with Trespass. Prof Dan Burke, University of Minnesota law School
- European Union Data Protection Directive: Adequacy of Data Protection in Singapore, Vili Lehdonvirta, Singapore Journal of legal studies (2004) 511 – 546

6.3.Legislation

- The South African Convergence Bill
- The South African Copyright Act 98 of 1978
- The Electronic communications and transaction act 2002, act 25 of 2002
- The Sarbanes-Oxley Act of 2002
- The Gramm-Leech Bliley Financial Services Modernization Act

- The Fair Credit Reporting Act and the Fair and accurate credit reporting Act
- The Privacy Act of 1974
- The Cable TV privacy Act of 1984
- Children's online privacy Protection Act
- The Patriot Act
- The Can Spam Act
- The California 2003 Security Breach Notification Act

6.4.Issue papers

- Implementation of the directive on privacy and electronic communications , DTI march 2003 Consultative document
- OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data
- Council of the European Union – Inter institutional file 2005/0202(CNS) – Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co operation in criminal matters
- OECD Directorate for Science, Technology and Industry, Working paper on Information Security and Privacy, 16 December 2005
- Council of the European Union – Report on the EU – US informal High Level meeting on Freedom, Security and Justice on 2-3 March 2006 in Vienna, Brussels 27 March 2006 7618/06
- Uncitral Model law on Electronic Commerce with the guide to Enactment 1996
- Privacy Impact Assessments – By Rodger Clarke, visiting fellow , Department of Computer Science, Australian National University, 19 April 1999
- Online protection – a survey of consumer, industry and regulatory mechanisms and systems – OFCOM, Office of Communications. The office of the privacy protector United Kingdom
- Model law on electronic transactions and Data Protection – Report and Explanatory Note Draft Final Version 5.0

- International Telecommunications Union- telecommunications Development Bureau, E strategies unit, Research on legislation in data privacy , security and prevention of cyber crime October 15, 2005
- Article 29 Data Protection Working party, Working party 29 opinion 2/2006 on privacy issues related to the provision of email screening services adopted 21 February 2006 00451/06/EN
- Commission Decision of 9 February 2006 Concerning the adoption of the Programme of Work 2006 for the Preparatory Action in the field of Security Research, Brussels 09.02.2006 C(2006)331
- Data Protection and employment in the European Union – An analytical study of the law and practise of data protection and the employemt relationship in the EU and its member states , Mark Freedland, Professor of employment law , University of Oxford
- Protection of the workers' personal data in the EU: surveillance and monitoring at work. Professor Frank Hendrickx, University of Leuven, University of Tilburg
- Protection of the workers' personal data in the EU: general issues and sensitive data. Professor Frank Hendrickx, University of Leuven, University of Tilburg
- The future of privacy protection: Cyber trust and crime prevention project. Charles D Raab, Edinburgh University
-

6.5.Books

- Harmonizing Cyber tort law for Europe and America, Micheal L Rustad. Prof of Law Suffolk University law School Boston, USA, Thomas H Koening, Prof Law Policy and Society program, North Eastern University
- Cyberlaw : the Law of the internet in South Africa edited by Reinhardt Buys
- Internet and Electronic Commerce Law in the European Union, John Dickie, LLB, MA , The University of Warwick, Hart Publishing
- Privacy in the information Age, Harry Henderson, Facts on File , Inc

- Privacy in the information Age, Fred H. Cate Brookings Institute Press, Washington DC
- Aspects of Privacy Law – Essays in honour of John M Sharp, Dale Gibson, University of Manitoba, Butterworths, Toronto