INTRODUCTION

Computer use in the workplace is now a standard occurrence. In the ordinary performance of their tasks employees are required to make use of increasingly sophisticated electronic communications tools. Computer networking, the use of email facilities and internet access, have significantly broadened an employee’s access to information reposited on the company computer network and the internet has allowed employees virtually unrestricted access to the world wide web from their desktops. Never before have employers faced a more difficult task in policing the information which employees either access or disseminate within the business environment than at present.

Highly sensitive business information and trade secrets can now be accessed and disseminated with relative ease and anonymity with the incremental potential for exposing a company to loss and litigation. Moreover, abuses of the electronic communication facilities for non-business related activities by employees who often unwittingly compromise the employer occur daily in the business environment. How to police employee use of these electronic communications tools raises a number of vexed legal issues as it is extremely difficult to differentiate between business and private usage, and in particular, to monitor the content of such usage.

Whilst the use by employees of electronic communications tools for non-business purposes will not increase the direct costs to the company significantly, the hidden and contingent costs to a company are potentially enormous: lost productivity and potential exposure to law suits emanating from third parties as a result of inappropriate use of these tools being the most dominant.

To reduce and potentially eliminate these potential risks and losses, companies must address the issue of how best to control employee use of electronic communications tools. This will require a re-education of both employer and employee as to what dangers exist where appropriate controls

---

1 Portions of this chapter contain material from the draft American Bar Association Model Policy on Electronic Communications Policies and the author's comments thereon in terms of the necessary adaptations for use in South Africa by Multi National companies based in the United States of America wanting to do business in South Africa.
are not put in place and will necessitate, *inter alia*, the development of a detailed written Electronic Communications Policy ("ECP") and educating employees on the potential which reckless use of email and the internet poses to the company.

**THE NECESSITY FOR AN ECP**

It is vital, rather than optional, that companies introduce a written Electronic Communications Policy ("ECP"). An ECP serves several purposes:

- To protect the company by reducing potential legal liability in respect of claims by employees or third parties;
- To protect proprietary or confidential business information from unauthorised access or disclosure to third parties;
- To prevent losses (e.g. of data and other proprietary information), errors, and mistakes; and
- To educate employees in the proper use of email and create an awareness of the risks that are associated with conducting business using electronic communication tools in an online environment (for example, the fact that when you surf the internet, you may be leaving an audit trail that identifies you or your company as the source).

By articulating what is permissible and what is not, a company may be able to demonstrate that certain activities engaged in by its employees fall outside the course and scope of their employment with the company (thereby avoiding vicarious liability for the employees’ actions), when called upon to defend its position (or institute legal proceedings to protect or enforce its rights).

**EMPLOYEE REACTION TO IMPOSED ECPS**

Whilst the imposition of ECPs in the workplace has distinct advantages for an employer, the real or perceived rights of the employee will potentially conflict with those of the employer.

Issues of privacy aside, one of the most important issues is whether the implementation of an ECP amounts to a change in the employee’s terms and conditions of employment.² Whilst this has not yet been tested in the South African courts, it has been argued by certain labour lawyers that the implementation of an ECP does not amount to a change in contract and is part of the directives which constitute the ordinary and necessary running of the business i.e. it is the prerogative of management (which, for example, can be equated to changing working hours from 08h00 to 08h30).

² Another issue is whether a so-called “workplace forum” can compel an employer to discuss the implementation of an ECP, bearing in mind that such a forum can compel an employer to discuss issues such as restructuring the workplace (which includes the introduction of new technology and new work methods), changes in the organisation of work, education and training (employers may have to train employees how to use electronic communications tools).

³ Section 64(4) of the Labour Relations Act 66 of 1995 prevents employers from unilaterally changing terms and conditions of employment. The question is whether an ECP would fall under this category.
Employees could also argue that the implementation of an ECP is not a “fair labour practice” under the Constitution. It is, however, submitted that as long as there is a genuine business reason for implementing the ECP from a business point of view, it can be justified.\textsuperscript{4}

It is also important to remember that in terms of employment law, employees have a right to strike in certain circumstances.\textsuperscript{5} Considerations of rights to privacy aside, it could be argued that the reading of email by an employer could, for example, constitute a legitimate grievance. The employees could call to strike on the basis of such grievance and force the employer to abandon the ECP.

**ASSIMILATING ECPs WITH EXISTING POLICIES**

If the company has other formal policies, it might be necessary to co-ordinate the ECP with such policies (e.g. in an employee handbook). Other policies which may have some bearing on an ECP include policies on:

- confidentiality of company and customer proprietary information,
- security practices;
- pre-publication clearance requirements;
- monitoring of telephone conversations;
- telecommuting;
- using company computer equipment at home; and
- personal use of company telephones, photocopiers, facsimile machines, etc.

The ECP should not be at variance with other agreements which might apply in given circumstances - for example, the Company may have third-party software license agreements permitting (under certain circumstances) simultaneous home-installations of Company-licensed software.

Finally, it is important to carefully determine the scope of the ECP when measured against the range of company facilities and equipment which might possibly be involved. Does the company wish to reach email facilities only? Email and internet browsers? Company-owned computers? What about fax machines, or company-paid cellular phones?

**ACCESS TO ELECTRONIC COMMUNICATION TOOLS**

\textsuperscript{4} Section 23 of the Constitution of the Republic of South Africa Act No 108 of 1996.

\textsuperscript{5} Section 23 of the Constitution of the Republic of South Africa Act No 108 of 1996. The right to strike only relates to an “interest dispute”. An “interest dispute” includes a grievance, but excludes any issue where the law allows for arbitration or adjudication (schedule 7 deals with residual unfair labour practices that gives the employees the right to go to court).
Certain employees will be furnished with communication tools that are owned by the company to assist them in the performance of their jobs. The term "electronic communication tools" includes the following:

- telephones, mobile phones and voice mail facilities;
- e-mail facilities;
- fax machines, modems and servers;
- computers; and
- network tools (e.g. Internet browsers and Internet access facilities).

It is important to remember that the tools are provided to facilitate business communications and to enhance the productivity of company employees. As the tools are owned by the company, the company should be able to decide the manner in which they should be used as well as to regulate their use.

Such regulation should address issues pertaining to personal use of the communications tools by employees. Decisions affecting personal such use by employees must be clearly formulated and stated in an ECP as this is the area which is likely portend potential pitfalls regarding employee rights to privacy in particular.

It is essential that where communications tools are provided by the company for business purposes, the rights of employees to privacy limited. One of the principal purposes of an ECP is to state, clearly, what kind of privacy expectations employees should hold. Failure to do so will entitle employees to argue with persuasion that both their common law and constitutional rights to privacy are being abrogated by company scrutiny of personal communications: This notwithstanding that they may have been conducted on the employers time and expense and on company owned communications tools.

A well drafted computer security policy should contain guidelines on individual password management (e.g. requirements that passwords contain a mixture of letters and other characters, are of minimum length, are not written-down, and are changed frequently). In most cases, effective execution of these procedures requires that employees choose (and periodically change) their own passwords. The simple fact that employees are permitted to choose their own passwords should not support an argument-by-implication that they thereby have justifiable privacy expectations in the material protected by the password⁶.

Every ECP should address the question of which persons’ conduct will be affected or regulated:

- do you have only employees who use your systems?

⁶ The existence of “superuser” accounts with systems privileges and the ability to also change all users’ passwords is well-known (at least to anyone who has ever forgotten one of their passwords), and also should negative any such possible argument.
• do any independent contractors have access to affected systems?

• do any clients or customers have access?

• do any employees' spouses, children, or other family members have access?

Non-employees should be provided access to secure communications facilities only with some form of written agreement restricting their use and disclosure of confidential and proprietary information to which such facilities may provide them access. In addition, such persons should be provided with notice of the Company's “rules of access and use”, and/or a specially tailored ECP.

ACCEPTABLE AND UNACCEPTABLE USE

Personal Use

To what extent should an employer permit personal (i.e., non-company related) use of email facilities and other communications facilities by its employees?

The use of email as a communication medium in the work place is an attractive proposition for many reasons:

Firstly, absolute prohibitions on personal use of email simply are not realistic (such prohibitions are difficult to police, and widely ignored where they have been imposed).

Secondly, unless the company’s policy does permit and acknowledge the possibility of "personal use", the policy cannot consistently and logically address Company inspection/review rights - i.e., if all personal use is flatly prohibited, then no employee would have any possible privacy expectation in any stored material (e.g., computer files or email). Thus, there would be no reason for the policy to discuss privacy expectations or inspection criteria, and any such discussion could create internal inconsistencies difficult to reconcile in subsequent litigation.

Thirdly, personal email (as distinct from mobile phones or certain other business communications tools) typically imposes very little (if any) additional costs (such as postage and transportation costs would for example traditionally do). Most corporate intranets support email exchanges at no incremental cost; many corporate intranets are connected to the Internet via a “gateway” on a fixed-price basis. Again, there is no incremental cost for email (personal or business-related) which is transmitted from the Company.

Fourthly, as South Africa becomes part of the "global village" many employees in South Africa are beginning to work in non-traditional locations (e.g. on the road or at home) and at non-traditional times (e.g., outside of normal working hours). If these working activities eat into "personal time", it may be fair to permit employees to take care of some "personal business" during office hours.

Perhaps the better practice is to permit restricted personal use of email, either, either internally or externally, and then incorporate other policies (such as privacy expectations, misuse of company resources, etc.) around this pragmatic acknowledgement.
If restricted personal use is permitted, it becomes essential for the Company to discuss (and set) employee expectations of privacy.\(^7\)

**Constraints on personal use**

If personal use is permitted, there must inevitably be some articulated constraints on such use. For example, permissible personal use should not be allowed to consume significant amounts of the employee’s work-day, and should not be permitted to consume substantial amounts of the Company’s intranet bandwidth. Email software now is able to embed photographs, voice recordings, and even full motion video into once-simple email messages. Employees making excessive use of these multimedia email capabilities will consume significant portions of the Company’s intranet bandwidth, leading to network performance problems and increased network operation costs.

**Expressly-Prohibited Use**

Employers would be well advised to impose an outright prohibition on certain broad classes of internet-related activities, both to prevent losses and to establish defences in possible litigation.\(^8\) Two of these will be discussed:

**Carrying any obscene, defamatory or discriminatory material**

In South Africa, the provisions of the Films and Publications Act 65 of 1996 prohibit the *distribution* of child pornography\(^9\), explicit violent sexual conduct, bestiality, explicit sexual conduct which degrades a person and which constitutes incitement to cause harm or explicit infliction of extreme violence.

Whilst this Act does not deal specifically with the internet, the definition of a 'publication' is wide enough to include the internet.

Although the provisions of this Act seek to regulate the distribution of films and publications (including pornography), one must interpret them having due regard to the fundamental rights to privacy\(^10\) and of freedom of expression\(^11\) which are protected in the Bill of Rights.

With regard to “hate speech”, the right to freedom of expression does not extend to advocacy of hatred that is based on race, ethnicity, gender of religion and that causes incitement to cause harm. It must be noted that like pornography, it is only the *distribution* of such material which is an offence under the Act.

---

\(^7\) See discussion infra.

\(^8\) Mere issuance of an ECP may erect some legal defenses, but certainly will do little to prevent accidental or inadvertent losses. To be truly useful, all ECPs should be broadly distributed to employees, and should be coupled with training and education programs that illustrate the principles of the ECP and the underlying reasoning.

\(^9\) Possession of child pornography is also expressly prohibited under the Act.

\(^10\) Section 14(d) of the Constitution of the Republic of South Africa Act No 108 of 1996.

With regard to defamation\textsuperscript{12} by companies and employees of companies, one of the important issues is where the duty to regulate lies: whether there is a duty on the company or internet service provider to regulate the publication of material (whether it be by way of email or a bulletin board on the company’s intranet) is a moot point. Unfortunately, this issue has not been decided in South Africa and companies who decide not to regulate and instead do nothing, could be exposing themselves to a possible claim for negligence on grounds that they owed a duty of care to their employees and third parties to impose some restrictions.\textsuperscript{13}

Insofar as email might be the medium for the defamatory statement in the workplace, it is important to remember that the defamation will probably occur at the place where the offending material is accessed. This might impact on defamatory email which is received from a foreign jurisdiction, as a South African court will only have jurisdiction in South Africa if the words were published (accessed) in South Africa.\textsuperscript{14}

Choice of law and jurisdiction on the internet are therefore important issues for any company as it could be argued that the company is exposing itself to the risk of being sued in countries which have access to the company’s website or access email which emanates from one of its employees – which practically means every country in the world. Do those countries have a right to insist on some form of censorship? Which country’s laws apply? What if the company has operations in both countries?

The proper knowledge of an ISP’s terms and conditions of use of that service especially insofar as it might pertain to website content, or the use of email is therefore very important and is usually contractually determined.\textsuperscript{15}

For South African companies, the Business Protection Act\textsuperscript{16} offers some degree of protection for South African businesses in that whilst a foreign judgement for damages is enforceable in South Africa, no foreign judgement which provides for the payment of multiple or punitive damages can be enforced by a foreigner in South Africa.

Until such time as clear rules have been laid down and principles established, companies wishing to sell their products abroad and engage internet users in foreign countries, but who wish to avoid the danger of being sued in another country, should carefully consider the objectives of their website. If necessary, they should impose certain restrictions on the interactive use of the website, particularly with regard to those interactive services and activities which are normally regulated around the world, such as pornography by way of example.

\textsuperscript{12} In South Africa, defamation is fault based (in the form of intention or negligence) and the principle of strict liability no longer applies to any type of defendant.

\textsuperscript{13} The British High Court in the March 1999 decision of Laurence Godfrey v Daemon Internet (presently on appeal) stripped the ISPs of their “innocent dissemination” defence afforded under the Defamation Act of 1996 and held them to be liable for defamatory material posted through their servers. Most of the cases in the United States revolve around the interpretation of section 230 of the Communications Decency Act of 1996 which was enacted to remove the aspect of self regulation created by the decision of Stratton Oakmont Inc vs Prodigy Services Company.

\textsuperscript{14} Publication is the act of conveying an imputation to a person or persons who are not the subject of the defamatory imputation.

\textsuperscript{15} Usually found in the ISP’s Acceptable Use Policy posted on it’s website and incorporated in it’s subscription agreement concluded with the subscriber.

\textsuperscript{16} Section 1A of the Business Protection Act (99 of 1978).
Violating the terms of any laws governing transborder data flow (e.g. laws dealing with data collection, protection, privacy, confidentiality, and security)

Many countries have broad data protection laws, or have sector-specific privacy laws (e.g., in the United States). Data protection is based on the principle that personal data should not be automatically available to others, and even where such data is processed by another party, the individual must be able to exercise a substantial degree of control over the data that it uses.

South Africa does not have any data protection legislation. The closest analogous legislation it has is the Open Democracy Bill. Whilst the right to privacy is recognised in South Africa as a fundamental right, the right to privacy must be balanced against the right to access, use and have personal information disclosed.

In the absence of specific South African legislation, it is important to take cognisance of the European Union’s Data Protection Directive, as this directive prevents companies operating in the European Union from transmitting data electronically to non-member countries, such as South Africa, unless those countries provide "adequate protections" for the information. The obvious question is, what is "adequate protection"? According to the European Commission Policy paper released in July 1997, in deciding whether a country’s privacy rules are sufficient, will be determined on a case-by-case basis. It is important to bear in mind that the directive would cover the processing of personal data by European subsidiaries situated in South Africa, for example. It would restrict the subsidiary from transmitting data to its parent country if it is located in a country which does not have adequate protection measures. This poses potential business constraints on the conduct of company business.

Unacceptable Content

A distinction must be drawn between “unacceptable content” and “illegal” content. Unacceptable content must not be sent or shown to others; whereas illegal content shall not even be acquired or possessed. The “acceptability” of content will vary from viewer to viewer. Therefore, the wording of the ECP is aimed at preventing others from being offended by content (even if it is legal content). On the other hand, an adult who is making a measured choice to access various kinds of content will be limited only to legal content, whether or not it might be acceptable to her colleagues.

It is important, however, for the drafters of the ECP to remember not to impose regulation merely for the sake of regulation.

“Unacceptable Content”

It is appreciated that sexual harassment can occur through electronic means—such as coarse jokes sent via email, salacious screen-savers and crude graphics. Racial and religious discrimination cases can also be based on offensive electronic content, regardless of the sender’s intentions. In such cases, it is important to remember that the South African courts do not consider the disclosure of defamatory words or behaviour to an outsider who is unaware of the defamatory character or meaning thereof as publication.

18 (95/46/EC)
The ECP should decide whether or not to prohibit the possession of “unacceptable content”. On the one hand, were the company to impose such a standard, it would of necessity require that someone in the company adjudicate on what is acceptable or not. On the other hand, failure to delineate a clear policy in this regard could leave the company without the defence that the employee was on a "frolic of his own".

“Illegal Content”

It is essential that any ECP should contain the limitation that no illegal content be accessed or downloaded. Of course, the “illegality” of content will vary from jurisdiction to jurisdiction as previously discussed, and presents a veritable minefield to both employers and users in general as it requires a broad knowledge of foreign domestic and local law.

Examples of Unacceptable and Illegal Content

Employees should be forbidden from using communications tools which-

- carries any defamatory, discriminatory or obscene material;
- carries sexually explicit messages, images, cartoons or jokes;
- carries religious or racial slurs;
- is used in connection with any infringement of another person's (whether natural or legal) intellectual property rights (e.g copyright);
- may be seen to be insulting, disruptive, offensive to other employees, harmful to company morale;
- is used in connection with any attempt to penetrate the computer network or network security of the company or other companies computer system, or to gain unauthorised access to any other person's computer or email.

REPRESENTING THE COMPANY IN ONE'S POSTINGS

Vicarious liability

It is a principle of South African law that an employer can be held liable for a delict committed by his employee, as long as it can be shown that (1) the employee is in fact liable for the delict, (2) that an employer/employee relationship existed at the time the delict was committed and (3) the delict was committed by the employee "in the course and scope of his or her employment". This phrase refers to acts committed by the employee in the exercise of the functions to which he or she was appointed, including such acts as are reasonably necessary to carry out the employer's instructions.\(^\text{20}\)

Can a South African employer be held liable for the content of emails generated by its employees? Whilst South African Law recognises that the employer creates a risk that third parties may be harmed by its employees committing wrongful acts in the course of their duties and that it should be liable to compensate people who suffer harm when the risk materialises, the question posed above has not yet been tested in the South African courts, and the answer will depend on all of the facts and circumstances of the case. The enquiries will include an examination of the nature and content of the email, the employee’s position, title, scope of responsibilities (and perhaps experience), and the nature of the employer (public or private company, close corporation or partnership). Most importantly one should consider whether the offending act was committed in pursuance of the execution of the employer's business or whether the employee can be said to have engaged in a “frolic of his own”.

It is important to remember that binding contracts can be concluded by email and an employer could be bound to a contract entered into by the employee for and on behalf of the company if the employee was either authorised to conclude the contract or if the employee’s responsibilities typically included such activities. It is also important to remember that the contracting parties need not be human beings, as sale agreements are now commonly being concluded with "electronic agents" online. In addition, when entering into purchase and sale agreements online, it must be remembered that the South African Reserve Bank ("SARB") exchange controls apply to all residents in South Africa who wish to remit moneys abroad. This applies to the payment in respect of goods purchased abroad. South African residents are also required to pay customs duties and VAT on any imported items when they are collected at the point of entry (which is usually the recipients local post office).

Email can contain binding “admissions”, just as can regular mail or other documents—again the determination will turn on authority and scope of employment.

To avert this possibility, some companies have taken to suggesting that their employees draft fairly-lengthy electronic “signatures” (which are affixed automatically to the end of all email messages) that expressly disclaim the employee’s authority to act for or bind the employer. Even if the employee disclaims official connection with the employer (i.e., by stating that “the following are only my opinions, and do not reflect those of my employer”), can the reputation of the employer be adversely affected? Certainly. In most cases, email from Company-provided systems will contain routing information that identifies the Company's internet "domain" (e.g., name-of-your-company.co.za).

---

21 Verification of electronic “identity” (through use of digital signature, Certificate Authorities, and the like) is beyond the scope of this effort.  
22 An electronic agent is no more than a computer program that is designed, selected, or programmed by a party to initiate or respond to electronic messages without being supervised by a human being and is accordingly known as a "bot" or "robot".  
23 The present exchange control measures where introduced by way of the Exchange Control Regulations in 1961 and are governed by the Currency and Exchanges Act 9 of 1933). Whilst the government is committed to a gradual relaxation and eventual abolition of exchange controls, authorised dealers (being those persons to whom the SARB has delegated certain of it’s powers) may approach the SARB on a case by case basis where the transaction, or the amount does not fall within the general mandate given by the SARB to the authorised dealers.  
24 When a company is drafting such a signature, it must ensure that it complies with the provisions of section 50(1)(c) of the Companies Act 61 of 1973 which requires a company to mention it’s name and registration number in all notices and official publications of the company.
Aware of this possibility, some employees have taken to posting their scurrilous messages using pseudonyms whilst trying to remain anonymous. Unfortunately, this is easier to contemplate than to accomplish. Traffic on the internet is composed of “packets” which may be likened to post-cards, carrying a message, an address, and a return address (these are called “IP addresses”). Every email message and browser enquiry is conveyed over the internet in “packet” format, and monitoring software can easily capture the IP address of the sender’s computer. Whether this IP address is sufficient to actually identify a specific individual depends on the sender's computer configuration and local computer environment (e.g., a corporate intranet or LAN, or dial-up through an Internet Service Provider or Online Service Provider). Again, where the sender uses a corporate direct connection to the internet, her email and browser requests will carry the corporation’s ".co.za" or ".com" imprimatur and will appear to observers to have come from someone in the company. True anonymity is very difficult to attain.

From the aforesaid, it should be apparent that employees need to be educated in the risks of sending emails or browsing the internet. It often happens that they are horrified to learn that their every move leaves an audit trail (irrespective of whether or not anyone actually is monitoring their exchanges or later decides to review the system logs). After employees have been educated in these points they are much more likely to act with circumspection in their posting and surfing (both official and personal).

While Company-related postings should all be professional, messages sent to certain newsgroups may be so closely related to important parts of the company’s business as to merit special rules. These rules may include pre-publication review approvals by the Marketing, Engineering, and/or Legal divisions within a company.

'ELECTRONIC FRAUD'

In an electronic environment, it is possible to manipulate an email so that it appears as if the email is being sent by another person (i.e. where somebody impersonates another person's identity).

In most instances it will be almost impossible to determine the true identity of the sender, as our reliance on the email headers (which would normally reveal the name and email address of the sender) would have been manipulated by the sender and it would be incorrect to assume in such circumstances that the sender must be the source of the email simply because he appears to be working from these otherwise trustworthy electronic addresses.

While there are emerging technologies and practices that could verify the true identity of the sender of the email, the present situation is fraught with unreliability.  

In South Africa, there have been no reported civil decisions involving "electronic fraud".

It is therefore imperative that an ECP prohibits impersonation in all forms. The policy is aimed at using another’s email facility without permission.

25 The identity of the sender could be verified if a digital signature was used, or in certain instances where an internet service provider has email tracking facilities, it might be possible to trace the route of the email thereby identifying the computer which transmitted the email.
If the company implements a policy of banning impersonation in all forms, they should remember that there are certain instances where anonymity should be protected and where the sending of anonymous messages should be permitted, and even possibly encouraged. It must be stressed that these should only apply in limited instances. For example so-called internal “whistle blowing hot lines” may be available to employees to report incidents of potential wrongdoing by other employees which are brought to their attention. Furthermore, a company may permit its employees to feel that they can safely surf the internet for important medical information, without disclosing their identity to others (for example to locate current information on HIV treatment programs). Furthermore, employees may want to post messages to news groups without having their email addresses “harvested” by vendors who send unsolicited commercial email (i.e., SPAM). In such cases anonymity would be appropriate.

However, in an electronic environment true anonymity can be quite hard to attain. If it is important to permit anonymous use of electronic tools, then special arrangements need to be made (e.g., use of anonymous remailers) and employees should be informed about invisible audit-trails and system logs that may capture information about their web activities, so that they can make responsible, informed decisions about where and how to surf the web.

INTELLECTUAL PROPERTY

One of the main attractions of the world wide web is that it is possible to download magazine articles, reports, song titles, video and photographs, all of which are protected by copyright. A computer software program placed on the internet can also be downloaded at sites around the world and re-posted and yet never leaves the computer of its designer. It is also possible to download copyrighted graphic and textual material posted to a website where it can be changed, merged with other material, returned to cyberspace and perhaps even sold as a different product all together.

This has created a headache for publishers and a potential nightmare for the creators of articles, songs, software and films as the owners will want to protect their materials. Laws to date simply do not adequately cover electronically transmitted copyright material. Even if they did, it would be extremely expensive and time consuming to monitor possible infringements and to litigate.

Website operators are beginning to take measures to protect the content of their websites against indiscriminate copying - musical recordings may be available in their entirety only after a credit card has supported their “purchase”; before that time, only snippets or excerpts can be copied or downloaded. However, much online content is not technically protected against copying, and in this lies a potentially serious risk for unwary users (and their corporate employers)—which such copying may be feasible (as a technical matter), it still likely is illegal.

Electronic content is subject to copyright. Under South African copyright law, copyright is the right given to the owner of certain types of works not to have his work copied without his authorisation.

---

26 See discussion above.
27 See http://www.well.com/user/abacard/remail.html for a useful discussion of anonymous remailer systems.
28 See for example TUCOWS (http://tucows.is.co.za) and Strouds Consummate Winsock Apps List (http://cws.internet.com/index.html).
29 In certain instances so-called “MP3” sound files can be downloaded in their entirety, which is currently a grave cause for concern to artists and their publishers.
30 Section 23 of the Copyright Act 98 of 1978.
Generally speaking, the work is copyrighted when it has been created by the authors original skill and effort and has been reduced to a material form and is therefore not merely an idea.

In South Africa, one does not have to register copyright (as is the case with other forms of intellectual property, such as patents of trademarks). A copyright situation will arise automatically as soon as something tangible is produced as a result of the authors original skill and effort. For the most part, once an expression is entered into a computer in a form that can be read on a screen, it is considered fixed in a material medium even if it is never printed out or saved to a disk. This means that employees surfing websites are not entitled to freely copy and distribute the content obtained from those websites which is owned by that company without first obtaining prior permission. This extends to copying images and text found on the website. Copyright law, however, does not prohibit an employee quoting something interesting that he finds online, as long as he acknowledges the source.

Insofar as trademarks are concerned, a trademark is essentially a means of identifying a product whether it be in the form of goods or services. It extents to a brand name and any sign capable of being represented graphically. Employees should therefore be on the lookout for trademark notices which are placed on websites informing internet users that graphics, logos, domain names and other materials are protected by trademark law.

**COMPUTER VIRUSES**

A computer virus is an unauthorised software programme or portion of a programme that is being introduced into a computer or network. The purpose of a virus is to damage data files, delete data or perform other harmful actions. Depending on the purpose of a particular virus, the reformatting of an infected diskette and/or hard drive may be the only method of dealing with the virus. This will result in the loss of all the data on the diskette or hard drive.

Computer viruses are becoming more common and the number of viruses being detected has increased. The downloading or copying of unauthorised software onto employee's PCs is one of the easiest ways for these viruses to invade a computer or network.

It is therefore important that the company not permit its employees to download data of whatever nature except possibly to a standalone PC set aside for this purpose. Further, all information downloaded onto the PC should be virus checked using virus scan software which the company should have.

The ECP should accordingly contain stringent rules in this regard to safeguard it's data and computer system.

---

31 Section 3 of the Copyright Act 98 of 1878.
32 It is important, however, from a practical viewpoint to understand the difference between a computer virus proper and "virus warnings" which refer to the existence of a computer virus "doing the rounds" at any point in time, as these warnings are often "hoaxes". Two good up to date repositories which deal with the latest hoaxes are located at the United States Department of Energy Computer Incident Advisory Capability Web site at [http://ciac.llnl.gov/ciac/CIACHoaxes.html](http://ciac.llnl.gov/ciac/CIACHoaxes.html) and the Computer Virus Myths home page at [http://kumite.com/myths/home.htm](http://kumite.com/myths/home.htm).
TRANSMITTING CONFIDENTIAL INFORMATION

Accidental Disclosure

Companies are making increasing use of the Web to manage and distribute proprietary and confidential information. For example, inter-company email messages can contain information on business plans, and can carry as attachments detailed spreadsheets, drawings, charts, and supporting documentation. Moving beyond email, the company may place equipment design and operations manuals on the company’s intranet, to enable authorized users to access this material when they need it, on-demand. Increasingly, web-based information storage-and-retrieval is becoming the rule, rather than the exception.

In this context, there may be heightened risk of accidental electronic “disclosure” of confidential information\(^{33}\). “Disclosure” could occur in a number of ways:

- an email to a distribution list that includes a non-employee (or even co-employees who do not have a need-to-know, in the case of some particularly sensitive information);
- posting information to a bulletin board or newsgroup that contains non-employee members;
- placing information onto a company-controlled intranet\(^{34}\), which has been mis-configured and which allows access by non-employees;
- the temporary collapse of an intranet firewall, permitting temporary access by outsiders (whether or not such access actually occurs);
- posting information to a password-controlled, externally-accessible web page (where the password is compromised);
- loss of the computer on which the information has been stored (e.g., loss through theft of a notebook computer);
- sale of a used computer (and disk), from which confidential information has not been thoroughly removed;

---

\(^{33}\) The confidential information may be owned by the company, or by other persons (such as the company's customers or suppliers). In the context of a law firm, it is important to remember that the attorneys and their employees should never make reference to the names of their clients, any unannounced or unpublished details about their clients and their affairs (for example listings on the Johannesburg Stock Exchange or whom they are negotiating with or litigating against), matters which the firm is working on at any given time, or in general furnish any information in any manner which in any way concerns any of the firm's clients, the relationship of the firm with those clients and the business of those clients, by using any of the communications tools that are at their disposal.

\(^{34}\) The term “intranet” is commonly used to refer to world-wide web facilities that can only be accessed from computers that are within the company's internet-numbering “domain”. Protected from third-party access (perhaps through security devices called “firewalls”), corporate intranets permit use of standard network access tools (e.g., using the common TCP/IP protocols), such as Netscape’s Navigator and/or Communicator web browsers (and Microsoft’s Internet Explorer).
• the loss, theft, or improper destruction\textsuperscript{35} of computer media (e.g., diskettes or CD-ROMs) containing the confidential information;

Complicating the matter, it may be increasingly difficult to keep track of which audience is entitled to see what material. While technological systems can be relied upon to assist in maintaining confidentiality, they cannot assure confidentiality and must be complemented by employee training and awareness\textsuperscript{36}.

**Premature Disclosure**

Premature disclosure of confidential information which have or are likely to have a material effect on the financial results, the financial position or cash flow of a public company listed on the Johannesburg Stock Exchange or any information pertaining to new developments in its area of activity which is not public knowledge and which may have an effect on a public company's assets and liabilities or financial position is regulated in South Africa.\textsuperscript{37}

In the sphere of patent law, the disclosure of proprietary information can prevent the subsequent issuance of letters patent for related inventions\textsuperscript{38}.

**ENCRYPTION**

What follows is a discussion of the use of encryption, if at all, in the workplace in order to protect confidential information and trade secrets (or privileged information in certain instances). Ultimately, employers will have to decide whether they wish to permit the use of public key encryption in the workplace and if so, its regulation, if any, in an ECP.

**What is encryption**

Encryption is "the process of disguising, that is, encrypting, a readable communication, into an unintelligible scramble of characters according to some code or cipher. The readable

\textsuperscript{35} Simply “deleting” files on a diskette, without more, does not destroy the contents of the diskette, and CD-ROMs cannot be easily “erased”. Employees should be educated as to the proper use of “disk-wipe” software programs (or should re-format diskettes), before throwing them into the trash. CD-ROMs with important content should be physically broken, shredded, and/or burned.

\textsuperscript{36} Some companies have instituted broad employee security awareness training programs, supplemented by posters and other reminders, such as:

- Is your client’s data safely put away?
- Have you recently changed your passwords?
- Do you leave your computer running unattended?
- Is your password-protected screen saver active?
- Do you regularly back-up critical data?
- Do you have current software virus protection?
- Do you use only properly licensed software?
- Have you destroyed out-of-date CDs and stiffies?

\textsuperscript{37} See the Johannesburg Stock Exchange Listing Requirements.

\textsuperscript{38} The Patents Act of 1978 requires that the invention must be new, namely, that it must not have been described sufficiently to enable the invention to be understood, by word of mouth, use, in any printed publication, or in any other way, anywhere in the world before a first application is made for a patent (often referred to as "absolute novelty").
communication is called plaintext. The encrypted communication is called ciphertext. Decryption is the process of converting the ciphertext back to its original, readable form.

Most encryption software programmes use algorithms and encryption keys. These keys contain a string of zeros' and ones' of varying links. Each character in the string is called a bit. Encryption software combines the message or attachment to be transmitted and the key on a complex mathematical algorithm, resulting in the ciphertext. The longer the bits in the key, the more difficult it is to "crack" the encryption system without the key.

Given the fact that the internet is an open network, it is important to remember that if one is going to send messages which are not encrypted, this would be the equivalent of sending electronic postcards, as oppose to the equivalent of sealed envelopes where one makes use of encryption.

Types of cryptography

There are two types of cryptography: private key (symmetric) and public (asymmetric) key. In a private key system, the same key is used for encrypting and decrypting the material. In a public key system, two complementary keys are used, one for encrypting and the other for decrypting the message. One is called the private key and the other the public key. The private key is kept secret by the signer and is never shared. The public key is shared with anyone whom the author wants to communicate with. The private key is used to do one and/or two things: to sign a message and/or encrypt a message or both. One must remember that a document can be signed without having been encrypted. If it is not encrypted, confidentiality is lost.

A message is signed by the author using his private key. To sign a message, the software makes a so-called "message digest" (also known as a "hash value") of the communication. The message digest is a series of numbers and letters which are unique to each message. If one letter or number is changed in the message, the message digest will also change. The message digest is the digital signature which is so commonly associated with encryption.

The status of encryption software in South Africa

It appears as if the use of encryption software is free for use by commercial or private organisations (i.e. one does not need a permit to use it from the relevant governmental department). The situation is governed by the Armaments Development and Production Act. This Act must be read in conjunction with Schedule 1 of the General Armaments Control Schedule. In terms of the Schedule, the South African government controls encryption as a dual-use item. This means that the export of encryption software requires an individual validated license. Whilst the Act does not specifically include encryption software in its definition of "armaments", item 8 of Schedule places controls on the export of military equipment which possesses cryptographic capabilities. Hence, a valid permit is required from the Armaments Control Division for the import of cryptographic equipment for software.

---

40 See also RSA Laboratories FAQ's about cryptography at www.rsa.com/rsalabs/faq/.
41 Act 57 of 1968 (as amended).
42 Published in Regulation 888 on 13 May 1994.
It is important for South African users to note that the export of encryption software is regulated in many countries\(^{43}\). In the United States, these regulations take the form of export controls\(^{44}\). The practical effect of this for South African users is that they are not able to use PGP. However, there is an international version of PGP (known as PGPi) which is available for use by South African users.

**Is a digital signature legal in South Africa**

Unlike certain states in the United States of America and certain countries in the European union,\(^{45}\) South Africa has not yet recognized the need to provide a legal infrastructure to support the use of digital signatures and accordingly, no digital signature legislation exists. Applying the South African common law in an attempt to address the issue of the legality of the use of digital signatures in South Africa it would, however, appear that certain categories of legal documents are not capable at present of being signed with a digital signature, whilst there appears to be no legal bar to other categories of documents being validly concluded in this manner.

**Business reasons for using cryptography**

The use of encryption, and in particular digital signatures serves important evidentiary and security purposes. A digital signature serves the same purpose as a handwritten signature in that it may signify authorship, acknowledgement or assent. What sets a digital signature apart from its traditional handwritten counterpart, is that an encrypted digital signature is by its very nature not able to be proved by the tried and tested methods employed by handwriting experts, such as pen pressure, slope of characters and the like. The security purposes that handwritten signatures cannot, however, achieve, are the following:

- **Integrity** – it allows the recipient of a digitally signed communication to determine whether the communication was changed after it was digitally signed i.e. a digital signature provides assurance about the source and integrity of the communication;

- **Authenticity** – the recipient knows the communication came from the sender because only the sender’s public key will decrypt a digital signature encrypted with the sender’s private key; and

- **Non-repudiation** – once integrity and authenticity have been established, the sender is prevented from repudiating both the contents of the communication and having sent it.

In the business context, companies have legitimate and compelling reasons for using cryptography. For example, cryptography can secure internal and confidential business

---

\(^{43}\) For a useful, current survey of various laws on possession and use of encryption technologies in various countries, see \texttt{cwis.kub.nl/~frw/people/koops/lawsurvy.htm}.

\(^{44}\) In several countries, even domestic “use” of cryptography (at least use for “confidentiality” purposes, if not also for integrity, authorisation, and non-repudiation purposes) may be subject to local regulation. Such local regulation may take the form of outright prohibition, or prior “declaration” of an intent to use (e.g., in the case of certain crypto systems in France). Such regulations also may vary depending on the cryptography system employed, the underlying algorithm(s) (e.g., DES, Triple-DES, IDEA, CAST, Skipjack, etc.), and the length of the encryption key (key-length roughly correlates to the “strength” of the crypto system - content that is encrypted with shorter-length keys is generally easier to crack than material encoded with longer-length keys).

\(^{45}\) For an excellent summary of digital signature legislation world-wide, see \url{www.mbc.com/ds_sum.html}. 
communications from accidental loss (e.g. through misdelivery) and from intentional interception (e.g., because of corporate espionage). Likewise, crypto systems are used to protect non-message data, such as business plans, new product design information, and employee listings – such information may be stored on company computers and/or media such as CD-ROMs, disks, floppies, and tapes. On the other hand, if employees are free to use any encryption technology, the employer may have great difficulty in de-coding or decrypting proprietary files that have been scrambled by its employees, unless the employer has the “key” that was used to encrypt the files. Without some method of assuring that the encryption keys are held by the employer (or available to it), there is risk that important company-proprietary information may be unavailable (if the employee is absent) or unreachable (if the employee has died), or if the employee simply has lost the decryption key (or has forgotten the password used to “lock” the decryption key).

One solution to this problem lies in an approach called “key-recovery”, or "key-escrow". This is a technique whereby a private key would not only be held by the user, but also by his employer.

As companies deploy encryption technologies within their organizations (by making them available to employees), it is important that they take care to negate any implication that employees have enhanced privacy expectations (otherwise arising out of their ability to encrypt files). In part this can be accomplished by using “key recovery” technologies - still, the prudent employer will spell out the implications flowing from adoption of such technologies so that employees are fully aware that the employer can and may decrypt and read any employee-generated files prepared on the employer's systems (see discussion in footnote below).

RETENTION AND SECURITY OF MESSAGES

E-mail, voicemail messages and items stored on employees' computers are the property of the company. They in all probability will have the same legal effect as that of traditional hard copy documents (for example, they are "discoverable" in litigation and can be used in evidence). Accordingly, all e-mail messages should be treated as though they may later be viewed by others (while confidential information may be contained in such messages, these messages should be created with the same care that one would use in creating hard copy documents).

PRIVACY OF ELECTRONIC COMMUNICATIONS

As a general proposition it is fair to assume that a Court will view email provided by employers to employees as a tool intended for work-related communications in the first instance. As such, the employer would generally be presumed to have the right to access and monitor employee email messages, as long as the employer does so for legitimate business or related purposes.

Notwithstanding that the foregoing proposition appears to be a reasonable departure point, there are nevertheless two inherently conflicting interests in regard to any such communications: in the first instance there is the unarguable legitimate business interests of the employer which require protection and can fairly be said to justify the monitoring of its information systems on the one hand, whilst there is simultaneously the competing interest of the employee’s reasonable expectation of privacy regarding his communications made with third parties whilst in the workplace.

The judicial determination of which interest should be given paramount consideration is, however, a vexed one. The questions which arise are moreover not only whether or not such
communication may be intercepted legitimately by an employer in breach of the employee’s reasonable expectations or privacy of communication, but, in the event of it being established that the employer is so entitled to do, the question of the introduction of the evidence so obtained before a tribunal presents a separate set of legal problems.

There are certain pieces of legislation and case law in South Africa which must be considered in an attempt to provide an answer to the question of which of the two rights should, in the first instance, enjoy supremacy.


Section 14(d) of the Constitution of the Republic of South Africa guarantees the right to privacy as a fundamental right, which includes the right not to have “the privacy of their communications infringed”. Had the Constitution contained no further provision regarding how the rights in the Bill of Rights should operate, it would have been arguable that the right to privacy of communications was an absolute right which could never be departed from.

However, section 36 of the Constitution contains a so-called “limitations clause” which provides that inroads into the rights as contained in the Bill of Rights can be made by the enactment of other laws provided that it would be reasonable and justifiable to do so “in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including –

(a) the nature of the right;
(b) the importance of the purpose of the limitation;
(c) the nature and extent of the limitation;
(d) the relation between the limitation and its purpose; and
(e) less restrictive means to achieve the purpose.”

In S v Makwanyane46 Chaskelson P remarked that this involved a balancing process “...which calls for the balancing of different interests. In the balancing process, the relevant considerations will include the nature of the right that is limited, and its importance to an open and democratic society based on freedom and equality; and purpose for which the right is limited and the importance of that purpose to such a society; the extent of the limitation, its efficacy, and particularly where the limitation has to be necessary, whether the desired ends could reasonably be achieved through other means less damaging to the right in question.”

In determining an individual’s right to claim absolute privacy of communications in terms of section 14(d) of the Constitution, one must also have regard to the context in which this right will operate: namely, whether it will operate between citizen and the State (e.g. a State department or agency and a citizen) or between citizens (e.g. employer and employee), bearing in mind that the primary

46 S v Makwanyane, 1995 (6) 665 (CC) 104.
aim of the Bill of Rights is to protect individual citizens against unacceptable State interference with their fundamental rights.\textsuperscript{47}

It is clear from a reading of section 14, that some of the provisions may apply as between citizens, whereas other provisions in the same section, and pertaining to the same right, will not. It is also clear from our case law that whether or not a provision will apply between citizens will depend on the nature of the private conduct in question as well as the circumstances of a particular case.

The Constitutional Court has already made clear the importance of the right to privacy in the new South Africa.\textsuperscript{48} In the \textit{Case and Another} \textsuperscript{49} matter, Madala J recognised that \textit{“the protection accorded to the right of privacy is broad but it can also be limited in appropriate circumstances”}.

In the \textbf{Bernstein} case (\textit{supra}), Ackermann J analysed and discussed the concept of personal privacy and essayed \textit{“some preliminary observations”} on the right to privacy. One of the observations made by Ackermann J is that the scope of a person's privacy should extend only to those aspects in regard to which a legitimate expectation of privacy can be had.

It has been argued by certain academics that \textit{“this subjective expectation component simply recognises that someone cannot complain about an infringement of privacy if they have consented explicitly or implicitly to having their privacy invaded.”}\textsuperscript{50}

These sentiments were also echoed by Ackermann J in the Bernstein decision (\textit{supra}) who stated that \textit{“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.”}

Although it is not theoretically sound to speak of contracting out of, or waiving constitutional rights and obligations, in the context of employers infringing any rights to privacy that an employee may have within the workplace, it is clearly vital for employers to inform employees of, and to obtain their consent to, the possible monitoring and interception of their electronic communications in order that they do not have any legitimate expectations in this regard.

Having regard to the balancing process referred to by Chaskelson P in \textit{S v Makwanyane},\textsuperscript{51} employers would be well advised to act “reasonably” in formulating their ECPs, to consider less invasive means of achieving their objectives, and above all, to obtain the consent of their employees whenever possible as well ensuring that they are well informed. Most notably, employers should formulate their ECP with the view in mind that they have to expressly address the limits of an employees legitimate expectation to privacy.

\textsuperscript{47} One must also have regard to the Courts inherent common law discretion to admit evidence, which discretion will be exercised by weighing up the relevance of the evidence, against the fundamental right to privacy which has been infringed.

\textsuperscript{48} \textit{Bernstein v Bester} NO 1992 (2) SA 751 (CC), \textit{Case v Minister of Safety and Security} 1996 3 SA 617 (CC); \textit{Curtis v Minister of Safety and Security} 1996 3 SA 617 (CC) 656 - 657 (per Didcott J) and 659 F-H per Langa J.

\textsuperscript{49} \textit{Case supra} 661 E.


\textsuperscript{51} See footnote 1 infra
Interception and Monitoring Prohibition Act (Act No 127 of 1992)

The provisions of section 14(d) of the Constitution have been circumscribed to some extent by the coming into being of the Interception and Monitoring Prohibition Act ("the Monitoring Act")\(^{52}\). This Act came into operation on 1 February 1993\(^{53}\), and whilst it was drafted before the adoption of the Interim Constitution, it was nevertheless drafted with the knowledge that its validity would be tested against the provisions of the Constitution and in particular, the right to privacy contained in the Constitution.

It has been held by the Durban and Coast Local Division of the High Court that the Monitoring Act is an act of general application within the meaning of Section 36 of the Constitution and accordingly the provisions of the Monitoring Act are at present deemed to set out the only legitimate departure from the fundamental right to privacy as enshrined in the Bill of Rights.\(^{54}\)

The Monitoring Act provides for the Minister of Justice to designate power to a judge in a Local or Provincial Division of the High Court to consider applications for interception and monitoring of “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”\(^{55}\). In practice, however, only one judge has been appointed for all the divisions and all applications for interception and monitoring are being considered by that judge (Gordon J).

To date there are no reported cases concerning whether or not email communications would fall within the definition of “a communication” as contemplated by section 2(1)(a) of the Monitoring Act. The analysis of what types of communication would fall within the ambit of one “to be transmitted by telephone or in any other manner over a telecommunications line” was very superficially analysed by Heher J (as he then was) in the Protea\(^{56}\) case, and in particular, the issue of whether or not email communications would be deemed to fall within the ambit of section 2(1)(a) was not even discussed in this case. The transmission of email between two distant personal computers by using modems, a telephone line and a communications program in each computer would appear, subject to the necessary technical proof being provided to the satisfaction of the Court, to be relatively easily capable of being brought within the meaning of the words “to be transmitted by telephone”.

Not all email communications are, however, transmitted in this manner. For example email can be transferred between two local computers by cabling them together with cable and a file transfer program in each computer, or between personal computers which are part of a local area network.

Where these forms of transmission occur, it is a question of whether or not they are nevertheless transmitted “over a telecommunications line”. The definition of “telecommunications line” in section 1 of the Act includes a very wide definition and reads as follows:

\(^{52}\) Act 127 of 1992.
\(^{53}\) Notwithstanding that the Act was put into operation in 1993, it was only made applicable to the whole territory of the Republic (including the previous TBVC states) on 1 April 1997 when the Justice Laws Rationalisation Act 18 of 1996 came into operation.
\(^{54}\) State v Naidoo (1998] 1 All SA 189 at 213.
\(^{55}\) Section 2(1)(a).
\(^{56}\) Protea Technology Ltd v Wainer [1997] 3 All SA 594.
“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 the sending, conveying, transmitting or receiving of signs, signals, sounds, communications or other information”.

Whilst the inclusion of email in the definition is accordingly a moot point in our law, it is likely that the technical requirements for the transmission of email are such that email will be deemed to be a communication within the meaning of the Monitoring Act.

Furthermore, there is no differentiation in terms of this Act regarding matters of national security and applications relating to crime investigation on the one hand, or monitoring and interception required for private purposes on the other.

The Monitoring Act therefore effectively prohibits the interception of a communication which has been or is intended to be transmitted by telephone, or in any other manner over a telecommunication line, where such interception occurs intentionally and without the knowledge and permission of the dispatcher. It furthermore prohibits the intentional monitoring of a conversation or communication by means of a monitoring device so as to gather confidential information concerning any person.57

It must be remembered, however, that a distinction needs to be drawn between the right of privacy of a private citizen to interception or monitoring by State authorities on the one hand and the monitoring of communications on internal telephones in a workplace on the other hand. It would appear that in view of the PROTEA-case58 it is arguable that the principle has been accepted in the case of businesses that communications on internal telephones may be monitored and indeed sanctioned, without there necessarily being an invasion of the individual’s rights of privacy.

In the Protea case the Court made the important finding that the effect of the Monitoring Act was not to remove a Court’s discretion to admit evidence obtained in contravention of the Act. It held further that with regard to the admissibility of evidence, the Act should furthermore not be interpreted so that grave injustice might result. It concluded further that the Act did not render the production of recordings made in contravention of its provisions inadmissible before a Court trying a civil dispute.

In November 1998 the South African Law Commission in its Discussion Paper 78 undertook a review of the Monitoring Act59 and in which it made certain recommendations concerning the Act is recommended, *inter alia*, that Section 2 of the Act should be amended to provide that no person

57 The act does not define “confidential” information. In the Protea case 603, the court remarked as follows: “That expression must surely mean such information as 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 that information is necessary or impliedly to be restricted. I think that there is a distinction between ‘confidential’ information and ‘private’ information.”

58 Supra, 608 - 609 (a - b):
“The First Respondent was employed by the Applicants in a position of trust. The telephone conversations were conducted from the Applicants’ business premises within business hours. The Applicants were entitled to require the First Respondent to account for his activities during their time. (In addition the First Respondent was contractually obliged to devote his full attention to the affairs of the group). It may be accepted that, even in this context, and within reason and at the direction of the employer, an employee’s private life is not excluded. Thus he may receive and make calls which have nothing to do with his employer’s business. The employee making such calls has a legitimate expectation of privacy.”

59 The commission is still engaged in it’s task and the closing date for comments on it’s proposals was 25 January 1999.
shall *inter alia* intentionally monitor a conversation or communication, *without the knowledge or permission of the parties to such conversation or communication, .......*.

This recommendation would have the effect of addressing an employer’s concern regarding the monitoring and interception of employees’ communications to some extent. This is the more so where it can be argued by the employer that the employee has been given fair warning (e.g. in the ECP) of the possibility of the monitoring and interception of his communications and where indeed a company policy document has stated clearly that the company reserves its right to do so. The employee’s acquiescence to such term, whether express or implied, would then effectively render an argument far more compellable that such monitoring and interception is legal.

**CONTRACTUAL LIMITATIONS TO PRIVACY RIGHTS**

A fundamental premise of our law is that individuals should be allowed to contract freely, without interference by the Court provided only that the terms of such contract are not deemed to be *contra bonos mores* or against public policy. It may well be argued that the sanctity of contract is a fundamental principle of our law which should enjoy predominance even over fundamental rights as contained in the Constitution. The only stumbling block to the acceptance by our Courts of this proposition may be that if individuals are allowed to abrogate the very pillars of the Constitution as contained in the Bill of Rights, this must, as a matter of course, be deemed to be against public policy and contractual terms should accordingly not enjoy supremacy over constitutional norms. Jurisprudential arguments aside, however, there would appear to be nothing unacceptable in principle to parties agreeing in terms of the provisions of an employment contract that an employee’s rights of privacy regarding communications made whilst in the workplace and on the employer’s time, should not be susceptible to interception and monitoring by the employer in the ordinary course of conduct of its business.

Whilst in the ordinary course agreement can be reached either expressly or impliedly, given that the right to privacy is guarded so jealously as a fundamental right, it would be fair to assume that a Court will require an individual to expressly and unequivocally waive the right to privacy before such waiver will be deemed to have occurred.

**The position in The United States**

Given the absence of clear authority in South Africa concerning the interception, monitoring and use of electronic communications of employees in the workplace, it is necessary to examine the position in other jurisdictions in an attempt to formulate potentially persuasive arguments which could be used to good effect in South Africa.

Arguably the one country in the world which not only generates more litigation than any other, but which is also superior in the area of the use of computers, is the United States of America. It too has a Constitution which enshrines the right to privacy.

It is accordingly useful to investigate how the issue of the privacy of electronic communications has been approached and applied in the Courts of the United States.
In the United States of America the **Electronic Communications Privacy Act** (ECPA hereafter) is currently the only federal statute that addresses the privacy of electronic communications such as email, voicemail, fax and cellular phone communications. This Act generally prohibits anyone, other than the sender and the intended recipient of the message, from intercepting an electronic communication or accessing a stored electronic communication or disclosing the contents of an electronic communication. This Act also applies to both government and private citizens and provides for certain penalties (both criminal and civil) for its breach.

Although the ECPA prohibits interception of email messages during the communications process, two exceptions appear to authorise employer monitoring of employee email messages. These two exceptions are commonly known as the **“prior consent exception”** and the **“business use exception”**. Under these two exceptions, the ECPA provides private employers considerable, indeed almost unlimited, latitude in monitoring the electronic communications of their employees.

Under the "prior consent exception" it is not unlawful to intercept electronic communications when one of the parties to the communication has given prior consent to the interception. Thus, if employees give their consent to employer monitoring, there is no question that the monitoring is lawful. This consent may take many forms, including an employee’s signature on an email policy statement that notifies the employee that all email communications may be subject to monitoring. Implied consent is also possible, depending on the circumstances of each case. Implied consent can be derived from a situation where employees have been informed that solicitation calls will be monitored as part of the company’s regular security program.

Similarly, when an employee knows that personal calls on monitored phone lines are not permitted, it has been accepted that the employee has no reasonable expectation that such calls will be protected from an employer’s intrusion. In the online context, implied consent may occur when an on-screen message appears each time that the employee uses the company’s system. This message warns that there is no guarantee of privacy in email messages and conditions the use of the company’s system on exceptions of this policy. It is, however, more difficult to imply consent than it is to prove that express consent has been obtained from the employee.

Even where employees have not consented, the business use exception will normally allow the employer to intercept and monitor employees' email activities. Under the provision of the ECPA, the entity that provides the electronic communication service through which the messages flow, is ordinarily authorised to intercept messages. This gives the provider of the email system in the workplace great latitude in monitoring company-owned electronic communication systems, including email and voicemail. The "business use exception" of the ECPA does not limit the message or degree of employee monitoring, nor does it require employers to provide employees with notice. It does, however, require that the employer’s monitoring be **“within the ordinary course of its business”** and that the subject matter of the intercepted communication is one in which the employer has a **“legal interest”**.

The more limited in purpose and time the interception or listening-in takes place for, and the more business orientated the intercepted communication is, the more likely it is that a Court in the United States will allow the use of such intercepted messages by the employer.

Another aspect of the ECPA provisions in the United States is that even when an employer does not have a right to intercept a message in transit, it may have a right to access and review a

---

60. 18 U.S.C., paragraph 2510 – 2711.
“stored message” residing on its system. In most cases, employer monitoring of email messages will probably involve access to stored communications which reside on the system, rather than the interception of communications “in transit”. The ECPA provides an even broader exception for employers in regard to access to stored communications: specifically, the electronic communication service provider is exempt from the statutes ordinary prohibitions. This clearly has a major implication for email messages that are stored on the employer’s system.

The Monitoring Act in South Africa does not appear to cater as widely as the American ECPA Act does for the categories of exclusion, although the latest recommendations from the Law Commission appear certainly to be moving in the direction of allowing the legal interception of messages where prior consent has been obtained. Specific categories of exclusion such as those discussed above, do not appear in the draft Bill which the Law Commission has, however, proposed to date for South Africa.

The rule of thumb in the United States appears to be that where an employer has a written email policy warning of possible interception, an employer’s chances of warding-off invasion of privacy suits is increased significantly. Such a policy would minimise the employee’s reasonable expectation of privacy. If one uses the American legal system as a guideline in this regard it is significant to note that even in states such as California which has amongst the strictest state privacy laws in force (privacy laws that are widely regarded as being even stricter than those contained in the Fourth Amendment of the United States Constitution) employees have unsuccessfully sued employers for breach of their rights of privacy where written email communication policies have removed the legitimate expectation of privacy regarding email communications.

In what is commonly regarded as the leading American case on the issue of privacy in the workplace, the United States Court of Appeal held in the case of O’Connor v Ortega⁶¹ that “the realities of the workplace” made some expectations of privacy among public employees unreasonable when the intrusion was by a supervisor rather than a law-enforcement official. Work-related searches, the Court found, were “merely incidental to the primary business of the agency,” and a warrant requirement would “seriously disrupt the routine conduct of business”. The Court thus held that a standard of “reasonableness” was sufficient for work-related intrusion by public employers.

Conclusions relating to the usability of intercepted computer generated email evidence

In the light of the foregoing it would appear that:

In terms of section 14(d) of the South African Constitution privacy of communications is recognised as a fundamental right;

⁶¹ 480 U.S. 709 (1987). The facts of the case briefly were that in 1981, officials at a hospital, including executive director Dr. Dennis O’Connor, suspected improprieties in Dr. Ortega’s management of a residency program. The officials conducted an investigation of Ortega, which included multiple searches of his office and seizure of a number of items. The items were later used in proceedings before the California State Personnel Board to impeach the credibility of witnesses that testified on Dr. Ortega’s behalf. The question which presented itself for decision by the Court was whether or not the supervisor’s search of the office violated Dr Ortega’s “reasonable expectation of privacy” guaranteed by the Fourth Amendment.
Notwithstanding that the **Interception and Monitoring Prohibition Act** provides that no person shall intentionally and without the 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, nor is any person entitled to intentionally monitor a conversation by means of a monitoring device, the Witwatersrand Local Division of the High Court has held in the **Protea Technology** case\(^\text{62}\) that the Court nevertheless retains the discretion to admit evidence intercepted in contravention of the provisions of the Act in a civil dispute where to refuse to do so might allow a grave injustice to occur.

Whilst the position in the United States of America is such that, notwithstanding their strict privacy laws, certain exceptions exist allowing for the interception and monitoring of communications in the employer / employee context within the legitimate business arena, the current position in South Africa is quite different. Pending the proposed legislative reforms to the **Monitoring Act** put forward by the South African Law Commission, (which recommendations will hopefully be further expanded upon to cater specifically for legitimate interceptions for business use and/or prior consent situations), the South African position is at present extremely prohibitive and accordingly more far-reaching in its effect than the American position.\(^\text{63}\)

The argument moreover which can be raised in the American Courts, namely that a differentiation can be drawn between the interception and monitoring of a **“live”** communication and a **“stored”** communication, cannot readily be used as a justification for legitimising an interception in South Africa, inasmuch as Section 2(1)(a) of the **Monitoring Act** in its present form provides specifically for the prohibition to intercept the communication which **“...has been or is being or is intended to be transmitted.”** (Own emphasis)

The only remaining argument which an employer can accordingly put forward in favour of having intercepted and/or monitored email or other electronic communications of an employee, would possibly be that, notwithstanding the employee's right to privacy as set forth above, the employee has, contractually, waived his constitutional rights. This would arise in circumstances where there has been an agreement to adhere to the employer's policy of use of the email or other electronic facility provided by the employer for business purposes only within the employer's premises. The waiver of rights are not lightly implied, however, in South African law and it is therefore unlikely that such a fundamental Constitutional right will be deemed to have been impliedly waived by an employee. Rather, where an employee can be shown to have expressly consented to the monitoring or interception of his or her communications the employer will be far more likely to succeed with such an argument. At present, and pending possible judicial reforms in this regard, this would appear to be the only possible legitimisation for the interception, monitoring and use of electronic information against an employee. This underscores the importance of the ECP within the workplace.

**CONSEQUENCES OF MISUSE**

It is a broad principle of South African law that the dismissal of an employee is only justified if that employees misconduct leads to the irretrievable breakdown of the relationship between the employer and the employee. If the employer is seeking to discipline the employee on grounds that

\(^{62}\) Supra.

\(^{63}\) The possible explanation for this position having arisen is that the South African Constitution is modelled predominantly on the Canadian Constitution and not the American Constitution, and that the absolute prohibitions against the invasion of privacy contained in the Canadian Constitution are renowned world-wide for the strictness of their approach.
it has broken one of the rules set forth in the ECP, then it is incumbent on the employer to establish three things:

- That there was a rule;
- That the rule was reasonable; and
- The rule was brought to the attention of the employee.

If the employer is able to establish these three requirements, one would proceed to the next step of the enquiry, namely to establish whether or not the particular rule has been breached. If it has, then there has been misconduct. Once misconduct has been established, one would then move to the next step of the enquiry which would be to ascertain whether or not the misconduct justifies dismissal. In evaluating whether or not dismissal is justified, one must establish two things:

- Firstly, whether not damage has been caused to the employer; and
- Secondly, whether or not the misconduct has led to the irretrievable breakdown of the relationship between the employer and employee.

In all instances, the employer must convene a disciplinary enquiry in order to enable the employee to respond to the allegations of misuse which would have been levied against him.

It is therefore very important not only to have a well formulated ECP, but that the terms and conditions of the ECP be pertinently brought to the attention of the employee.

CONCLUSION

Few companies at present have an ECP in place. Of those who do, it is questionable how many comprehensively address the many problem areas that employers face. In certain instances, this may be due to a failure on the part of the employer to appreciate the full extent of the potential problems that may arise from inappropriate and unmonitored use of email and internet facilities provided to employees. The drafting of appropriate ECPs is moreover one that requires an intimate knowledge of the company's internal requirements, operating procedures and policies, as well as an extensive knowledge of both domestic and foreign law. Failure to provide an ECP leaves the company sitting on a potential litigation timebomb.

oOo
BIBLIOGRAPHY

BOOKS

- Smedinghoff *Online Law* (1996) 497

TABLE OF CASES (SA)

- Bernstein *v* Bester NO 1992 2 SA 751 (CC).
- *Case v Minister of Safety and Security* 1996 3 SA 617 (CC).
- *Curtis v Minister of Safety and Security* 1996 3 SA 617 (CC).
- *Protea Technology Ltd v Wainer* [1997] 3 All SA 594.
- S *v* Naidoo [1998] 1 All SA 189.

TABLE OF CASES (FOREIGN)

- *Lawrence Godfrey v Daemon Internet*
- O’Connor *v* Ortega 480 U.S. 709 (1987)
- *Stratton Oakmont Inc vs Prodigy Services Company* 1995 N.Y. Sup

TABLE OF STATUTES (SA)

- Patents Act 57 of 1978.
• Business Protection Act 99 of 1978.
• Labour Relations Act 66 of 1995.
• Justice Laws Rationalisation Act 18 of 1996.
• Films and Publications Act 65 of 1996.
• Open Democracy Bill 67 of 1998

TABLE OF STATUTES (FOREIGN)

• Defamation Act of 1996
• Electronic Communications Privacy Act 18 U.S.C
• Communications Decency Act of 1996

INTERNATIONAL CONVENTIONS

• European Union’s Data Protection Directive 95/46/EC.

WEBSITES

• ANONYMOUS REMAILER FAQ ANDRE BACARD (www.well.com/user/abacard/remail.html 23 May 1999)
• BERT-JAAP KOOPS CRYPTO LAW SURVEY VERSION 14.3, FEBRUARY 1999 (cwis.kub.nl/~frw/people/koops/lawsurvy.htm 23 May 1999)
• MCBRIDE BAKER COLES SUMMARY OF ELECTRONIC COMMERCCE AND DIGITAL SIGNATURE LEGISLATION (www.mbc.com/ds_sum.htm 23 May 1999)
• RSA LABORATORIES FREQUENTLY ASKED QUESTIONS ABOUT TODAYS CRYPTOGRAPHY (www.rsa.com/rsalabs/faq/ 23 May 1999)