LAW SOCIETY
OF SOUTH AFRICA

# The management of e-mail – guidelines for South African law firms

**Drafted for the**
**Law Society of South Africa**
**by Mark Heyink**

# Management of eMail for South African Law Firms

## LSSA Guidelines

**VERSION 01 (DRAFT)**

MARK HEYINK

Attorney, Notary & Conveyancer
Specialising in Information Law

# Table of Contents

# Foreword

## Please read this foreword carefully.

**This guideline has been compiled for the Law Society of South Africa primarily as a tool to assist attorneys in governance and management of eMail.**

**By its nature the guideline is general, not exhaustive, and intended as a starting point to guide attorneys in the effective management of electronic communications. This guideline is not intended and must not be construed as establishing any legal obligation. Neither is the guideline intended, nor must it be construed, as providing legal advice.**

**This guideline is supplementary to the Information Security Guideline and the Protection of Personal Information Guideline published by the Law Society of South Africa which should also be considered in using this Guideline.**

# Copyright

# Chapter 1

## 1. INTRODUCTION

1.1 The Law Society of South Africa has published guidelines entitled "Information Security Guideline 2011" and "Protection of Personal Information Guideline 2011". This Guideline is supplementary to those guidelines which will be referred to and parts of which may need to be read to achieve a greater depth of understanding of the information security and protection of personal information issues which apply to electronic communications. The Guidelines are available on the Law Society of South Africa website at www.lssa.org.za.

1.2 For the vast majority of attorneys eMail has become the de facto mechanism of communication of written information. The communications may be external (to clients or third parties) or internal (between an attorney, a secretary or an assistant). In many instances eMail will also have documents attached to them, which have been created using other applications (eg. Word, Excel, Powerpoint). Often the eMails or the documents attached to the eMails will, by the nature of the work done by attorneys, be confidential and in certain circumstances it is also important that the integrity of the communication or document (ensuring that it cannot be accidentally or maliciously altered) may also be desirable or essential.

1.3 In using eMail without properly protecting the eMail or attached documents there is a risk that the attorney's professional duty of confidentiality may be compromised and that eMail communications or attachments may be accidentally or maliciously amended.

1.4 The benefit of properly implementing information technology in legal practice, an information intensive profession, is that this will promote more effective communication, speed, efficiency and cost reduction. However, the use of these technologies does not free attorneys from their professional duty to manage information with appropriate caution. The duty to safeguard the confidentiality and integrity of clients' information as well as ensure that it is available to those persons authorised by the client to access the information is no different now than before the advent of electronic communications.

1.5 The risks inherent in the use of electronic communications differ vastly from and have to be managed very differently to paper-based information and communications. While the safeguards that we have developed over centuries for printed communications remain critically important in the management of information in paper and text, these protections are of little relevance in safeguarding information in electronic form.

1.6 This Guideline highlights the explosive and exponential growth of electronic communications globally. It discusses the "why's" and "how's" of eMail governance and management and proposes an approach that will assist attorneys in addressing some of the more common risks attached to electronic communications and how they may be avoided or managed.

# Chapter 2

## 2. ELECTRONIC COMMUNICATIONS

**The aim of this chapter is to provide the reader with a brief background to:**

- The information revolution;
- Statistics illustrating the exponential growth of electronic communications; and
- The effect of the information revolution on the practice of law.

### Background

2.1 As with all revolutions in history, the information revolution has brought with it sudden and fundamental changes to our society. However, no revolution in history has changed our society and commercial practices more quickly or more dramatically than the information revolution.

2.2 This chapter highlights both the magnitude and the swiftness of changes which, in the context of this Guideline, profoundly influence the way attorneys communicate and manage written information. It further alerts attorneys to novel applications of the technologies which may in the future hold important advantages but all potential risks should these technologies be used without proper management within an attorney's practice.

2.3 While eMail has been commercially available since 1993, the initial uptake was slow from a business perspective and it was only after 10 years that we saw eMail becoming used in the main stream of business. Since then its growth has been exponential, to the extent that in most modern businesses eMail has become the chosen method of communication of written information both internally and externally.

2.4 We have also seen the emergence of short message services (SMS) as the method of communication which, due largely to the attractiveness of the portability of a mobile phone, has also quickly been adopted as a method of communication in certain circumstances. The convergence of technologies which now allow eMails, SMS and instant messaging (IM) to be communicated using a mobile phone will continue to significantly change and further enhance electronic communications in the immediate future.

2.5 More recently the explosion of social networking technologies (among the more popular being Facebook and Twitter) have been an important development in electronic communication. While only the most progressive practices in South Africa have adopted social networking technologies, in other areas of the information economy, social networking has been recognised and is being exploited. It will not be long before attorneys will have to adopt these communications techniques to meet client requirements.

### Prevalence of Electronic Communication

2.6 To illustrate the fundamental and irreversible changes in the processing of information brought about by electronic communications the following statistics are illuminating.

**Internet Growth**

2.7 In 2008 (15 years after the Internet first became commercially available in 1993), the information communicated on average in any one second during the course of that year equated to the entire Internet traffic communicated in 1993. It should be borne in mind that prior to 1993 and its commercial availability, the Internet was already extensively used by academics globally and the military in the United States to communicate electronically.

## eMail

2.8 Statistics published in early 2011 indicate that over 2 billion people have access to the Internet globally. There are 1,9 billion eMail addresses on the Internet and annually 107 trillion eMail messages are communicated. This amounts to 294 billion emails' per day.

2.9 Depending on the source, estimates of SPAM (unsolicited electronic communications) vary vastly. At the lower end it is estimated that 63% of eMail traffic is SPAM and at the higher end 92%. This is an important statistic as it brings starkly into focus the necessity for protection of networks by appropriately configured firewalls and the use of virus protection software. (Many SPAM messages contain malicious code which may have adverse consequences for the recipients of the SPAM and the networks within which those recipients work.)

## Short Message Services (SMS)

2.10 By the end of 2010 it was estimated that there were 5,282 billion mobile cellular subscribers worldwide (in excess of twice the number of Internet users). In Africa the discrepancy is far greater. In South Africa there are just on 7 million computers while there are between 38 to 40 million cellphone users.

2.11 The convergence of cellular and Internet technologies means that many times the number of people will have access to eMail facilities through their mobile devices than is currently the case. As older handsets are replaced by newer devices which enable this convergence, the number of people having access to eMail will increase dramatically.

2.12 By the end of 2010 it was estimated that 6.1 trillion SMS messages were communicated and it is predicted that by 2013, despite the emergence of mobile eMail, instant messaging and multimedia solutions, SMS communications will exceed 10 trillion.

## Instant Messaging (IM)

2.13 Instant messaging has been available for some considerable time in the form of Internet relay chat (IRC) and has gained popularity through solutions such as MXIT (a South African product widely adopted by school children in South Africa) and products such as Blackberry Messenger. Many of the social networking sites have also integrated within their services Instant Messaging.

2.14 In September 2010, 175 million people were registered with Twitter and 25 billion tweets were sent between October 2009 and September 2010.

## Social Networking

2.15 The explosion of social networking technologies and applications such as Facebook, MySpace and Twitter (to name a few) have seen progressive organisations encouraging the use of social networking tools as a mainstream business communication.

2.16 The exponential growth in Facebook users has been the most significant phenomenon evident in Internet use in past years. Facebook reports that it has 500 million active users (active users are users who access Facebook at least once every 30 days). Only 2 countries in the world, China and India, have larger populations.

2.17 To illustrate this phenomenal growth, at the end of 2010 Facebook had over 600 million subscribers (1 in every 13 people on earth). Over 250 million of its subscribers logged in every day. Over 700 billion minutes a month are spent on Facebook and over 200 million people access Facebook using their mobile phone.

**The Future of Law**

2.18 Professor Richard Susskind is an independent advisor to global professional law firms and national governments. He is the IT advisor of the Lord Chief Justice in England and is widely recognised as a leading futurist in the use of IT in the practice of law.

2.19 Professor Susskind suggested in his book "The Future of Law" published in 1996 that the legal world (fundamentally an information economy) was on the brink of a seismic shift. He suggested that huge changes in legal practice and the administration of justice would occur as a result of the information revolution and that the provision of legal services would be fundamentally changed.

2.20 In a later book he writes:

> *"In the two years that followed the publication of the book, I had the opportunity to present my ideas in person to thousands of lawyers around the world – at seminars, workshops and conferences. The question-and-answer sessions that followed my talks were particularly illuminating for me. The running theme of those who offered views during that period was that of incredulity – not a denial that the Internet would have a substantial impact on the business and domestic lives of all, but a disbelief, or at least a considerable doubt, that the online revolution would really extend into the legal domain. To be sure, in every audience there were enthusiasts who were exasperated by their colleagues' scepticism but, generally, lawyers expected adjustments at the periphery of their world rather than the fundamental transformations that I was predicting."*

2.21 Susskind goes on to observe that while his predictions were regarded as science fiction, at the time of writing a further book "Transforming the Law" published in 2003, attitudes have shifted dramatically and the sceptics who regarded his views as science fiction had come to accept that the shifts that he predicted would be at least as dramatic and their influence on the legal profession at least as profound as he had asserted. While it is beyond the scope of this guideline to deal with Professor Susskind's predictions, it is important to understand that central to the changes that he predicts is the electronic communication of information.

## Mainstream

2.22 Against this background there can be little doubt that the mainstream of communication in the world and South Africa is electronic. Attorneys who deny the importance of these developments run the risk of losing touch with their clients and failing to optimise their practice to meet the demands of modern business in a modern world.

2.23 In considering the transition and the proper governance and management of electronic communications, attorneys must be mindful that the technologies and their application have resulted

in novel risks. In addressing the transition of practice from exclusively paper and text environments to predominantly electronic communication environments, attorneys have to manage the risks inherent in electronic communication. Failure to do so is a fundamental failure of the discharge of an attorney's professional duty.

# Chapter 3

## 3. WHY MANAGE EMAIL (and other electronic communications)?

**The aim of this chapter is to draw attention to:**

- The attorney's professional duty to safeguard information;
- The governance and management of electronic communication in the fulfilment of this duty;
- Where appropriate to ensure the evidentiary value of electronic communications; and
- The attorney's responsibility in the discovery of electronic communications.

### Professional Duty

3.1 The professional duty of attorneys to provide information security, which is a critical element in the governance and management of electronic communications, is more fully addressed in Chapter 3 of the LSSA Guideline on Information Security for South African Law Firms. Nonetheless, due to its importance, certain of these provisions are repeated for ease of reference.

3.2 The International Code of Ethics governing the behaviour of attorneys provides that:

> *"Lawyers should never disclose, unless lawfully ordered to do so by the courts or as required by statute, what has been communicated to them in their capacity as lawyers, even after they have ceased to be the client's counsel. This duty extends to their partners, to junior lawyers assisting them and to their employees."*

3.3 This duty of confidentiality is echoed in rules governing attorneys' conduct in jurisdictions around the world and in South Africa.[1]

3.4 As has been indicated earlier in this Guideline, practices underlying the maintenance of confidentiality in electronic records and communications are vastly different to the practices which we have employed in the paper and text environment. It is interesting to note that the Canadian Bar Association guidelines for "Practicing Ethically with New Information Technology", a supplement to its "Code of Professional Conduct", makes the following comment:

> *"To meet the ethical obligation for competence in Rule 2 (perform any legal services undertaken on a client's behalf competently) lawyers must be able to recognise when the use of technology may be necessary to perform a legal service on that client's behalf* ***and must use the technology responsibly and ethically***[2].

[1] Examples: In England and Wales the Solicitors Code of Conduct, published in 2007, provides that solicitors must keep affairs of clients and former clients confidential except when disclosure is required or permitted by law or by clients. A provision very similar to the international code of ethics is contained in Section 14 of that schedule of the rules of the KZN Law Society.

[2] The emphasis is the author's.

*Lawyers must satisfy this duty by personally having a reasonable understanding of the technology and using it, or by seeking assistance from others who have the necessary proficiency."*

3.5 It is submitted that while there is no formal equivalent of the Canadian Bar Association's guideline in South Africa, attorneys are required to act reasonably and diligently in fulfilling their professional obligations. One of these obligations must be that in using modern technology they do not compromise the rights of their clients arising from the attorney/client relationship.

3.6 An important fact is that even though documents which may be created and stored in other programmes (for instance Microsoft Word or Word Perfect), these documents are more often than note communicated electronically by way of attachment to eMail. Thus, most eMail systems will have, in addition to native eMail communications, other documents and information which may be accessed through the eMail system.

3.7 Against this background the necessity to manage eMail communications as part of the professional duties of an attorney are self evident.

**eMail as Evidence**

3.8 The Electronic Communications and Transactions Act No. 25 of 2002 (ECTA) governs electronic communications in South Africa. An electronic communication is by definition a "data message" and in the context of this Guideline regard must be had to Chapter III (Part 1) of ECTA which governs the facilitation of electronic transactions and the legal requirements of "data messages".

3.9 While it is not necessary to deal with these provisions in any detail in this Guideline, nonetheless attention is drawn specifically to the provisions of Section 15 which govern the admissibility and evidential weight of data messages.

3.10 In many instances electronic communications communicated or stored by attorneys may constitute evidence which, if they are to be used in legal proceedings will be admitted as evidence in legal proceedings[3] and their evidential weight will be assessed by the presiding officer against the following criteria:

*"15(3) In assessing the evidential weight of a data message, regard must be had to-*

*(a) the reliability of the manner in which the data message was generated, stored or communicated;*

*(b) the reliability of the manner in which the integrity of the data message was maintained;*

*(c) the manner in which its originator was identified; and*

*(d) any other relevant factor."*

3.11 In the circumstances it is important that attorneys can ensure that their electronic communication can be demonstrated to meet the criteria required in this Act.

[3] Section 15(1) of the Electronic Communications and Transactions Act No. 25 of 2002

3.12 The information security required to promote the reliability and integrity referred to in Section 15(3) is more fully dealt with in the Information Security for South African Law Firms Guideline.

### E-Discovery

3.13 In the same manner as communication by way of paper and text are discoverable, so are electronic communications.

3.14 Care must be taken by attorneys in dealing with legal proceedings that electronic communications relevant to the proceeding and which may be subject to discovery are properly retained in the manner in which the integrity of the communications is not compromised and that the communications are not inadvertently destroyed.

3.15 It is important that attorneys develop policies, procedures and standards that govern and manage the retention of eMail and its destruction. Various technologies and techniques are available to facilitate the archiving of electronic communications, and if implemented properly, will assist attorneys in fulfilling their obligations of managing eMail in a manner that will enhance its evidential weight and allow appropriate discovery in legal proceedings.

### Access to Information

3.16 Records in the possession of an attorney may be subject to a request for the information in terms of the Promotion of Access to Information Act No. 2 of 2002. These records include electronic communications. Where requested, all reasonable efforts must be made to find the record and if the records cannot be found or appear not to exist, the head of the firm (in the absence of this duty being delegated to an information officer) is required by way of affidavit or affirmation to notify the requestor that it is not possible to give access to the record. The affidavit must give a full account of the steps taken to find the record to establish whether it exists. In the circumstances, unless eMail records are properly archived, the investigation required may be extremely time consuming and costly.

### Protection of Personal Information

3.17 The Protection of Personal Information Bill currently being considered by Parliament provides conditions for lawful processing of personal information. These conditions are more fully dealt with in the Protection of Personal Information for South African Law Firms Guideline but it is worth reminding attorneys that the communication of personal information electronically is part of the processing of personal information, and as a responsible party (or as an operator on behalf of a responsible party)[4], an attorney will be obliged to ensure that the security safeguards contemplated are established and maintained.

### Good Practice

3.18 There is a duty on attorneys to manage information in whatever form securely and with due cognizance of their professional and other duties. In light of the already prevalent and increasing business requirement, driven to a large degree by clients, that attorneys communicate by way of eMail, the critical importance of the management of eMail, including but not limited to, fulfilling an attorney's professional obligation make it abundantly clear that eMail and other electronic communication must either not be used or should be appropriately managed.

[4] Attorneys are referred to the definitions of "responsible party" and "operator" in the Protection of Personal Information Bill

3.19 Of necessity this management requires ensuring that information remains, where necessary, confidential in both its communication and retention, that the information can be easily found and appropriate processes mitigating the potential legal and business risks inherent in electronic communications are established and adhered to in using the technologies required for electronic communication.

3.20 The issue of who is responsible for eMail management is dealt with in greater depth in Chapter 4 of the LSSA Guideline on Information Security for South African Law Firms.

# Chapter 4

## 4. GETTING STARTED

**The aim of this chapter is to assist the reader in understanding:**

- How to initiate the development of an eMail Policy;
- The investigation necessary; and
- Issues that need to be considered prior to drafting the policy and procedures.

### Philosophy and Investigation

4.1 To enable proper governance of eMail it will be necessary to document the practice's policy and the procedures that need to be established to enable the management of eMail in terms of that policy.

4.2 The policy should reflect the philosophy or thinking of the firm's leaders in addressing eMail communications. This requires that the firm's leaders properly inform themselves to ensure that the use of eMail is appropriate to the practice. Questions that should be asked are:

- How essential is eMail communication to the practice?
- How important is eMail to internal information management processes?
- What are the information security risks in using eMail communication? (The reader is referred to Chapter 5 of this Guideline)
- To what extent do information security risks threaten to compromise the professional duties of attorneys within the practice?
- What technological protections have been established?
- Do current processes limit or eliminate unacceptable risk?
- Are the attorneys and employees of the practice properly trained to use eMail?

4.3 Clearly, each practice will have many additional questions which may need to be investigated. However, using the questions provided as a base will facilitate the initiation of an investigation.

4.4 The success of the investigation will largely hinge on the authority provided to the investigators and the cooperation and active support provided to achieving the intended goal. Appointing a junior candidate attorney (even if the candidate attorney is the most technologically advanced person in the practice), who may either be too timid to highlight the failings of seniors or who may be fobbed off on the basis that seniors have far more important things to do than to provide cooperation, is self-defeating and a waste of time. Whoever conducts the investigation must have sufficient authority and support to at the highest level of the firm to ensure that the investigation is honest and effective.

4.5 Policy by its nature is a distillation of the practice's overall attitude towards, in this instance, eMail. The philosophy of the practice needs to be firmly established and clearly reflected on the policy documentation and the procedures that support the policy.

4.6 It is useful in investigating the establishment of any information security policy (of which an eMail policy is an integral part) to separate the investigation into three specific areas, technology, process and people.

4.7 The investigation into the **technology** will in most cases for attorneys in South Africa require the assistance of persons expert in the technology and the manner in which the technologies have been implemented and configured for the practice. Very often inherent in the technologies deployed in the practice is a capability of providing the controls and security required if they are correctly configured to do so. However, as a matter of convenience (security always having an element of inconvenience), the technologies used by a practice are often configured to allow for ease of use rather than security.

4.8 In investigating the security capability of technologies employed by a practice questions to ask of the technologists will include how the technologies will assist in ensuring compliance with the law and discharge of professional duties as well as address the risks attendant on electronic communications dealt with in this Guideline.

4.9 One of the outcomes of the investigation must be to establish whether the technologies used by a practice facilitate or inhibit appropriate safeguards in the use of eMail. If not, whether the technologies can be configured to achieve the required safeguards or whether it is necessary to invest in alternative or additional technologies to do so. It is obvious but still worth stating that care should be taken in requesting existing suppliers to evaluate their own technologies. The danger is that the investigation will be self-serving and possibly cover up the deficiencies which there may be in the technologies supplied to the firm.

4.10 Turning to the issue of **process.** If the practice has implemented an information security project, the organisational infrastructure for the implementation of an eMail policy and supporting processes should already be in place. In the absence of an organisational framework and the appointment of persons to govern and manage eMail, however good an electronic communications policy may be it is bound to fail. It is therefore important that an appropriate governance and management framework is established and the people assigned this responsibility are properly empowered.

4.11 The final element of the investigation is to establish how the **people** within the practice currently use eMail and ancillary technologies in the processing of information. Does this behaviour constitute a risk to the security of information processed by the practice? If so, how will the practice's staff be educated in the preferred behaviour of the practice, this behaviour monitored, where necessary non-adherence addressed and if appropriate, sanctioned?

4.12 In conducting the investigation it would also be wise to establish who among the practice's employees understand the information workflows in various areas of the practice and may be able to assist in the formulation of policy and procedures in this regard.

### Policy Development

4.13 After the investigation has been concluded it will be necessary to document the desired policy in an electronic communications policy. This policy should be supported by procedures and standards which, along with the policy, are statements of mandatory behaviours or prohibitions.

4.14 Often guidelines are also provided which are discretionary recommendations to be followed by managers and users of information. These are often used as training tools.

4.15 Recommendations relating to information security policies are contained in Chapter 7 of the Information Security Guideline (from paragraph 7.8) and it is recommended that practitioners consider this guidance before embarking on the policy documentation process.

# Chapter 5

## 5. EMAIL RISK

**The aim of this chapter is to assist the reader in:**

- Identifying risks relating to eMail; and
- Considering interventions which may mitigate the risks.

### General

5.1 The purpose of this chapter is to highlight risks which may need to be addressed in dealing with electronic communications. The Guideline deliberately does not provide suggested wordings as it is believed firstly that each attorney should be capable of drafting appropriate wordings and secondly, the mind of the drafter should be applied to what is appropriate to the practice rather than general statements.

### Confidentiality

5.2 A non-negotiable obligation owed by an attorney to clients is that of confidentiality. The risk of the potential compromise of confidentiality in using eMail in the normal course without properly protecting the communication is that it may be compromised.

5.3 eMail in itself is not secure, neither is the communication of client information contained in attachments to eMails. It is not suggested that all eMail has to be secured as often information communicated by eMail relates to issues in respect of which confidentiality may not be important. However, there is often a fine line between what may be confidential and communications that are not confidential. Attorneys would do well to consider what eMails they require to be secured and what the appropriate safeguards may be.

5.4 While there are methods of securing documents sent by eMail by way of attachment (for instance protecting the document using a password) the protection provided is often more illusory than real. An example of this is, as frequently happens, the documents are communicated by way of attachment to an eMail and the document is password protected. However, the password required to access the document is sent in the same eMail. Even the transmission of a password by a separate eMail but to the same eMail address will provide little security if a person with malicious intent has access to the eMail address.

5.5 It is suggested that users of an attorney's information system be trained to create strong passwords. These should be at least 8 characters long (the length of a strong password will make it more difficult to "crack"), use alpha characters in both upper and lower case, use numeric characters and special characters.

5.6 While in some instances the use of passwords to protect confidentiality may be appropriate, one of the accepted mechanisms of protecting confidential information while it is being communicated and while it is being stored by either party, is encryption. Encryption technologies and techniques, if properly used, ensure that only the intended recipient is able to read the information. Many of the standard operating and eMail systems facilitate encryption which may be appropriate for all but the most

sensitive information. Typically these are easily used but their use requires planning, training of staff and in certain instances the education of recipients of the encrypted information.

5.7 While some of the encryption technologies are not particularly strong and would not withstand a serious hacking effort, they are, like the password protection of documents, better than nothing.

5.8 Attorneys who are serious about their professional obligation of maintenance of the confidentiality of their own and client's information should consider the use of digital certificates and electronic signatures provided by reputable public key infrastructure (PKI) providers. By doing so, they will protect against, not only the potential interception and hacking of eMails and attached information while being transmitted between the sender and the recipient, but also provide protection against confidential information which is inadvertently sent to an incorrect recipient from being opened. While it is beyond the scope of this Guideline to provide attorneys with a full background of the advantages of the use of encryption, digital certificates and electronic signatures (the appropriateness of which may differ from practice to practice) attorneys are nonetheless urged to consider this as an important consideration in their information security in general and, in particular, in the safeguarding of their electronic communications.

**Acceptable and Lawful Use**

5.9 All unlawful use of an eMail system should be expressly prohibited in an eMail policy. However, sometimes use of eMail may be unlawful without the user being aware that it is unlawful. Specific training should be provided in what activities may be unlawful or unacceptable to the practice.

5.10 In some instances behaviour may be legal but unacceptable within the practice. For instance the distribution, dissemination and storage of images, text or materials that may be considered indecent, pornographic, obscene or discriminatory, may also be prohibited by the practice's eMail policy.

5.11 Provisions of this nature are aimed at preventing harm to staff, discontent and disputes amongst staff, reputational risk which may attach to the practice as the result of an external dissemination of the information, or loss in productivity and unnecessary burdens on the technological infrastructure of the practice.

5.12 It is also recommended that there are prohibitions against the forwarding of chain letters, unsolicited commercial advertising material or the access of copyrighted information in a manner that may violate the copyright.

**Reputational Risk**

5.13 eMails which are unlawful, alternatively contain unacceptable content which may be communicated by an employee of a practice, even where the eMails may be subject to disclaimers, will be seen by the recipient(s) as coming from the practice and may cause embarrassment or even liability and claims against the practice.

5.14 In view of the accepted norm that organisations using eMail should properly manage its use, reputational damage that may be caused to a practice may be considerably greater than monetary damages that may be suffered.

5.15 The importance of mitigating against reputational risk and educating employees so that they may appreciate this risk should not be under estimated.

5.16 In this regard prohibitions against forwarding eMails received, sending chain letters (however benign they may be) and using the "reply to all" button should be considered.

5.17 One of the mechanisms that has been used successfully is that some organisation prohibit the use of eMail for anything but the most formal responses (For instance responding to information to set up a meeting or advising on times of availability). All other correspondence is communicated by way of letters on the organisation's letterhead which are attached and sent by eMail.

5.18 The rationale, and apparently proven results of this policy are:

- Immediate, unnecessarily emotional and precipitous responses are avoided;
- The psychological effect of using a company's letterhead and the realisation of the fact that the response is not, or should not, be personal, leads to a more considered and appropriate response; and
- A more careful consideration of parties to whom the response may be addressed or copied.

5.19 In certain instances policy provisions have been established which provide that only more senior members of the organisation's staff actually dispatch such letters from their eMail addresses. This allows for a checking of the content and ensuring that it meets the language and grammatical standards of the organisation as well as ensuring that the content is accurate and appropriate.

**Personal Use**

5.20 One of the most taxing issues in developing eMail policy is the issue of personal use. Many organisations state in policies that the use of their eMail system is solely for the purpose of business and personal use is prohibited. However, despite this prohibition, in the vast majority of cases the general behaviour within the organisation is quite different. Where this occurs, the prohibition is negated from a legal perspective by the actual practice and internally it becomes difficult to enforce this prohibition in disciplinary or legal proceedings. Against third parties, the fact that there may be disclaimers providing that eMails are to be used for business purposes only may, if the behaviour in the organisation differs from this policy, prove difficult to support.

5.21 Another issue which may become relevant, in the absence of the express agreement of users of the firms information system, is the monitoring and reading of the content of personal communications.

5.22 While some may argue that merely by virtue of the fact that the employer owns the technology they have the right to monitor communications, the fact that the privacy of communications is a constitutional right needs proper consideration. The fallacy of this argument is illustrated when one considers that very often the telephone may be owned by the employer, however it is quite clear that the employer has no right to monitor communications (particularly personal communications) which may be made using a telephone.

5.23 It is suggested that a practical solution to this problem would be to create a distinction between personal communications and business communications. In these circumstances in order to allow the monitoring of business communications (which it is the duty of attorneys to properly manage) and personal communications would be to facilitate a separate mechanism for the communications.

5.24 In some instances this could be facilitated by using separate eMail templates for personal communications and business communications. This will allow different rules to apply to business and personal communications.

5.25 In this instance the eMail policy would prohibit any personal communication being made using the business template and the user would waive any rights that they may have against the monitoring of personal communications which are made using the business or any other template save for the template provided for personal communications.

5.26 The advantages of this approach could be that personal communications may be:

- Limited to short communications;
- Not permitted to carry attachments;
- Have a different (much shorter) retention period; and
- Include appropriate disclaimers protecting the practice against inappropriate use of personal eMails.

5.27 Certain organisations have taken the step of providing separate eMail boxes to their employees. One is used exclusively for business and the other exclusively for personal eMails. The same principles of many of the same policy statements applying to both eMail boxes, with appropriate distinctions and prohibitions, where necessary, applying to the different eMail boxes, has allowed these organisations to far more easily manage personal eMail, avoid issues relating to the monitoring of personal eMail and significantly decrease the technological overhead required for their eMail facilities.

### Malware (Viruses and SPAM)

5.28 While the protection against SPAM and viruses is typically technological, firewalls and the anti-virus software are not infallible. In the circumstances not only the technological issues relating to firewalls and anti-virus software should be addressed by a practice but so too must users be made aware of the implications of opening suspicious eMails, SPAM or software from unknown sources.

5.29 While not necessarily part of an eMail policy, the establishment of firewall and anti-virus protection is something that practice's need to be aware of. It is also important to ensure that these protections remain up to date and protect against the ongoing and continuous assault that the Internet is subjected to in this regard. A failure to maintain updated protection can have disastrous results.

5.30 As indicated in Chapter 2, at least two thirds of eMail traffic is SPAM (Unsolicited Electronic Communications). The detrimental effect of SPAM ranges from the unnecessary eMail traffic which may burden, slow and sometimes even cripple eMail systems.

5.31 More insidious is the fact that SPAM very often contains software which, if opened or executed, will allow the spread of viruses through the organisation's information system. Users should be educated not to open unsolicited electronic communications or any communication which appears suspicious. They should be advised that the offer of prizes and money in this manner is "too good to be true" and is always untrue. It must also be borne in mind that some SPAM (particularly where the personal information of the recipient may be used by the sender) can be well disguised and even the most sophisticated users sometimes fall into the trap of opening potentially malicious eMails. If this happens users must be required and encouraged to immediately report the breach as may be appropriate in terms of the information security policies of the organisation.

5.32 The access to eMail should be governed and managed to ensure that only the user of an eMail address is able to access the eMail at that address. This is addressed more fully in the Information Security for South African Law Firms Guideline dealing with access control. However, in view of the prevalence of the use of eMail within an organisation, it may be wise to repeat, amended as may be appropriate for

eMail, the restrictions on controlling access to a person's email address. Users must understand that the use of another's eMail address is unauthorised in all circumstances and therefore falls to be disciplined in the same manner as any unauthorised access to a computer. Users may also be warned that the unauthorised access to interception of or interference with data is a crime in terms of the Electronic Communications and Transactions Act.[5]

5.33 If a firm has a well established information security policy and framework the retention of its records, including eMail may be addressed in a record retention policy. Nonetheless, an eMail policy should, preferably by way of reference, advise users of the manner in which eMail will be backed up and retained. In many instances the retention of information would be vital to the business of clients and in more limited instances, may be subject to discovery of these electronic records. Users should understand that even if they delete eMails that these may still be in existence elsewhere and that in the normal course all business eMails should be retained. The issue of the distinction between private communications and business communications and the retention is addressed in dealing with personal use of eMail in paragraphs 5.20 to 5.27 above.

5.34 In view of the fact that eMail archiving needs to be done properly and in terms of considered policy, it is often worthwhile for practice's to investigate the tools available. There are eMail archiving tools which go a long way to ensuring that eMail is retained in such a way that it is easily searchable, and that it is encrypted in order to protect its integrity and provide appropriate evidential weight where necessary.

### Monitoring

5.35 The monitoring of business eMail both from the perspective of properly managing eMail and ensuring that unlawful use of the eMail is avoided (or where not avoided breaches can be detected) need to be established. In many instances legal firms in South Africa will have to rely on technologists to assist them in this process. However, the technologists must understand what is permitted in terms of the eMail policy and what prohibitions may be in place. It is strongly suggested that they are not made policemen but where they detect abuse of the system that they report an incident to the appropriate person within the firm so that the incident may be dealt with.

5.36 Where permission is given for personal use of the eMail system by employees or third parties the constitutional right of privacy must be taken into account. If adequate restrictions are in place the monitoring of the traffic relating to private use should be sufficient to detect any abuse of this privilege. However, if there is no clear distinction between personal and business eMail this becomes a lot more complicated, even if the consent to intercept and monitor electronic communications has been obtained in terms of Section 6 of the Regulation of Interception of Communications Act.[6]

### Sanctions

5.37 If it is suspected that an employee is in breach of provisions governing the use of the electronic mail system appropriate sanctions should be enforced. In most instances this should happen in conformance with the disciplinary policy of the practice and no specific mechanisms need be established in the eMail policy. However, it may be that the sanctions for certain breaches need to be highlighted in the policy.

[5] Section 86 of the Electronic Communications and Transactions Act, 2002

[6] Section 6 of the Regulation of Interception of Communications Act, 2002

# Chapter 6

## 6. THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT ("ECT ACT")

**The aim of this chapter is:**

- To draw the attention of attorneys to the provisions of the ECT Act governing electronic communications, including eMail; and
- Provide some commentary on compliance with the ECT Act.

6.1 The **Electronic Communications and Transactions Act No. 25 of 2002** governs electronic communications. The Act defines an electronic communication as a communication by means of a "data message" and a "data message" in turn is defined as:

> *"data generated, sent, received or stored by electronic means and includes*
>
> *a) voice, where the voice is used in an automated transaction; and*
>
> *b) a stored record;"*

6.2 eMail, short message services (SMS), instant messaging (IM), multimedia services (MMS), telefacsimile (fax), telephony (in particular digital telephony) and mobile messaging all fall within the ambit of the definition of "data message".

6.3 eMail is also expressly defined as a data message used or intended to be used as a mail message between the originator and the addressee in an electronic communication[7]. In the circumstances it may be argued that the forms of electronic communication referred to above also fall within the definition of eMail. From the perspective of this guideline the distinction is not really significant in that all electronic communications, if they are used in the course of the conduct of the practices business, should be properly governed. Alternatively, their use should be prohibited.

6.4 Chapter III (Part I) of the ECT Act is applicable to facilitating electronic transactions. One of the more important pronouncements in our modern law is that information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.[8]

6.5 Where the law requires that a document be in writing, this requirement is met by an electronic communication, if it is accessible in a manner usable for subsequent reference.[9]

6.6 In most instances electronic communications (including digital telephony) are accessible in a manner usable for subsequent reference. It should also be borne in mind that even where an electronic communication may be deleted by one of the parties to the communication, it is possible that it will remain accessible in a manner usable for subsequent reference, by the other or another party to the communication retaining the communication. Alternatively the communication may be retained by a service provider.

---

[7] Section 1(Definitions) of the ECT Act

[8] Section 11(1) of the ECT Act

[9] Section 12 of the ECT Act

6.7 Where the law requires information to be presented or retained in its original form, the requirement is met by a data message if the integrity of the data message can be demonstrated to have remained complete and unaltered in the light of the purpose for which the information was generated and having regard to all other relevant circumstances.[10]

6.8 It must be stressed that unlike the paper and text environment, electronic communications are in many circumstances indistinguishable in the original or in a copied form. Further, that the ability to change an original without it being detected is far greater in the electronic environment than with paper and text. As a result of this the emphasis on the integrity of the purported original having to be established is high. Disputes relating to eMail often arise as a result of parties having different versions of purportedly the same eMail, quite often maliciously amended. To meet the requirements of this provision regard should be had to the provisions relating to retention and admissibility of evidence which are dealt with below.

6.9 The retention of electronic communications are dealt with in Section 16 of the ECT Act which provides:

*"16.* ***Retention***

1) *Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if-*
   a) *the information contained in the data message is* ***accessible so as to be usable for subsequent reference****;*
   b) *the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and*
   c) *the origin and destination of that data message and the date and time it was sent or received can be determined.*
2) *The obligation to retain information as contemplated in subsection (I) does not extend to any information the sole purpose of which is to enable the message to be sent or received."*

(Emphasis added by the author)

6.10 The importance of secure retention of data messages and electronic communications is highlighted by the words emphasised in this section and the words "reliable" and "integrity" are used in dealing with the evidential weight of data messages in 6.11. This indicates the high premium that should be placed on information security in ensuring compliance with the ECT Act. If eMail is to be relied upon by attorneys in the conduct of their business, by administrative bodies with which they may be required to interact within discharging duties to clients and in legal proceedings, care must be taken to ensure that the appropriate security is applied to the creation, communication, retention and deletion of eMail.

6.11 The admissibility and evidential weight of data messages is governed by Section 15 of the ECT Act which reads:

*"15.* ***Admissibility and evidential weight of data messages***

1) *In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence*

[10] Section 14 of the ECT Act

*a) on the mere grounds that it is constituted by a data message; or*

*b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.*

*2) Information in the form of a data message must be given due evidential weight.*

*3) In assessing the evidential weight of a data message, regard must be had to*

*a) the **reliability** of the manner in which the data message was generated, stored or communicated;*

*b) the reliability of the manner in which the **integrity** of the data message was maintained;*

*c) the manner in which its originator was identified; and*

*d) any other relevant factor.*

*4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract."*

(Emphasis added by the author)

6.12 As attorneys we should be mindful of the fact that although it only occurs infrequently, transactions which we are dealing with may, if disputed, require the adducement of evidence in dispute resolution or legal proceedings. While the legal rules relating to retention of records will always apply, it is important that attorneys understand what is required in the retention of electronic communication to ensure its efficacy in the normal conduct of business, and where necessary, in legal proceedings.

**Information Security**

6.13 As has been demonstrated in this Chapter, there is a high premium on the secure retention of electronic communications. The techniques and practices which will assist attorneys in establishing the integrity of records are more fully dealt with in the LSSA Guideline on Information Security. These should be considered in the management of eMail.

# Chapter 7

## 7. DEVELOPMENT OF AN ELECTRONIC COMMUNICATIONS POLICY

**This Chapter is aimed at assisting attorneys in:**

- Considering issues and risks important in the development of an electronic communications policy;
- How to develop an electronic communications policy.

### How to Develop an Electronic Communications Policy

7.1 It is recommended that among the information security policies that are developed by attorneys that electronic communications are expressly dealt with in an Electronic Communications Policy

7.2 The issues highlighted in 7.5 to 7.24 should be dealt with in an Electronic Communications Policy. Every practice is different. Therefore recommended wordings are not provided as the temptation is always to cut and paste without properly considering the specific requirements of the practice. This Chapter should rather be used as a checklist of issues which may be addressed by attorneys in governing and managing eMails, which will assist them in drafting policies appropriate to the practice.

7.3 In developing this policy regard must be had to the technologies employed by the practice as well as how those technologies are configured. However, while the technologies may in certain circumstances place limitations on the controls that can be exercised, it is strongly recommended that the policy must firstly address the obligations of the practice and in the event the technologies limit the desired policy, that consideration needs to be given to replacing or enhancing the technologies to ensure that the practice's legal obligations (legislative and contractual) may be discharged.

7.4 The issues which are addressed in this guideline are, by their nature, general and there may be electronic communication technologies and techniques that are used which will need to be more comprehensively addressed.

### ISSUES AND RISKS TO BE CONSIDERED IN AN ELECTRONIC COMMUNICATIONS POLICY

### Admissible Technologies and Techniques

7.5 Most practices will be in control of and have servers through which eMail is facilitated. However, the same control may not be exercised over SMS or instant messaging (IM) or cellular technologies in which control of the communications and records are in the hands of a third party. In these circumstances it may be wise to require that all business communications will be by way of eMail facilitated by the practice only.

7.6 Of course there may be instances where other technologies such as SMS are used for business purposes. For instance if SMS is used to report registration from a Deeds Office it should be stipulated that SMS may be used only for that purpose and that records of the SMS messages and if required, records are to be retained and backed up. It may also be important to ensure that the practice actually purchases the mobile device used for the communication of SMS messages and that it does not rely on a mobile device owed by an employee.

7.7 It may also be expressly stipulated that SMS may be used for arranging and confirming meetings but not as a formal mechanism of communication which can be considered to be binding on the practice.

7.8 Where control may not be exercised over the technologies or retention of information communicated using the technologies, it would be wise to ensure that service level agreements, expressly stipulating the practise's right to access the records are concluded.

**Access to eMail**

7.9 Access to eMail is often provided with little thought to ensuring that users understand the conditions on which access has been granted. It is recommended that the access should be granted conditional upon acceptance of an electronic communications policy.

7.10 In practices where electronic communications policies have not been established, it is recommended that a programme be instituted to introduce policy and guidelines around which access to electronic communications are governed within the practice. Further, that all users are provided a deadline against which they must accept the conditions of the electronic communications policy, failing which access will be revoked. Ideally, in logging on to a practice's network, users should accept the terms and conditions governing their access to and use of the networks which would include the electronic communications policy. However, many practices will not have the facility or know-how to incorporate electronic acceptance of the conditions in the practice's logon procedures. In these circumstances it will be necessary to ensure paper and text agreements are signed and properly retained.

7.11 It should be a part of the induction programme for any new employees that they are educated in the use of the practice's information systems, the safeguards required and that they accept the policies, procedures and standards which govern the use of the practice's information systems.

7.12 An oversight which is often committed is that on termination of the employees employment access to information systems is not properly revoked. The result of this may be that if the employee has remote access that they continue to have access to the practice's information systems after the termination of their employment. Further, what often happens is that communications intended for the employee continue to be received without being redirected to whoever has taken over the employees responsibilities.

7.13 The control of access, agreement by users to policies governing the use of electronic communications and the revocation of access on the termination of an employee's employment, for whatever reason, requires strict and meticulous control.

**Personal eMail**

7.14 The personal use of eMail is one of the most taxing of issues facing most organisations in managing electronic communication. The fact is that permission allowing personal use is often abused.

7.15 In certain instances the prohibition of personal electronic communication (in most cases limited to eMail) is stipulated in policies. However, practically this simply does not work. The fact is that despite these prohibitions, in almost every circumstance (certainly in every circumstance that the author has had to investigate for the purposes of policy development, information security breaches or disciplinary action) the practise is that from the senior echelons in the organisation to the most junior, private use is made of electronic communication facilities.

7.16 Even if a policy prohibits personal use, if the practice of the organisation allows personal use and does not discipline breaches of the prohibition, it is unlikely that in disciplinary or legal proceedings, personal use in the normal course will be capable of being properly and justly enforced.

7.17 In the circumstances organisations are generally accepting that electronic communication facilities may be used for personal, incidental, limited purpose. However, this restriction is subject to interpretation and may still create difficulties in determining what is reasonable. It also raises the issue, once personal communication is allowed, of the privacy of personal communication. This issue is dealt with later in this chapter.

7.18 The solution to the distinction between personal and business eMail is in many circumstances easily accommodated by the technologies. It also allows that different rules relating to the use of eMail accounts for personal and private communication may be applied. In certain circumstances this is being regulated and enforced merely through policy which may require differing "signatures" (facilitated by eMail templates created and applied to eMail within the eMail application), including appropriate disclaimers, to be used in the case of personal as opposed to business eMail.

7.19 In other instances organisations are beginning to provide employees with separate eMail accounts which are stipulated for personal and business use respectively, each of which are governed by specific rules and which may have different technological limitations and restraints.

7.20 Thus, an organisation may stipulate that for all business eMail:

- A specific template and disclaimers, ensuring compliance of the organisation with all regulatory issues governing its communication and documentation must be used;
- That a letter addressed on the practice's letterhead must be used in all communications other than those that are not of legal importance, and transmitted as an attachment to an eMail communication.
- That where a letter bearing the practice's letterhead, as contemplated in the bullet above, is used that it is appropriately secured to avoid tampering or loss of confidentiality (eg. in PDF, password protected or encrypted);
- The transmission of communications on the organisation's letterhead attached to eMails may be restricted to certain levels of seniority or authority.

7.21 Personal eMails on the other hand may have the following restrictions:

- Only a personal "template" which incorporates appropriate disclaimers may be used for personal eMails;
- A restriction on the length of the personal communication;
- No attachments will be communicated using personal eMail;
- The eMail may not be encrypted in any manner;
- The eMail will not be subject to the normal backup retention procedures of the employer and if the employee wishes to retain the eMail it will have to be backed up separately; and
- The eMail will be automatically deleted from the employer's information system after a specified period.

7.22 To enable the practice to maintain control over eMail there should be a prohibition against any other eMail accounts being opened and used for business purposes by an employee. Thus business

communications should not be sent to personal eMail accounts other than those under the control of the practice.

7.23 Other risks which should be considered in developing an eMail Policy are, without limitation:

- Unwitting conclusion of contracts not intended;
- Exposing confidential information of the practice or its clients;
- Potential misuse of intellectual property rights of third parties;
- Failure to protect the personal information of third parties;
- Potential liability for the distribution of sexually explicit, discriminatory or defamatory content;
- Possibly introducing viruses or other damaging software to the practice's information system;
- Failure to use appropriate disclaimers;
- The use of electronic communication which may disrupt or delay the use of the practice's information systems; and
- Personal use of electronic communications which may not be reasonably incidental or limited and which may adversely affect an employee's productivity during work hours.

7.24 If the risks identified as a threat are not accepted by the practice they should be appropriately dealt with in an electronic communications policy.

7.25 The size of the practice and the nature of information communicated will determine the nature and content of an electronic communications policy. The policy should also provide clear parameters outlining the use of electronic communications facilities provided by the practice but also how breaches, accidental or malicious, should be reported and dealt with as well as disciplinary measures which may need to be taken. In this regard the reader is referred to "Policy Structure" (paragraph 7(10) to 7(16) contained in the LSSA Guideline on Information Security for South African Law Firms.

# Chapter 8

## 8. UNWITTING CONCLUSION OF CONTRACTS NOT INTENDED

**This Chapter is intended to:**

- Draw the attention of practitioners to the risk of contracts being "signed" by persons lacking the requisite authority.

8.1 One of the risks of electronic communication is that contracts, agreements or arrangements may be entered into unwittingly, alternatively be entered into by persons who lack the authority to do so. In certain circumstances, particularly if it appears from the eMail that the person has authority, the practice may be held to a contract to which it did not intend to be bound. While disclaimers are used in a rather cavalier fashion and regarded as a protection against the risk, often, particularly where the conduct of the user may be consistent with a person having proper authority, the disclaimers may prove to be of little value.

8.2 The traditional controls inherent in "wet signatures" (signatures signed on paper with a writing instrument) will not apply to electronic communications. In fact the definition of an "electronic signature" is that "data attached to or logically associated with other data and intended by the user to serve as a signature" constitutes a signature. Thus, where an electronic signature (as opposed to a digital signature) is used, issues as to the intent of the user may create some difficulty and may prevent the practice from disclaiming that the signatory had the necessary authority.

8.3 Thus, even a typed name would constitute a signature and a person disclaiming the signatory's authority, particularly if the signature is provided in a context which may indicate authority (for example through the practice's eMail system) may be estopped from claiming that the employee had no authority.

8.4 A mechanism which may be used to mitigate against this risk is that all documents which may be intended to be binding on the practice be stipulated in the policy to have to be on the practice's letterhead (electronic template) and communicated by way of an attachment to an eMail. A disclaimer clearly indicating that only electronic communications communicated in this manner are binding on the practice would, if the practise is consistently followed, afford greater protection.

# Chapter 9

## 9. EMAIL DISCLAIMERS

**The aim of this chapter is to assist attorneys in:**

- Providing guidelines for the consideration of appropriate disclaimers;
- Highlighting the ineffectiveness of inappropriate disclaimers.

9.1 Many eMails bear disclaimers relating to the use of eMail itself. Unfortunately, for the most part these are used by cutting and pasting, alternatively copying, disclaimers from other eMails. In all too many instances the disclaimers are inappropriate.

9.2 Against this background it is not unusual to see disclaimers which run counter to the use of the eMail and the ostensible authority of the user of the eMail. An example is the statement that any representations made by the user cannot be attributed to the organisation. In many cases the conduct of the user and quite often the user's authority as established in legislation (for instance the Companies Act) gainsay this disclaimer.

9.3 In the circumstances legal firms would do well to carefully consider the disclaimers they make. If they do distinguish between personal eMails and business eMails the disclaimers will be quite different and can specifically address the different nature of the communications.

9.4 Subject to the legal consideration of ensuring that reasonable steps have been taken to bring the terms of disclaimers (or any other terms governing the use of eMail) to the attention of the recipient, the disclaimers may be provided by way of reference, which is easily done by creating a link to a website on which the organisation may post these terms and conditions. This allows for disclaimers not to clutter an eMail and more extensive terms relating to the use of eMail to be published to the recipient.

9.5 It should also be noted that in terms of the Companies Act the name and registration number of the company must be mentioned in legible characters in publications, which include all letters of the company. While it is not expressly stated, the context of the provision indicates that this would include eMail. This provision should be adhered to in the design of eMail templates and the drafting of conditions of use of the Mail, whether contained in the eMail itself or by way of reference.

# Chapter 10

## 10. EMAIL DISCLAIMERS AND COMPLIANCE WITH THE COMPANIES ACT

### Disclaimers

10.1 There appears to be little consistent use of disclaimers in eMails by South African attorneys. In many instances eMail disclaimers are examples of a "cut" and "paste" mentality rather than careful thought being provided to the risks relating to the eMails.

10.2 Unless eMail disclaimers are properly thought through and apply properly to the eMails to which they are attached the protection that they provide may be extremely limited.

10.3 For instance a disclaimer that I have in innumerable eMails is the disclaimer which reads "The contents of this eMail and any attachments are confidential, may be privileged and are intended solely for the use of the named recipient(s). If you have received this eMail in error, **you are not to read it**, disclose, distribute or retain any part of it. Please will you notify the sender immediately on receipt of this eMail that you are an unintended recipient and delete the eMail." This disclaimer almost invariably appears at the bottom of the eMail. As most people will read from top to bottom it is highly improbable that they will read the disclaimer before reading the eMail and therefore makes a nonsense of the disclaimer itself and probably renders it unenforceable.

10.4 The above example, allied to the fact that in our law the person whose attention is not drawn to disclaimers or other conditions governing the behaviour of a third party, care needs to be taken to ensuring the proper placement of disclaimers in eMail and that they are appropriately prominent.

# Chapter 11

## 11. CONCLUSION

- Law is an information intensive profession.
- eMail has become the de facto method of communication for most practices.
- Attorneys have certain obligations of confidentiality in attorney and client privilege which they are duty-bound to discharge.
- Without a clear electronic communications policy governing electronic communication, it is unlikely that attorneys can discharge their obligation appropriately.
- Attorneys need to devote time and effort to the development of appropriate electronic communications policies as they are a critical aspect of any modern attorneys practice.
- The benefits to attorneys will not only be an improvement in the proper use of electronic communications and the security of electronic communications but will also be evidenced in more efficient and better management of communications generally.