COMPUTER TECHNOLOGY: IT'S RAMIFICATIONS ON DATA PROTECTION AND THE RIGHT TO PRIVACY IN ZAMBIA.

BY

PROSPER TAURAI MUYATWA

AN ESSAY SUBMITTED TO THE UNIVERSITY OF ZAMBIA IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF THE DEGREE OF BACHELOR OF LAWS.

THE UNIVERSITY OF ZAMBIA

FACULTY OF LAW

LUSAKA

2000

THE UNIVERSITY OF ZAMBIA

SCHOOL OF LAW

I RECOMMEND THAT THE OBLIGATORY ESSAY PREPARED UNDER MY SUPERVISION BY:

PROSPER TAURAI MUYATWA

Entitled

COMPUTER TECHNOLOGY: ITS RAMIFICATIONS ON DATA PROTECTION AND THE RIGHT TO PRIVACY IN ZAMBIA

Be accepted for examination. I have checked it carefully and I am satisfied that it fulfills the requirements relating to format as laid down in the regulations governing obligatory essays.

Date: 5th May, 2002

Supervisor: Mr L. Kalinde

Signature: L. Kalinde

DEDICATION

This piece of work goes to the most beautiful and staunch love of my life, Rose Muyatwa – a mother and half.

ACKNOWLEDGEMENTS

The author is indebted to the scholastic prowess prevailing in the School of Law at the University of Zambia. The invaluable contribution of the learned men and women lecturing in the School of Law moulded me into a lawyer. There jest will certainly for a long time to come linger in my mind.

My special thanks are due to Mr. L. Kalinde, my supervisor, who through his incisive comments and guidance, this work became a worthwhile academic undertaking. You allowed being disturbed even in places of relaxation. I wish to pay tribute to all relatives, friends and family, failure to do so would be equivalent to "Contempt of Court" given the valuable support they all gave me.

Finally, I wish to thank Mr. P. Khunga for the typing and the patience, looking at the flaws in my handwriting

TABLE OF CASES

TABLE OF STATUTES AND INSTRUMENTS

The Constitution for Zambia as amended in 1996.

The Criminal Procedure Code Chapter 88 of the Laws of Zambia.

The banking and Financial Services Act Chapter of the Laws of Zambia.

The State Secrets Act Chapter III of the Laws of Zambia.

The Federal Protection of Privacy Act (Canada).

The Data Protection Act (1984) (British).

The Credit Control Act (British).

The Computer Security Act (1987) (British).

The Privacy Act (USA).

The Canadian Criminal Code.

The Universal Declaration of Human Rights.

The European Convention for the Protection of Human Rights and Fundamental Freedoms.

The African Charter on Human and Peoples' Rights.

The Consumer Credit Act (1974) (British).

ABBREVIATIONS

EFTPOS	Electronic Funds Transfers at Points of Sale
PC	Personal Computer
e-mail	Electronic Mail
CD	Compact Disk
BSA	Business Software Alliance
CSA	Computer Services Department
OECD	Organisation for Economic Co-operation and Development
COMSA	African Computer Supplies Association
SAP	Structural Adjustment Programme
FBI	Federal Bureau of Investigations
IT	Information Technology

TABLE OF CONTENTS

Chapter 4

Chapter 5

"Although it is difficult to limit a discussion about computers to the present, the future is hostage to them. It is no way remarkable that computer technology is such a pervasive problem for the law and its institutions. Law making tends to move slowly in the hands of non-technologists. Computing technology has developed rapidly beyond the understanding of all but few changes of the beginning of the twentieth century such as the development of the automobile, aviation and energy industries. As the century closes, the pervasive industry is that of informatics. Its impact on the law will be no less, and in all probability far greater, than that of its forerunners, for the law is itself overwhelmingly dependent on information".

(per Mr Justice M. D. Kirby :Chairman of the Australian Law Reform Commission, Paper presented on 7 July (1981) at the 21st Australian Legal Convection).

CHAPTER 1

INTRODUCTION

BACKGROUND TO THE TOPIC

Computer law as a research topic may raise a lot of eyebrows and curiosity among conventional conservative academic lawyers because the subject is not as clearly defined as the Law of Torts, Family Law or Criminal Law. However incidence of computer technology use and abuse has become more prevalent and has metamorphosised into a reality of the present and the future age.

Although the invention of the computer is the greatest contribution to the quality of human life, it is predicted that computers will become the singular most important asset in affecting the lives of virtually every member of the Zambian Society and the shape itself. Today's computers and communication systems, to say nothing of the future, are less expensive and are more accessible. With the increased use of information and as we step into the epoch of informatics, tomorrow will presage a dramatic narrowing of the already narrowed sphere of personal privacy.

It has to be accepted that the problems of privacy today are new and overwhelmingly technical. The present law not only accords too little

weight to legitimate privacy claims and protection, but will become increasingly inadequate as computers proliferate and connect up to form huge pools of information: with the undoubted evidence that this new technology is, and will influence many aspects of life. Thus, for instance Lawyers must address, more urgently than before the implications of the computer for their discipline.

The debate that this paper will seek to address about privacy and the security of personal information is that invasion of privacy is a serious and widespread problem worth a critical analysis and that measures should be adopted that will reduce the incidence of such invasion. The legal remedies that exist in Zambia to protect an individual whose privacy is threatened by information retrieval systems is too scattered within varied statutes such as the Banking and Financial Services Act, The Criminal Procedure Code, The State Secrets Act and others.

Chapter (iii) of the Constitution of Zambia also provides for the protection for the privacy of One's home and other property.[1] There is a natural difficulty in enforcing legislation that is so scattered and hotchpotch in approach. If a serious approach to the protection of privacy is to be made, then there is need that an omnibus statute on the protection of privacy be created to deal with the situation.

Quite admittedly the law is slow to change and such slowness is even more marked in an area where technical change is so rapid. As we ask computers to do more for us, the opportunity for their use to touch on a broadening range of human activities must expand and this generates legal problems. Therefore as the technology becomes more pervasive, more daring and more sophisticated the importance of making sure its use is properly regulated and controlled increases. Such a revolution has become even more scary as it was predicted that by the turn of the century the strength of computers would be more than formidable. Already computers have taken over our routine jobs like the handling of reservations at airports, running bank accounts, taking care of records in the hospital and handling cash flows at points of sale in supermarkets, among many other functions.[2]

Due to such advancements, even the self-preservation in the legal profession has not been sparred. Arising to haunt us is the jurisprudential question for legal theory and development. Legal thought has been to a large extent a preserve of a legal practitioner because of his rigorous training, his Irish wit and Solomonic wisdom, his encyclopaedic mind, his ability to collate legal information from the voluminous books from which it appears. The way Lawyers and non-lawyers thought, was harnessed by the limitation in print, but today, we are finding ourselves free of such limitations because of technological

innovation. It is therefore important to envisage and to ask ourselves questions like what will happen to the sacred, the secretly and jealously guarded monopoly of the legal practitioner, if laypersons can access legal precedents and their interpretations on the computer? Worse still the diminution in privacy due to the ability of computers to control what the individual has, over the way he is held by others? We are not alone in this predicament. An American judge had this to say about the coming computer age:

"Lawyers and courts need no longer feel ashamed or even sensitive about this charge, often made that they confuse the masses by comparison, the misnomer and industrial short hands of the computer world would make the most esoteric legal writing look like Gettysburg address "[3]

In March 1997, Butterworths SA a major publishing powerhouse introduced on CD-ROM an index capable of accessing, in Southern African countries, Law Reports and Statutes by the touch of the button, which facility has blossomed in some more technologically advanced countries such as our Africa counterparts in South Africa. This facility will make research and the study in law more pleasurable and far easier.

As a preliminary remark, the intentions of this paper is more than a restatement of what other disciplines and jurisdictions have already identified as the fastest growing discipline of the present legal age. It seeks to convince authorities in the Law Faculty that there now is an inevitable take-over and shift towards what has been termed DEMATERIALISATION, which is the movement away from paper towards electronic means as the favoured medium of records. In as far as the process of computerisation is concerned, the legal profession may be in the early stages of this evolution, but change will come quickly.

The fact that most graduating lawyers will be found wanting in such basic skills will be a reality. The inadequacy of having acquired a law degree without the command of the language of the present computer age shall provide an embarrassment and a serious handicap to our hard earned qualifications.

In a survey carried out at the University Of Zambia Law Faculty, It. was revealed that about 80% of the present enrolment of Law students can not use a computer.[4] In an interview, however, with Mr Jeff Ryan of Cornell University formally attached to the faculty and one of those that spearheaded the faculty 's computerisation process, he mentioned that

computer appreciation courses should be offered to enable final year students to use Data Base created in the Library because a Lawyer nowadays requires more than operational and typing skills.[5] He is inadequate if equipped with only solomonic wisdom for it may be antiquated without Bill Gates Craftsmanship.[6] He cannot be of chamelionic caution in a world that relies on CYBERSPEED.

More so, he cannot be proud of his Glossatic Scribes tendencies in an age where Computer proficiency and manipulation is what counts most. The University of Zambia has to be awake to such changes in technological pace and thus follow examples of Law schools elsewhere. One very active institution has been the University of Windsor Faculty of Law in Windsor, Ontario and another has been the faculty of Law at the University of Alberta. Some Canadian Law Schools now teach a course specifically called 'Computer and Law'. At Dalhouse University in Halifax Professor Bankier teaches a seminar on 'Law and Technology .[7] The syllabus includes topics such as Intellectual Property or Computer Crime, a multi disciplinary course on the social impact of computers which includes Computer and Labour, Information as Power, privacy etc.[8] The University of Toronto has also began teaching a course in 'Computer Law and Technology'[9].

Despite the youth of computers and their practical application in African Universities, their importance cannot be underestimated. Human literacy today, unlike the days before us, is no longer measured by the ability to read and write. It now involves the ability to use a computer in daily applications. Arguably, in the developed countries, Computer Law is now firmly established as a discipline in its own right. It is the biggest growing academic field at Harvard and Cambridge University. [10] its application in those jurisdictions cannot be explained only on the level of technological advancement of those countries but also on their reasoned assessment and predictions of the near present and the future.

If computers are to take over the world in this millennium (as they will indeed do) then for the law to choose to concentrate on conventional legal thought may be pedantic and a stubborn conservative means that refuses to adapt to change.

The Law School at the University of Zambia should be persuaded to consider reforms within such examples as above. It is recommended to the faculty Board to consider 'Computer and Law' as an option to its curriculum and keep pace with reality.

However the thrust of this paper shall be on Data protection with particular emphasis being paid to the need to protect privacy by securing information held on computers. The ability of computers to collate mountains of information held on individuals has given rise to the concern about the effects that this may have on privacy. These effects are many and numerous to mention. They include their anticipated suffocation of privacy and their reduction of routine labour. Although it is conceded that old information systems also have their dangers and that the computerization of records and the new information technology in aggregate do not alone explain contemporary concerns about individual privacy, it should equally be accepted that because of computers: [11]

i) The assault and intrusion upon privacy are greater now because of technological advancement than they have been before, that such intrusions are increasing and the rate of increase itself is increasing;

ii) That part of the blame for such deterioration must be ascribed to the development of modern technology and especially to the application of computers to data processing and collection;

iii) That much of the information is inaccurate and goes unchecked and is regarded by its users as irresistible evidence of whatever it asserts or suggests;

iv) It is feared that this information, even though it requires technique and skill to access than information on paper can be hacked by very simple methods. The more damaging feature being that the process is less tedious, faster and provides more information in a short period of time;

v) The present legal remedies available have been so far behind by the speed of technological change as to become quite incapable of protecting the subject of the information.

The increase in invasion of privacy is a pointer to the need for its protection and a proportional realization that a commitment to privacy is no different than the commitment to other values, such as freedom of expression or liberty. A clear statement in law that privacy is a central value could make us more aware of the valuable functions that privacy can serve. Privacy as a concept is a perception that begins with ourselves. It is selfish but more necessary than most other rights.

The manner in which it should be observed and respected should be ultimate and practical: as it has been more precisely placed:

"The wish to have privacy must be in our hearts, not only in laws. But this does not mean that a commitment to the value of privacy should not be in our laws as well." [12]

If privacy as a right is not respected as fundamental by ourselves, then it becomes necessary that the law, as it protects other rights to free speech, freedom of association and the right to a fair trial, there is no reason why the right to privacy should not be protected, as it is a right as paramount to a human being as the others. It is about time that our laws should respect the autonomy in a human being and ensure that he is prevented from violation and undesirable exposure whose consequences will be a low estimation of the victim in the way that others hold him.

CHAPTER 1 - ENDNOTES

1. Article 13 of Chapter III OF THE Constitution for Zambia as amended in 1996. Subsection (c) of the Article provides for the protection for the privacy of one's home and other property. Also compare the provisions found in the Banking and Financial Services Act and the State Secrets Act. These provisions do not basically yield their legitimacy from the constitution in a straightforward manner and alas they are not consistent with each other.
2. B.W Napoer, **The Nature of Information Technology** Cambridge Law Journal, 1992 (S1) PP.4
3. See **Honeywell V. Lithonia Lighting jnc** 317 supp.407, 408 (N. D 1970)
4. Statistics are based not on the sampling method but indepth interviews and critical observation of almost each and every member of the class.
5. This research was carried out by the author, with assistance from the data base authorisation centre specifically Mr. Kambole formally conductor of internal management techniques.

   The research was however focused on the **final** year students as of 1999.

6. Bill Gates is an international Software magnate who discovered windows. He is the chief Executive of Microsoft and he has made billions of dollars through major breakthroughs in the computer world. He is a household mogul in the computer world and currently working on using computer technology in a bid to effectively vaccinate children especially in the third world.

7. Association of commonwealth Universities, **Commonwealth Universities yearbook** 1997 Volume 2 London P1779.

8. **Dalhouse University undergraduate prospectus,** 1999/2000 Dalhouse University.

9. **University of Toronto prospectus,** 1999/2000 University of Toronto

10. **American Unversities catalogue for International students,** 1996 - 1998, American information centre.

11. Halsey D.William, **Collier's Encyclopaedia,** 1987 Volume 9,Crowell Collier and Mcmillan, USA. PP457

Chapter 2

WHAT IS DATA AND WHY IS THERE A NEED TO PROTECT IT.

The technical features of computers are double edged in that modern computer systems can store more personal information in a more limited space and can collate it more quickly and more cheaply than was ever possible in older conventional systems and that the aim of such systems is to make that information more readily accessible. The first question that needs to be addressed is what really is a computer?

In simpler terms, it has been described:

"as an electronic device which can perform arithmetical and logical functions at extremely high speed under the control of a stored program."[1]

The question that this chapter seeks to address is whether the mountains of personal data held on computers could be secured and prevented from unauthorised access and whether computer use has created new threats to the protection of privacy than before.

For the purposes of this paper, Data is defined as ***information recorded in a form in which it can be processed by equipment***

operating automatically in response to instructions given for that purpose.[2]

Personal data consists of ***information, which relates to a living individual who can be identified from that information or from that and other information in the processing of the data user.***[3]

The freedom to control information contained about oneself on a computer exists in the ability to control the use made of personal data inserted in a computer program, therefore the right to check its exactness, the right to bring them up to date and to correct such data, the right to secrecy of sensitive data and the right to authorise their dissemination. All these rights together today constitute the new Right to Privacy.

Computers pose a threat to such individual privacy because they are new, regulation is slow in coming and because computing is becoming far more ubiquituous and less remote. It is possible to speculate that the time may well be not far distant when computerization of the most mundane administrative tasks will be commonplace in every office and place of business in the developing countries as ourselves and even perhaps in many homes, as is becoming the increasing trend in the more technologically advanced countries.

The speed of computers, their capacity to store, combine, retrieve and transfer data, their flexibility and the low unit cost of the work, which they can manage, do have serious implications:

i) They facilitate the maintenance of extensive record systems and the retention of data on those systems;

ii) They can make data easily and quickly accessible from many distant points;

iii) They make it possible for data to be transferred quickly from one information system to another;

iv) They make it possible for data to be combined in ways, which might not otherwise be practicable;

v) Because the data is stored, processed and often transmitted in a form that is not directly intelligible, few people may know what is in the records, or what is happening to them.

Dematerialisation

The present data processing industry is in the midst of change to an information processing industry, with consequent new applications. Many systems are being introduced on a daily basis and these include word processing message systems, electronic fund transfers at points of sale (EFTPOS), electronic mail systems.[4] The Internet Worldwide Web and many other businesses have been installing computer-based systems without end. During the 1980s the most remarkable advances in technology were in two areas. The first involved the extension of miniature technology by the development of the so-called "microchip" integrated circuits containing ever-expanding components reduced to tiny wafer of crystal silicon by procedure of photo reduction.[5]

The second was the extensive linkage of computers by telecommunications permitting vastly increased storage of information, even-speedier retrieval, processing and management of data and transmission of messages over vast distances at ever diminishing costs.[6]

Despite the increase in efficiency and the more important commercial reasons, the need for adopting modern privacy and data protection laws

are no substitute for a clear-sighted recognition of the important individual liberties which are at stake.

Individuals are now equally appreciating the importance of Personal Computers (PC) to make their errands even easier. The implications that this will have on personal information record-keeping systems are clear. Many systems that are manual will be automated; very new systems will be created to support new services and meeting new demands. Decisions that are today made by people will be turned over to automated processes. Systems will regularly communicate with another through automated interfaces.

The pace of affairs in the world is faster because escalating costs are driving labour-intensive systems into automation, partly because the mere existence of a device or a technical capability spurs innovative applications and also because the use of information by automated means caters to any organisation's inherent motivation to function better, to move in new directions and to make decisions based on the largest amount of relevant data.

The movement away from paper and towards electronic means as the inevitable medium of communication, trade and record is called dematerialisation.[7] It is natural that the process will mutate the problems

in the security of that information now held electronically even though it has been argued that, it can not be proved with certainty that computers pose a greater threat than the manual storage systems, and that the problem they presage is so novel that the present law cannot deal with it.

The advantage of electronic as opposed to paper documents is that it is easy to state and is readily comprehensive.[8] In terms of business, paper is expensive to use, slow to send and poses time consuming delays. Processing information by electronic means, however, is not only cheap but also magically and astonishingly quick and much easier. The disadvantages of paperless transactions should however never be overlooked; they are among others the need for certainty and security for that information.

The business community for example knows and trusts paper records and feels secure with this because of the certainty in conventional legal rules and the absence of the equivalent in electronic systems. Law commissions are beginning to appreciate that reforms in such laws should be presented in a form that will be compatible with the introduction of paperless transactions.

The most notable case that dealt with the problems associated with the introduction of computers was the case of Whalen v Brown[9] in which Justice Breuniam said:

"the central storage and easy accessibility of computerised data vastly increase the potential for abuse of that information and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[10]

Whalen v Brown is a judicial relief. It is a brave realisation by the active U. S. Judiciary that the law is slow to change compared to technological advancements. The court however refused to commit itself to any general opinion about the constitutionality of other situations of storage or disclosure. The computer industry in the United States has consistently out-performed the predictions of its technical properties. Computer technology will continue to create unforeseen capabilities, which will exert irresistible pressure for their adoption in record keeping systems.

Security of Data on Computers

There are different views as to the extent to which information held on computers can be accessed. To a greater extent, it is true that an

intruder may be able to break into a system without risk to himself via a remote terminal or even by telephone.[11] The Conventional approach has assumed that the security of every computer system can be broken into no matter how much effort has been devoted to safeguarding its security.[12] This approach further contends that when systems are implemented and are in place, it is often too late to prevent harmful uses or intrusions into privacy. Alongside that most erudite observation, the conventional wisdom approach also moved a couple of other arguments on computer security which today can be dismissed as ill founded, flawed and having no place in the world of informatics.

It contends that the use of computers has somehow converted good users of personal information into evil users. This assumption is based on a wrong understanding of computers and diverts the truth that a computer being a piece of made machinery, is itself a morally neutral agent. The evil result that may arise out of its use will be the fault of the operators and not the computer itself. The best remedy is therefore not a blanket prohibition on the use or exchange of personal information but to look at each different computer application to determine how far their opportunities for human wrongdoing might be reduced.[13]

The second school of thought dismisses the conventional wisdom as alarmists since no serious threat of data stored on computer has been

positively identified to an extent that safeguards may be considered as being necessary now or in the immediate future. If anything, computerised systems provides better security because not anyone is capable of accessing information on a computer unless they possess the technical art of how to break passwords or how to make an unauthorised access through a remote terminal.[14] This approach can be criticised in that it is remedial rather that preventive. Legal protection of data cannot be underestimated because incidences of violation of privacy have not been reported. The reality and the sociology of crime is that criminals adapt to the present. As technology becomes more sophisticated and overwhelming, criminals also become equally intelligent and difficult to detect. Despite the difference in emphasis in these two schools of thought, it can never be in dispute that the proliferation of computers will at some extent, if that extent has not already been attained, cause serious harm to privacy. There is therefore the practical necessity to ensure protection in future such that consequences are less drastic.

It can never be in doubt that we can do more things on a computer than we could ever imagine possible. Business is now conducted on the internet, communication by electronic mail (e-mail) is becoming more popular between countries, students are finding that they need no encyclopeadic minds to store and search for information when there is

computerised research. The information that can be stored on a floppy diskette or a CD can be less than equivalent to a whole storage of Law Reports in the Law Library and that a database can be created, as has been the case with the Zambia Revenue Authority or some government departments wherein mountains and mountains of information are stored on private persons.[15]

This ability of computers to collate all this information, and the capacity of such information to be accessed at the touch of a button, obviously raises novel threats to the conventional protection of the right to privacy. The public authorities in the government and the local government can create database to increase efficiency in public processes. This, if unused, can also be fertile for abuse.

Throughout the course of history, people have always been distrustful of the activities of those in power, mainly because of their infinite manipulation of people's lives to suit their political ends. What, therefore, in this age, can stop the state from preparing a dossier on a private citizen without his knowledge and use it against him? Computers have thus raised serious implications on the protection of privacy of an individual, and it will suffice to look at this new threat to privacy and how the law may be found inadequate in its endeavours to protect privacy.

Personal data has already been defined elsewhere in this paper as consisting of information which relates to a living individual who can be identified from that information or from that and other information in the processing of the data stored about him.

The difficulty however with personal information is that there are different concepts about sensitivity by different people. Some people are sensitive about their age and others are not, some are sensitive about their finances and others are not and others boast about theirs and the same is true for sexual activities, medical history and a host of other classes of personal information.

The reasons why we claim privacy in different situations are similar; they are related to the function that privacy has in our lives. The promotion of liberty, autonomy, personal well being and security of individuals and furthering the existence of a free society. But, the big question is whether privacy is capable of a precise legal definition and whether the law is capable of protecting its virtues since it eludes a precise formulation as it involves many fundamental rights and sub rights. **Alan Westin**[16] has defined privacy as:

"the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others"

More simply and precisely, Louis Brandels[17] has defined privacy as "The right to be left alone." Privacy as a concept is necessary to enhance an individual's dignity, to the extent that, dignity requires non-exposure. Violation of that freedom involves the intrusion, trespass, falsification, appropriation or exposure of the individual to direct observation.

The general trend of thought for a long time now has been simple, it advocates that an individual should be vested with a legal right to privacy, such a right that already exists to a greater or lesser extent in France, United Kingdom, West Germany and the United States of America. [18] The invasion of privacy should be a delict actionable at the hands of the subject, either by way of injunction to prevent an apprehended infringement or by the recovery of damages after such an infringement has occurred. The popular demands therefore are for the increased protection of privacy, discussions of new threats to privacy and an intensified interest in the relationship between privacy and other values such as liberty, autonomy and mental health and even popular tenets as democracy.

Is Privacy a New Concept?

Perhaps before beginning a further analysis of the importance of privacy, the question that has to be asked is whether the need to protect it is a new concept and whether technology has resulted in any increased threat to privacy than before?

The wish to invade privacy and the need to control such wishes has been a feature of the human condition from antiquity.[19] There is the common law maxim, that a person's home is his castle which provides the basis for the restriction on the power of the government officials to search, detain or enter a person's property without a warrant and also manner in which the court frowns upon 'Peeping Toms.' The courts over the years have always jealously guarded such rights.

The reasons why there are increased concerns today about privacy is usually because of the nature and magnitude of the threats rather than its novelty in its influence on privacy, due to technological change. The other way to think about privacy is to raise the question as to why people want privacy? What is it that although they want it, they do not make claims for its legal protection, and, if they do, why is the law so reluctant to respond?[20]

Arguments have been raised however, against using the law to protect privacy. It has been argued that the law should only seek to protect those rights that are precise, and capable of enforcement in their formulation, privacy is far to o weak and indefinite a concept, that it is too fragmented a notion for it to be possible for any one common approach to cope with every part of it.[21]

The present formulation is far too limiting to be enforced by an individual whose privacy has been misused by use of data held on computers. This probably is because of the limitations in the conventional rules on privacy. The law in many cases cannot compensate for loses of privacy. In many cases, actions for the invasion of privacy are not initiated and this may be explained by the fact that law does not cover such injuries and that legal remedies are inappropriate in that the bringing of the legal action itself involves the additional loss of privacy.

Secondly, such invasions of privacy are hurtful because they expose us, they may cause us to lose our dignity, and our capacity to have meaningful relations with others. 'The law as one of the most public mechanism is completely out of place in most of the contexts in which privacy is deemed valuable, some of the most serious limitations include the following:[22]

i) There seems to be many ways to invade an individual's privacy without the person being aware of it and since our legal system relies primarily on complaints initiated by the victims, the absence of knowledge of such intrusions becomes a serious handicap. The absence of complaints is therefore no indication that invasion of privacy does not exist;

ii) Legal actions are lengthy, expensive and involve additional *loss* of privacy. For a victim of loss of privacy, a legal action will further publicise the very information he sought to keep private and will thus diminish the point of seeking vindication for the original loss;

iii) The limits of law in protecting privacy also stem from the law's commitment to interests that sometimes require losses of privacy, such as freedom of expression, interest in research and the needs of law enforcement. Even though privacy as a concept may elude scientific exactness, it is important to realise that the rights to one's privacy should be autonomous. Such a right should be considered as a derivative and a sine qua non to the civil liberties that we enjoy today because they are constitutionally protected, the freedom of association, liberty, unlawful search and seizure and the freedom to express ourselves, among others;

The right to personal liberty cannot be protected, if government officials were to continuously manipulate information about our private lives and use it against us, so will our autonomy be devastated together with our freedom of expression. With the arrival of this new millennium, our privacy as a freedom seems threatened and the law seems to be taking too long to safeguard such sentimental values. The detriment in the forecasted invasion is expected to be enormous and very serious.

How computers affect people's lives depends on how they are used or abused. The principal dangers to privacy come from three main sources:

i) Inaccurate, incomplete or irrelevant information;

ii) The possibility of access to information by people who should not or need not have it;

iii) The use of information in a context or for a purpose other than that for which it was collected.[23] Those responsible for the protection of personal data in computers should be placed under serious obligations to take all reasonable protective

measures to ensure that the information does not fall into the wrong hands, whether through inadvertence or otherwise.

Further, the scope of operations by those who hold personal information on computers should never be concealed, more particularly, from those to whom the information relates. People who are asked to provide information should have the right to know for what purpose it will be used and who is likely to have access to it. The operator of the system should also be in a position of responsibility to guarantee its accuracy and relevance. The information should only be kept for as long as it is needed.

The commitment to privacy and the information held on computers should be more than serious, it should be realistic and capable of keeping abreast with the level of technological advancements in any particular country. The measures that should be taken to ensure protection should be adaptable and affordable. The report of the United States Privacy Protection Study Commission recognised the importance of a preventive approach to one that relies on remedying a situation after it has occurred. The working paper suggested that:

"Projects in information technology and its inevitable use to support a country already large and complex and always striving for efficiency, innovation and

progress makes it mandatory that proper safeguards for personal privacy must come before and not after the fact?[24]

The implications of computer proliferation on privacy are drastic than we can ever imagine. The increased growth and popularity of computer use can be attributed in part to the wealth of information and functionality available and in part to its affordability.

The manner in which technology is advancing is shocking. It is at an astronomic speed. We could wake up tomorrow to find that we have lost control of the world, over our privacy and ourselves. It is only reasonable that our concern be concentrated on ensuring that safeguarding measures are in place before the problem goes out of hand.

CHAPTER 2 ENDNOTES

1. C. Tapper, Computer Law (1978) Page 151.
2. Ibid page 197.
3. F. Whitaker, Whitaker's Almanack 1995 page 903.
4. The Independent, Saturday Edition, 9th January 2000, UK Page 19.
5. D. G. Beanland "The New Technology" In Ibid of 23d January 2000. Page 8 - 9.
6. J. H. Curtis, Information Technology and Communications. In Ibid page 16.
7. Halsey D. William, Collier's Encyclopeadia,, 1987 volume 9 page 457.
8. OP cit.
9. 429 US 589 (1977).
10. Ibid at page 609.
11. This is an interesting case not yet published in the British Legal Journals where a teenage boy was found guilty of making illegal phone calls the world over using his computer. The bill came up to thousands of pounds but was only charged a few pence for the little electricity he used up. The Enquirer of 8th November 1999 page 7.
12. Ibid.
13. C. Tapper, Computer Law (1978) page 197.
14. Newsweek January 2000, "Hijacking the Internet" page 13.

15. Report on Data Protection, University of Newcastle.

16. Invasion of Privacy and Clarification of Concepts 72, Col. Law Review 693 1972).

17. Ibid (at 715).

18. Opcit (at 244).

19. Yale Law Journal Vol. 89 (1980) page 453.

20. Page 445 YLS Vol. 89 (1980).

21. Gawison (Supra).

22. Ibid (at 4).

23. Report on Data Prof. (page 457).

24. Appendix S. (extract) Technology and Privacy.

CHAPTER 3

DATA PROTECTION LEGISLATION IN THE UNITED KINGDOM: A COMPARATIVE STUDY

The United Kingdom provides an easy example of a country that has to a greater extent dealt with the question of Data Protection and Privacy. The measures of protecting information held on computers have emerged mainly as a foundation to the Data Protection Act enacted in 1984 and in regard to the remedial measures by the Computer Security Act of 1987. The Data and Privacy Protection legislation was enacted after recommendations were made by the Young Committee, which had been tasked to investigate incidences of threats of the security of governmental information on computers. The committee was also to look at protection of privacy and to recommend measures that can be adopted to avoid any abuse. It was on the influence of the Young Committee working paper and report that the DATA PROTECTION ACT was enacted. The Committee's terms of reference in their investigations were:

"To consider whether legislation is needed to give further protection to the individual citizen and the commercial and industrial interests, against Intrusion into privacy by private persons and organisations, or by companies". [1]

Ironically, the concern of the government at the time was not on the protection of privacy of individuals but to protect the data processing industry in the light of the threats that were posed to it by the European Convention. The protection of privacy can therefore be considered as having been incidental to the fact. However, the formulation of the Data Protection Act in Britain has inspired many other legislations in other jurisdictions as Canada and Australia. It is therefore important that the Act be analysed here in detail.

The Background of the Data Protection Act

The concern with privacy of individuals was alive in Britain as early back as 1960. In 1961, Lord Mancroft was obligated to look into the need to protect information and the rights of the subjects whose data was held on computers. As a result of this study, Lord Mancroft introduced the Right to Privacy Bill which never passed into law due to lack of support.

In 1970, the Committee on Privacy was appointed under the chairmanship of Kenneth Young with terms of references as described above. Their report was completed and presented to Parliament in July 1972. The report had this to say about computers:

"We cannot on the evidence before us conclude that the computer as used in the private sector is at present a threat to privacy, but we recognise that there is a possibility of such a threat becoming a reality in the future." [2]

A question will therefore be raised as to whether the future of 1972 is here and whether in line with the Young Commission's warning, our legal system has adapted to enable itself to be in line with technological advancements.

The Committee also managed to set up a Working Party to look specifically on computers. The Party's terms of reference were to examine the alternative means of controlling the handling of information by computers and to recommend those which seemed most appropriate, having regard to practicability and cost and also to survey the present scale of computer use and likely evolution, with special reference to the implications for controls.

The committee noted that the most credible anxieties were those held about computers in the public sector and that of public concern were universities, bank records and credit agencies.

The white paper on Data Protection produced by the committee proposed legislation to cover both public and private sector information systems. The creation of a Data Protection Authority was also proposed in order to supervise the legislation and ensure that individual privacy is maintained through appropriate safeguards. The Data Protection Authority was required to draft codes of practice within various sectors based on consultations with interested parties and associations, which would then become law. Failure to comply with these regulations would lead to a criminal sanction.

General Public Reaction to the White Paper

When the Young Commission presented its paper to the public for its consideration, there was a general opposition to the proposals in the committee's paper. The main grounds of opposition were that:

a) The Young Committee had not found significant evidence of infringement of privacy by the use of computers, and that these findings are only confirmed by their own experience;

b) It was suggested that there was not enough experiences of data invasion and theft of information to justify legislation (i.e.) data

protection should be tried out on a voluntary basis before law lays down any measures;

Alternatives to Legislation were suggested, including a voluntary Code of Practice[3] and reliance on the proposals of the Law Commission to extend the law of breach of confidence;

c) A number of submissions argued that the cost to society of the legislation would considerably outweigh the benefits.[4]

A case for reform in Zambia may probably be met with equal resistance. It may be necessary to assess if there has been any significant evidence of abuse in the Zambian computer industry of individuals' privacy to warrant recommendations by the Law Development Commission enactment of legislation in that regard. Undoubtedly Zambia's computer industry is still in its infancy although this should not be used to divert attention from the reality of the problem.

The Chairman of the Computer Department at the University of Zambia said that it is a debatable point whether data held in a computer system is more secure or less secure than data held in a manual record.[5] He said that greater expertise is needed to obtain and interpret data held in a computerised system. In Africa, there is a high illiteracy ratio and

knowledge on the use of computers is still very limited for the common people but much more on the increase in companies, government departments and other organisations. This may be attributed mainly to the pace at which we develop, the accessibility and affordability of those computers to private individuals. It is however surprising that Africa has the highest piracy rates in the software industry.[6] Tackling the software piracy issue in Africa was Microsoft's biggest concern in the 1997 Regional African Partner Conference held in Swakopmund, Namibia. Microsoft called on 120 channel delegates to stamp out the growing problem of piracy, which now accounts for over US$300 million loses for the industry in Africa. Nigeria and Kenya have the rate of over 80% in piracy.[7]

The reasons for high piracy rates in Africa were given as the following:

a) In most African states there is a general lack of effective intellectual property laws, resulting in little or no enforcement activity;

b) Lack of education among users about what actually constitutes software piracy. Microsoft through the Business Software Alliance (BSA) is involved in lobbying activity to ensure that

adequate intellectual property laws are put in place throughout the region.

In Zambia computer use is also becoming far more widespread, many private companies and some government departments as the Immigration and Customs Department, the Police and the Central Statistics Department, Emigration and Customs have been computerised. The Computer Services Department (CSD), a department within Barclays Bank Zambia Limited agrees that the user of any computerised information systems must be under an obligation to take all reasonable protective measures to ensure that information cannot fall into the wrong hands whether by design, inadvertence or deliberate penetration.[8] Further the department recommends that there should be legislation that should deal directly with protection of data held on computers to ensure confidentiality and privacy and that those who violate such protected interests should be punished by criminal law.

Theft of Information under Criminal Law

There are various handicaps that can be faced in any bid to ensure that information on a computer is secured. As the case with other forms of theft and violation of someone's rights there should be a requirement

that a third party who, without authorisation interrupts, deletes or gains access to confidential information concerning others can be punished by criminal law or that victims should be able to vindicate their rights through a civil action. As stated earlier, it has been recommended that invasion of privacy should be a tort actionable in the hands of the subject either by way of injunction to prevent an apprehended infringement, or by the recovery of damages after such an infringement has occurred. The delictual limitations to enforcement of that right have been analysed elsewhere in this paper. Besides delict, there is the obvious remedy in Criminal Law. Although this could be an effective remedy, the Zambian Criminal Law in relation to Data Protection is far too archaic and retrogressive. This is made even worse by the capacity of the new technology to frustrate and circumvent domestic law on Data Protection and security.

In a report by the Organisation for Economic Co-operation and Development (OECD) [9] headed "Computer-related Crime: An Analysis of Legal Policy", following a survey that was carried out, countries were divided into different categories following their response to computer related crime.

a) The first group consisted of those countries that regard computer crime as presenting no special feature requiring any particular

new measures, seeing no need for any distinction between information in general and computerised information, the computer being simply an instrument for committing an act, which is already prescribed by the Criminal Law;

b) The second consisting of those countries that consider that legislative measures are needed, to extend existing offences and introduce new ones to cater for one significant form of criminality.

The nature of the substantive criminal law in Zambia is an inheritance from British Common Law; its flexibility in adapting to novel situations is as slow as in many other legal systems. Whether Zambia fits within the first or second group of countries may also depend on the extent of computerisation within the country, the law reform initiatives and legislative priorities.

It may also be appreciated that most computer crimes are sophisticated crimes; they are often founded on expert knowledge of the new technology and are therefore difficult to discover and to prove. One example is what is known as the logical bombs, which are data programs that, a long time after they have been inserted in the computer system, perform an action like deleting or changing certain data. In most jurisdictions, the most common crimes on computers are:

i) The erasure or falsification of computer data - Such conduct is common to people who are normally authorised to use the computer or by a hacker who can access computer terminals by a remote control system;

ii) Unauthorised access and unauthorised use - (i.e.) an employee of a company who is not authorised to use the computer;

iii) The third type is theft of information on computers occurring mainly in the form of theft of trade secrets and copyrights. Presently however, breach of copyright is regarded as being equivalent to theft.

In criminal law, the conventional definition of theft was the unlawful taking or appropriation with intent to steal a thing capable of being stolen. The position being that incorporeals cannot be stolen.[10] In R v Cheeseborough & Another[11] it was held that there cannot be theft of a design or an idea. Malan J, quashing the convictions in the court below held that:

"In the court below, it is quite apparent that all parties, including the magistrate, were under the impression that a design or an idea or information could be stolen and his whole evidence is coloured by that outlook, that, of course is clearly not so."[12]

However, a document evidencing a right, such as a share certificate or containing ideas can be stolen. It is therefore clear that the law is protective of trade secrets and commercial transactions, which they have protected as confidential information. Information about an individual is not given the same attention, yet it is necessary to do so if individuals are to be accorded the right to privacy and security of their personal details held on computer.

What is Confidential Information?

In Saltman Engineering Co. v Campbell Engineering Co. Ltd[13], confidential Information is described as something that is not public property nor public knowledge. There are probably three categories of confidential information:

i) Personal information;

ii) Governmental secrets - which is mainly necessary for the preservation of national security;

iii) Trade secrets - being valuable commercial assets, and to a large extent are intangible commercial assets (i.e.) patents and copyright - curtailing unfair competition by limiting the opportunities for piracy.

In English law, there are 3 conditions that must be satisfied before an action for breach of confidence can succeed.

i) The information must be confidential;

ii) The information must be disclosed in circumstances which give rise to an obligation of confidence;

iii) There must be an actual or anticipated unauthorised use or disclosure of the information.

A more objective test of confidentiality was given in Thomas Marshal (Exports) Ltd v Eimule[14] by Sir Robert Megarry V.C. The Honourable

Judge said that there were 4 elements which might be of assistance in identifying confidential information in a trade or industrial setting:

i) The information must be information, the release of which the owner believes would be injurious to him or of advantage to his rivals or others;

ii) The owner must believe the information is confidential or secret, that is, not already in the public domain;

iii) The owner's belief under (a) and (b) above must be reasonable;

iv) The information must be judged in the light of the usage and practices of the particular industry concerned.

In Zambia, the concern with confidential information is thought to be important for governmental secrets than personal privacy. This is evidenced by the fact that the only statute that perhaps deals with protection of information is the State Secrets Act.[15]

In Canada, a case was brought before the Ontario Court of Appeal on the status of confidential information.[16] The issue in that case was

whether confidential information could constitute the subject matter of theft. Section 283 (1) of the Canadian Criminal Code found in the part of the Code entitled offence against Rights of Property, states that:

"Everyone commits theft, who fraudulently and without colour or right converts to his use or the use of another person, anything whether animate or inanimate

a) *To deprive temporarily or absolutely the owner of it, or a person who has a special property or interest in it or;*

b) *To deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was converted.*

The facts of this matter were that a Union wanted to form a labour unit in a hotel complex. It needed the names, addresses and telephone numbers of several hundred employees for that purpose. This information was regarded as confidential by the hotel management, and was protected by certain security arrangements, and would not have been disclosed to the union. The union made several attempts to solicit hotel employees and was formally barred form the hotel premises. The defendant, Stewart, was an independent consultant. He was approached by someone from the Union to obtain relevant information.

He contracted one Hart, a security officer employed by the hotel. **Stewart** and **Hart** had previously worked together. Stewart suggested that Hart procure the information and suggested methods by which this could be done. The information was to be copied without removing or affecting the actual personnel files and computer printouts in which the information appeared. The operation was not carried out, but the communications between Hart and Stewart were recorded. In the High Court, Krewer J, held that the word "anything" refers to something which must be capable of being property and that confidential information is not property.[15] He further noted that if the interpretations should be thought to be inadequate to meet the needs of the Canadian society, particularly because of its implications for the computer age, the remedy must be a change in the law by Parliament.[19]

On appeal, the decision of the court below was quashed. The court of appeal, by a majority, held that that particular confidential information was property. The court went on to say that whilst not all confidential information was property there was a right of property in confidential information which brought it within the definition. When the information was taken, its character of confidentiality would have been lost.

The Stewart case shows an example of judicial activism to bring about law reform. Although the Zambian Supreme Court has exhibited

characteristics of activism, it is doubtful whether they would consider it necessary to extend the law as was done by the Canadian Supreme Court. The reasons given by Cory JA for the decision were that:

i) By various amendments to the Code, the breath of the definition of theft has been progressively broadened over the years in Canada and now extends well beyond the traditional formula of things that are capable of being stolen;

ii) Cory J A, further argued that since copyright is a property interest, by analogy confidential information should be treated in the same manner.

His Lordship went on to refer to four elements suggested by Megarry V C in Thomas Marshall (Exports) Ltd v Eimule as being useful in that context: that the information must be of a kind which would cause injury to the owner or; be of advantage to his rivals if released. It must not be in the public domain and the owner's belief in the two preceding conditions must be reasonable.

In conclusion therefore, theft of information is now an offence in Canada. It is suggested that the Zambian legislation must make changes in our Penal Code to make theft of information an offence if we

are to be serious in our commitment to the tenets of privacy and the security of information on computers.

The main criticism of the Stewart decision by academics was that it would open the floodgate of litigation to cases of a given kind. This, however, may not be very true because judges have proved to be sensible persons who are equipped with the necessary techniques to ensure that frivolous and vexatious litigation does not find its way to the courts. The Stewart case is also a reminder that much of our law is badly out of date and inadequate to deal with contemporary technological issues; coupled with the systematic abruptness with which technology advances pause a temptation to the Judiciary to make ad hoc changes without waiting for legislative change.

By contrast, another case to come before the British Courts was Oxford v Moss.[18] In that case, the defendant students were convicted of theft in respect of making a copy of an unseen examination paper. This conviction was quashed on appeal, notwithstanding that the offence of theft in English law was applicable to both tangible and intangible property.

The other case that was of significance to Data Protection was Schifren and Gold (April 1986). This case involved "hacking" into the computer

system and gaining access to private mailboxes, which included that of the Duke of Edinburgh. It seemed that by taking advantage of some luck, ingenuinity and sheer security faults, Shrifren was able to gain access to the computerised information services in particular to user files containing the identification numbers and passwords of subscribers. He was thereby able to add or alter data or deny access to legitimate users. The defendants were charged with several counts of forgery in that on various occasions they had made a fake instrument by electronic means with the intention of making the said Computer to accept it as genuine, to the prejudice of Britain Telecom Private Company. The conviction of Schifren brought to the fore the crime of hacking and the need to protect both software and information held on different programmes.

The Scottish Law Commission Proposal

Perhaps the best source available in Britain over the current years on the problem of the security of data is the Scottish Law Commission's Consultative Memorandum on computer crime, [19] that was published in March 1986.

Having acknowledged that an unauthorised access to a computer should be criminal offence, the commission recommended legislation to

deal with the problems of unauthorised access of a computer system and hacking by means of a remote terminal. Hacking was defined in that report as,

"An unauthorised and objectionable invasion of privacy".

Hacking is a 'process by which a person can be capable of eavesdropping on a computer, spying upon and reading from a distance, information being displayed on one's terminal by using special equipment which can pick up electro-magnetic radiation surrounding the terminal. The material to achieve such a purpose is fairly inexpensive and could be easily accessible to the Hackers. The Commission suggested, however that computer eavesdropping could be adequately dealt with if legislation were to be enacted to cover the unauthorised access of information held on computers. If a hacker were to cause physical damage to the computer program, then their opinion was that this conduct would fall under the common law offences on damage to property. Besides these changes by the Commission, provisions intended to protect data have already been incorporated as part of the Canadian Criminal Code.

Section 385 of the Canadian Code provided in part that property means real or personal corporeal property.

It provides that;

1. Everyone commits mischief who wilfully;
    a) Damages property;
    b) Renders property dangerous, useless, inoperative or ineffective;
    c) Obstructs, interrupts or interferes with lawful use, enjoyment or operation of property or;
    d) Obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

An amendment to the Code in 1985 added a new subsection to section 385 and 387 of the Code[21]. The general effect of the amendment is to equate data with property.

It is submitted that the provisions in the Canadian Code are very wide and are an example of how unauthorised access and erasure of data can be dealt with by means of legislation. It is suggested that in Zambia, the common law crime of theft should be modified and that such a modification has to be along the lines of the Canadian Code that equates data with property and therefore an incorporeal that is capable of being stolen. Data protection legislation has to be enacted in our

statute books to ensure that the problem is dealt with before it pauses a serious threat to the computer industry and the privacy of individuals.

CHAPTER 3 ENDNOTES

1. Published by Her Majesty Publication (in 1972).
2. 1972 (Paragraph 619) incl.
3. Discussed in last chapter of this paper.
4. Report of the Data Committee on Data Protection page 92.
5. Interview conducted with the Head of Computer Science Department at the University of Zambia on 22nd September 1999.
6. The Post, August 2 (1997).
7. Source: The Independent Technology Supp. To THE BRITISH INDEPENDENT, AUGUST 1 1999 (Pg TS).
8. "Positive Outlook for Zambia's IT Industry" PC World (August 1998) IT Africa Bumper Issue pg 16.
9. Paris, 1986.
10. S. V. Kotze (1965) (1) SA 118 Milne and Ecleigh's.
11. 1948 (4) SA 756.
12. Chapter 111 of the Laws of Zambia.
13. Stewart: 1983 S CCC (3d) 481).
14. (1982) 68 CCC (3d) 481.
15. (1982) 68 CCC (2d) 305, 317.
16. Ibid.
17. (1979) Ch. 727.
18. (1979) 68 Cr. App. R183 (1979) Crim.LR.119.
19. Report on Computer Crime No. 68 (Edinburg, 1986).

20. Section 385 of the Canadian code basically sets out the conditions that must be fulfilled in order to sue for damage to property. Section 387 is structured in the same manner and expands conditions fulfilling the offence of theft – it simply qualifies section 283 of the same code.

CHAPTER 4

PRACTICAL DATA PROTECTION COMPLICATIONS IN ZAMBIA

Is Data Under Threat in Zambia

Although Zambia is a developing country that is struggling for liberalisation, computer technology has become a significant threat to warrant legislative intervention. At an Information Technology Exhibition (IT Africa 1997) conducted by the African Computer Supplies Association (COMSA)[1], the appreciation of the Zambian community of information technology was overwhelming. Computer users interviewed at the exhibition recognised the significant progress which had been made in the provision of state of the art technology to the current market. It was revealed by Delvin Thompson,[2] the Director of Computer Connection, that there was a vast amount of uncertainty among the Zambian public about the importance of Information Technology, the security of the systems and the increasing role it will play in the future. It is however, anticipated that as the Structural Adjustment Programme (SAP) begins to bear fruits the liberalised market will increase access to computers for the common person. As one distributor said:

"Trends locally, as with those worldwide, are headed towards high stepped data communication with ever increasing systems providing the

ideal base for networking solutions. Access to information .is fast becoming the telling difference between success and fallure."[3]

Besides these predictions, problems with data control and protection have already been identified.

Software Piracy

Evidence acquired from interviews has suggested that software piracy is rampant within the IT industry. Software Piracy is the unauthorised copying, reproduction, use or manufacture of software product(s) protected by US and International Copyright Law and treaties.[4] Locally, software piracy is protected by copyright law and other intellectual property law regulations in force. Copying software without the permission of the owner is copyright infringement and the law imposes penalties for such infringements. In Zambia, we saw an interesting development two years ago in that the first Data Security Case was filed in our courts by Microsoft Corporation and this appears to be the first meaningful attempt to stamp out software piracy and data protection. Microsoft Corporation, a company organised and existing under the laws of the United States filed an anti-software privacy suit against a local company called Datamatics.[5]

In its application Microsoft requested that Datamatics be interdicted from infringing its right under its copyright for computer programme entitled MS Windows 95 and MS Office 95. Datamatics was also restrained from infringing Microsoft's rights under the copyright for the copyrighted works by selling, exposing for sale, or distributing for trade or for any other purposes, personal computers containing unauthorised reproductions of the copyrighted works. The intention of Microsoft to sue was interesting because the conglomerate did not intend to sue Datamatics for a fee, but more for the need to protect its copyright and incidences of violations of protection of data on computers.

The case may be justified on the resolutions made at the regional meeting held in Namibia which attempted to stamp out the rising piracy rates in Africa, which are estimated to cost the Software industry well over $300 million in loses. The Datamatics case, although it is not directly on the need to protect information held on private individuals (and the matter was settled ex curia) was expected to have far-reaching consequences. It was also expected that the case would have important implications on computer technology and the interpretation of the law in that field. It was also reported at the IT Exhibition that cases have arisen when computer viruses have been implanted in systems to erase and destroy data files.[6] A virus is a programme that copies itself by mutation. It is capable of devastating consequences including being

commanded to erase data. In light of the above developments in public sophistication, the question that needs to be asked is whether the problem has not become real enough to warrant legislative intervention considering the incapacities that antiquates our legal definitions and their inflexibility to adapting to novel circumstances.

The limitation in the cases brought before the courts should not be interpreted to suggest that there are no computer crimes in Zambia, but that companies are usually reluctant to bring such cases for litigation because of the more pressing need to protect their goodwill. The Datamatics case was therefore a good starting point. Before the law can develop in this regard, however, there is a need for more computer criminals to be brought before the courts. Despite the reluctance of the victims of computer crimes to bring the cases before the courts (which may also be interpreted mainly due to the lack of knowledge on their part) a question also will remain over the ability of the machinery of Justice to investigate and prosecute this type of crime. In the United States, some 200 FBI agents have already been trained in this area and the metropolitan police of London also has a special computer crime squad.[7] This equally applies to the Attorney General's Office. I propose that a section of the Attorney General's office should concentrate entirely on this type of crime and should endeavour to obtain basic

training in order to be able to match the emerging syndicates of computer criminals. It is worth repeating that the Zambian police and the prosecutors will learn a lot from what their counterparts overseas are doing to combat the problem.

Computerisation of Government and Local Government Departments

Although to date, the greater percentage of government departments in Zambia use manual systems as opposed to computer systems. An official from the Ministry of Education[8] revealed that the government appreciates the need to computerise their systems to ensure efficiency, accuracy and to lessen burdens on the understaffed governmental services. Mainly the funding process has over the years limited this programme. Some government departments have already been computerised and these include the following among others;

1. Ministry of Finance (salaries Service Bureau (SSB));

2. Ministry of Defence;

3. Ministry of Labour (National Pensions Scheme Authority);

4. Ministry of Legal Affairs;

5. Lands and Deeds Registry Office;

6. The President's Office – Special Branch;

7. Local Government: The Lusaka City Council has a Data Processing Department where all the information concerning its services is stored. (i.e. rates collection, salaries and employment details, house allocation systems).

It is important that the method of storage of information by' Government departments be studied because of the way they centralise and control the affairs of the people. The Young Committee in the white paper produced on Data protection recognised this need:

"The state Provides or gives financial help towards a number of services for its actions - for example health, social services and education. To do this, it collects duties, taxes and contributions. These functions could not be carried out effectively without a good deal of information about the needs and circumstances of individuals. Such information is also required to provide the statistics needed for effective planning and effective allocation of resources."

In Britain, many of the anxieties which have led to a demand for the creation of a legal right of privacy concerned the activities of government departments and other public agencies. There certainly is no doubt that the government of Zambia now collects and holds a good deal of information, about individuals; the greatest percentage being in Social Security, Public Service National Insurance, Pensions and Finance, Medical Records, Births Records and Travelling Documents. People at several occasions in their lifetime; have been asked to fill in numerous commercial forms pertaining to their personal information for government administrative purposes. It is the introduction of computers to deal with the information, which has resulted in the growing increase and scepticism in security mechanisms.

The fear is the consequences that the collection of information may have on the question of democracy, the ability of an individual to feel autonomous and the liberty to act without undue pressure from anyone. The main fear pointed out by a computer programmer at the Lusaka City Council is the possibility that the government might, with the aid of computers, collate and centralise all the government-held information about an individual to form a personal dossier. Such a collection even if it were intended for beneficial purposes like increasing efficiency in governmental services, would be greatly undesirable. It would give any

government too great a potential power over its citizens and would be dangerous if it fell in wrong hands.

Regulation of information held on computers should therefore start with the government's computerisation system since it consists of the largest pool of data storage network. The White paper entitled "Computers and Privacy" [9] by the Data Protection Committee made very useful recommendations in regard to regulatory information held by the government, which may be essential to any government. The Young Committee, in its recommendations came up with working principles intended to ensure that the government does not misuse the information it collects and further, that the privacy of that individual be guaranteed besides the necessity of such collection.

The Young Committee's Principles

1. Information should be regarded as held for a specific purpose and not to be used without appropriate authorisation, for other purposes.

2. Access to information should be confined to those authorised to have it for the purpose for which it was supplied.

3. The amount of information collected and held should be the minimum necessary for the achievement of a specified purpose.

4. In computerised systems handling information for statistical purposes, adequate provision should be made in their design and programme for separating identities from the rest of the data.

5. There could be arrangements whereby the subject could be told about the information held concerning him.

6. The level of security to be archived by the system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.

7. A monitoring system should be provided to facilitate the detection of any violation of the security system.

8. In the design of information systems, period should be specified beyond which the information should be retained.

9. Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.

10. Care should be taken in allowing value judgments on such information.

Having identified the need for more security of information held by the art and the recommendations by the Young Commission, it is recommended to the computer community in Zambia to try and ameliorate the problem by the consideration that when systems are implemented and in place, it is often too late to prevent harmful uses or intrusions into privacy. Such protective measures should always come before and not after the fact. An important precedent can be extracted from the Computer Security Act in the United States which allocated to the National Bureau of Standards the responsibility of developing technical, management, physical and administrative standards and guidelines for the cost effective security and privacy of sensitive information in federal computers. The primary purpose of these standards and guidelines were to control loss and unauthorised modification or disclosure of sensitive information in such systems and to prevent computer related fraud and misuse.

It has already been pointed out that Public authorities store information concerning records of births, marriages and deaths, medical records, records of education, military service, passport applications, employment records, social security records, declarations for tax

returns, application for licenses of many forms, motor vehicle registration, Post office savings books and telephone accounts, and even more scary are covert police and intelligence records.

The amount of information stored and its threat to privacy (which resulted in people not knowing if an information profile existed on them, how it was used and whether it was accurate) led to the introduction in the United States of the Privacy Act of 1974. It is said that in the United States more than 100 million people appear on data dossiers, in the United Kingdom the largest credit protection agency has over 14 million people on file. By 1976, the credit bureau in South Africa had over 6 million files. In Zambia, it is estimated that the government has over 5 million people on dossiers.

The government now collects more information than we can imagine. Few of us can remember how much information we have given the state and the manner in which that information may be used. The collection of information by the government is now formidable and these are colossal operations covering large sections of the total population. Information is even more dangerous in the hands of the state than of a private individual. The state can be manipulative and with the strength of its machinery can prejudice individuals by eroding their autonomy and destroying their acquisition of basic rights as

democracy, or the right to acquire essential services as state documents like passports. It is therefore important that regulations be put in place to ensure that information collected by the state is not abused.

Chapter 4 Endnotes

1. Conference was held at the Intercontinental Hotel between the 4th and 6th of August 1998.
2. Delvin Thompson is the Director of Computer Connection (Pvt) Ltd, a member of the African Computer Supplies Association with offices in most parts of Central and Southern Africa.
3. Tom Heubner: OEM Account Manger for Africa (Microsoft).
4. Microsoft Licensing Policies (1997) page 12.
5. Datamatics is a firm incorporated in accordance with the laws of Zambia. It is a computer retailer and does not manufacture any computer products.
6. This was disclosed by Musa Mushili of Masscomm, a company that distributes Dr. Solomon Anti-virus Tool kit called Dr. Solomon's Homeguard which provides home computer users with the best possible protection against computer viruses.
7. Tapper op cit (3rd) 219 n 4.
8. Interview with the author, 23rd July 1999.
9. Set out in paragraph 592 to 599 of their Report, cmnd. 5012.

CHAPTER 5

Before recommendations are submitted, it suffices to mention the fact that whenever the right to privacy is alleged, other renowned rights such as the right to the protection of property, state security or peace and order come into question. While it is conceded that there are some rights which could be more fundamental than others (at least in principle) when they are ranked, this must be done with prudent caution as this is a process of striking a balance between competing rights. Their probative values must be ranked according to each particular case if a reasoned assessment must be made.

The Freedom to Receive Information

Efficient conduct of industry, commerce and general administration in any given society is paramount. While the social economic and political machinery must be protected in the interest of all, individual data protection cannot be completely ignored. On one extreme is the need for the preservation of national security, law and order in society while the other extreme must cater for the individual components of society. A balance must be struck between these two extremes to reach the optimum standard. Whilst it is accepted that the state must be rendered the necessary discretionary power possible within the law, the

equivalent must not be disregarded as it pertains to the individual. In a computerised society, connections between databases transmitting information turns out to be very speedy. This efficiency in information flow puts the individual in a vulnerable position. There is little doubt that this increased vulnerability gives rise to calls for new laws to curb any novel situations that may arise.

In international law, Article 12 of the Universal Declaration of Human Rights provides:

"12 (1) No one shall be subject to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

The European convention for the protection of Human Rights and Fundamental Freedoms signed at Rome on 4th November 1950 provides in article 8 as follows:

i) Everyone has the right to respect for his personal and family life, his home and his correspondence.

ii) There shall be no interference by a public authority with the exercise of his right to except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well being of the country, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Zambia acceded and remains a declarant under the Universal Declaration of Human Rights. She is thus a member of the International Community and must learn from international instruments such as the European Convention. In fact Zambia is a party to the African Charter on Human and Peoples' Rights adopted by the 18th Assembly of the Heads of states and Governments of the Organisation of African Unity on 27th June 1987 at Nairobi. Article 1 there of is an understanding by all states parties to adopt legislation or other measures to give effect to the rights therein. Article 5 of the same charter provides in part that:

Every individual shall have the right to the respect of the dignity inherent in a human being and to the recognition of his legal status...

From the foregoing, it is prevalence that privacy exists as a right and it is incumbent on the legislature, the executive and the judiciary to enact,

administer and uphold legislation in conformity with these instruments and others. Despite the community's right to receive information, this should obviously be within acceptable bounds. There has emerged a serious problem with transboundary data movement. The marriage between computers and telecommunications has made the problem even more complicated. The advent of rapid progress in international telecommunications including satellite and exponential growth of transboundary flows of data including personal data make it relatively simple to store intimate personal information on the citizens of one country in another not readily susceptible to the enforcement of protective laws.

The Position at British Common Law

At British Common Law, the root of our present law of privacy is founded in the Principle of action injuriarum, which protected a person's personality rights, consisting of *forma corpus* and dignitas[1]. Mason is of the view that injuries relating to *forma corpus* have developed into the modern wrongs of defamation, malicious prosecution, assault and false imprisonment, while the concept of dignitas has been left open to accommodate any future development of the law relating to injuries.[2] However, John Lester favours a different approach. He feels recent practices create a visibility of the private life of an individual as never

before.[3] Lester is critical of imprecise terminology, which subsumes privacy under dignitas even in decisions by the British courts. Nevertheless, the present situation in Britain and Zambia is that privacy is protected as part of dignitas[4].

A number of cases have been decided on "*actio injuriarium"(actual injury)* although none of those cases involved computers as a means of such violation. S v A [5] involved a "high tech" situation in that a private detective had planted a sensitive listening device in the room of the man he was observing, and the court found him guilty of a serious infringement of the complainant's right to privacy.

The right to privacy is also protected by the criminal law in the shape of *crimen injuria (Criminal injury).* In short the subject of Common law right to privacy in Zambia has been reduced by case law. There are, however, numerous fields where the individual's privacy is protected by common law. The question that needs to be asked however is whether the common law is adequate to prevent increasing intrusions into personal privacy by the government, social scientists and twenty first century technology.

The Privacy Act in the United States

The Privacy Act in the United States requires federal government to give notice of the record systems. It restricts intergovernmental transfer of personal records and ensures that interested individuals have access to their own records: it also allows them to correct errors in the information. The Act prohibits the disclosure of any record to any person or agency without the prior written consent of the individual concerned, except for instances where it is made to an officer of the same agency in the course of his duties or for routine purposes or in terms of the Freedom of Information Act. While the Freedom of Information Act makes access to government records available to the public at large, the Privacy Act controls the information held by federal (as opposed to local) states and private agencies by ensuring its accuracy, fairness, relevance and security.

Prior to the statutory changes, in the United States, as regards criminal law, the view that intangibles did not constitute property for the purpose of penal laws prevailed. In Lund v Common wealth of Virginia[6] it had been held that information was incapable of being stolen even if it was worth a considerable sum of money. This decision was met with a lot of criticism so that statutory reforms were effected.Misappropriation or abuse of information became indictable at criminal law.

The Position in England

The practice in England has already been analysed exhaustively elsewhere in this paper. It will do no harm to stress that in that country, the gravity of the threat of computers on the privacy of individuals has been recognised; attempts have also been made to introduce bills to curb the problem. In 1971, a bill was debated and passed in the form of the Personal Records (Computer)[7] Bill which proposed that any person whose personal profile has been recorded should be able to:

(a) Object to the type of information stored about them;

(b) Apply to the Registrar of Data Banks for the removal of such information;

(c) Be informed that such a profile exists; and

(d) Obtain a copy of the criminal profile and any subsequent amendments.

The Consumer Credit Act (1974) was also enacted to provide some protection concerning data collected by credit reference agencies. The

Act accords consumers the right to determine the use of information held about them. Some of its provisions give the consumer the right to:

(a) Obtain the name and address of any credit reference agency from which other contracting party has applied for information about his financial standing[8];

(b) On payment of a small fee, obtain a copy of the file relating to him kept by such an agency[9];

(c) Give notice to the agency requiring it to remove or amend certain information in his file'[10];

In the case of disputes, he can apply to the Director General of Fair Trading for a ruling on the matter. However, despite all these stringent and seemingly perfect control, neither the Consumer Credit Act nor the Personal Records Act provides any control over who has access to information about him. It should be appreciated though that their promulgation would go to some extent in the growing recognition of the value of privacy and the need for it to be protected by the law.

THE POSITION IN CANADA

In Canada the statutory protection of privacy is as strong as the provisions in the United States. The Principal Act for the protection of privacy is the Federal Protection of Privacy Act. This act criminalises electronic eavesdropping and surveillance in Canada. The combination of statute and common law seems to embrace most of the traditional categories of invasions. P Doherty in his criticism of the Stewart decision in an article entitled "When is a thief not a thief? Where he steals the candy but not the wrapper"[11] points out correctly that it is false to hold that information cannot be stolen, but the document that contains the information can, while in actual fact, it is the information more than the document which is important and which needs more protection by the criminal law. Theft of an idea stored in a computer should constitute theft because of the changes in the information storage systems. Also the process of using and accessing of information collected by an authority for purposes other than which it has been collected for should become a concern of the legislature to ensure that the privacy of individuals is not violated.

Criticism of the Current Legal Provisions

Mr. Zikonda[12] argues strongly for legislation in favour of creating legislative regimes to deal with computer crimes. He criticises the argument that there is no need to create new laws applicable to computers because the involvement of a computer is not central but only peripheral to the actor's motive or intention and therefore does not deserve separate treatment. He points out that there are some areas of computer use/abuse which are not currently covered by our common law.[13] He comes to the consequent conclusion that the wrongful obstraction or getting of information by people who effect unauthorised access such as hackers is not covered by our law of theft.

Mr. Zikonda also follows this argument further and considers the idea of information as property and advocates that our criminal law should regard the information as property and therefore capable of being stolen. An individual, whose personal details have been accessed through unauthorised means, suffers exposure and a serious breach of his autonomy and esteem in the public eye. A businessman whose confidential information has been stolen suffers loss in business, yet such access may only have been accessed by a hacker through a remote terminal and the condition of the information has not been

altered. Such situations should be legislated against. The reasons for such inadequacies are many, some of them being that:

a) For the essential elements of theft to be fulfilled, the accused Person must have had the intention to steal something that is capable of being stolen. Criminal law as any other facet of the law is slow to change and that the conventional definitions of theft have long since been overtaken by technological advancements. Computers have infiltrated most areas of human life. Crime is also now becoming sophisticated and technical. It has been put across aptly by T Mechine[14] in his discussions on the conventional definition of theft that technological advancement has made the commission of crimes an easy and habitual process in many parts of the human society, yet criminal law relating to property has chosen to ignore this. The crime of theft now has serious limitations in that it still presupposes a scenario in which a person goes out to remove the subject matter of theft physically and then running away. It is now possible for a person to steal in a situation that defies the traditional assumptions relating to the commission of crime of theft;[15] example being the use of remote terminals.

b) The introduction of computers has cast the requirement of an intention as an essential element of an offence in disarray. It is also

a requirement of the crime of theft that the person intended to deprive the owner permanently of his property. In hacking, nothing may be removed, physically copied, altered or destroyed but that the Hacker may have the opportunity through a remote terminal to look at valuable information and even personal information about other people and this will not criminalise his actions because when he looks and to his fascination lands on such information he does not have an intention to deprive the owner of i.e. the fact that such a person has been arrested fourteen times for drug trafficking, or that they have been arrested for prostitution and that they earn a wage far below the minimum wage. Through the advent of computers, information may be accessed without an intention to temporarily deprive. This requirement will therefore be inadequate today.

c) Mental Blameworthiness: The problem with this was analysed by Mr. Zikonda[16]. It is that Hackers sometimes discover that they can access people's computer systems by accident through remote terminals. The question of an intention may therefore be lacking and this may cause problems with the present formulation as the hacker may access one's remote terminal without even an intention to do so, but out of fascination may then choose to continue doing so.

Civil law as a means of safeguarding the invasion of privacy by the unauthorised accessing has already been analysed with its shortcomings in detail in chapter 2. Undoubtedly, our law is inadequate to deal with the present technological changes. There is the urgent need to create new guidelines and new laws by the legislature to deal with the problem.

THE CREATION OF SAFEGUARDS FOR DATA PROTECTION

Since the main threat to the protection of data has been identified as the government storage system, which lacks methods of accountability for the information they store and the purposes for which it is stored. It has already been established that the government of Zambia has embarked on an extensive programme to computerise most of its essential departments to ensure that the process of administration is more efficacious.

Fears are therefore justifiably high in regard to information which is dedicated to the creation of a record relating to the affairs of an identified individual for use in relation to him personally. Typical collections of this type being police records, vehicle identification, income tax returns in the public sphere and credit ratings, bank

statements and insurance files. The main fear is that there is cross-referencing between government departments on different files held pertaining to private citizens. However, what is questionable is the accuracy and selectivity of information and their use in an unauthorised manner. It is feared that bank statements will be checked against tax returns and that old convictions for trivial offences will be ranked up to delay employment; or that past wages may be used to reduce the bargaining power of job seekers.[17] It is feared that a pool of information collected by government is possible and this information will make privacy impossible. Safeguards will have to be put in place to ensure that protection is ensured before than after the fact.

Preventive Safeguards

1. As illustrated by the Credit Control Act in Britain and the Privacy Act in the United States, public justification must be given for all data, which is proposed to be collected. The requirements among others being that each collecting agent should specify in detail what it intends to do with the data that it is collecting and how it proposes to collect it. A means of an enquiry should be set up when such information has been held to be inaccurate or having been used for purposes other than for which it has been collected.

2. The other preventive method that is often ignored is that of providing physical security for the data. The security systems and the accessing methods of those areas where data is held are not safeguarded; this may be an attitude by authorities that undermines the importance of such information storage systems.

3. It is also suggested that it is desirable to create an advisory committee comprising representatives of users (Computer Association of Zambia), the suppliers and the government, which would forward suggestions to the agency responsible for establishing the conditions under which licenses for use is granted. Such a body will be more effective to assess public pressure than the institutions like the Parliament or the office of the ombudsman.

4. Preventive measures designed to safeguard could also be proposed (i.e.), the provision of physical security for all parts of the equipment including communicating lines and remote terminals. The operating system should also contain stringent precautions against any data being left in the central store after being used, so as to minimise the danger of it being picked up by an unauthorised terminal.[18]

Remedial Safeguards

Although there are options open to a person whose privacy has been violated, such remedies through an act in delict are damaging where the essence of the complaint is the invasion of personal privacy. It is some what ironic to compel the subject to institute public proceedings because that would constitute a further loss of the privacy that he intends to protect. Criminal law has already been analysed as being inadequate. In the United States, however, a new tort of infringement of privacy has emerged and is enforceable. The position that has been taken in other jurisdictions such as in Canada, United Kingdom and Germany to protect data in their criminal codes also provides the best working examples.

CONCLUSION

"Privacy is a delicate concept endangered as much by apprehension of infringement as by proved infringement. It is therefore not necessary to be able to show that infringements have taken place in order to recommend appropriate safeguards"[19]

The threat of privacy by computers is real. The current legal framework for the protection of privacy is a step behind because the level of privacy it once protected cannot be equated to the present dangers. The advances in surveillance and in the recording, storage and retrieval of information has made it impossible for individuals to expect the same level of privacy that was once enjoyed before.[20] The ability of computers to process mountains of information completely reverses the manual system as we go into a new era that has been described more aptly as the computer age

However, the right to privacy, like many other rights, must be derogated upon to accommodate other rights such as the right by people to receive information and the need for the state to access as much information as possible so that the government machinery is able to operate efficiently and effectively. In the United States of America, such a conflict was apparent between the Information Act and the Privacy

Act. The Information Act allows the government to acquire information from individuals for the purposes stipulated above. In March 1997, internet users in Washington protested against censorship of the internet when the Supreme Court was considering arguments about the dilemmas new technology has brought to the old debate. The United States Supreme Court was considering questions on whether censorship can ever be justified, whether the need to protect children from obscenity was overridden by adult's rights to free speech.

Cyber Surfing in reality offers unlimited, unrequired and sometimes harmful information.[21] Manifestations of such harmful effects are not hard to find. In the Pentagon cases some civilians accessed high profile intelligence files and almost caused a nuclear holocaust between USA and Russia. In the Oklohoma Bomb case the military formula of creating bombs was accessed and almost led to drastic consequences. The opportunities that are opened by the Cyber net are too wide and will have drastic consequences if they are not regulated.

The argument further contended that new information components have to be regulated because the unregulated global computer network known as the internet has brought new opportunities to pornographers. Those able to navigate cyberspace now find wide pictures and explicit sexual discussions as easily accessible as scientific discourse on any

other subject. To curb these problems, in 1996 President Bill Clinton signed the Communications Decency Act that makes it a federal crime for anyone to use on-line computer communications to transmit or deploy in a manner available to minors any indecent or patently offensive materials. The irony of the matter is that the American Civil Liberties Union went to court to challenge the Act claiming that it was a violation of the nation's constitutionally-guaranteed right to free speech.[22]

The effects however are far reaching. While the size of the internet is very difficult to estimate due to its rapid growth, it is believed that there are 70 million people connected to the internet. Although there is a need to protect privacy of information, a balance has to be struck with the question of access of information. The move today is towards dematerialisation. The shift from conventional mail to electronic mail is significant as incidences of interference may be easier than steaming a letter open, since all that is required is to access a person's code by a remote terminal. Although finding that code may require expertise, many people are becoming more and more knowledgeable in computer applications and where the means to break into a security code have been found, it becomes an obsession rather than a necessity. As much as we do have psycho killers, we have to accept that psycho-hackers are also becoming even more threatening.

By way of conclusion it is necessary to point out that privacy is a right derivative from the first generation of rights as the right to free speech and free association. It is essential for democracy and the autonomy of an individual. The level that privacy has to be protected has to be the same as all the other rights. As per Weston's definition,[23]

"Privacy is an individual, group or institutions' right to determine for themselves when, how and to what extent information about them is communicated to others".

Such an intrusion of the right to privacy constitutes a serious infringement on an individual's autonomy as it amounts to trespass and exposure of individuals to direct observation. Computers contribute a great deal to the fact. Although computer law in Zambia is still in its infancy, there can be no doubt that those responsible for holding personal information on computers must be under an obligation to take all reasonable measures to ensure that the information cannot fall into wrong hands: whether by design; inadvertence or; by penetration.[24]

There can be no doubt either, that there is a need for legislation for this problem as it was reasonably predicted that computers will overtake may facets of our lives. The law has to keep pace with technology and

be more realistic. Perhaps the best way to sum this up is by way of a quotation from the preparatory papers of the Privacy Act where it was said (in reference to America and the Act):

"Progress in information technology, and its inevitable use to support a country already large and complex and always striving for efficiency, innovation and progress, makes it mandatory that proper safeguards for personal privacy must come before and not after the fact."[25]

Most significantly there is a need for urgent and extensive law reform to facilitate a comprehensive, systematic and timely response to the widespread, important, complicated and rapidly growing methods of computer technology.[26]

CHAPTER 5 ENDNOTES

1. David M^{C}Quoid Mason: 1975. The Law of privacy in the Commonwealth. Page 28.
2. Butterworths, 1985. Ibid page 28.
3. Lester J. Jurisprudential Analysis of the Crime of Defamation. 1981 page 44.
4. See S v A 1971 (2) SA 293 (T) and SV1 1970 (1) SA 781 (RA).
5. Ibid page 38.
6. 232 S. E. 2nd 745 (Va 1977).
7. R. Miller. The Assault on privacy (Computer, Data and Dossiers) 1971 227: of Lester.
8. Section 157 (Consumer Credit Act).
9. Section 158 of the same Act.
10. Section 159 (Consumer Credit Act).
11. 63 CR (3rd) 322 (1988)
12. Computer Crime: The need for an extension of Zambian Criminal Law: (1993) 5 Legal Forum No. 3 pp 28.
13. At page 28.
14. The cost of a free lunch (1989) 3 SA Commercial and Legal quarterly No. 1 page 19.
15. Page 114 D. Chisha.

16. At page 29.

17. Colin Tapper, at 48.

18. Tapper at page 57. Ibid at page 57.

19. See the Young Commmittee, Gupra note 13 at 153.

20. The US Supreme Court unanimously declared unconstitutional the bill enabling language censorship of the Communication Decency Act (1996) in September 1997.

21. Cyber surfing is the process of browsing through the internet on different home pages without particular interest or aim.

22. Tapier Clf (1992) page 46.

23. See Allan Weston, Col. Law Review 693 (1972).

24. Young Committee 799.

25. Extract from Technology and Privacy, Appendix 5. The Report of the US Pricacy Protection Study Commission.

26. JWK Burnside "The Legal Implications of Computers" (1981) ss A. L. F. 79.

BIBLIOGRAPHY

Van Der Merwe — Computers and the Law. (Cape Town, Juta and Company) 1982.

Tapper C — Computer Law (4th Ed.) London, Longman (1989).

McQuoid – Mason — The Law of Privacy in South Africa (cape Town, Juta and Company) 1978.

Lester John — The Law of Delict (Durban, Butterworths) 1990.

Williams G — Textbook of Criminal Law (2nd ed) London, Stevens and Sons, 1983.

Hunt and Milton — South African Criminal Law and Procedure (Cape Town, Juta and Company) 1982.

Brazier M — Street on Torts (5th Ed.) Harmondsworth, Penguin.

Landes D S — The Unbound Prometheus: Technological Change and Industrial Development in Western Europe. Chicago University Press, 1969.

JOURNAL ARTICLES

Silungwe C J — "Computer Crime: The Need for an Extension of Zambian Criminal Law" (1993) Legal Forum Vol. 5 No. 3

Hammond P — (a) "Theft of Information" (1984) Law Quarterly Review Vol. 100 pg 252

(b) "Electronic Crime in Canadian Courts" (1986) Ontario Journal of the Law Society. No. 6

Doherty P — "Stewart: When is a Thief not a Thief" (1988) Ontario Law Journal Vol. 12 pg 84

West M — "Computer Crime: The Scottish Law Commission Proposals" Yearbook of Law Computers and Technology. Vol. 3 (1987) pg 109

Skelly J — "Data Protection Legislation in Canada" YLCT (supra) at pg 79.

Young Committee — "The Report of the Committee on Data Protection" (Dec 1978) London Press.

Michine T — "The Cost of a Free Lunch" (1987). Zambian Commercial and Legal Quarterly Vol. 1 No. 4 pg 19

Weston A "Privacy" Columbian Law Review, 72 (1972) pg 693

Napier B. W "The Future of Information Technology" Cambridge Law Journal (1992) 51 pg 47

Zikonda N "A Critical Analysis of the Current Laws Pertaining to the Protection of Trade Secrets in Zambia" (1994) Unpublished dissertation.

Chisha D "The Implications of Computer Technology on the Laws of Fraud and Theft" (1995) Unpublished dissertation.