INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA

UMI®
800-521-0600
THE SECURITY AND PROTECTION OF PRIVATE INFORMATION IN THE COMPUTER AGE

by

Marcus John Senior

A thesis submitted in conformity with the requirements for the degree of Master of Laws
Graduate Department of the Faculty of Law
University of Toronto

© Copyright by Marcus John Senior 1998
The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L’auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L’auteur conserve la propriété du droit d’auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-40998-8
ABSTRACT

THE SECURITY AND PROTECTION OF PRIVATE INFORMATION IN THE COMPUTER AGE

MARCUS JOHN SENIOR

MASTER OF LAWS, 1998

GRADUATE DEPARTMENT OF LAW

UNIVERSITY OF TORONTO

This thesis is concerned with the security and protection of private information in the computer age. Information is a vitally important commodity in today's economy, and there are many reasons why different individuals, organisations and government agencies wish to control and protect it. The task of securing information is especially difficult in this time of high technology, as information can be acquired in a number of ways, and through a variety of mediums. This paper will focus on the methods which can be employed to protect private information, both from a legal and practical point of view.
For Mum, Dad and Sally
ACKNOWLEDGEMENTS

I would like to take this opportunity to thank all those persons who have made the completion of this thesis possible. First, to Professor Hudson Janisch, for supervising this project, and for feeding me on several occasions. Second, to Professor Arnold Weinrib for acting as the second reader, and third to Leonard Green, friend and confidant, for performing the excruciating duty of proof-reading this tome. I must also thank Ian Kyer, of Fasken, Campbell & Godfrey, Toronto, Ontario for his helpful suggestions in the preparation of this project, and Julia Hall, the Administrative Assistant to the Graduate Programme, for all her hard work and support. Special thanks must also go to Gian Medves, who has saved this thesis from the jaws of my demonic computer on more than one occasion.

I must also thank the Faculty of Law, the University of Toronto, my parents and grandparents for their financial assistance, and the many people who have provided friendship and emotional support throughout the course of the year. Included in this number are my fellow inmates at the law school, as well as Fiona Wu, Preeti Adhopia, the aforementioned Leonard Green, my mother and father, and of course Sally, without whose inspiration I could not have completed this task. Finally, I must thank the City of Toronto, Ontario, and Canada for many unforgettable memories.

Marc. J. Senior
Toronto, August 19, 1998

- iv -
# SUMMARY

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>ii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>iv</td>
</tr>
<tr>
<td>INTRODUCTION: THE SECURITY AND PROTECTION OF PRIVATE INFORMATION IN THE COMPUTER AGE</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER 1: INFORMATION EXCLUSIVITY AND PRIVACY</td>
<td>6</td>
</tr>
<tr>
<td>CHAPTER 2: THE LEGAL PROTECTION OF PRIVATE INFORMATION</td>
<td>26</td>
</tr>
<tr>
<td>CHAPTER 3: PRIVATE INFORMATION AND PRIVACY IN THE COMPUTER AGE</td>
<td>64</td>
</tr>
<tr>
<td>CHAPTER 4: A PRACTICAL APPROACH</td>
<td>111</td>
</tr>
<tr>
<td>CONCLUSION: LAW AND PRACTICALITY</td>
<td>173</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>179</td>
</tr>
</tbody>
</table>
# DETAILED TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>ii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>iv</td>
</tr>
<tr>
<td>INTRODUCTION: THE SECURITY AND PROTECTION OF PRIVATE INFORMATION IN THE COMPUTER AGE</td>
<td>1</td>
</tr>
<tr>
<td>A. PRIVATE INFORMATION</td>
<td>1</td>
</tr>
<tr>
<td>B. STRUCTURE OF THE THESIS</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 1: INFORMATION EXCLUSIVITY AND PRIVACY</td>
<td>6</td>
</tr>
<tr>
<td>A. THE VALUE OF INFORMATION</td>
<td>6</td>
</tr>
<tr>
<td>B. THREE RATIONALES</td>
<td>10</td>
</tr>
<tr>
<td>(a) Privacy</td>
<td>12</td>
</tr>
<tr>
<td>(b) Commercial Viability</td>
<td>14</td>
</tr>
<tr>
<td>(c) Government Interest</td>
<td>15</td>
</tr>
<tr>
<td>C. PROTECTING INFORMATION - A FOCUS ON PRIVACY</td>
<td>16</td>
</tr>
<tr>
<td>(a) The Essence of Privacy</td>
<td>18</td>
</tr>
<tr>
<td>(b) Privacy as Control over the Dissemination of Information</td>
<td>21</td>
</tr>
</tbody>
</table>
CHAPTER 4: A PRACTICAL APPROACH ............................................. 111

A. THE INADEQUACY OF LAW .................................................... 111

B. THEORETICAL AND PRACTICAL PROTECTIONS .................... 113
   *The Twelve Techniques of Situational Crime Prevention* .................. 116
   A. Increasing the Effort ............................................................ 117
      1. Target Hardening ............................................................ 117
      2. Access Control ............................................................... 120
      3. Deflecting Offenders ....................................................... 128
      4. Controlling Facilitators .................................................. 129
   B. Increasing the Risks ............................................................. 131
      5. Entry/Exit Screening ....................................................... 131
      6. Formal Surveillance ....................................................... 137
      7. Employee Surveillance .................................................... 139
      8. Natural Surveillance ...................................................... 143
   C. Reducing the Rewards ......................................................... 148
      9. Target Removal .............................................................. 148
     10. Identifying Property ....................................................... 157
     11. Removing Inducements ................................................... 158
     12. Rule Setting ................................................................. 160
   C. ANALYSIS ............................................................................. 162
      (a) Can Information be Protected by Ensuring Computer Network Security? .... 162
      (b) Can SCP Protect Computer Networks? .................................. 163
      (c) Should Practical Protections be Employed? ............................. 168

CONCLUSION: LAW AND PRACTICALITY ...................................... 173

A. SUMMARY ................................................................................. 173

B. CONCLUDING THOUGHTS .......................................................... 175

BIBLIOGRAPHY .............................................................................. 179
INTRODUCTION

THE SECURITY AND PROTECTION OF PRIVATE INFORMATION IN THE COMPUTER AGE

A. PRIVATE INFORMATION

The aim of this thesis is to discuss the security and protection of private information in the computer age. Information is a vitally important commodity in today's economy, and there are many reasons why different individuals, organisations and government agencies wish to control and protect it. The task of securing information is especially difficult in this time of high technology, as information can be acquired in a number of ways, and through a variety of mediums. This paper will focus on the methods which can be employed to protect private information, both from a legal and practical point of view.

The different varieties of information, are however, almost infinite in number, and
include amongst other things, "personal information\(^1\), information held in government hands\(^2\), public information\(^3\), research and academic information\(^4\), and commercial or business information\(^5\)"\(^6\). It would be impossible, and indeed undesirable, to discuss the legal protection afforded all of these categories, and this paper will focus only on the protection of private information.

The term "private information", is itself an elusive and wide-ranging concept. It encompasses elements of personal information\(^7\), confidential information\(^8\) and

---

\(^1\)R. Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989) at 26, defined personal information as consisting of, "those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or distribution".

\(^2\)This category refers to all information generated by, for, or on behalf of the government, and includes not only state information, but also any public, personal, private or commercial and academic information held by state organisations. See text below, *supra* note 1 and *infra* notes 3, 4, 5 and 9.

\(^3\)This is all information in the public domain. Much of it is legally protected through one of the many intellectual property regimes, including copyright, patent or trade secrets. However, great amounts of information are unprotected, including cultural, geographical, historical and linguistic data. Although, the expression, presentation and compilation of such data is usually protected under copyright law. See the *Copyright Act*, R.S.C. 1985, c.C-42.

\(^4\)This category is relatively self-explanatory. However, the distinction between educational knowledge and public information is not always easy to draw. This is primarily because the structured delivery of academic information has pecuniary value attached to it, and is hence private in nature.

\(^5\)This category includes all those types of information which may be valuable in a commercial sense, as well as any other information which may be readily quantified in pecuniary terms. Generally speaking, this category will cover any information of a business nature which can affect the profit or efficiency of an organisation, or of an individual. The most obvious examples include trade secret information, or other knowledge which is important for companies in maintaining their competitive edge. Trade Secrets and Breach of Confidence are discussed in the *Breach of Confidence* section, Chapter 2.

\(^6\)D.K. Piragoff, "Computer Crimes and Other Crimes against Information Technology in Canada", in U. Sieber, ed., *Information Technology Crime: National Legislations and International Initiatives, Vol.6* (Verlag KG, Berlin: Carl Heymanns, 1994) 85, at 118. Piragoff, at 117, also notes many other varieties of information, such as state secrets, trade secrets, copyright, trademark, contracts, employment law, fiduciary duties, economic torts, privacy, access to information and breach of confidence. See also *infra* notes 25 and 29.

\(^7\)The definition of personal information outlined by Wacks, *supra* note 1 at 26, is clearly an objective standard, and although it has clear benefits for providing legal protection and removing ambiguity, our model requires a subjective standard as the focus of this thesis is upon what people themselves want to
government information⁹, but is broader than all of them. It is any information which an individual, organisation or government agency wishes to keep secret or share only with a selected few. Personal information focuses primarily on factual data about a person¹⁰, and confidential information on matters of commercial or professional significance¹¹. Private information includes all of these objective classifications¹², plus all subjectively defined private matters¹³, regardless of their inclusion under any of the above categories¹⁴.

As noted, the scope of private information is extremely broad, and it is necessary to focus our discussion even further. In so doing, the concentration will be upon privacy, and the protection of private information of a personal, intimate or emotional nature¹⁵. This is because the concepts of privacy and private information are inextricably linked.

---

⁹By which I mean state secrets, and other confidential national security and law enforcement data. See Government Interest section, Chapter 1, and infra notes 59, 60 and 229.

¹⁰At least this is the immediate perception of the term, and I wish to avoid this narrow misconception by using the term private information in its place.

¹¹See Breach of Confidence section, Chapter 2, and infra notes 209-216.

¹²Confidential information is certainly objectively structured and defined by the courts, see supra note 8. Personal information is also strictly interpreted, however it does have a strong subjective component to it, see supra note 1.

¹³It is up to the individual to decide what they regard as private, and hence what they wish to protect. This is a crucial element of privacy, which is discussed in the Privacy as Control over the Dissemination of Information section, Chapter 1.

¹⁴We are able to cater for such subjectivity in this paper, because the focus is upon how the law can be used to obtain the protection desired, rather than whether the law should provide such protection. See supra note 7.

¹⁵This thesis is concentrating purely on the home environment, and matters of employee privacy will not be discussed. Although, the problems of employee e-mail privacy will be noted in passing. See Employee Surveillance section, Chapter 4, and infra note 565.
Not only do both require subjective control over their definition, but each is dependent on the other. Private information is both an aspect of privacy\textsuperscript{16}, and a concept of greater application\textsuperscript{17}. Indeed, much private information is likely to consist of personal information, and an unauthorised acquisition or dissemination of either would constitute an infringement of privacy\textsuperscript{18}. Conversely, however, privacy is only one component of private information, and the use of privacy purely as an example must be borne in mind.

\textbf{B. STRUCTURE OF THE THESIS}

The first chapter will discuss many of the issues highlighted above, including the value of information, the desirability of exclusivity, and the close connection which exists between privacy and private information. In focusing upon privacy, an understanding of its core elements will be necessary, and this will be seen to centre around control over the dissemination, use and accuracy of information.

The second chapter will discuss the traditional legal protections afforded private information, and the debate will be divided into two halves. The first will concentrate on

\textsuperscript{16}As D. Tapscott, \textit{The Digital Economy: Promise and Peril in the Age of Networked Intelligence} (Toronto: McGraw-Hill, 1995), notes at 273, “Confidentiality is a narrower concept. Violation of the confidentiality of your personal information undermines privacy. But privacy can be achieved without confidentiality. You may choose not to share your information in the first place - that is, not entrust others to keep it confidential. Security is required to maintain confidentiality and therefore privacy”.

\textsuperscript{17}As discussed in the text, private information also includes confidential information and state secrets, as well as personal information and other subjectively defined matters.

\textsuperscript{18}This issue is discussed in the \textit{Private Information in the Computer Age} section, Chapter 3.
preventing the acquisition of information, and the second on preventing its unauthorised dissemination by others. The discussion of acquisition will itself be broken down into three parts; acquisition during creation, transmission, and storage. The areas of law discussed will include, privacy and surveillance, interception of private communications, theft, fraud, data protection legislation, breach of confidence and public disclosure.

The third chapter will focus on the protection of privacy and private information in the computer age, where the implications of high technology will be discussed. With regards to privacy, it will be noted that traditional problems have been exacerbated and new ones created. With regards to private information, both general and specific legal protections will be discussed, including computer specific theft provisions, mischief, communications protections and unauthorised computer use offences.

The fourth chapter will explain the limits of law in protecting information, and the application of theoretical, psychological and practical measures will be seen to be the best approach to securing information exclusivity. To this end, a Situational Crime Prevention framework will be employed in defending against unauthorised system and network access.

In conclusion, it will be suggested that a combination of both legal protection and practical security must be used if private information is to be effectively secured in the computer age.
CHAPTER 1

INFORMATION EXCLUSIVITY AND PRIVACY

A. THE VALUE OF INFORMATION

Information is a curious thing. It is both a generic concept encapsulating every aspect of human understanding, whilst at the same referring to specific knowledge about isolated facts, events, ideas, and opinions. It permeates every aspect of human endeavour, and is infinite in form, variety, and application. It is intangible in essence, existing purely as a mental stimulus in the mind of the beholder, and unlike tangible goods, it does not obey the economic laws of scarcity because it is capable of universal possession and infinite replication.\(^{19}\)

Viewed as a generic concept, information is the vehicle which carries, holds,

\(^{19}\)See *Nature of Information* section, Chapter 2 and *infra* notes 96-101.
stores, and disseminates all that constitutes humanity\(^{20}\). It is our cultures, philosophies, inventions, knowledge, history, geography, and language. It is all that we are. If this understanding is followed, the value of information is beyond calculation. It is priceless.

However, if information is regarded as specific units of data, it takes on a very different guise\(^{21}\). We live in what is often termed an “information age”\(^{22}\), where the most valuable commodities in society are data, information, knowledge\(^{23}\), and know-how\(^{24}\). As such, information is vital in many capacities, with certain units of data being

\(^{20}\)Following this notion, information should not be sub-categorised or protected at all. For example, M. Pendleton, “Intellectual Property, Information-Based Society and a New International Economic Order”, in J. Phillips & A. Firth, eds., An Introduction to Intellectual Property Law (London: Butterworths, 1995 (3rd ed.)), notes that, “All inventions can be regarded as being comprised of units of information. Under this view, that which appears to our eyes to be an ‘invention’, a creation of something new, is no more than a synthesis of known units of information, not really an invention at all. Correlative to this view is the assumption that, if each unit of information is a community resource, part of the common heritage of mankind, no edifice constructed from such communal blocks should be able to constitute a privately-owned invention”. See also, R.G. Hammond, “Quantum Physics, Econometric Models and Property Rights to Information” (1981) 27 McGill L.J. 47, at 69-72 (Hereinafter referred to as “Quantum Physics”).

\(^{21}\)This humanitarian notion of information is important to note, although many of the dilemmas over information are connected with the individualistic, selfish side of human-kind. However, without the motivation of self-gain it is unlikely that the current state of the art would ever have been reached. See J.T. Cross, “Trade Secrets, Confidential Information, and the Criminal Law” (1991) 36 McGill L.R. 525, at 526-527, and Piragoff, supra note 6 at 89-90.


\(^{23}\)T. Stewart, Intellectual Capital: The New Wealth of Organizations (New York: Doubleday, 1997), defined the concepts of data, information, and knowledge, and noted the relationships between them. Beginning with symbols and ending in wisdom, he notes that: “Symbols” are individual digits or letters, whose aggregation into numbers and words create “data”. As such, “information” is the aggregation of data into useful portions of meaning, such as sentences and paragraphs, “knowledge” is the distillation of ideas, concepts and techniques from the information, and “wisdom” is an advanced state of knowledge implying understanding. Regardless of these distinctions, the terms data and information will be used interchangeably throughout the course of this thesis. See Nature of Information section, Chapter 2 and infra notes 96-101.
important to different people at different times. It is important to individuals in the maintenance of privacy, to organisations in the course of business, and to governments in the administration and protection of a country. In addition, the dynamic nature of human relations, social interaction, and technological advance means that information is perpetually changing in form, nature, and importance, and as such, is extremely temporal in value.

Information can be regarded as a means to an end, with its true value accruing from the purposes it serves and the goals it achieves. As information is almost infinite in volume, it is only useful in achieving any goal if it can be selected and separated from the vast amounts of amorphous data which exist; and if it can be put into some kind of

---

24 This can be defined as the knowledge required to carry out certain processes or procedures, or the possession of any information which would aid efficiency in a task or otherwise reduce costs of production. See Cross, supra note 21 at 526-527 and "Quantum Physics", supra note 20 at 50.

25 As R.G. Hammond, "The Misappropriation of Commercial Information in the Computer Age" (1986) 64 Can. Bar. Rev. 342 (Hereinafter referred to as "The Misappropriation of Commercial Information in the Computer Age"), at 352, notes, "Information is neither a static nor even a relative term for legal purposes. Information is what it is. That is, there are many different kinds of information and people want it for many different purposes". Examples of the ephemeral value and importance of information are almost infinite in number, but include such things as knowledge of technological innovation, traffic information and weather data. For example, traffic and weather information is only relevant at the time it is released, and is only valid for a short period of time. The information is connected to a geographical location, and is only of importance to the people in the location at that time. It is, however, of interest to different people for different reasons; a farmer may wish to know the weather in order to plan his harvesting activity, and a holiday-maker to choose a vacation destination. See also, infra note 32.

26 See Privacy section, below.
27 See Commercial Viability section, below.
28 See Government Interest section, below.
29 As Hammond states in "The Misappropriation of Commercial Information in the Computer Age", supra note 25 at 349, '[With regards to information, is it] is thus worth asking the question: is there any central concept being addressed here, or are we dealing with an amorphous or elastic term which means different things in different contexts?". See supra note 25 and infra note 32.
30 Cross, supra note 21 at 557, referred to this value of information as the "use value".
31 E. MacKaay, "Economics of Information and Law" (1982), at 3.
context. The only way the importance of such selection could be negated, would be if every unit of information in existence could be assimilated, and this is not only impossible, but also futile.

By far the greatest value of information, however, is in its exclusivity. Although universally available knowledge is valuable, it is not nearly as valuable as information which is only available to a few of those who have an interest in it. It is a well known maxim that "knowledge is power," and knowledge of information or know-how which

---

32 G.S. Takach, Computer Law (Toronto: Carswell, 1998), at 194-195. Using the weather example from supra note 25, holiday-makers only wish to know the weather forecast for their destination during the period they are intending to be there. Although the climate of the region may be of general interest to them, it is more likely to be important for an ulterior motive, for example, to plan their holiday activities, or to ensure they will obtain a suntan. The weather information will be useless if it is unrelated to a time and a location. This is not to say that general climatic changes are not of interest. Indeed, they too will be of interest to meteorologists and climatologists. However, even this information must be linked to a time and a place.

33 In the field of economics this concept is referred to as "perfect knowledge", and is a basic assumption behind many economic models.

34 Although a valid theoretical concept, "perfect knowledge" is impossible to obtain in reality. This is due partly to the infinite number of combinations and permutations of information which exist, and also because of the ephemeral and dynamic nature of information. See supra notes 25, 32 and 33, and infra note 98, point 1.

35 This is because the time and expense required to obtain all of the world's information, even on one specific topic or technological innovation, would be too prohibitive and counter-productive to be efficient or effective. In any event, by the time all of the information was acquired and compiled, it would be so out of date that it would be useless in anything except a historical context. For example, by the time all knowledge about the Intel Pentium computer processor chip and its market was obtained, the computer industry would already have advanced technology so far beyond the Pentium chip that such knowledge would be of no commercial value. See supra note 33.

36 Cross, supra note 21 at 558, referred to this value of information as the "monopoly value". As R.J. Roberts, "Is Information Property?" (1987) Intell. Prop. J. 209, at 211, notes, "Because it is capable of universal possession, information does not derive its value from inherent scarcity; its value derives from the creation and preservation of scarcity .... Kept secret, an idea might be worth millions. Once published, it becomes worthless".

37 See supra note 30.

38 Indeed, P. Burns, "The Law and Privacy: The Canadian Experience" (1976) 54 Can. Bar. Rev. 1, at 61 notes that, "Knowledge is the key to power in human institutions and the capacity and will to invade core-
others do not possess bestows great power indeed; and in order to maintain this power it is essential that such information remain secret and be kept from prying eyes.

B. THREE RATIONALES

There are three separate rationales behind the desire to keep information secret, and although different in approach, they all bear one thing in common: benefit and detriment. In many fields of human interaction, there are great benefits in possessing and obtaining exclusive information, and great detriments in losing, or not having such information. These benefits and detriments are not necessarily comparative in nature nor tangible in value, and acquiring exclusive information can not only be of great economic advantage, but also of great strategic, or psychological gain. Conversely, losing exclusivity over one’s information can result in extreme physical, emotional, and financial harm.

zones of privacy turns that key. Indeed the turning of that key affects the behaviour of those who know of it as well as the objects.”

39See Commercial Viability section, below.
40For example, knowledge of another country’s national security intelligence puts the country who possesses this knowledge in a position of great power.
41Psychological control can be gained by knowing intimate facts about another person. This creates a power differential which could be utilised to blackmail or extort money from that individual. These are, of course, criminal offences, proscribed in Section 346 of the Criminal Code.
42For example, if confidential military intelligence was obtained by a foreign power, this could have a very real impact on the lives of military personnel, as well as the citizens of that country.
43For example, the public airing of a personal psychological or medical problem could cause great emotional upset.
44For example, the acquisition of a trade secret by another company would be likely to cause a great deal of economic loss. See Breach of Confidence section, Chapter 2.
It is common sense, therefore, that individuals and institutions wish to acquire as much information from and about others as possible, whilst securing their own information to protect themselves from these detrimental consequences. Indeed, the protection of information and the acquisition of it are inextricably linked. The ability to protect information depends on the capability to defend against acquisition methods, techniques and technologies, and any discussion of information protection would be incomplete without a full understanding of acquisition.

The three motivations which drive the desire to protect information are based largely around who wants the protection, and in this respect, three groups can be isolated: individuals45, organisations46, and governments47. Each group requires information exclusivity for different reasons, which will be expanded upon below. I have labelled these rationales: privacy, commercial viability, and government interest.

---

45 Including individual citizens, families, or non-commercial groups or associations of people. For example, community groups and religious sects.
46 Including all commercial and voluntary organisations, professional bodies, and anything from a sole practitioner and small business owner to a multi-national corporation. Of course, organisations consist of individuals, but as noted in the text, it is the purpose of information exclusivity which is the guiding criteria, and individuals in a business capacity are likely to desire secrecy for very different reasons than in personal settings.
47 Including all levels of government and public administration, the courts, the police (including criminal investigations), armed forces, and other functions of the state, such as taxation and the provision of social security. Some functions of the state do not need to operate in secrecy, and indeed, it is in our interests for some of them to operate in the open, to ensure accountability. I am not including these functions in my definition. Again, governments consist of individuals, although the focus of protection is likely to be different in this context than it is in the personal arena. See supra notes 45 and 46.
(a) Privacy

The individual’s desire for information exclusivity is based on the basic human need for privacy48. In the privacy sphere, this can be referred to as secrecy, which as we will discuss below, is a crucial component of privacy. Indeed, it is presumed by many49 that humans have an innate psychological necessity for secrecy, and that this is vital for social functioning50.

In addition to these instinctual cravings, many individuals wish to keep things secret for other more cynical and self-serving reasons. Examples are infinite in number, and involve maintaining secrecy in order to prevent hurting the feelings of a loved one, to create a surprise, or to serve some other end which facilitates social interaction. Most of us can think of many situations where we desire secrecy, and it is enough for us to understand that individuals in personal capacities demand privacy, and that in order to maintain it, they must be able to control the accuracy and dissemination of their personal information.

The benefits and detriments accrued from losing exclusivity over one’s information in the privacy sphere are extremely hard to determine. The benefit for the individual of maintaining secrecy is that privacy is ensured, and the detriment of losing it is that privacy is lost. In ensuring privacy, an individual is potentially saved from a great deal of emotional and psychological hardship, and if privacy is infringed, the individual is vulnerable to these hardships.

The benefits to be gained by others in obtaining your private information are even more difficult to quantify. In the commercial sector, personal information possesses a great deal of economic value through its ability to enhance demographic and statistical analysis, and to focus marketing and advertising campaigns. However, not all private information possesses such value, and although its exclusivity loss may be of detriment to you, its gain by others may not be of benefit to them. Such information can be regarded as possessing “sentimental value,” and although not of tangible value to anyone else, it may advantage them in other ways. For example, it may satisfy their curiosity or endow them with emotional control, or it may afford them financial gain in more indirect ways, such as through blackmail or ransom.

---

51 Cross, supra note 21 at 557.
52 This is similar to the scenario where a thief steals something from your home which has no tangible value, and is of no practical use; for example, an photograph or letter which does not reveal anything of an incriminating nature. It is of no benefit to the thief, and yet its loss may be of great emotional significance to you.
53 Supra note 41.
(b) Commercial Viability

This demand for exclusivity is based on “capitalistic need”. In order for organisations to prosper they must maintain their competitive edge, and in the information age, this means successfully utilising exclusive information to increase profits and efficiency. If a company possesses knowledge and know-how which its competitors do not, then it is at an economic advantage\(^5^4\), and in order to maintain this advantage it must endeavour to keep the information secret as long as possible. In addition, as this information has such great value in the commercial field, companies not possessing it, will do anything in their power to obtain it\(^5^5\). As Cross\(^5^6\) notes, “As information has grown in importance, so have the benefits of secrecy. Because information plays such a crucial role in a technology-driven society, parties with exclusive knowledge of valuable information enjoy a tremendous advantage over their competitors”\(^5^7\).


\(^{55}\)With the current level of technology, information is even more difficult to protect from electronic surveillance, interception and eavesdropping. Piragoff, supra note 6 at 116, notes the advantage of stealing information, because it saves competing companies great amounts of time and money. R.W.K. Davis and S.C. Hutchinson, Computer Crime in Canada (Toronto: Carswell, 1997) at 115-118, note the extent of industrial espionage. See also, “Quantum Physics”, supra note 20, and infra note 98 at 54, point 6.

\(^{56}\)Supra note 21.

\(^{57}\)Cross, supra note 21 at 527.
(c) Government Interest

The motivations behind the state's desires for exclusivity are multiple. Government operates in many capacities, and the state has various reasons for wishing to keep different types of information secret; and in many cases, the public also has an interest in this. The details of these individual rationales are not important, however, some motivations can be noted in passing and include: preserving national security, enhancing national pride, increasing social effectiveness, aiding crime detection and apprehension, and advancing the economy.

The benefits and detriments of exclusivity in the public sphere depend on the type of information under discussion, and a detailed analysis here is unnecessary. However, it is easy to hypothesise what the disadvantages of exclusivity loss will be in many branches of government, especially in the military intelligence and law enforcement sectors.

58 The state holds a lot of personal information about us, and a lot of commercial information about corporations. It is in our interest that this private information be kept from the prying eyes of others. In addition, it is also in our best interests that matters of national security are kept secret, as this preserves our safety.
59 Exclusivity loss in this sphere could endanger the security of the nation as well as cause losses of both military and civilian lives. To this end, "Official Secrets" legislation exists to prevent the disclosure of sensitive government information. See Breach of Confidence section, Chapter 2, and infra note 229.
60 Exclusivity loss of this kind could significantly affect crime detection and apprehension rates.
61 Of course, it must also be noted that in many capacities, the government, and other state agencies have a counter-interest in secure communications, i.e., they want to be able, both legally and practically, to listen in on other people's conversations, for national security and law enforcement purposes. In connection with this, governments wish to control technology such as encryption, so that their eavesdropping activities are
C. PROTECTING INFORMATION - A FOCUS ON PRIVACY

It is clear that individuals and organisations wish to maintain the exclusivity of information for many reasons, and it is equally as clear that information must be protected from acquisition if this exclusivity is to be maintained. Information can be protected in a number of ways, not only legally, but also psychologically, economically, physically and electronically, and all of these methods will be discussed in later chapters\(^{62}\).

The focus of this thesis is upon the security and protection of private information, which, as we have discussed, is any information which an individual or organisation wishes to keep secret and share only with those whom he, she, or it desires. This, however, encompasses a wide variety of information, and includes anything from privacy and personal information, commercial confidential information and trade secrets to state secrets. It is, therefore, necessary to limit our analysis, and in so doing, the concentration will be upon the security and protection of personal information, private information relating to the individual in a personal capacity, and privacy in general.

The reasons for focusing upon privacy are multiple. First, due to its intangible

---

\(^{62}\)The definitions of these different varieties of protection will be discussed in Chapter 4. Legal protection however, will be the focus of discussion in Chapters 2 and 3.
nature, private information, in a personal capacity, involves a more complex discussion than private information in a commercial capacity, and is of a more general application than private government information. The reason for tackling the most complex facet of the problem is because a resolution in this sphere should aid an understanding of the issues in less complex spheres; and, as this thesis is aimed at addressing private information as a whole, this will be the best approach if any rules or principles of general application are to be found.

Second, any complex discussion regarding privacy and information protection will automatically involve a discussion of the commercial and public spheres, and as such, many issues of concern to these sectors will be discussed in passing.

Third, privacy issues are of concern to all spheres of society, not just the personal sector. As such, the matters under discussion apply equally to the commercial and government spheres, and a separate discussion of these protections would be repetitious.

It is also important to note, before moving on, that this focus on privacy will only be maintained in relation to the legal protection of information, and specifically only in connection with the traditional non-computer laws and legislation. This is because computer specific legislation and psychological and practical protections, are, by their very nature, of general application to the security of all private information. In addition, it should be noted that the normative question of whether privacy, secrecy and
information exclusivity should be protected is not a matter under discussion in this thesis.

(a) The Essence of Privacy

In discussing the protection of privacy and private information, it is important to understand the precise nature of privacy and its relationship to information. It will become clear through our discussion, that privacy is very closely related to the flow and dissemination of information, and that the protection of information is crucial if privacy is to be maintained.

Privacy is an elusive concept. Many theorists have attempted to define its core elements, but as yet, no empirical definition exists. Indeed, no empirical definition can ever exist, because privacy is a relative, fluid, and dynamic concept, meaning different things to different people. The definition changes depending upon the context in which it is used, and as Simmel notes, privacy is. “a value that does not exist in isolation, but

---

63 This issue will be addressed briefly in the conclusion however. See Concluding Thoughts section, Conclusion, and infra notes 698-703.
64 Wacks, supra note 1 at 7-30, notes that privacy should be regarded as a changing concept consisting of the relationship between the individual and society, and that it should be viewed in relation to its status, features and coherence.
65 For example, Communications Canada, Telecommunications Privacy Principles (Ottawa: Supply and Services Canada, 1992), at 5, states that, in the context of telecommunications, privacy means, “protection against unwanted intrusion, that is the right to be left alone and not to be monitored; the ability to control information about oneself, and one’s activities; the right to remain anonymous”.
Privacy has been defined as, "the right to be let alone"\(^6\), which includes the ability to physically exclude others from your "personal space", and to prevent unwanted intrusion into your life. However, this notion is simplistic, and although it embodies some aspects of privacy, does not include the most important components.

In the information age, the concept of privacy is geared towards protection and control over the dissemination of personal details, and any other information which can be used to trace the activities, understand the lifestyle, or detrimentally affect the physical, mental, or emotional well-being of an individual.

Gavison\(^6\) explained privacy as "limited accessibility", a cluster of three related but independent components, which includes aspects of both physical and informational privacy: (a) \textit{secrecy} - information known about an individual; (b) \textit{anonymity} - attention paid to an individual, and; (c) \textit{solitude} - physical access to an individual\(^7\).

\(^{67}\textit{Ibid.}, at 72.\) It is, of course, necessary in some way to develop an objective standard or understanding of privacy, even if it is a flexible definition meaning different things to different people at different times. It is possible that a two tier subjective and objective test could be applied, such as the English recklessness test in \textit{R. v. Cunningham} (U.K.) \([1957]\) 2 Q.B. 396, and \textit{R. v. Caldwell} (U.K.) \([1981]\) 1 All ER 961. Although, as discussed below, any objective standard is likely to destroy any meaningful concept of privacy. See \textit{Privacy as Control over the Dissemination of Information} section, and \textit{infra} notes 85-87.

\(^{68}\text{Cooley, } \textit{Torts} \text{ (2nd ed.)} \text{ (1895)} \text{ at 188, quoting L. Brandeis in the United States Supreme Court in 1890.}\)

\(^{69}\text{R. Gavison, "Privacy and the Limits of Law" (1980) 89 Yale L.J. 421, at 428-440.}\)

\(^{70}\text{\textit{Ibid.}, at 427-428.}\)
Prosser's\textsuperscript{71} definition concentrates more on control over information, and expresses privacy as, "the fourfold right to: control intrusion into a person's seclusion or solitude; control the disclosure of embarrassing private facts about the person; prevent being put into a false light in the public eye; and control the exploitation of a person's image and likeness"\textsuperscript{72}.

One of the most comprehensive conceptions of privacy was proposed by David Flaherty, British Columbia's first Information and Privacy Commissioner. He noted privacy interests to include the right to, "personal autonomy; to be left alone; to a private life; to control information about oneself; to limit accessibility; to exclusive control of access to private realms; to minimise intrusiveness; to expect confiden
tiality; to secrecy; and to enjoy solitude, intimacy, anonymity and reserve"\textsuperscript{73}.

The most useful component of this definition for our purposes however, is the right, "to enjoy solitude, intimacy, anonymity and reserve". Indeed, these four aspects of privacy were originally conceived by Westin\textsuperscript{74}, and understanding the definitions of these four principles is crucial in understanding the nature of privacy. Westin described solitude as, "the state where an individual is separated from the group and freed from the

\textsuperscript{71}W.M. Prosser, "Privacy" (1960) 48 Calif. L.R. 383.
\textsuperscript{72}Ibid., at 389.

- 20 -
observations of others”75; intimacy as, “the state where the individual is acting as part of a small group”76; anonymity as occurring, “where the individual, although doing public things in public places, finds freedom from identification and surveillance”77; and reserve as, “the individual’s need to withhold information, and to create mental distance to protect his personality”78.

(b) Privacy as Control over the Dissemination of Information

The above definitions have all outlined the close connection between privacy and information. However, most of them only view control over the dissemination of information as one small part of privacy, and it is my contention that the two are far more closely related.

Westin defines privacy as, “the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others”79. This definition is key to understanding the link between

---

75Ibid., at 1020.
76Ibid.
77Additionally, Westin, supra note 74 at 1021, also identified anonymity as, “the anonymous expression of views whereby the individual may publicly air his views but have his identity remain unknown”. In the U.S., there are firm legal routes in anonymity; see for example, NAACP v. Alabama, (U.S.) 357 U.S. 449 (1958) and Thornburgh v. American College of Obstetricians, (U.S.) 106 Sup. Ct. 2169 (1986).
78Ibid.
privacy and information, and indeed Westin acknowledges this observation in his own principle of reserve. However, privacy and control over the dissemination of information are intrinsically intertwined in all aspects of privacy, not just reserve\textsuperscript{80}.

Following Westin's four components, solitude is in reality the control and protection of information about physical movement or mental thoughts. There can be no physical solitude if others are watching your every move, and there can be no mental solitude if others can know your every thought. Surveillance of this kind is directly linked to information because information can be regarded as a mental process, stimulated by data and verbal representations\textsuperscript{81}, with knowledge and understanding being the final product derived from information\textsuperscript{82}. In this way, knowledge of an individual’s movements or thoughts constitutes information, and any acquisition of such information without the consent of the individual in question would constitute an infringement of privacy. This is regardless of to whom the information is passed, because privacy is lost once the knowledge resides in the mind of any one person who acquired the information without the consent of the individual to which it pertains.

Similar issues arise in connection with intimacy and anonymity. Intimacy is the selection of the people with whom an individual wishes to share information. This


\textsuperscript{81}See The Nature of Information section, Chapter 2, and infra notes 96-101.
information is not limited to personal details, facts, and opinions, but relates to any knowledge and understanding which others may possess of an individual's thoughts or actions. Controlling the dissemination of information is vital for selection, which in turn, is essential for intimacy and privacy. If individuals have no control over who knows their private information then they cannot possess intimacy nor exist in a state of privacy. *Anonymity* is the protection of information regarding a person's whereabouts in public, and the identity of an individual in the expression of his or her opinion. As such, anonymity is closely related to controlling the dissemination of information, because control is necessary to prevent others from knowing the individual's identity, which is the crux of anonymity, and a crucial component of privacy.

Another important aspect of privacy which is linked to controlling dissemination is accuracy. The freedom of the individual to represent him or herself to society in whatever way he or she wishes, is a fundamental principle of personal autonomy and a cornerstone of privacy. In order to ensure the accurate social perception of this representation, it is essential to control the flow of information about oneself. A lack of control in such matters would, therefore, constitute a serious breach of privacy.

---

82See *supra* note 23.
84This is presuming that personal autonomy is a right in itself, and is not a value subject to the vagaries of privacy, and its control over definitions. True autonomy is the ability to determine what is autonomy. Indeed, this raises issues of whether individuals have the right to lie to society and represent themselves in a false light. See *infra* note 136.
Control is also paramount to privacy in another way. As we have discussed, privacy is a relative concept, and in order for an individual to possess privacy, he or she must be living according to their construction of the concept. As Madgwick\textsuperscript{85} notes, "[privacy is] the right of the individual to be in a state of privacy to whatever extent he [or she] might wish and an invasion of privacy as anything which in any way interferes with his [or her] right"\textsuperscript{86}. One person's ideal of privacy may be different from another's, and there can be no true privacy for any individual if the construction of the term is externally determined\textsuperscript{87}.

In short, privacy is a subjective concept, and can be regarded as a claim to be staked by the individual, rather than an externally set, empirical right\textsuperscript{88}. The only objective component which can be identified is control, and specifically, control over the dissemination and accuracy of information. In this light, control must be broadly interpreted, and refers not only to power over information, and control over its

\textsuperscript{85}Madgwick, \textit{Privacy Under Attack} (1968).
\textsuperscript{86}Ibid., at 4.
\textsuperscript{87}For example, in relation to solitude. "A" may only regard mental solitude as being necessary for privacy, whereas "B" may regard any kind of physical proximity or observation as an infringement. If solitude was empirically defined as purely mental solitude, "B" would have no solitude and hence no privacy. Indeed, in reality "A" would also have no privacy, as his or her solitude is simply coincidental to the external construction of the term. With regards to intimacy, individuals must be able to decide for themselves what they regard as intimate. If others can determine this, they have no control, no intimacy, and hence no privacy. Similarly with anonymity, individuals must be able to construct their own definitions in order to regard themselves as being anonymous in any given situation; and without this feeling of anonymity, the individual can never exist in a state of privacy.
\textsuperscript{88}There is a great deal of contention over this issue. For a detailed explanation, see Wacks, \textit{supra} note 1 at 14-15, and Gavison, \textit{supra} note 69 at 427-428.
dissemination and accuracy, but also to the ability to be able to relinquish this control\textsuperscript{89}. As we have discussed, a key element of privacy is being able to determine one’s own definition of the concept, which is in itself an aspect of control. Following this line of thought, individuals must possess the power, not only to prevent the disclose of their private information and protect it from acquisition by others, but also the ability to forsake such protection and deem themselves as having no control, if this is what they desire. Without the power to relinquish control, there is no control.

A related matter is the crucial distinction between “control over information” and “control over the dissemination and accuracy of information”. Privacy has very little to do with the former, and everything to do with the latter. Once information is disseminated to the public, the individual has very little control over the information, and in this case privacy would evaporate as a right once the information was released\textsuperscript{90}. In reality, individuals can only control information before it is released, and hence the key aspect of privacy is the ability to decide when, where and how to disseminate this information to others\textsuperscript{91}.

\textsuperscript{89}See E.L. Beardsley, “Privacy: Autonomy and Selective Discourse” (1971) Nomos XIII. See also \textit{supra} note 80.

\textsuperscript{90}Wacks, \textit{supra} note 1 at 14-15.

\textsuperscript{91}Indeed, many individuals are happy to divulge information to others in order to attract business or enhance their image or career. People rarely wish to hide beneficial information, but instead wish to disseminate it to specific people in certain situations. See Branscomb, \textit{supra} note 22 at 183, and Westin, \textit{supra} note 79, at 7.
A. PROTECTING INFORMATION

In the previous chapter, it was noted that a fundamental aspect of privacy was control over the dissemination and accuracy of information\textsuperscript{92}. In order to maintain this control it is necessary to protect information from acquisition by others. There can be no privacy without control, and there can be no control without protection. If information could be obtained without the individual's consent, control would be negated and privacy destroyed\textsuperscript{93}.

In relation to private information as a broader concept, it is also necessary to protect information in order to keep it secret. Without protection, private information

\textsuperscript{92}See Privacy as Control over the Dissemination of Information section, Chapter 1.
would be available to all regardless of the desire for exclusivity. Unfortunately however, the nature of information\textsuperscript{94} means that secrecy is extremely difficult to maintain, and many individual protection measures must be employed if information is to be defended against the multitude of acquisition techniques which exist\textsuperscript{95}.

Information can indeed be obtained in many ways, including direct surveillance, interception of communications, theft of the storage medium and dissemination by others. However, it is possible to divide these methods into two principal categories. Namely, unauthorised acquisition and unauthorised dissemination. The adequate protection of information will depend on the success of legal, practical and theoretical measures in defending against these two lines of attack.

In this chapter, the focus of discussion is upon the legal protections afforded privacy and private information, and following the analysis above, this topic will be separated into two groups. However, before we begin, it is important to gain a deeper understanding of the nature of information.

\textsuperscript{93}This is still the case even if the individual has relinquished control as part of their ideal of privacy, because no real choice ever existed in relinquishing control if information could be obtained regardless of their decision.

\textsuperscript{94}See *The Nature of Information* section, below, *supra* note 23 and *infra* notes 96-101.

\textsuperscript{95}General acquisition categories will be discussed below. Specific practical and electronic techniques related to computer technology will be discussed in *Chapters 3 and 4*. 

- 27 -
B. THE NATURE OF INFORMATION

As discussed in the introduction and the previous chapter in this thesis, information is an intangible mental stimulus\(^96\) which is capable of universal possession\(^97\). Combined, these factors make information extremely difficult to control, and cause great difficulties in ensuring secrecy\(^98\). The ability to control the dissemination of information is severely compromised once others have learned it, because it is impossible to perpetually control and observe the actions of those who possess the information. In

---

\(^96\)As Hammond notes in “The Misappropriation of Commercial Information in the Computer Age”, *supra* note 25 at 349, “Communications theorists commonly draw a distinction between “data” on the one hand and “knowledge” or “information” on the other hand. Data is thought of as “cognitive stimuli” that do not change us. Information, on this view, is what changes us”.

\(^97\)See Takach, *supra* note 32 at 51-53. See also Roberts, *supra* note 36 at 209, where information is likened to “The Miracle of the Loaves and the Fishes”, recorded in the Gospel according to St. Mark, c.6, vs.34-44, and Cross, *supra* note 21 at 525, where information is likened to the spreading of light from one candle to another (taken from the *Writings of Thomas Jefferson*, vol. 6, H.A. Washington, ed. (1854)).

\(^98\)Hammond in “Quantum Physics”, *supra* note 20 at 54, notes the following problems with information, “First, sole ownership is vastly complicated in the case of information. The act of theft is often impossible to detect and difficult to prove. A piece of information can be “owned” by two people at the same time without any of the denial of the conventional benefits of ownership. Second, some kinds of information can be infinitely multiplied at low cost. Third, information generally does not depreciate with use and some kinds of information of a theoretical character actually inflate in value with usage. Fourth, unused information is, in general, of no use but the moment information is used it reveals both its existence and content and may actually enter what is conventionally referred to as the "public domain". Fifth, the creation of information is routinely a joint activity and the apportionment of “creativity” is then rendered extraordinarily difficult. Sixth, the creation of technology and information is tending to move on shorter frequencies: commercial advantage is today inextricably intertwined with innovation. Longer-frequency functional vehicles such as the statutory monopolies, are becoming increasingly inapt for this pronounced shift in commercial timeframes. Seventh, the volume of available information has reached overwhelming proportions. Classical economics assumes the possession of complete information about the availability of different goods, estimation of costs and maximisation of utility preferences. But more information is not complete information. The disabilities of the individual in relation to the sum of knowledge become progressively more severe as the sum increases. Eighth, in economic terms, public goods are separated from private goods by a principle of exclusion. Although that principle can still apply to information it is routinely invoked only at a considerable cost.”.
addition, further dissemination is undetectable, due to information’s capacity for universal possession, and its nature as a mental process\textsuperscript{99}.

In the information age, the ability to control the dissemination of information is further diminished due to information’s capacity for infinite replication\textsuperscript{100}. In light of this, the only way to control the flow of information is to protect its “carrier”. As information is a mental stimulus, the way to stop its transmission is to prevent the mind being stimulated. This means preventing individuals from coming into contact with the physical manifestation and representation of the information, which is referred to as data\textsuperscript{101}, and protecting and controlling data is the key to maintaining information exclusivity and privacy.

\textsuperscript{99} At present, it is impossible to “read the minds” of individuals, and hence it is impossible to know for certain whether other people possess certain information or knowledge. The closest practical technique available is interrogation in combination with the use of a lie-detector or “polygraph”. In addition, it is also extremely difficult at this time to erase a person’s memories, and as such, there is no way of rescinding information once it has been acquired. It is, however, entirely possible that efficient and effective telepathic interception and memory-erasing equipment will be available in the future.

\textsuperscript{100} See supra note 98, “Quantum Physics” at 54, point 2. This problem is exacerbated in the computer age. See Takach, supra note 32 at 13-47, and The Nature of Information section, Chapter 3.

\textsuperscript{101} Data can be regarded as the elements or units of information, or as the representation of it. Data can be seen as the carrier or conveyor of information, with each of us gaining our knowledge and understanding by interpreting data and obtaining information from it. It is probably easiest, for our purposes, to regard data as the physical foundation and manifestation of information, and information as the mental process stimulated by that data. As Piragoff, supra note 6 at 94, explains, “information is not a thing, but a process or relationship that occurs between a person’s mind and some sort of stimulus ... [whereas] data is merely a representation of information or of some concept”.

- 29 -
C. PREVENTION AGAINST UNAUTHORISED ACQUISITION

As noted earlier, there are many methods of acquisition which can be employed in obtaining information, and in order to adequately protect information it is necessary to defend against all of these techniques. In addition, information can be acquired from many sources, usually from either the individual him or herself, or from tangible information carriers under their control\textsuperscript{102}; or through unauthorised acquisition from another person or organisation entrusted with the information\textsuperscript{103}.

The methods of acquisition can be divided into three groups: the acquisition of information during its creation, the acquisition of information during its transmission, and the acquisition of information in storage. These will be addressed in turn.

(a) The Acquisition of Information During its Creation

Information is created about individuals when they respond to stimuli, perform actions, or move from one physical position or geographical location to another\textsuperscript{104}.

\textsuperscript{102}For example, the paper which carries the data can be taken away. This is discussed under Theft in both Chapters 3 and 4.

\textsuperscript{103}Situations where a person who is entrusted with your information authorises its dissemination to others, without your knowledge or consent, are topics for discussion in the next section. See Prevention Against Unauthorised Disclosure section, below.

\textsuperscript{104}Of course, speech and communication can also be regarded as the creation of information in the sense that information can be developed in the mind and enunciated to others for the first time. However, we
Information of this nature is acquired through surveillance, and if privacy and private
information are to be protected, it is essential that the prohibition of surveillance be
enshrined in law.

(i) Surveillance and General Privacy Protections

Surveillance is regarded as an infringement of privacy\(^{105}\), and although there is no
general right to privacy in Canada\(^{106}\), many individual freedoms and rights to privacy are
protected through specific rights arising from miscellaneous statutory provisions and the
common law\(^{107}\); and as Burns\(^{108}\) notes, "Although many provinces lack general privacy
legislation, the combined effect of the extant common law, and provincial and federal
legislation, grants Canadians a fair measure of protection against invasions of
privacy"\(^{109}\). For example, Burns highlights trespass to land as a protection\(^{110}\), and this is
indeed likely to reduce the success of surveillance, because access to the physical
locations used to observe and eavesdrop is prohibited.

\(^{105}\) See infra notes 111-115.
\(^{106}\) See Piragoff, supra note 6 at 119.
\(^{107}\) Such as contract, tort, and equity. Examples include trespass to land, trespass to chattels, trespass to the
person, nuisance, defamation, injurious falsehood, wilful infliction of nervous suffering, passing-off and
appropriation, and breach of confidence. See Burns, supra note 38 at 12-31.
\(^{108}\) Ibid.
\(^{109}\) Ibid., at 64.
\(^{110}\) Ibid., at 14-16.
Of particular note, in relation to surveillance, is Section 8 of the Canadian Charter of Rights and Freedoms. This provision provides every person a constitutional right against unreasonable search and seizure by the state, and prohibits any kind of unauthorised electronic surveillance or information gathering. However, by broadly interpreting the Charter, cases such as R. v. Wise, R. v. Wong and R. v. Duarte, have extended this protection to prohibit surveillance by individuals acting independently of the state. In this way, the Charter now clearly provides for the protection of a person’s “reasonable expectation of privacy”.

In addition, the Provinces of Newfoundland, Saskatchewan, Manitoba and British Columbia also have provisions which establish a tort of the “invasion of privacy”; and

---

111Hereinafter referred to as the Charter. It is Part I of the Constitution Act, 1982, enacted by the Canada Act, 1982 (U.K.) c.11. Section 8 states that, “Everyone has the right to be free from unreasonable search and seizure”.

112See R. v. Dyment [1988] 2 S.C.R. 417, at 429, where the court stated that, “Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual”. However, the decision in R. v. Plant (1993) 3 S.C.R. 381 (S.C.C.), seems to indicate that this privacy is limited to a biographical core of data (the item under question in R. v. Dyment was a blood sample), and that electricity consumption records will not be protected, even if they do reveal something about an individual’s lifestyle or activities. For information to be protected by the constitutional protection under Section 8 of the Charter, it must be of a “personal and confidential nature” (R. v. Plant, at 213).

113(1992) 70 C.C.C. (3d) 193 (S.C.C.). Use of an electronic tracking device attached to an automobile considered a violation of privacy under Section 8 of the Charter.

114(1990) 1 C.R. (4th) 1, 60 C.C.C. (3d) 460 (S.C.C.). Use of hidden cameras considered a violation of privacy under Section 8 of the Charter.


116See Piragoff, supra note 6 at 121.

117As Takach, supra note 32 at 209-210, notes that, “In four provinces there are privacy statutes which establish a tort, actionable without proof of damages, where someone knowingly and unreasonably violates the privacy of another person. These statutes do not define “privacy”, but generally set out the following as acts which constitute a violation of privacy: audio or visual surveillance of a person or the person’s home by any means; listening to or recording a person’s conversation or listening to or recording messages travelling to or coming from that person by telecommunication; use of a person’s letters, diaries
these provisions, amongst other things, prohibit any audio or visual surveillance of a person or the person's home by any means. Of particular interest is the Quebec legislation, which, under its civil code, provides, in Article 35, that, "Every person has the right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person or his heirs unless authorised by law."  

It must also be borne in mind that Canada is bound to the Universal Declaration of Human Rights, which protects privacy under Article 12, stating that, "No one shall be subjected 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."  

It is important to note that surveillance is not only a violation of privacy when it is

---

118 Ibid.
121 Technically speaking, Canada is not bound by the Universal Declaration of Human Rights of 1948 (infra note 122), but is bound by the International Covenant on Civil and Political Rights of 1976, which under Article 17, reiterates the privacy rights included in Article 12 of the Universal Declaration of Human Rights. See S. Alter (Law and Government Division, Library of Parliament), Privacy Issues in Telecommunications (Ottawa: Supply and Services Canada, 1996), at 18.
123 Ibid.
conducted in private places, but also when it is conducted in public, and in this time of high technology such infringements are easy to perpetrate\textsuperscript{124}. As noted in the case of \textit{R. v. Wong}\textsuperscript{125}, "\textit{modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy}"\textsuperscript{126}.

\textbf{(b) The Acquisition of Information During its Communication}

If private information and privacy are to be fully protected, it is necessary not only to protect against surveillance, but also to protect against the acquisition of information during its transmission and communication. This communication can take the form of personally conducted verbal, written, signed\textsuperscript{127} or visual conversation, or any kind of postal or telecommunication transmission. The protection of communications is very closely related to surveillance, because the vast majority of surveillance involves eavesdropping on personally conducted or telecommunicated conversations. As such, the legal protections afforded information in communication are also heavily based in privacy. However, specific legislation also exists.

\textsuperscript{124}In the case of \textit{R. v. Elzein} (1993) 82 C.C.C. (3d) 455 (Que. C.A.), public surveillance with high powered cameras was deemed not to be a violation of s.8 of the Charter.

\textsuperscript{125}\textit{Supra} note 114.

\textsuperscript{126}\textit{Ibid.}, at 479.

\textsuperscript{127}Meaning signalled, as in sign language or semaphore.
(i) Specific Communications Protections

Section 184 of the *Criminal Code* specifically prohibits the interception of private communications, and reads as follows:

SECTION 184

(1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

The provision is very broad, and protects any kind of direct or telecommunicated communication, and would certainly protect all voice telephony, facsimile, and data transmissions.

---

128 The *Criminal Code of Canada*, R.S.C. 1985, Part VI. This provision was originally created by the *Protection of Privacy Act*, S.C. 1973-74, c.50, and exists as part of the “Invasion of Privacy” provisions.
129 Interception is defined in s.183 as including, to, “listen to, record or acquire a communication or acquire the substance, meaning or purport thereof”.
130 “Private communication” is defined in s.183 as meaning, “any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it”, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.” “Telecommunication” is defined under The *Interpretation Act*, R.S.C. 1985, c. I-21, s.35, as, “any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio or other electromagnetic system”. The *Telecommunications Act*, 1993, S.C. c.38, defines “telecommunications”, under Part I, s.2(1) as, “the emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system”.
131 Subsection (2) lists certain circumstances in which subsection (1) does not apply, for example, where authorisation has been given by one of the parties to the communication, or where interception is required for law enforcement purposes. See also the cases of *R. v. Duarte* (supra note 115) and *R. v. Thompson* [1990] 2 S.C.R. 1111.
In relation to postal communication, very strong legal provisions exist which protect the security and integrity of the mail, both in its carriage and content. For example, Section 345 of the Criminal Code provides that, "Everyone who stops a mail conveyance with intent to rob or search it is guilty of an indictable offence and liable to imprisonment for life".

Various other Acts and Sections of the Criminal Code protect communication in general. Section 193 states that it is an offence to unlawfully use or disclose an intercepted private communication, and Section 193(1) makes it illegal to use or disclose a radio-based telephone communication. Indeed, privacy in communications is a component of Canadian Telecommunications Policy, and is included in Section 7 of the Telecommunications Act.

132See for example, the extremely broad definition of "private communication", supra note 130.
133The protection which s.184 affords electronic-mail will be discussed in Telecommunication Protections section, Chapter 3.
134Weingarten, supra note 49 at 739, notes the legally guaranteed confidentiality of "first-class" mail in the United States. See infra note 142.
135Takah, supra note 32 at 191-192, states that, "Subsection 9(1.1) of the Radiocommunication Act ([R.S.C. 1985, c. R-2]), for example, makes it an offence to intercept and make use of, or intercept and divulge, any radiocommunication, which essentially covers any transmission of signals lower than 3,000 GHz". Alterations were also made to the Criminal Code to protect this type of communication (see s.193(1), discussed in the text). There is however, much controversy over this point. Originally, only the disclosure of radio-based communications was prohibited and not interception per se. The rationale lies in the fact that radio-based communications use public airwaves, and hence cannot be regarded as private communications unless they are encrypted. See supra note 130, A Proactive Approach to Protecting Information section, Chapter 3, and Target Removal section, Chapter 4. See also Bill C-109. The Information Highway Advisory Council (IHAC) recommended that the same level of protection be afforded radio-based communications as wire-line services, and also that the devices used to intercept such communications be banned. They also advised that encryption should be developed and used in radio-based communications to enhance privacy (see Alter, supra note 121 at 7-8).
136Telecommunications Act, 1993, R.S.C., c.38, Part I, s.7(i) states as one of the policy objectives, "to contribute to the protection of the privacy of persons". Section 47 of the Act directs the Canadian Radio-television and Telecommunications Commission (CRTC) to exercise its powers and perform its duties with
(ii) Privacy Related Protections

In addition to these specific provisions, extensions of general privacy statutes also protect direct and telecommunication\(^{137}\). For example, as discussed above, four provinces\(^{138}\) have legislation which establish a tort of the invasion of privacy, and each contains provisions, "making it a tort, amongst other things, to listen to or record a person's conversation or to listen to or record messages travelling to or from that person by telecommunication"\(^{139}\). Also of note is Article 36 of the Quebec Civil Code which states that, "intentionally intercepting or using [another individual's] private communications", is strictly prohibited as, "an invasion of the privacy of a person"\(^{140}\).

Of greater importance however, is the fact that the "interception of communications" offence, and privacy, are inextricably linked. This is because both

\(^{137}\)Other aspects of telecommunications privacy which will be touched upon in Privacy Concerns in the Computer Age section, Chapter 3, are the use of “Caller ID” or “Call Display” technologies, and the use of dial number recorders (DNRs) or pen registers. See infra notes 303-304 and 511.

\(^{138}\)Such as Manitoba, Saskatchewan, British Columbia and Newfoundland. See supra note 117.

\(^{139}\)Takach, supra note 32 at 192.

\(^{140}\)Supra note 120.
Section 184 of the *Criminal Code* and Section 8 of the *Charter* only afford protection to communications when there is a reasonable expectation by the originator of the communication, that it will not be intercepted\(^\text{141}\). As an example of this, a conversation shouted across a crowded plaza would not possess a reasonable expectation of privacy, whereas a whisper uttered in the corner of a private room would.

In relation to telecommunications, many different transmission mediums and communication technologies exist, and the situation is very complex. Some mediums and technologies, and not others, will be regarded as private. For example, mail\(^\text{142}\), and

---

\(^{140}\) *Supra* note 120.

\(^{141}\) See *Criminal Code*, s.183 and *supra* note 130. This is not the case in England however, where it was held, in the case of *Malone v. Metropolitan Police Commissioner* (U.K.) [1979] Ch.344, that telephone communications could not be regarded as private. Megarry V.-C., at 376-378 stated, “I do not see why someone who has overheard some secret in such a way should be exposed to legal proceedings if he uses or divulges what he has heard. No doubt an honourable man would give some warning when he realises that what he is hearing is not intended for his ears; but I have to concern myself with the law, and not with moral standards. There are of course, many moral precepts which are not legally enforceable... When this is applied to telephone conversations, it appears to me that the speaker is taking such risks of being overheard as are inherent in the system... No doubt a person who uses a telephone to give confidential information to another may do so in such a way as to impose an obligation of confidence on that other: but I do not see how it could be said that any such obligation is imposed on those who overhear the conversation, whether by means of tapping or otherwise.” See infra notes 143 and 232.

\(^{142}\) This is by no means unanimous, however. *R. v. Newell*, (1982) 69 C.C.C. (2d) 284 (B.C.S.C.) held that mail was not to be regarded as a secure communications medium. This was because letters can be stored and read later by others, and because they may pass through the hands of many people before eventually reaching the intended recipient. This is especially the case with postcards. However, *R. v. Crane*, (1985) 45 C.R. (3d) 368 (Nfld. D. Ct.) held otherwise, and mail is now afforded privacy protection in Canada.
ground line based telephony\textsuperscript{143} will all possess this reasonable expectation of privacy, whereas pager communications\textsuperscript{144} and cellular telephony\textsuperscript{145} will not\textsuperscript{146}.

The complexity of the situation is added to when it is considered that technological change is constantly upsetting the balance. As McLachlin J. noted, in the case of \textit{R. v. Cheung}\textsuperscript{147}, "As technological advance and counter-advance leapfrog each other, I am sure that ease and difficulty of interception will shift from time to time. The state of technology at the time of any disputed interception will be important, because it will bear on the reasonable expectations of the caller"\textsuperscript{148}.

This constant fluctuation can be seen by comparing this case with that of \textit{R. v. Solomon}\textsuperscript{149}. In \textit{Solomon}, cellular telephony was not regarded as private due to its vulnerability to scanning, whereas in \textit{Cheung}, cellular telephony was regarded as private due to the difficulty of scanning such communications. The "reasonable expectation of

\textsuperscript{143} In Canada, this reasonable expectation to privacy can be inferred from the presence of the "interception of communications" provision in the \textit{Criminal Code} (s.184). The English Law Commission, in a report by Lord Diplock entitled, \textit{The Interception of Communications in Great Britain} (U.K.), 1981, Cmnd. 8191, stated in para.6.35 that, "We do not think that in a civilised society a law abiding citizen using a telephone should have to accept that it may be tapped". See \textit{supra} note 141.

\textsuperscript{144} See \textit{R. v. Nin}, (1985) 34 C.C.C. (3d) 89 (Que. Ct. Sess.), and \textit{R. v. Lubovac}, (1989) 52 C.C.C. (3d) 551 (Alta. C.A.). Pagers are generally not protected because an external party passes on the message to the paging device. However, as technology advances, the expectation of privacy regarding this communication medium will undoubtedly change.

\textsuperscript{145} See the discussion in the text, and \textit{supra} notes 147-150.

\textsuperscript{146} However, in 1993, \textit{Bill C-109} extended s.184 of the \textit{Criminal Code} to protect cellular communications if the communication is encrypted. See \textit{supra} notes 130 and 135.

\textsuperscript{147} (1995) 100 C.C.C. (3d) 441 (B.C.S.C.).

\textsuperscript{148} \textit{ibid.}, at 443.

privacy” pendulum is likely to swing in perpetual motion as more advanced security devices and scanners become available.\textsuperscript{150}

\textit{(c) The Acquisition of Information in Storage}

In protecting information, it is not enough simply to protect information during its creation and transmission. It is also necessary to protect it whilst in storage. Many storage mediums exist, such as paper, magnetic tapes\textsuperscript{151}, and the human mind, and in order to adequately defend information it is crucial that these “data carriers” be prescribed protection in law. Two criminal provisions are of interest here: theft and fraud.

\textit{(i) Theft}

The theft provisions of the \textit{Criminal Code} are set out in Section 322, and the basic premise of the offence is contained within subsection (1), and reads as follows:

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{150}See Privacy Commissioner of Canada, \textit{Annual Report 1992-1993} (Ottawa: Canada Communications Group, 1993) (Hereinafter referred to as the \textit{Annual Report}).
\item \textsuperscript{151}We will discuss computer specific storage mediums in \textit{Chapter 3}. However, it should be noted that information is not only stored on magnetic media in the computer age, such as on hard and floppy disks, but also in optical and biological storage systems.
\end{itemize}
\end{footnotesize}
SECTION 322

(1) Every one commits theft who fraudulently and without colour or right takes, or fraudulently and without colour or right converts to his use or to the use of another person, anything whether animate or inanimate, with intent,

(a) to deprive, temporarily or absolutely, the owner of it or a person who has a special property or interest in it, of the thing or of his property or interest in it,

(b) to pledge it or deposit it as security,

(c) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform, or

(d) 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 taken or converted.

Although the section clearly protects against the unauthorised permanent removal of physical and tangible goods, the question of whether information can be regarded as property for the purposes of theft is one which has created a great deal of controversy152.

The matter was addressed in a number of cases153, the most important of which are R. v. Stewart154 and R. v. Offley155. In Stewart, the Ontario Court of Appeal held that

153 See also R. v. Scallen (1974), 15 C.C.C. (2d) 441 (B.C.C.A.); and R. v. Falconi (1976), 31 C.C.C. (2d) 144 (Ont.Co.Ct.).
information could be regarded as property for the purposes of the criminal law, and hence that it could be the subject of theft\textsuperscript{156}. However, in \textit{Offley}, the Alberta Court of Appeal concluded that information could not be the subject of theft.

This divergence was resolved by the Supreme Court of Canada whilst hearing the case of \textit{R. v. Stewart}\textsuperscript{157} on appeal. The court concluded that, although information could be the subject of theft under the criminal law, it would not be regarded as such on policy grounds\textsuperscript{158}.

In addition, the technicalities of the theft provisions also make the offence extremely difficult to apply to information. This is because a necessary element of the offence is the temporal or permanent deprivation of property, and as discussed above, information is not regarded as property and hence cannot be the subject of deprivation or theft. However, even if information was regarded as property and its taking capable of deprivation, it is unlikely in practicality that any deprivation would be suffered by the interest owner in the taking of information. This is because physical or electronic copies

\textsuperscript{156}In \textit{R. v. Scallen} (supra note 153), it was noted that the term, "\textit{anything, animate or inanimate}" (in s.322(1)), need not be limited to tangible or material goods, and that as such, information could be protected by the provision.
\textsuperscript{158}In the case, Lamer J. stated that, "Confidential information should not be, for policy reasons, considered as property by the courts for the purposes of the law of theft. In any event, were it considered such, it is not capable of being taken as only tangibles can be taken. It cannot be converted, not because it is intangible, but because, save very exceptional far-fetched circumstances, the owner would never be deprived of it" (ibid. at 495-496).
of data are usually maintained by the victim\textsuperscript{159}, and also because a mental copy of the information may permanently reside in the mind or memory of the individual. As memories are not easily erased\textsuperscript{160}, deprivation can only occur if the information is forgotten; and although this is likely to be the case in the realm of business and government where vast amounts of anonymous data are compiled and analysed, it is unlikely to the case in the privacy sphere, where many of our most intimate and troubling moments are etched in our minds.

In the taking of information, one deprivation has always occurred. Namely, the loss of exclusivity, and as we have discussed, the protection of exclusivity is crucial for the protection of private information and privacy\textsuperscript{161}. Unfortunately, the Supreme Court of Canada, in \textit{Stewart}, held that confidentiality cannot be stolen, because it cannot be owned, merely enjoyed\textsuperscript{162}, and in this light it seems the theft provisions will be of limited use in protecting information\textsuperscript{163}.

\textsuperscript{159}As in s.322(1)(a). This is especially the case in the computer age with the theft of computer stored information. These issues will be addressed in \textit{Chapter 3}.
\textsuperscript{160}This may be possible in the future, however, see \textit{supra} note 99.
\textsuperscript{161}Of course, exclusivity is also important for the commercial and government sectors. Such losses frequently occur through disclosure by employees and others who are entrusted with private information. These matters will be discussed under the \textit{Prevention Against Unauthorised Disclosure} section, below, and in \textit{Chapter 3 and 4}. See also, \textit{infra} note 565.
\textsuperscript{162}See Takach, \textit{supra} note 32 at 151. Loss of exclusivity is protected under the civil law if the information was a trade secret, or constituted some other form of data specifically protected by an intellectual property regime, the common law, or statute.
\textsuperscript{163}Indeed, in discussing information, the court focused on the protection of confidential information. The court was concerned that it might not be able to adequately define, identify, and isolate confidential information from the many other varieties of information which exist. As Lamer J. noted, in \textit{R. v. Stewart} (\textit{supra} note 157), on appeal to the Supreme Court of Canada, at 492, "Moreover, because of the inherent nature of information, treating information as property simpliciter for the purposes of the law of theft would create a host of practical problems. For instance, what is the precise definition of 'confidential
In discussing theft, however, we do not have to concentrate on the theft of information directly. This point was alluded to above, and just as data is the “carrier” of information, the storage medium is the “carrier” of data, and the taking of the physical storage medium which contains the data is indeed theft under s.322(1). In this way, although information itself is not protected by the theft provisions, it can be protected indirectly. However, it is important to note that even this application of the theft offence is not trouble-free, because problems arise in relation to the quantum of the stolen item, as very little value subsists in a sheet of paper\textsuperscript{164}, or a magnetic tape.

Before closing our discussion on theft, it should be noted that one other related provision could help protect information. This is the prohibition against breaking and entering\textsuperscript{165}, which makes it an offence to illegally enter buildings and other premises. The provision would enhance information security because it prevents those wishing to take information from entering the physical location in which the information is stored, and without physical access to the data they would be unable to acquire any knowledge

---

\textsuperscript{164} See \textit{Oxford v. Moss} (U.K.) [1979] Cr. App. R. 183. Indeed, the cost of the piece of paper is of little value in comparison to the value of the information which it contains. It seems peculiar that the law would not protect the thing of value, whilst at the same time protecting the thing of “no value”.

\textsuperscript{165} \textit{Criminal Code}, Sections 348-351.
from it.  

(ii) Fraud

The offence of fraud, which is contained in Section 380 of the Criminal Code, prohibits the attempted dishonest deprivation of valuable goods and services. This provision is generally more helpful in the protection of "valuable" information than the theft provisions, not only because attempted as well as actual deprivation is prohibited, but also because exclusivity is protected. As Davis and Hutchinson note:

If the loss of exclusive domain over information will cause economic or pecuniary harm to the person or business with a lawful right to such exclusivity (usually because the information is copyrighted or is a trade secret), the element of deprivation will be made out. If the deprivation is the product of some dishonest act by the accused (whether a

---

166 It should be noted that the law does not physically prevent perpetrators from breaking and entering. However, the existence of the law does provide a psychological deterrent which will be discussed in greater depth in A Proactive Approach to Protecting Information section, Chapter 3.

167 Section 380: (1) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security [is guilty of the offence of fraud].

168 See R. v. Olan (1978), 41 C.C.C. (2d) 145 (S.C.C.). In R. v. Stewart (supra note 157), Lamer J., referring to the case of R. v. Olan stated that, the proof of a risk of prejudice to the economic interests of the victim is sufficient evidence of the deprivation: actual economic loss is not essential” (Applying Section 338(1), and the definition of “defraud”).

169 Supra note 55.

falsehood or some other "underhanded" deed) then the offence will be complete. Fraud will, therefore, offer some relief [in the context of information]. 171

As noted in our discussion above, there can be no deprivation in the taking of information, and this situation is the same in relation to the fraud provision as it is in relation to the theft provision. However, deprivation can occur in relation to fraud in the form of economic loss incurred through the loss of exclusivity in the information, but it is important to note that this is in no way connected to any deprivation accruing in the information itself. Loss of information, or exclusivity in it, is still not protected by fraud, even though economic loss suffered due to its loss is covered172.

This distinction is important, because it highlights the fact that the offence of fraud can only be used to protect commercial information, or any other information with a readily quantifiable tangible value173. It will not protect private information of a personal, emotional, or psychological nature. In this capacity, it seems that the only protection fraud will provide is in preventing174 the unauthorised acquisition of information from others who are holding it in a commercial context, and even then, some

171 Davis & Hutchinson, supra note 55 at 182.
172 The nature of information as a means to an end is highlighted here. See The Value of Information section, Chapter 1.
173 As Takach, supra note 32 at 157, states, "Thus, in appropriate circumstances, creators and owners of intellectual property can find the Criminal Code's fraud provision helpful in combating bootleggers, counterfeiters and others who would unfairly misappropriate the fruits of intellectual labour".
174 Once again, it should be borne in mind that the law cannot physically prevent fraudulent activity occurring, although it can provide a deterrent effect. See supra note 166, and A Proactive Approach to Protecting Information section, Chapter 3.
financial loss must occur to the institution in question if a fraud claim is to succeed.

D. PREVENTION AGAINST UNAUTHORISED DISCLOSURE

In order to ensure the complete protection of privacy and private information, it is necessary not only to prevent the unauthorised acquisition of information, but also to prevent its unauthorised disclosure by parties with whom it is entrusted. As we have noted, in the information age, the concept of privacy is primarily geared towards the need to control the dissemination of personal information which can be used to trace an individual’s activities or assess their lifestyle; and if privacy is to be maintained, it is essential that agencies possessing an individual’s information be prohibited from disseminating it without consent. In addition, the protection of private information as a broader concept, also requires that information imparted to others be protected from disclosure175.

We entrust others with our personal and private information in many capacities, most of which seem irrelevant and go unnoticed. Information is not only confided in our

175 As Tapscott, supra note 16 at 282, states, “You own it. It is your property. Others who obtain your personal information act as its custodians and are entrusted with its care. If such information has value, the owner should receive compensation for its use”.
doctors, lawyers, banks, and government agencies\textsuperscript{176}, but it is also shared with clothing stores, supermarkets, video shops, transit authorities, and many other retail organisations, service providers and commercial ventures\textsuperscript{177}. In short, our interactions with society produce a vast amount of information, and if this is combined and collated it can reveal a great deal about a person's life, including their activities, movements, medical history, consumption patterns and financial situation\textsuperscript{178}. Such unauthorised information collection and processing clearly poses a great threat to privacy\textsuperscript{179}, and in order to maintain privacy it is essential that the individual be able to control the accuracy, use and further dissemination of their private and personal information\textsuperscript{180}.

In addition to these privacy concerns, much private information does not consist of personal information or "privacy data". A great deal of information consisting of far

\textsuperscript{176}Discussed in greater depth in the Breach of Confidence section, below. Governments store many different components of data about individuals, and it would also constitute an infringement of privacy for them to collate all of their data to create a more detailed profile of a person's life.

\textsuperscript{177}Commercial organisations usually only possess personal data and information relating to an individual's name and address, matched with an activity or credit card number. This is very different from the more intimate information stored by doctors and lawyers for example. In addition, this information is usually stored for wider-scale commercial purposes, and does not generally relate or refer to specific individuals. For example, video shops are only likely to be interested to know what films people rent in general, so they can purchase the correct number of copies for hire; and transit authorities are only likely to be interested in the number of people using services at a particular time in order to allocate resources accordingly. However, clothing stores and supermarkets may have a deeper purpose in obtaining personal information. Not only does transaction data aid stock-taking, but it also allows retailers to gear marketing and advertising campaigns directly to the individual, because a person's consumption patterns can be precisely calculated. See Data Protection section, below, and Privacy Concerns in the Computer Age section, Chapter 3.

\textsuperscript{178}Ibid.

\textsuperscript{179}For example, it violates all of Westin's (supra note 74) aspects of privacy: solitude, intimacy, anonymity and reserve. See The Essence of Privacy section, Chapter 1, and supra notes 74-78.

\textsuperscript{180}This is of course providing the individual requires control for privacy. If he or she decides that control over the dissemination, use and accuracy of information is not necessary for privacy then protection from
more than personal details is disclosed to others in a wide variety of personal and professional settings\textsuperscript{181}, and it is essential that this type of information also be protected from disclosure.

The primary legal regimes which protect the unauthorised disclosure of private information are data protection legislation, breach of confidence, and the public disclosure of private information.

\textit{(a) Data Protection}

Data protection generally refers to legislation which protects personal information given in a specific capacity to an individual financial, consumer or government organisation. Such legislation limits the ability of these organisations to disclose the information\textsuperscript{182}, and also places constraints on the time and purpose for which the information can be held and used\textsuperscript{183}.

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{181}Examples noted above were lawyers, doctors, and bankers. However, priests and personal friends are also covered here. See \textit{Breach of Confidence} section, below.
\item \textsuperscript{182}See Piragoff, \textit{ supra} note 6 at 120. See also \textit{infra} notes 184 and 185.
\item \textsuperscript{183}See A.P. Williams, R. Wilkes and M. Erdle, “Data Transmission and Privacy: Canada”, in D. Campbell and J. Fisher, eds., \textit{Data Transmission and Privacy} (Dordrecht: Martinus Nijhoff Publishers, 1994) at 31-77. See also \textit{infra} notes 184 and 185.
\end{enumerate}
\end{footnotesize}
Although there is no general right to privacy in Canada, as we have discussed, many specific federal and provincial acts protect against the disclosure of information in certain contexts. Examples include the variously titled freedom of information and protection of privacy acts of many of the provinces\textsuperscript{184}, and the federal *Privacy Act\textsuperscript{185}.

\textsuperscript{184}Such as the Ontario, British Columbia and Saskatchewan, *Freedom of Information and Protection of Privacy Acts* (Ontario, R.S.O. 1990, c.F-31; British Columbia, R.S.B.C. 1996, c.165; Saskatchewan, S.S. 1990-91, c.F-22.01); the Manitoba, Newfoundland and Nova Scotia, *Freedom of Information Acts* (Manitoba, S.M. 1985-86, c.6, c.F-175.; Newfoundland, S.N. 1981, c.5; Nova Scotia, S.N.S. 1990, c.11); the New Brunswick, *Right to Information Act* (S.N.B. 1978, c.R-10.3); and the Quebec, *Loi sur l'accès aux documents des organismes publics sur la protection des renseignements personnels*. The Quebec legislation is of particular interest. It contains extremely comprehensive provisions governing the protection of private information in the private sector. The "*Act Respecting the Protection of Personal Information in the Private Sector*", also known as Bill 68, came into force in January 1994, S.C. 1993, c.17. The Act fleshes out provisions included in the new Quebec Civil Code, passed in 1991 (S.C. 1991, c.64, Articles 35-41). As R.C. Owens, T. Onyshko and P.C. Goode, "Reform Proposals Relating to Customer Privacy and Tied Selling in the Federally-Regulated Financial Services Sector", Paper Presented at The Queen's Annual Business Law Symposium, Queen's University, Kingston, Ontario, November 22, 1996, note at 13, the Act, "applies to a wide range of private sector entities, including corporations, sole proprietorships, partnerships, organisations and associations. Various provisions govern the collection, use and transfer of personal information; the Act also establishes the individual's right to gain access to personal information and request a correction where it appears inaccurate". Of particular note is a provision in Division III, *Confidentiality of Personal Information*, which states: 1 - Retention, Use and Non-Communication of Information: (10) "Every person carrying on an enterprise who collects, holds, uses or communicates personal information about other persons must establish and apply such safety measures as are appropriate to ensure the confidentiality of the information". See also, E. Dubreuil, "Quebec Bill 68: Is It Sufficient for the Federal Canadian Financial Institutions Sector?", in *Privacy in Financial Services* (Toronto: Canadian Institute, 1994).

\textsuperscript{185}Privacy Act, R.S.C. 1985, c. P-21. Of particular note are Sections 7 and 8. Section 7 provides that the government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which it was obtained or compiled; and Section 8 prohibits the disclosure of such information except under thirteen statutory exceptions, which involve mainly national security, law enforcement, statistical or public interest criteria. It must be noted, however, that there are no criminal provisions of general application, even though the R.C.M.P. is open to criminal prosecution under other areas of the *Criminal Code* for such things as unauthorised surveillance. It is interesting to note that under the act, the transborder flow of information by government is prohibited, as is the linking of various governmental databases. In addition, the *Access to Information Act* (R.S.C. 1985, c. A-1) provides a right of public access to information in records under the control of a federal government institution, subject to a number of exceptions which protect various social, economic or political interests. As with the Privacy Act, these exceptions cover mainly issues of importance to national security and law enforcement, as well as matters of commercial, financial or scientific interest. See House of Commons, Standing Committee on Justice and Solicitor-General, *Open and Shut: Enhancing the Right to Know and the Right to Privacy* (Ottawa: Supply and Services Canada, 1987).
based ostensibly on O.E.C.D. privacy guidelines\(^{186}\), which "governs the collection, retention, use and disclosure of personal information by federal government institutions"\(^{187}\). In addition, many professional and industry specific legislations exist, which govern the use of particular types of data under the control of these bodies\(^{188}\).

Unfortunately, there is a great deal of geographical and jurisdictional inconsistency in the levels of protection afforded by these enactments. Protection varies from province to province, and is different at the federal level than at the provincial level. Discrepancies also exist between the public, private, and hybrid sectors, and even vary between individual industries within these sectors\(^{189}\).

The reason for this inconsistency is the structure of the Canadian political and governmental framework. Canada is a federated state, and the federal government has jurisdiction over certain matters, and the provincial governments over others. As such, no one authority has power over all privacy and data protection legislation. For example,

\footnotesize

\(^{187}\)Piragoff, *supra* note 6 at 119-120.


\(^{189}\)See infra note 204 and the discussion on the application of voluntary codes.
The federal government has constitutional control over banking, finance, and the criminal law, and the provinces over business, property, industry, and civil rights. These inconsistencies have created many problems, and have caused a great deal of concern. As Bennett notes:

The critique of the privacy patchwork is that it has been insufficient on three fronts: first, by failing to allay the fears of the general public; second, by failing to provide suitable measures of enforceability in the private sector; and third, by not providing an adequate level of protection, it has created an unlevel playing field for the conduct of business between jurisdictions within and outside Canada.

These problems, especially the public/private inconsistencies, have led to pressure for a uniform data protection initiative. In 1996, Allan Rock, then Minister of Justice, commented that federal legislation was needed to, "provide effective, enforceable protection of privacy rights in the private sector [because] the protection of personal information can no longer depend on whether the data is held by a public or private institution".

---

190 See Williams, Wilkes and Erdle, supra note 183 at 31.
192 Ibid.
193 Takach, supra note 32 at 434-436, notes this blurring of the public and the private spheres as his third dynamic of information technology and computer law.
194 Advances in technology have also led to pressure for such an initiative. See infra notes 254, 266 and 278.
A more pressing incentive, however, may have come from the European Union (E.U.). Recent changes in European law have meant that Canada may be excluded from receiving personal information regarding E.U. citizens, unless it can ensure adequate universal legal protection for the data. To this end, extensive proposals have been put forward regarding the possible implementation and content of a new uniform data protection code and universal personal information act.

Although many different approaches were taken with varying degrees of success, it now seems likely that the model which will be used in creating this uniform data protection act will be the one developed by the Canadian Standards Association.

---


198The Privacy Commissioner, Bruce Phillips, proposed new legislation which would apply uniformly to the public and private sectors. Many individual reforms took place in light of this new philosophy, and alterations were made to many industry specific acts such as the Bank Act (S.C. 1991), Insurance Companies Act (S.C. 1991) and the Trust and Loan Companies Act (S.C. 1991) (see “Privacy and the Canadian Information Highway”, supra note 136). In the mid-1980s, the Canadian federal government wanted to encourage the private sector to adopt its own privacy and data protection codes, although in 1987 a Parliamentary Committee recommended that the Privacy Act which governs personal information held by federal governmental institutions, organisations and agencies, be extended to the federally-regulated private sector. Although extensive consultation took place with many of these industries, no consensus was reached. See Owens, Onyshko and Goode. supra note 184 at 8-13).
(C.S.A.) in the late 1980s and early 1990s. This code which is based almost entirely on the O.E.C.D. Privacy Guidelines of 1984, was finally adopted in 1996 by the C.S.A. and served as a set of principles, which individual firms could use in developing their own privacy and data protection regimes. However, allowing for the voluntary

---

199 Alternative approaches included the extension of existing public sector laws to the private sector, or an emulation of the Quebec legislation. See also Government of Canada (Department of Justice), The Steps Ahead (Ottawa: Department of Justice, 1987).


201 The “C.S.A. Guidelines” (ibid) include the following principles: “(1) Accountability: An organisation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organisation’s compliance with the following principles; (2) Identifying Purposes: The purposes for which information is collected shall be identified by the organisation at or before the time the information is collected; (3) Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate; (4) Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means; (5) Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the purposes; (6) Accuracy: Personal information shall be as accurate, complete and up-to-date as necessary for the purposes for which it is used; (7) Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information; (8) Openness: An organisation shall make readily available to individuals specific information about its policies and practices relating to the management of information; (9) Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate, and; (10) Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organisation’s compliance”.


203 Principle (7) of the “C.S.A. Guidelines” (supra note 200), “Safeguards” (see supra note 201), is of particular importance. It is adapted from the “Security Safeguards Principle” of the O.E.C.D. Guidelines (ibid), which state that, “Personal data should be protected by reasonable security safeguards against
introduction of these codes has proven a failure\textsuperscript{204}, and it is now thought that their introduction should be legally enforced\textsuperscript{205}.

(b) Breach of Confidence

Breach of Confidence\textsuperscript{206} is a vast and complex body of law, and one which there is little time to discuss in depth here. However, just as data protection legislation focuses on the protection of privacy and personal information on a wide-scale, breach of confidence focuses on the protection of private information on an individual level. The basic premise of the doctrine is that information which is imparted in confidence must not be disclosed\textsuperscript{207}, and hence protects any information which is imparted to others in both personal and professional situations.

\begin{itemize}
\item \textit{such risks as loss or unauthorised access, destruction, use, modification or disclosure of data"}. Practical security measures will be discussed in the \textit{Theoretical and Practical Protections} section, \textit{Chapter 4}.
\item \textsuperscript{204}In his 1994-5 Annual Report (\textit{supra} note 150, 1994-95), Bruce Phillips, Privacy Commissioner at that time, noted that legal regulation and enforcement was needed to force these industries to inculcate privacy and data protection principles into their business practices, due to the failure of the voluntary scheme. See also the 1993 report of the Canadian Direct Marketing Association (Direct Marketing Association, \textit{Annual Report 1993} (Toronto: Direct Marketing Association, 1993). The failure of the voluntary schemes is somewhat surprising given the strong economic incentive to provide security and privacy in the information age. The popularity of these privacy measures with consumers has been observed in the telecommunications, credit, financial and direct-marketing sectors. See C.J. Bennett and J.M. Young, "Toward Effective and Enforceable Privacy Protection: Policy Solutions for the Canadian Information Market", 13(2) \textit{C.I.P.R.} 243, at 245, and \textit{supra} notes 188 and 189.
\item \textsuperscript{205}See \textit{ibid.}, and Alter, \textit{supra} note 121 at 13-16.
\item \textsuperscript{206}Breach of confidence became the dominate vehicle for protecting confidential information in \textit{Saltman Engineering Co. v. Campbell Engineering Co.} (U.K.) (1948), 65 R.P.C. 203 (H.C.J. & C.A.) (Hereinafter referred to as \textit{Saltman}).
\end{itemize}
However, in order for a breach of confidence to be established, certain criteria must be met. *L.A.C. Minerals v. International Corona Resources Ltd.* Canada’s leading authority on trade secret law, explained the test for breach of confidence as consisting of three elements: “*that the information conveyed [must be] confidential, that it [is] communicated in confidence, and that it [is] misused by the party to whom it was communicated*”.

Ascertaining the existence of these three elements is imperative if a claim of breach of confidence is to succeed, and the most difficult component to establish, especially in relation to privacy and private information, is the confidential status of the information. The doctrine only protects information if it is confidential in nature. As

---

209*L.A.C. Minerals* (ibid.), at 20. In *Coco v. A.N. Clark (Engineers) Ltd.* (U.K.) [1969] R.P.C. 41 (Ch.) (Hereinafter referred to as *Coco*), Megarry J. (as he then was) at 47, stated, "In my judgement, three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information itself, in the words of Lord Greene, M.R. in the Saltman case on page 215, must ‘have the necessary quality, of confidence about it’. Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Third, there must be an unauthorised use of that information to the detriment of the party communicating it’.
210Cross, *supra* note 21 at 529-530, states, "The dispute over the proprietary nature of confidential information can be traced to the middle of the eighteenth century, when the law of confidential information was emerging in its modern form. Many of the very early trade secret cases dealt with confidential information as a form of property right (Dean v. McDowell [(U.K.)] (1878), 8 Ch.D. 345 at 354 and Peabody v. Norfolk [(U.S.)] 98 Mass. 452 (1868)). However, it was not until 1917 that the issue was clearly addressed by Justice Holmes speaking for the majority in *E.I. Du Pont de Nemours Powder Co. v. Masland*, [(U.S.)] 244 U.S. 100 (1917)). Instead of using property analysis, Holmes reasoned that the law of trade secrets was primarily concerned with the conduct of the defendant in acquiring the information from the plaintiff. The key question that courts must face in trade secret cases is whether the defendant violated a duty of ‘fair dealing’. Under Holmes’ view, commercial morality, not property, formed the basis for liability (Notions of Commercial Morality were also pointed to in *International News Service v. Associated Press*, [(U.S.)] 248 U.S. 215 (1918))”. See *infra* notes 211 to 216.
Lord Greene noted in the case of *Saltman Engineering Co. v. Campbell Engineering Co.*[^211], "the disclosure of information will only be restrained if it has the necessary quality of confidence about it"[^212].

It is indeed questionable whether private and personal information will be regarded as confidential. In order to be accorded confidential status, information must not be trivial in nature[^213], and it seems likely that information solely affecting an individual's emotional or psychological state will be regarded as such. Lord Greene stated that what makes information confidential, "is the fact that the maker of the document has used his brain and thus produced a result which can only be produced by someone who goes through the same process"[^214]. Intimate details and memories require

[^211]: Supra note 206.
[^212]: See *Saltman* (supra note 206) and *Thomas Marshall v. Guinle* (U.K.) [1979] Ch. 227.
[^213]: *Facenda Chicken Ltd. v. Fowler* (U.K.) [1987] Ch. 117 and *Stephens v. Avery* (U.K.) [1988] 2 W.L.R. 1280. The information must also not be public property or public knowledge. See also the cases of *Mustad v. Dosen* (U.K.) [1963] R.P.C. 41; *Stevenson Jordan & Harrison Ltd. v. MacDonald & Evans* (U.K.) (1952) 69 R.P.C. 10; *Peter Pan Manufacturing Corporation v. Corsets Silhouette Ltd.* (U.K.) [1964] 1 W.L.R. 96; *Franchi v. Franchi* (U.K.) [1967] R.P.C. 149; and *Lennon v. News Group Newspapers Ltd.* (U.K.) [1978] F.S.R. 573. As Clerk and Lindsell, supra note 207 at 1652, go on to say, "that does not mean that all matters which the public could find out about if they made the effort, or did the necessary work, will be regarded as being in the public domain and therefore not capable of being protected". As noted in *Coco* (supra note 209), "Novelty depends on the thing itself, and not upon the quality of its constituent parts".
[^214]: *Saltman*, supra note 206 at 415. It is important to understand the rest of the passage (per Lord Greene), "I think that I shall not be stating the principle wrongly if I say this with regard to the use of confidential information. The information, to be confidential, must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge. On the other hand, it is perfectly possible to have a confidential document, be it a formula, a plan, a sketch, or something of that kind, which is the result of work done by the maker on materials which may be available for the use of anybody; but what makes it confidential is the fact that the maker of the document has used his brain and thus produced a result which can only be produced by somebody who goes through the same process". See also, *Terrapin v. Builders Supply Co. (Hayes) Ltd.* (U.K.) [1960] R.P.C. 128; and *Cranleigh Precision Engineering v. Bryant* (U.K.) [1965] 1 W.L.R. 1293.
absolutely no mental effort to produce as they already exist in their final form\textsuperscript{215}, and as such, it is unlikely that breach of confidence would protect private information of this nature\textsuperscript{216}.

However, obligations of confidence arise in many situations\textsuperscript{217}, for example, through commercial and professional relationships\textsuperscript{218}, employer and employee interactions\textsuperscript{219}, and over discussions regarding personal matters\textsuperscript{220}; and, as alluded to

\begin{footnotesize}
\textsuperscript{215}This is not always the case. It can take a great deal of mental thought and exertion to work through and understand many personal problems and dilemmas; although it is difficult to quantify the end result as a product.

\textsuperscript{216}However, such information would be protected if it was under the control of a commercial enterprise. See infra notes 227 and 228.

\textsuperscript{217}Obligations may arise expressly through contract, usually in the form of an express term, as in Peter Pan Manufacturing Corporation v. Corsets Silhouette Ltd. (U.K.) [1964] 1 W.L.R. 96, although the court may imply a term of confidentiality, but only where this is called for in the context of the relationship existing between the parties, as in Saltman (supra note 206) and Coco (supra note 209). Obligations can also arise through statutory provisions. As Clerk and Lindsell, supra note 207 at 1651, state, “many statutes and orders prohibit the communication of state or private secrets and may be widely drawn or directed to specific kinds of information. Most provide for criminal sanctions but some also found civil causes of action. Of the former, the principal statute is the Official Secrets Act 1989. Others include: the Atomic Energy Act 1946, ss.11,14; ... the Abortion Act 1967, s.2(1)(c); ... the Consumer Credit Act 1974, s.174, Sched.1; ... the Contempt of Court Act 1981, ss.8,10,11; ... the Data Protection Act 1984, ss.15,16,19. ... The latter include: the Data Protection Act 1994, s.22; the Copyright, Design and Patents Act 1988, s.85; and the Legal Aid Act 1988, s.34. Statutes may also oblige holders of information to make it available to those concerned. These include the Consumer Credit Act 1974, ss.137,138,139, Sched.1; the Contempt of Court Act 1981, s10; the Data Protection Act 1984, ss.21,22,25; and the Criminal Justice Act 1988, s.98”.

\textsuperscript{218}This is indeed where most cases of breach of confidence arise. In cases where agreements have been entered into to exploit a certain industrial process or invention, or apparatus, specifications and drawings, confidentiality has been inferred. See James Industries Ltd. 's Patent (U.K.) [1987] R.P.C. 235, Prince Albert v. Strange (U.K.) (1869) 2 De G. & Sm. 652. With regards to the professions, Clerk and Lindsell, supra note 207 at 1650-1651, state, “In the course of seeking advice or the provision of services, it is usual and indeed inevitable that confidential matters should be disclosed, and those to whom they are disclosed will be restrained from divulging and making use of them. This applies, for instance, to lawyers [infra note 222], bankers [infra note 223], doctors [infra note 221], clergymen [infra note 224], anthropologists and even photographers”.

\textsuperscript{219}This is an extremely complex area of breach of confidence, and generally it is held that an employee owes a duty of fidelity to his employer (Normalec Ltd. v. Britton (U.K.) [1983] F.S.R. 318). This may be expressed directly in a contract of employment (Reid and Sigrist Ltd. v. Moss and Mechanism Ltd. (U.K.) (1932) 49 R.P.C. 461), but may also be inferred by the courts (Tipping v. Clarke (U.K.) 2 Hare 383).
\end{footnotesize}
above, information which is divulged in confidence to doctors\textsuperscript{221}, lawyers\textsuperscript{222}, bankers\textsuperscript{223}, clergymen\textsuperscript{224}, and family and friends\textsuperscript{225} to name but a few\textsuperscript{226}, will all be protected by the doctrine of breach of confidence.

In addition, similar to the fraud provision discussed above\textsuperscript{227}, breach of confidence will also protect any information which is disclosed to a commercial enterprise, providing the further unauthorised disclose of the information will harm the organisation or its revenue flow\textsuperscript{228}.

\textsuperscript{220}It seems that the courts will restrain the disclosure of information imparted in confidence between spouses (Argyll v. Argyll (U.K.) [1967] Ch. 302), and between those engaged in sexual relationships (Stephens v. Avery, supra note 213).


\textsuperscript{222}Tournier v. National Provincial (U.K.) [1924] 1 K.B. 461.


\textsuperscript{224}Broad v. Pitt (U.K.) (1828) 3 C. & P. 518.

\textsuperscript{225}See Stephens v. Avery, supra note 213, and Argyll v. Argyll, supra note 220.

\textsuperscript{226}Other examples include anthropologists (Foster v. Mountford and Rigby (U.K.) [1978] F.S.R. 582) and photographers (Pollard v. Photographic Co. (U.K.) (1888) 40 Ch. D. 345).

\textsuperscript{227}See Fraud section, above.

\textsuperscript{228}See Ansell Rubber Co. Pty Ltd. v. Allied Rubber Industries Pty Ltd. (U.K.) [1967] V.R. 37 and Deta Nominees Pty Ltd. v. Viscount Plastics Products Pty Ltd. (U.K.) [1979] V.R. 167. Deta Nominees, at 193, lists six components for identifying confidential information, and although the criteria are not to be regarded as complete, they all relate to business information and its acquisition by competitors. The six components used to ascertain the confidential nature of information are: "(1) the extent to which the information is known outside the owner's business; (2) the extent to which it is known by employees and others involved in the owner's business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and his competitors; (5) the amount of money or effort expended by him in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others [i.e. by their independent endeavours]".
In the government and corporate spheres, additional protection for confidential information also exists in the form of the *Official Secrets Act*\(^{229}\) and trade secrets doctrine\(^{230}\), respectively. The former protects state secrets by prohibiting the unauthorised disclosure of sensitive government information, and the latter by protecting against the disclosure of commercial or industrial information which is imparted to others in confidence in the course of business\(^{231}\).

Returning to breach of confidence however, it is clear that the doctrine is extremely useful in protecting private information. Although it should be noted at this


\(^{230}\)This is also an extremely complex area of law. It can be regarded as a sub-set of confidential information, and contains components of breach of fiduciary duty, and includes the application of industry standards and practices. See *L.A.C. Minerals*, *supra* note 95 at 20-39. See also *Faccenda Chicken v. Fowler*, *supra* note 213.

\(^{231}\)The *Uniform Trade Secrets Act* was originally adopted in the United States in 1979, and amended in 1985. It has been implemented in various forms in most of the states in the U.S., and it defines a trade secret in s.1(4) as, "Information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) derives independent economic value, actual or potential from not being generally known to and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy". In 1986, The Institute of Law Research and Reform (ILRR) proposed two new separate offences for trade secrets. "The first, which focuses upon the misappropriation of a trade secret, would be analogous to existing theft offences. It would allow prosecution of anyone who 'fraudulently and without colour of right acquires, discloses or uses the trade secret of another person' with the intent to deprive that other person of either control of the trade secret, or of an 'economic advantage associated with the trade secret'.... Reverse engineering would be explicitly included as a defence.... The second offence would cover a situation where a defendant fraudulently induces an owner to disclose a trade secret. The proposal also includes a lesser offence under each of the above provisions in cases where the defendant did not know, but should have known, that the information was a trade secret" (Cross, *supra* note 21 at 573. See Institute of Law Research and Reform, *Trade Secrets, Report No.46* (Edmonton: ILRR, 1986). The criteria adopted by the *Restatement of Torts* (1939) (U.S.), for determining whether a trade secret exists are: "(1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken to guard the secrecy of the information; (4) the value of the information to the business and to competitors; (5) the amount of effort or money expended in developing the information, and; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others. *Restatement of Torts, 757, comment b (1939)*" (From Peterson, *supra* note 54 at 21-22).
stage, that limited protection is provided under breach of confidence for information which is surreptitiously or reprehensibly acquired, and in such a case the measures suggested in the previous section should be employed\(^\text{232}\).

\((c)\) Public Disclosure of Private Information

As the subtitle suggests, this principle prohibits the public disclosure of private information, and can be separated into two independent doctrines; the public disclosure of confidential information, and the public disclosure of personal information. The first is an extension of breach of confidence, the second a "privacy tort".

The public disclosure of confidential information has, in effect, been discussed above in relation to breach of confidence\(^\text{233}\), but concentrates on prohibiting the public release and wide-spread dissemination of information\(^\text{234}\), rather than the unauthorised

\(^{232}\)In 1981, The English Law Commission (Report on Breach of Confidence (U.K.) Cmdn. 8388. 1981, No.110) noted that the improper gain of information is not protected under breach of confidence. However, in \textit{I.T.C. Film Distributors v. Video Exchange Ltd.} (U.K.) [1982] Ch. 431, examining the case of \textit{Lord Ashburton v. Pape} (U.K.) [1913] 2 Ch. 431, it was held that information reprehensibly obtained may be subject to a duty of confidence. In this light, information obtained through computer misuse may be protected by breach of confidence, although the English Law Commission has recommended that this approach not be taken (para. 3.1). See \textit{Malone v. Metropolitan Police Commissioner} (supra note 141) and \textit{Saccomone v. Orr} (1981) 34 O.R. (2d) 317 (Ont.Co.Ct.).

\(^{233}\)This is in effect the publication of confidential information, and covers information which is both personal and confidential in nature. See \textit{Breach of Confidence} section, above. See also the cases of \textit{Argyll v. Argyll} (supra note 220); \textit{X. v. Y.} (U.K.) [1988] 2 All E.R. 648; \textit{Stephens v. Avery} (supra note 213); and \textit{Fraser v. Evans} (U.K.) [1969] 1 All E.R. 8 (C.A.).

\(^{234}\)This is primarily through the media, such as television, radio and newspaper. It is also feasible that dissemination over the Internet could be regarded as public disclosure. See Takach, supra note 32 at 170-173, and Davis and Hutchinson, supra note 55 at 184-190.
disclosure to private individuals and organisations; although it should be remembered that the unauthorised dissemination of information to even one individual is an infringement of privacy\textsuperscript{235}.

The public disclosure of personal information prohibits the disclosure of private details about an individual, and exists to prevent their subjection to unwanted or unauthorised publicity\textsuperscript{236}. In applying this doctrine it should be noted that certain criteria must be met in order for information to be regarded as private and hence unfair for publication\textsuperscript{237}. It should also be noted that there is a delicate balance between privacy and freedom of the press\textsuperscript{238}.

In this light, although confidential and personal information does gain some protection through the public disclosure prohibition, it is unlikely to be of relevance to the vast majority of people. Indeed, the only individuals who are likely to benefit from this protection in practice, are celebrities, politicians and other persons in the public eye.

\textsuperscript{235}In \textit{Fraser v. Evans} (supra note 233) it was noted that, "...the court will, in a proper case, restrain the publication of confidential information. The jurisdiction is based, not so much on property or contract, but rather on the duty to be of good faith. No person is permitted to divulge to the world information which he has received in confidence, unless he has just cause or excuse for doing so. Even if he comes by it innocently, nevertheless, once he gets to know that it was originally given in confidence, he can be restrained from breaking that confidence". However, this right is not actionable if the parties seek publicity, see \textit{Woodward v. Hutchins} (U.K.) [1977] 1 W.L.R. 760 (C.A.); \textit{Lennon v. News Group Newspapers Ltd.} (supra note 213); \textit{Robbins v. Canadian Broadcasting Corporation} (1957), 12 D.L.R. (2d) 35 (Que. S.C.); and \textit{Saccone v. Orr} (supra note 232).\textsuperscript{236}

\textsuperscript{237}For example, the Australian Law Reform Commission, in attempting to define the scope of legal protection, has created a category of sensitive private facts, which includes matters of health, private behaviour, home life, or personal or family relationships. See Australian Law Reform Commission, \textit{Unfair Publication: Defamation and Privacy} (Aus.) (Report No.11), 1979, Clause 19(1) and (2). \textit{Ibid.}, at 167.
Although, confidential information of great financial or public importance could gain some protection under this doctrine\textsuperscript{239}.

\textsuperscript{238}\textit{Ibid.}, at 155 and 171-175.

\textsuperscript{239}It is important to note that there is a public interest exception to the public disclosure of confidential and personal information. \textit{Ibid.}, at 167-175.
CHAPTER 3

PRIVATE INFORMATION AND PRIVACY IN THE COMPUTER AGE

A. THE COMPUTER AGE

Computer technology has had a dramatic impact on information. Monumental advances in computing, telecommunications, and networking have greatly increased the scale on which information can be obtained. The acquisition, analysis, and storage of vast amounts of data is now simple in execution and negligible in cost. Information can be acquired surreptitiously and automatically in contexts and capacities never

240 By this term I not only mean the advent of the computer, but also the use of sophisticated computing and telecommunication networks, as well as the existence of other electronic devices which aid the acquisition, transmission, collation, analysis, storage and retrieval of information.

241 Before the computer, surreptitiously acquiring vast amounts of information about an individual and compiling a profile of that person would have taken an extremely long time, and required a great deal of energy and resources. The computer has infinitely facilitated information gathering. See Tapscott, supra note 16 at 271, Westin, supra note 83 at 365, and the pervasive example of Jeremy Smith in A. Cavoukian and D. Tapscott, Who Knows: Safeguarding Your Privacy in a Networked World (Toronto: Random House of Canada, 1995).


243 Ibid., and supra note 241.
conceivable before the advent of the computer. In addition, the interconnectivity of these networks means that data can be instantly disseminated to great numbers of commercial organisations and government agencies. In short, this technological revolution has the capacity to annihilate privacy and destroy any possibility of maintaining information exclusivity\footnote{See supra notes 125 and 126.}.

It has been noted in previous chapters that privacy and exclusivity are inextricably linked, and that their protection is dependent upon controlling the acquisition, use, accuracy, and dissemination of information; and, as we will discuss below, computer technology poses serious threats to this control. The discussion will be divided into two distinct, but intertwined groups: first, privacy, and then private information.

**B. PRIVACY CONCERNS IN THE COMPUTER AGE**

In Chapter 1, the interconnected nature of privacy and private information was discussed, and although the focus of this thesis is on the acquisition and dissemination of the latter, a further discussion of privacy issues is necessary. This is not only because privacy is a key component of private information, and not only because it serves as a useful example which may be of general application, but also because it highlights a crucial facet of private information protection which would otherwise go un-mentioned.
In this regard, the computer age has not only made traditional privacy problems worse, but it has also created new ones. These will be addressed in turn.

(a) Traditional Privacy Problems Exacerbated

In chapter two, the threats to privacy posed by the collection and sharing of personal information were outlined, and computer technology has not altered these fundamental problems. However, it has heightened privacy concerns due to the broader scale and greater ease with which information can be obtained and compiled, and hence the greater speed and efficiency with which privacy can be infringed.

Indeed, public concern over privacy and data protection is extremely high. Many citizens of various countries of the world are clearly concerned by computer technology and the threats it poses. A 1970's survey carried out in the United Kingdom, which gauged responses to examples of invasions of privacy, found the use of a "central computer" to be of the greatest concern, with 87% viewing it as an invasion of privacy,

---

245 See the Prevention Against Unauthorised Disclosure and Data Protection sections, Chapter 2.
246 Such questions as, "Should there be a right to privacy?", and, "Should information be regarded as property?". See Concluding Thoughts section, Conclusion, supra notes 152, infra notes 273-281, 569-573 and 698-703.
71% being very annoyed by it, and 85% believing that it should be prohibited by law\textsuperscript{249}. A more recent Canadian survey, conducted in 1992\textsuperscript{250}, found that privacy was of moderate or greater concern\textsuperscript{251}, with 81% of respondents feeling that computers were reducing the level of privacy in Canada\textsuperscript{252}. A separate survey, conducted in 1995, found that the collection and use of personal information was high and that individuals felt they had less control over personal information than they did 10 years ago\textsuperscript{253}.

Such concerns are partly triggered by paranoia of an impending Orwellian “1984”\textsuperscript{254} situation, with government-controlled super-computers logging our every thought, movement, and activity. However, these delusions may not be as paranoid as they first appear. A serious threat to individual autonomy is indeed posed by the computer age. Although, in reality, the threat is more likely to come from industry and commerce than it is from government.

\textsuperscript{249}Wacks, supra note 1 at 137.
\textsuperscript{251}Ibid., at i. “Greater concern” refers to concern which is recorded as greater than moderate on the scale of concern used in the survey. A score of 5 was regarded as moderate, and anything above 5 on the scale would be regarded as being of “greater concern”.
\textsuperscript{252}In ranking five aspects of privacy, “controlling who gets information”, and “controlling what information is collected” ranked second and third, respectively. Supra note 249.
\textsuperscript{254}George Orwell’s novel “Nineteen Eighty-Four”, outlines a fascist police state, where the authorities create and control all knowledge and know the every thought and movement of each citizen. However, as Hammond notes in “The Misappropriation of Commercial Information in the Computer Age”. supra note 25 at 347, “The computer age turns on its ability to ingest and use vast amounts of information. That information is both commercially valuable and gives rise to enormous power in the hands of the possessors.
These increased concerns may be divided into two categories, which are by now quite familiar; namely, acquisition and dissemination²⁵⁵.

(i) Acquisition

In this technological era, computers and other electronic information acquiring and disseminating devices are present in almost every aspect of interaction in society²⁵⁶. The magnetic strips and encoded chips²⁵⁷ which carry our personal details are "swiped"²⁵⁸ with almost every transaction²⁵⁹, and the immense ability and capacity of computers to store information, means that incredible amounts of seemingly insignificant and mundane information can be stored, processed and collated²⁶⁰. In so doing, extremely detailed and accurate profiles about an individual's lifestyle, needs, and consumer demands can be created²⁶¹.

²⁵⁵This division was used in Chapter 2.
²⁵⁷Tapscott, supra note 16 at 275.
²⁵⁸meaning that the card is passed through a scanning device which acquires information from the card as it is passed through. Interestingly the term "swipe" also refers to theft, and, in this context, information could quite literally be swiped in both senses of the word.
²⁵⁹"Privacy and the Canadian Information Highway", supra note 136 at 5.
²⁶⁰See examples in the Prevention Against Unauthorised Disclosure section, Chapter 2.
²⁶¹D. Chaum, "Achieving Electronic Privacy", Scientific American, 1992, 96. See also "Privacy and the Canadian Information Highway", supra note 136 at 6, and Tapscott, supra 16 at 274-5.
Computer technology is also threatening privacy more than ever before, because information can now be acquired surreptitiously. The obtaining of personal information without consent, and worse, without knowledge, means that no control over the dissemination, accuracy or use of information can be exerted, and as such privacy cannot be said to exist in any meaningful way.

It is important to note, that the problem is not so much that our information is being "stolen"\(^{262}\), but rather that its transfer occurs in so many individual situations that it is impossible to keep track of whom it has been transferred to, and for what purposes it was transferred. Interestingly, following this line of argument, it has been suggested that privacy does still exist, and that we are voluntarily forsaking it for the convenience of contracting in today's society\(^{263}\). As stated in a recent Industry Canada report, "Most people may be aware that a credit card company could be selling their transactional data to vendors of products, but they might consider this a reasonable cost of doing business with a huge and reliable credit company, and one outweighed by the benefits"\(^{264}\).

\(^{262}\)It should be borne in mind, that technically speaking, information cannot be stolen, as it cannot be the subject of theft under the criminal law. See \textit{R. v. Stewart} (\textit{supra} note 157) and \textit{supra} note 163.

\(^{263}\)There is indeed an important balance which must be maintained between social and commercial need. See "Privacy and the Canadian Information Highway", \textit{supra} note 136.

\(^{264}\)\textit{Ibid.}, 5-6. See also Tapscott, \textit{supra} note 16 at 273-5.
However, no real choice\textsuperscript{265} can exist if individuals have no option but to forsake their privacy in order to survive\textsuperscript{266}. This is especially the case when it is considered that the computer age has extended these information acquisition and dissemination technologies to every firm and company, without regard to size or reputation. This means not only that our major credit card transactions are recorded, but also that every single commercial interaction can be catalogued and processed to aid in the creation of our personal profiles\textsuperscript{267}.

(ii) Dissemination

In addition to these acquisition fears, increased dissemination problems also arise in the computer age. Advanced network technology means that once your personal information has been acquired, it can easily be transmitted and disseminated to other

\textsuperscript{265}This situation is similar to the criminal law, where no criminal culpability is deemed to exist if an individual is forced to act under duress. See A. Norrie, Crime, Reason and History (London: Weidenfeld and Nicolson, 1993), at 163-168.

\textsuperscript{266}At first this may seem a little strong. However, if individuals are unable to buy anything without first losing privacy, they must succumb to these commercial pressures if they are to interact in society and successfully function in today’s economy. Indeed, Bruce Phillips, the Privacy Commissioner in 1994-5 (see supra note 204), noted that increased privacy protection was required at this time due to, “the growth of the personal information industry, the rapid pace of technological change and the threat to public sector privacy protection imposed by the increasing interconnectivity between public and private sector data bases and transmission systems” (see Annual Report, 1994-5 supra note 150). See also Bennett and Young, supra note 204 at 248-249.

\textsuperscript{267}Branscomb, supra note 22 at 15-27, notes the importance of information in the marketplace, and the crucial distinction between “opting in” and “opting out” in this information age. Monitoring technology is becoming extremely advanced, as R. Crawford, “Techno Prisoners”, Adbusters Quarterly (Summer 1994), at 21-22, notes in his example of Realtime Residential Power Line Surveillance (RRPLS).
organisations and matched with additional data\textsuperscript{268}. This allows for the development of
even more accurate profiles, and hence even more swift and serious infringements of
privacy\textsuperscript{269}.

The unregulateable dissemination of information is achieved through the
computer's new role as a communications device as well as an information processing
unit\textsuperscript{270}. In this way, data can be inputted, analysed, transmitted, linked, and matched
simultaneously. As it becomes more difficult to separate these functions, it will become
more difficult to distinguish acquisition from dissemination, and hence controlling
information will become even more problematic\textsuperscript{271}. Following this logic, once
information enters "cyberspace" all control over its dissemination will be lost, and in this
light privacy will be impossible to protect in the computer age\textsuperscript{272}. Indeed, it seems
inevitable that privacy must be sacrificed for the efficiency of transacting in today's

\textsuperscript{268}This section will be kept brief, as many of these issues have already been discussed in the \textit{Data Protection} section, \textit{Chapter 2}.
\textsuperscript{269}This is because more people will possess your private information, and because more accurate profiles
highlight can be composed, which infringe personal autonomy to a greater extent.
\textsuperscript{270}In the U.S., the Privacy Working Group of the National Information Infrastructure (NII) has developed
a number of principles to protect information in the information age, and have geared their provisions
specifically to computer technology. The basic principles afford individuals a reasonable expectation of
information privacy, and state that information on the NII has integrity, and that it must be secured through
the use of whatever means are appropriate. However, the proposals have been heavily criticised for
placing too much onus upon the individual (R. Weeder (chair), "Draft Principles for Providing and Using
Personal Information", April 21, 1994, produced by the \textit{Information Infrastructure Task Force's Privacy
Working Group}). See also the European Data Protection Initiative, \textit{supra} notes 196-197.
\textsuperscript{271}See \textit{infra} notes 329-331.
\textsuperscript{272}This is the case even if the individual's view of privacy is not to protect their private information. As
discussed in \textit{Privacy as Control over the Dissemination of Information} section, \textit{Chapter 1}, privacy is
related to control over the dissemination of information, and if information is acquired without consent
then privacy is infringed. However, it is also infringed even if the individual would wish to disclose their
private information, because they have had no choice in disclosing it if it has already been taken.
Many suggestions of how to deal with these additional concerns have been put forward, including voluntarism, government assisted and coerced voluntarism, self-regulation, added-on privacy regulation by existing privacy regulators, cyber-regulation, standards enforcement, and the re-modelling and re-application of data protection legislation\(^{274}\). Other ideas involve "shaming" or propagating adverse publicity for all those who do not uphold privacy ideals\(^{275}\), and perpetuating an ideology that "privacy is good for business"\(^{276}\).

Privacy doctrine and data protection legislation\(^{277}\) was discussed in some depth in the previous chapter, and the creation of a uniform data protection act would indeed offer a partial solution\(^{278}\). However, it seems that nothing less than international data economy\(^{273}\).

---

\(^{273}\)"Privacy and the Canadian Information Highway", supra note 136 at 6, and Lawson, supra note 247.

\(^{274}\)Lawson, supra note 247, c.10.

\(^{275}\)Ibid., c.9.

\(^{276}\)It is beneficial in very real terms, but also as a "sales gimmick". See Tapscott, supra note 16 at 278-279 and 282-283, H. Jeff Smith, Managing Privacy: Information Technology and Corporate America (Chapel Hill: University of North Carolina Press. 1994), at 55, and Bennett and Young, supra note 204 at 245.

\(^{277}\)See the Surveillance and General Privacy Protections and Data Protection sections, Chapter 2.

\(^{278}\)It is interesting to note that one of the greatest pressures for a uniform protection act is the onslaught of computer technology, and the difficulties which this is causing in separating the public and private spheres. See Lawson, supra note 247, c.11; Information Canada, Privacy and Computers (Ottawa: Information Canada, 1972); and "Virtual Privacy", The Economist, February 10, 1996, 16-17. See also, NetAction, <http://www.netaction.org>; Center for Democracy and Technology, <http://www.cdt.org>; Computer Professionals for Social Responsibility, <http://www.cpsr.org>; Electronic Frontier Foundation, <http://www.eff.org>; RAND, <http://www.rand.org>; and supra notes 266, 267 and 276.
protection legislation\textsuperscript{279}, combined with increased power invested in the individual\textsuperscript{280} will be necessary to protect traditional privacy and personal information problems in the 21st century\textsuperscript{281}.

\textbf{(b) New Privacy Concerns}

In addition to the traditional privacy concerns, many new dilemmas have arisen in relation to computer technology. The automation of many operations has meant that computer identification and authentication is necessary\textsuperscript{282}, and this requires the transmission of large amounts of important personal data\textsuperscript{283}, such as your name, address, and credit card number. With regards to cellular telephony, even the location of the individual can be ascertained. This is because encoded chips relay the location of the phone to the nearest beacon, so that the service provider can connect the call and bill the

\textsuperscript{279}Unfortunately, Canada has not even been able to introduce uniform national protection, and it is therefore unlikely that successful international legislation will be implemented any time soon. See \textit{ibid.}, and supra notes 189, 197-204.

\textsuperscript{280}Indeed, Lawson, \textit{supra} note 247, c.4, has suggested that if the individual had more power over his or her information that the massive privacy regulatory structure may not be necessary. He used the examples of air travel and smoking. The first has a great deal of regulation as their is little knowledge, difference or choice, and the latter has relatively little regulation because their is more freedom to decide. Tapscott, \textit{supra} note 16 at 282, also notes the advantages of greater rights in information. He states that, "\textit{All personal information, from your weight to your social security number belongs to you}". Cavoukian and Tapscott, \textit{supra} note 241 at 90, state that, "\textit{If people stop giving away their information and started thinking about it as they do other forms of property, expecting to have some control over it, and get paid for its use, then things would begin to change}". See supra note 152 and infra notes 568-573 and 698-703.

\textsuperscript{281}Indeed, in the computer age, theoretical protections will prove the most effective methods of controlling personal information, especially once it has been disseminated. These issues will be discussed in \textit{Chapter 4}.

\textsuperscript{282}Tapscott, \textit{supra} note 16 at 275 and "Privacy and the Canadian Information Highway", \textit{supra} note 136 at 6-7.
More general concerns have arisen through the widespread use of the Internet. This “network of networks” has converted the computer into a communications, entertainment, research, and shopping system\textsuperscript{285}, and the new browsing and business activities which are conducted over the “Net” create new sources of information which can be collected, analysed, and compiled. The ramifications of this are not to be taken lightly. The infringements of privacy, and in some cases the threats to personal safety and tangible property, are very real\textsuperscript{286}. As John Davis\textsuperscript{287} noted regarding hotel booking information:

If I can break into the network security, think about the information you provide when you book a hotel room on the Net. I've got your name, address, city, state, ZIP, phone number and credit card number. I know where you're going; where you're staying; when you'll be there; how much you're going to pay, and a rough idea of your income because of your choice of hotel. I've got enough information to apply for a credit card [in your name]. I know whether you're going to be staying alone or not. I even know what day to back my van up your driveway and start unloading your possessions. I'm in business big time!\textsuperscript{288}

\textsuperscript{283}Ibid. See also Coyle, supra note 265 at 149.
\textsuperscript{284}Of course, the location can only be roughly approximated, the precise location of an individual cannot be ascertained.
\textsuperscript{286}Tapscott, supra note 16 at 272.
\textsuperscript{287}A hotel industry executive, ibid.
Technology exists which can trace your “mouse-path”, and on the Internet this means that individuals, organisations, and government agencies can obtain information about exactly which web-sites you visit, when and how often. In this way, detailed profiles can be created not only of an individual’s interests and activities, but also of their physical movements. Each computer possesses its own identifier, similar to a telephone number, which can link the user to the computer and the computer to a location, and by cataloguing the individual’s on-line computer use, the location of the individual can be ascertained.

In addition, the information obtained and the profiles created are frequently used

---

288*ibid.*


290 Also referred to as “mouse-droppings”, these are the clicks and movements of the mouse (the dominant interface with the Internet), which can be recorded by a computer program. Such a list of actions reveals to a data-analyst exactly which Internet sites were visited. See *ibid.*, and Coyle, *supra* note 256 at 149.

291 Coyle, *supra* note 256 at 149. This is useful for governments in ascertaining political affiliation, and for marketers in gathering sales information. See also, “We Know You’re Reading This”, The Economist, February 10, 1996, 27-28.


293 *ibid.* This is not always the case, because many users can use one account. However, the terminal’s location and the fact that someone is using it can be ascertained through the “IP” address. This is similar to a speed camera taking a picture of a car registration plate, or someone using a telephone line. The use of the car or phone can be confirmed, but the identity of the driver or dialler cannot be determined. These difficulties are exacerbated if many terminals are in use, and can be accessed by any individual at any time, such as at a university. However, large corporations may well be able to determine individual users. See *Entry / Exit Screening and Employee Surveillance* sections, Chapter 4.

294 See “Privacy Rights Clearinghouse”, *supra* note 292 at 151-152. This is not necessarily the case, because anonymous addresses, remailers and ISP servers can be used, to conceal the identity of an originator.

295 Indeed, perhaps more important, it can be ascertained where the individual is not. If it can be determined that the individual is using a computer at work, then it means that his or her house may be
to aid direct-marketing efforts, by specifically gearing and orienting advertising campaigns to an individual’s revealed consumer demands. Privacy is infringed through endless intrusions caused by a perpetual bombardment of advertising material and commercial enticements, and alterations made to Internet search engines and browser programmes. The mail, fax, telephone, and electronic communication mediums can all be used to solicit individuals. This creates a great deal of frustration and physical inconvenience through the flooding of telephone and computer network connections, and the blocking of physical and electronic mail boxes. In light of these problems, various governments have passed legislation preventing the use of automated dialling and answering devices (ADADs), and automated dialler and recorded message players (ADRMPs).

New technology allows telecommunications privacy to be infringed in other ways. The use of “Caller ID” or “Call Display” permits the recipient of a call to know

unoccupied, and hence vulnerable for burgling. In the office-place, this technique could be used to make sure employees are working at their assigned terminals. See infra note 565.

Sending “junk” e-mails is known as “spamming”. See Alter, supra note 121 at 1-4, and Bacard, supra note 322 at 61. Indeed, such a waste of computing power could be actionable, although with the current state of technology, this is likely to be so minimal in cost that such actions would fail due to insufficient quantum (See infra notes 347-357). See also CRTC “Use of Telephone Company Facilities for the Provision of Unsolicited Telecommunications” (Telecom Decision CRTC, 94-10, Ottawa, 13 June 1994).

Principle 5 of the Telecommunications Privacy Principles (see infra note 306) limits the use of unsolicited phone-calls.

See infra notes 304, 306 and 307.

Cavoukian and Tapscott, supra note 241 at 152-3.

Branscomb, supra note 22 at 31.

This is, of course, related to traditional telephone technology. However, it is the advent of the computer which has enabled these new services to be offered, and it is important to note that this technology also has implications for e-mail and fax transmissions, and any data telecommunication.

See Alter, supra note 121 at 1.
the name and telephone number of the caller, regardless of whether the recipient answered the telephone or not. This destroys the anonymity of telephone users, as does the implementation of dial number recorder (DNR) technology which catalogues all call details, such as the number dialled and the time and duration of the conversation. Fortunately, however, many of these technologies can be safeguarded against. “Call Block” can be activated to prevent “Call Display” from logging the caller’s number, and telecom exchange computers can be programmed to “forget” the last few digits of dialled numbers.

In response to these breaches of telecommunications privacy, the federal government released a set of Telecommunications Privacy Principles designed to,

---

304 In Canada, the free availability of “Call Block” is enforced by a 1992 CRTC decision (CRTC, “Call Management Service - Blocking of Calling Number Identification” (Telecom Decision CRTC 92-7, Ottawa, 4 May 1992)). This matter is also addressed in Principle 3 of the Telecommunications Privacy Principles (see infra note 306). See also, Alter, supra note 121 at 5-6.
305 Privacy and the Canadian Information Highway”, supra note 136 at 13.
306 Communications Canada, Telecommunications Privacy Principles (Ottawa: Supply and Services Canada, 1992), at 6-8. These principles are as follows: “(1) Canadians value their privacy. Personal privacy considerations must be addressed explicitly in the provision, use and regulation of telecommunications services; (2) Canadians need to know the implications of the use of telecommunications services for their personal privacy. All providers of telecommunications services and government have a responsibility to communicate this information, in an understandable and accessible form; (3) When telecommunications services that compromise personal privacy are introduced, appropriate measures must be taken to maintain the consumers’ privacy at no extra cost unless there are compelling reasons for not doing so; (4) It is fundamental to privacy that there be limits to the collection, use and disclosure of personal information obtained by service providers and generated by telecommunications networks. Except where clearly in the public interest, or as authorised by law, such information should be collected, used and disclosed only with the express and informed consent of the persons involved; (5) Fundamental to privacy is the right to be left alone. A balance should exist between the legitimate use of unsolicited telecommunications and their potential for intrusion into personal privacy. All parties have a responsibility to establish ground rules and methods of redress so that Canadians are able to protect themselves from unwanted and intrusive telecommunications; (6) Privacy expectations may
"encourage awareness of privacy concerns within the industry and to promote a self-regulatory approach". The principles include measures which should protect the privacy and personal information of telecommunication users. However, given the vast amounts of information which can be acquired over the Internet, it seems that infringements of privacy will occur regardless of the protection afforded information relating to the caller or telecommunication connection.

C. PRIVATE INFORMATION IN THE COMPUTER AGE

The computer age not only poses threats to privacy, but also to private information in general. As defined in the introduction to this thesis, private information consists of any information which an individual, or organisation, wishes to keep secret or share only with a selected few. Private information is indeed both an

---

change over time. Methods of protecting telecommunications privacy must be reviewed from time to time to meet these changing expectations and to respond to changing technologies and services.

307 "Privacy and the Canadian Information Highway" supra note 136 at 10. These principles were designed with federal government, privacy advocates, telecommunications service providers, provincial governments and consumer groups to, "reinforce the rights of individuals to control their personal information and to be made aware of the privacy implications of new communications and information technology products and services" ("Privacy and the Canadian Information Highway", at 10). See also Communications Canada, Privacy Protection in Telecommunications - Discussion Paper and Proposed Principles (Ottawa: Department of Communications Information Services, 1992), and the New York State Public Service Commission Statement of Policy on Privacy in Telecommunications (1991).

308 ibid., and supra note 306.

309 U.S. Department of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (Washington D.C.: U.S. Department of Commerce, 1995) (Hereinafter referred to as "Privacy and the NII"). This is because every action in an "on-line" world will leave a path by which the individual can be traced (i.e., through the use of "cookie" technology, see supra notes 289-292).

310 See the Private Information section, Introduction and Private Information in the Computer Age section, below.

- 78 -
element of privacy and a concept of greater application\textsuperscript{311}. Much private information is likely to consist of personal information and other information pertinent to the maintenance of privacy. For example, telecommunication and DNR data is both personal and private information. However, private information focuses more on the content of communications and documentation, rather than on the peripheral and circumstantial data. Hence, the security of private information is concerned more with protecting the contents of a letter, than it is with protecting the identity of the recipient or sender, and is more concerned with protecting the conversation conducted between two parties than it is with the identities of those individuals\textsuperscript{312}. Of course, the contents of letters and conversations are also protected by privacy, and conversely, the identities of the parties involved in communications may also be regarded as private information\textsuperscript{313}. However, it is the focus rather than the content of protection which changes in relation to private information. In addition, it should also be noted that private information focuses on private communications, interactions, and data storage, and is not concerned with public transactions or information-browsing on the Internet.

In this light, the protection of private information is concerned primarily with prevention against acquisition, rather than dissemination. This is because the individual

\footnotesize
\textsuperscript{311}It covers government, commercial and confidential information as well as personal information, and relates not only to intimate or sensitive information which is reasonably held, following Wacks' (supra note 1 at 26) definition, but also anything which is subjectively regarded in this way.

\textsuperscript{312}Of course, storage and creation of information is also protected, communication is simply being used as an example.

\textsuperscript{313}This is, of course, assuming that the parties wish their identities to remain secret. See Privacy as Control over the Dissemination of Information section, Chapter 1.
usually only disseminates private information\textsuperscript{314} to a limited and selected number of people, who are trusted either by way of intimacy, friendship, moral rectitude or professional confidence\textsuperscript{315}. Indeed, in some ways, it is fortunate that concern over private information is focused on acquisition rather than dissemination, because, as discussed above, in this technological age there is very little chance of maintaining the exclusivity of information once it has been divulged to anonymous parties\textsuperscript{316}.

The computer age has created new mediums for the storage and transmission of private information, and this has created new opportunities for information gathering. Vast amounts of data are stored in private computer memory banks, and transmitted via electronic communication mediums, and as we will discuss below, a multitude of acquisition techniques exist through which this information can be obtained\textsuperscript{317}.

Following the categories used in chapter two, information can be acquired in three settings: during creation, transmission, or storage. During its creation, information can be acquired through advanced electronic surveillance, where the computer visual display

\textsuperscript{314}Which as we have discussed, involves far more than simple personal details.

\textsuperscript{315}See \textit{Breach of Confidence} section, Chapter 2.

\textsuperscript{316}See \textit{Privacy Concerns in the Computer Age} section, above.

\textsuperscript{317}See \textit{R. v. Cheung}, supra notes 147-148. As Cross, \textit{supra} note 21 at 527-528, states, "Nevertheless, the development of technology has also created a dilemma: although technology creates greater incentives to keep information secret, it also makes secrecy more difficult to maintain. Technology itself has produced a number of new devices which make the task of espionage much easier".
unit (VDU) can be read directly through the use of radiation scanners\textsuperscript{318} or long-range cameras and optics\textsuperscript{319}. During its transmission over private or public\textsuperscript{320} telecommunication or computer networks\textsuperscript{321}, information can be obtained through the use of physical or electronic wiretaps, or other eavesdropping equipment which can monitor the communications line\textsuperscript{322}. In addition, e-mail and other "packet-switched"\textsuperscript{323} electronic data transmissions can be intercepted through the use of "sniffer"\textsuperscript{324} programs, which can divert or copy data addressed to or from a particular computer\textsuperscript{325} or individual.

Whilst in storage, information can be obtained in many ways. It can be "stolen"\textsuperscript{326} through traditional methods, such as the removal of the computer or its hard drive, or the

\textsuperscript{318}This method is becoming less favoured at the present time due to the existence of "low radiation" VDUs, which make the task of radiation scanning much more difficult, and much less accurate. See Target Hardening section, Chapter 4, and infra note 322, 464-467.

\textsuperscript{319}Apart from the level of technology, the issues regarding surveillance are substantively the same as those discussed in the Surveillance and General Privacy Protections section, Chapter 2. The only new matter arising is whether a computer can be regarded as a "place" for the purposes of search and seizure, and if so whether the scanning of computer memory banks or the collection of e-mails will be regarded as a violation of search and seizure protections and Section 8 of the Charter. See Davis and Hutchinson, supra note 55, c.11, and S.C. Hutchinson, J.C. Morton and M.P. Bury, Search and Seizure Law in Canada (Toronto: Carswell, n.d.) (looseleaf), c.4. See also the Telecommunication Protections and Computer Specific Protections sections, below, and infra note 430.

\textsuperscript{320}Public Switched Telephone Networks (PSTN).

\textsuperscript{321}Such as Local Area Networks (LANs), Wide Area Networks (WANs) and Integrated Services Digital Networks (ISDNs).

\textsuperscript{322}Communication lines can act as giant antenna broadcasting any information which in passing through the network to external receptacles. As such, information can be read from VDUs much more easily and obtained with more accuracy and reliability. See A. Bacard, Computer Privacy Handbook: A Practical Guide to E-mail Encryption, Data Protection and PGP Privacy Software (Berkeley: PeachPitt Press, 1995), at 21-37. See also infra notes 464-467.

\textsuperscript{323}See especially Asynchronous Transfer Mode (ATM) technology, S.G. Steinberg, "Netheads v. Bellheads", Wired (October 1996). See also, infra notes 359 and 439.

\textsuperscript{324}These are programs which can trace, copy, divert and access documents, files and e-mails which are in transit through "packet-switched" data networks. The term "sniffing" is derived from "sniffing the ether" in an Ethernet network. See Davis, supra note 55 at 93-94.

\textsuperscript{325}This is accomplished using the "IP" identifier. See supra notes 293 and 294.

\textsuperscript{326}The discussions in Chapter 2, and the fact that information cannot be the subject of theft under the criminal law must be borne in mind.
taking of a floppy disk, or printout containing the information. In addition, the computer data banks or hard drives can also be remotely accessed via computer and telecommunications networks. Unauthorised access of this nature is referred to as “hacking”.

It should be noted, however, that in the computer age the boundaries between information creation, transmission and storage are extremely hard to draw. The similarities in the acquisition of information in creation and transmission were discussed in chapter two, and the difficulties of separating data storage from data transmission have been alluded to above. The convergence of technology means that the computer is now both a storage and telecommunications device, and any distinction between data storage and transmission is becoming increasingly more artificial and irrelevant. In addition, vast amounts of information are now stored “on-line”, and this information exists in a twilight zone, somewhere between storage and transmission, but in a limbo which consists of neither.

---

327 It is also disturbing to note at this point, that Internet Service Providers (ISPs) can access the hard drive of a client’s computer and search the files for information. See “Privacy Rights Clearinghouse”, supra note 292, and infra note 430.

328 Also known as “cracking”. See the Analysis section, Chapter 4.


330 However, as will be discussed below, the protection of telecommunication and computer networks is likely to protect both information in transmission, and information in storage. See the Theft of Telecommunications and A Proactive Approach to Protecting Information sections, below.

331 For example, much e-mail is stored at the ISPs’ servers, and many company records are now stored at the “host” instead of at the “client”. See Tapscott, supra note 16 at 95-121.
D. PROTECTING PRIVATE INFORMATION IN THE COMPUTER AGE

In the previous chapter, many traditional laws and doctrines were discussed, and these doctrines are still applicable in securing information in the computer age. However, other more relevant and computer-specific laws also exist, and it is likely that these will provide better legal protection for computer stored and transmitted information.332.

Before looking at computer specific protections, two surrounding areas of law should be re-examined. These are theft and mischief. The former was discussed in chapter two, and the latter is of relevance because it makes specific reference to computer data. In discussing these two protections however, the anti-surveillance principles333 and fraud provisions should not be forgotten, as they too are useful in securing information.334.

332 In reality, however, it is questionable whether these laws will provide much additional protection. This is because both the benefits these laws provide and the extent of computer crime are unknown. See Piragoff, supra note 6 at 86-87, Davis and Hutchinson, supra note 55 at 10-17, and House of Commons Canada (Standing Committee on Justice and Legal Affairs), Report of the Sub-Committee on Computer Crime (Ottawa: Supply and Services Canada, 1983), paras. 15-19 at 13-14 (Hereinafter referred to as "Report of the Sub-Committee on Computer Crime").

333 Meaning the general privacy, and freedom against search and seizure protections under Section 8 of the Charter. See Surveillance and General Privacy Protections section, Chapter 2.

334 However, as discussed in Chapter 2, the protection afforded by the fraud provisions is marginal. Its primary purpose is to provide remedy for software piracy and other copyright infringements. See D.M. Cameron, "Criminal Copyright Law", in Davis and Hutchinson, supra note 55, c. 8, and infra note 345.
(a) Theft

In discussing theft, the area may be usefully divided into two sections: the first focusing on traditional applications of the theft provisions, and the second focusing on computer-specific extensions of the offence.

(i) A Traditional Application of the Theft Provisions

It was noted in chapter two that Section 322 of the Criminal Code, which contains the theft provisions, cannot be applied to information\textsuperscript{335}. It was also noted that claims of exclusivity are not actionable under the criminal law. However, it was apparent that some security may be inadvertently afforded through the protection of the physical carrier of the data, and also through prohibitions against trespass and breaking and entering\textsuperscript{336}.

In the computer age, the theft provisions are geared more towards the protection of "stand-alone" machines\textsuperscript{337}, and the protection of the computer itself, or the hard drive within. Remedy will also be provided for the taking of a floppy disk or a print-out.

\textsuperscript{335}Interestingly, information may attract even less protection in the computer era because the information subsists as data, which itself exists as bits and bytes, as 1s and 0s on a magnetic surface. It could be questioned whether such incomprehensible representations of data could ever be regarded as information, and as such, whether they would be protected under any legal regime. However, under the Copyright Act (\textit{supra} note 3) computer programmes are protected, and so it seems that information in an electronic format can be the subject of legal protection.

\textsuperscript{336}See the \textit{Surveillance and General Privacy Protections} and \textit{Theft} sections, \textit{Chapter 2}.

\textsuperscript{337}Indeed, the theft of computers is especially severe with regards to Laptop or Notebook computers.
containing the information. However, in the latter cases, the items taken are unlikely to be of sufficient quantum for a criminal charge to succeed\textsuperscript{338}. It should also be noted that the theft provisions will not provide any protection against those who have acquired information simply by reading a printout, or viewing the information directly from a monitor screen, because nothing tangible has been removed\textsuperscript{339}. In addition, no remedy will be provided for information which is remotely acquired by access through computer or telecommunication networks. This is because, according to the criminal law\textsuperscript{340}, nothing of “value” has been taken.

In addition to these difficulties, it was also noted, in the previous chapter, that when information is stolen, the individual is rarely deprived of anything, because a copy of the information is usually maintained. This is certainly the case in the computer age, where “back-ups” of information are created as part of the operating procedure for many organisations\textsuperscript{341} and individuals. Indeed, automatic back-up and “auto-save” are standard features of many computer systems. Frequently, these back-ups are stored at remote locations, and so even the theft of an entire computer system would not necessarily eradicate the information.

\textsuperscript{338}Of course, in stealing a print-out of the information, a thief could not only be charged with stealing the paper, but also with stealing the ink required to print the data, and the electricity required to operate the printer. However, even combined, these factors are unlikely to create sufficient quantum. See the Theft of Computer Time and Services and Theft of Electricity sections, below.

\textsuperscript{339}It should be reiterated that the exclusivity of information is not protected under the criminal law. See R. v. Stewart (supra note 167), and supra notes 158 and 163.

\textsuperscript{340}See R. v. Stewart (supra note 167), and Theft section, Chapter 2.
Interestingly, even if a backup has not been created, it is still unlikely that the practical components of Section 322(1) will be fulfilled. This is because computer files are usually “copied” onto a floppy disk rather than transferred or moved. This means that a copy of the information is created on the floppy disk, whilst leaving another copy on the hard drive. In this way, taking the floppy disk does not remove the only copy of the information, and hence under the theft provisions, the owner is deprived of nothing\textsuperscript{342}. Of course, the problems are added to if the “information thief” uses his own floppy disk, because then, not even physical deprivation has taken place\textsuperscript{343}. Also, even if the thief copies the information and then destroys the original subsisting on the hard drive, this is still not theft. Under these circumstances, no deprivation has taken place through the taking of the information. Instead, two separate actions have taken place, and hence two separate offences have been committed. The two actions are the copying of information, and the destruction of property\textsuperscript{344}, and the two separate offences are the unauthorised copying of information\textsuperscript{345}, and mischief\textsuperscript{346}.

\textsuperscript{341}See \textit{Target Removal} section, \textit{Chapter 4}.
\textsuperscript{342}Except exclusivity, which as we have consistently noted is not protected under the criminal law (\textit{supra} note 339).
\textsuperscript{343}Conversely of course, if the floppy disk contains the only copy of the information, then taking this floppy disk would constitute not only information exclusivity loss, but complete loss, and it will also be the removal of a tangible entity actionable under s.322(1) as discussed in the text.
\textsuperscript{344}Once again, information is not regarded as property for the purposes of the criminal law. However, this is concentrating on the theft provisions, and under other sections of the \textit{Criminal Code}, it is likely that information will be regarded as property. For example, in relation to mischief, the manipulation or destruction of computer data is specifically proscribed. See \textit{Mischief} section, below.
\textsuperscript{345}In reality, this will only be an offence if it involves copyrightable material, or if it involves the resale of this information, which may be regarded as piracy. See \textit{R. v. Leahy} (\textit{supra} note 170) and \textit{R. v. Kirkwood} (\textit{supra} note 170).
\textsuperscript{346}See \textit{Mischief} section, below.
In this light, it is clear that a traditional application of the theft provisions will be unhelpful in protecting private information in the computer age. Fortunately, however, computer-specific theft provisions also exist.

(ii) *Computer Specific Theft Provisions*

In addition to the traditional theft provisions, several independent, and computer or telecommunication specific extensions of Section 322 exist. Examples include the theft of computer service, the theft of electricity and the theft of telecommunications service. The implications of these offences will be discussed below.

1. *Theft of Computer Time and Services*

   The theft of computer time and services\(^{347}\), originally an extension of the general theft of services provisions\(^{348}\), has now been superseded by Section 342(1)(a) of the *Criminal Code*, which will be discussed below. However, both offences relate to the theft of computer processing capacity, and can be used to prosecute any individual who is using a computer system without authorisation, or who is using it for an unauthorised


\(^{348}\)Piragoff, *supra* 6 note 105-106.
purpose\textsuperscript{349}. This is because any unauthorised activity on the computer, is in effect, “taking” the time and service of the computer, which is regarded as theft under the provision. Once again, however, some deprivation must be evident, and in this case the loss suffered by the computer facility owner is usually one of efficiency, which decreases profits due to detrimental effects on business data processing capacity.

Although important at one time, this offence is of limited application today. The current processing capacity of computers is vast, and the cost of computing is extremely low\textsuperscript{350}. As such, a computer’s efficiency is unlikely to be impaired through the processing of an unauthorised task, and little or no financial harm will be suffered by the system’s owner. It is likely, therefore, that any prosecution under these provisions would fail due to insufficient quantum\textsuperscript{351}. Additionally, these problems are exacerbated by the advent of extensive computer networking. A computer system can now be accessed remotely, and hence the perpetrator does not even have to occupy a terminal\textsuperscript{352}. This

\textsuperscript{349}Ibid.

\textsuperscript{350}It has been suggested that the cost of computing halves, and the processing capacity doubles, every 18 months.

\textsuperscript{351}Of course, the situation is likely to be different if there is only one computer, or only one access point to the mainframe. In these instances, all processing direction and capacity would be lost, and the quantum may be great enough for a criminal charge to succeed. However, in the business environment this scenario is unlikely to occur, although it may arise in the home.

\textsuperscript{352}Such unauthorised occupation of a workstation would cause economic loss to a company, especially if the occupation prevented an employee from performing his or her business duties. This problem is the same with the individual computer user at home.
reduces the inconvenience and loss suffered by the organisation, and hence increases the
difficulties of prosecution\textsuperscript{353}.

The theft of computer time and services offence, is clearly geared more towards
commerce than individual home computer use, and this may reduce its potency as a
privacy safeguard, although, it will provide protection against the acquisition of personal
information which is stored on business computers for commercial gain\textsuperscript{354}. In addition,
because the offence prevents unauthorised access or use for an unauthorised purpose, it
protects private information in a round-about way. This is because, if an owner of a
computer system secures certain files, and requires that they not be accessed, then any
attempt to access them would constitute unauthorised use, which in turn would constitute
a theft of computer time and service. However, this is an extreme exaggeration of the
provision, and it is unlikely that it would be used in this way. In any event, new
computer-specific provisions now exist which protect computer data, and as such, any
shortcoming in this offence is not a matter for concern\textsuperscript{355}.

\textsuperscript{353}Indeed, the data-base which the company itself is using may not even be owned, operated or controlled
by the company, but instead by a third party, and as such no loss will be accrued by the company. See
Tapscott, supra note 16 at 95-121.

\textsuperscript{354}Hence some protection is afforded. However, the largest deprivation will occur through economic loss
suffered as a result of losing exclusivity over information which could have been sold. See Theft and
Fraud sections, Chapter 2.

\textsuperscript{355}See Computer Specific Protections section, below.
2. Theft of Electricity

The theft of electricity is similar in nature to the theft of computer time and services offence, outlined above. Electricity is, in effect, stolen when a computer owned by another person or organisation is switched on and used to process data without authorisation\textsuperscript{356}. However, once again, in today’s world, computers use so little electricity, and the loss suffered would be so minimal, that no prosecution would be likely to succeed\textsuperscript{357}, if one would ever be brought at all.

3. Theft of Telecommunications

The offence of theft of telecommunications is, at first glance, unrelated to the protection of information. The basic concept of the offence is outlined in Sections 326 and 327 of the Criminal Code. Section 326(1)(b) states that, “Every one commits theft who fraudulently, maliciously, or without colour of right ... uses any telecommunication facility or obtains any telecommunication service”\textsuperscript{358}. Although the provision does not refer to information at all, Section 326 does protect it indirectly. This is because the theft of telecommunications offence can theoretically be used to prohibit unauthorised access


\textsuperscript{357}Indeed, it is unlikely that such a charge would even be brought today, given the introduction of the “Unauthorised Use of a Computer Offence”, outlined below. See \textit{Computer Specific Protections} section, below.
to computer networks. Telecommunication networks provide the backbone for computer communication\textsuperscript{359}, and prohibiting network access protects information because remote acquisition of data is prevented. It is similar, in effect, to stopping a thief from walking up the garden path to get to your front door. If he or she can be halted at the end of the path, there is no opportunity to even attempt a break-in. Of course, this is only a marginal protection, because computer systems can be accessed without the use of a network, and can be illegally accessed by legally obtained telecommunications services. However, many “hackers” and computer criminals do use unauthorised telecommunications to break into computer systems. This is because it conceals their identity and reduces the likelihood of detection\textsuperscript{360}. Indeed, it would seem only logical from the hacker’s point of view to do this, because following the old adage that one “may as well be hanged for a sheep as a lamb”\textsuperscript{361}, the hacker has nothing to lose in committing an additional offence which may decrease the possibility of his or her apprehension\textsuperscript{362}.

\textsuperscript{358}Criminal Code, Section 326.1.
\textsuperscript{360}In any event, hackers usually “Call Block” (*67) (see supra notes 302-306) their hacking attempts, so that their location cannot be traced. In addition, they frequently possess many different telephone lines through which they make their hacking attempts. It is also common to use “1-800” dial-up long distance services to increase anonymity. See Davis, supra note 55 at 75-79. See infra note 368.
\textsuperscript{361}This phrase dates from the 1600s, when a thief would be executed for stealing anything over a certain value. As a lamb was over this limit, and a sheep was more valuable, it would seem only logical to steal the sheep, as the punishment for the theft of either was the same. See J.A. Sharpe, Crime in Early Modern England, 1550-1750 (London: Longman, 1984).
\textsuperscript{362}This is similar to a criminal mugging an individual for money, and then murdering the victim to prevent identification. To take an example from the Louisiana death penalty statutes, committing murder during the commission of another crime is a capital offence (Louisiana Code of Criminal Procedure, Article 905.4: “Aggravating Circumstances - A. The following shall be considered aggravating circumstances: (1) The offender was engaged in the perpetration or attempted perpetration of aggravated rape, kidnapping, burglary, robbery, arson or escape”). Therefore, if a perpetrator kills a bank clerk during an armed
To this end, Section 327 prohibits the ownership of any device whose primary purpose is to obtain telecommunications services illegally. This creates additional barriers, both psychologically and legally, to obtaining unauthorised communications, which, through an increased deterrent effect, increases the protection of information which is in transmission or which is stored “on line”.

The theft of telecommunications offence may also prove useful in protecting unauthorised access to computer networks in another way. Computer criminals frequently use a variety of paths, and a string of many PBXs, LECs and ISPs to reach their target. This is, once again, in an attempt to conceal their identity and evade detection, and the unauthorised use or passage through these servers and exchanges may indeed constitute a theft of telecommunications.

Additionally, many large companies and computer user groups have extensive WANs and Internet connections, and operate dedicated high speed, high bandwidth

---

364 See A Proactive Approach to Protecting Information section, below, and infra notes 419-422.
365Private Branch Exchange.
366Local Exchange Carrier.
367Internet Service Provider.
368Davis and Hutchinson, supra note 55 at 75-80.
369Wide Area Networks.
fibre-optic or ISDN\textsuperscript{370} lines to these public exchanges or commercial servers. The use of these private lines to access the company's network for criminal purposes would clearly constitute an unauthorised use of their telecommunications facilities, and be protected by the theft of telecommunications provision. In this way, the offence could be used as a subjective and discretionary tool to protect computer networks and the data which they contain\textsuperscript{371}.

Indeed, the theft of telecommunications may be more applicable to computers than it might first appear, and certainly more than it was first intended\textsuperscript{372}. In 1980, in the case of \textit{R. v. McLaughlin}\textsuperscript{373}, it was stated by the Supreme Court of Canada that, "A computer is not a telecommunications facility, holding that the function of a computer is not to channel or transmit information to outside recipients so as to be susceptible to unauthorised use; rather a computer is a data processing device"\textsuperscript{374}.

\textsuperscript{370}Integrated Services Digital Network.

\textsuperscript{371}Once again, this is an extreme extension of the original meaning and application of the offence. This is because any prosecution would be based on the use of the line rather than any fraud or loss accruing from the theft of the service. In using the lines for an authorised purpose, no loss could be deemed to accrue, and hence no prosecution would be brought. However, if unauthorised use was affected then the company or individual owning the line may construct a loss of time, efficiency, and profits through the tying up of the communications link. This is similar, in effect, to the Theft of Computer Time and Services, and the Theft of Electricity offences outlined above. Indeed, it is also a virtual version of trespass. If the owner of a tract of land desires your presence or is unaffected by it, then he or she is unlikely to bring a civil action or press criminal charges (depending on whether it is a civil or criminal trespass). However, if the owner did not want your presence on his or her land, or if you were causing him or damage, then an action for trespass would probably be brought. See \textit{supra} note 110, and \textit{infra} note 430.

\textsuperscript{372}Of course, many Acts and provisions are extended to cater for advances in technology. See Takach, \textit{supra} note 32 at 153.

\textsuperscript{373}[1980] 2 S.C.R. 331. The case involved the prosecution of a hacker under the Theft of Telecommunications provisions.
However, as we have discussed, the convergence of technology in this field means that computers can no longer be regarded in this way. They are as much involved in the transmission of information and in the performance of a telecommunications role as they are in data processing, and any provision relating to telecommunications today would undoubtedly apply to computers. It is ironic in this instance that technology has caught up with the law.

(b) Mischief

In a discussion of the protection of information in the computer age, the offence of mischief should be addressed. Section 430, which contains the mischief provision, makes it an offence to damage or destroy the property of another, or to otherwise interfere with the lawful enjoyment of that property. Of course, this provision is only useful if information can be regarded as property, and as we have noted this is an issue of great contention\(^\text{375}\). However, since the amendment of the Criminal Code in 1985\(^\text{376}\), data is specifically provided for under the mischief provisions. Section 430(1.1) states:

\(^{374}\)Takach, *supra* note 32 at 157.
\(^{375}\)See *Theft* section, *Chapter 2*, and *supra* note 152, 158 and 163.
\(^{376}\)Before this amendment, it was questionable whether data could be the subject of mischief. The new provision was included due the problems arising in the case of *R. v. Turner* (1984), 13 C.C.C. (3d) 430 (Ont. H.C.).
SECTION 430(1.1)

1(1) Every one commits mischief who wilfully:

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data denies access to data to any person who is entitled to access thereto.

Although the mischief provision clearly protects data in a physical sense, it is less certain whether it serves any useful purpose in protecting the privacy of information. If a malefactor destroys your personal data without reading or absorbing it, no exclusivity has been lost. However, privacy has been infringed in a more indirect way. This is because, as we have consistently noted, privacy is related to control over the dissemination of information, and if data is erased then control over it has been negated. Indeed, the very fact that someone has entered your computer system without authorisation, means that a trespass has been committed, which in itself is an infringement of privacy. This is regardless of what the intruder does whilst he or she is “inside” the computer system.

377Section 429(1) states that the act must be wilful, which does not involve proving malicious intention or mens rea, as the voluntariness of the act will be enough (See R. v. Schmidtke (1985), 44 C.R. (3d) 392 at 396 (Ont. C.A.)).

378Section 429(3) ensures that no defence is available for the deletion of ones own information if it is partly owned by another (See R. v. Downs (1996) S.J. No.703 (Sask. Prov. Ct.), August 29, 1996). It also prohibits the deletion of ones own data, even if you are the sole owner, if it is for some mischievous purpose such as fraud.

In addition, as noted earlier, mischief is a more technically accurate offence than theft in relation to the copying of information, because as Cross notes, "Unlike theft, vandalism applies in the situation where the defendant damages or destroys the property of the victim, without necessarily taking possession". In this way, a defendant can be liable for the destruction of information, regardless of whether the information was copied or removed.

Another interesting utilisation of the vandalism offence comes in its defence and prohibition against the use of "viruses", "Trojan horses", "worms" and "bacteria". This is because Section 430.1(1) prohibits rendering "useless, inoperative or ineffective" any property, and also proscribes any interference with the "lawful use, enjoyment, or operation of property". The use of such data altering, inhibiting, and destroying programs clearly interferes with the lawful use and enjoyment of computer information, and will certainly be protected under the provisions of the offence. The only potential problem which could arise, is the lack of any human actor in the perpetration of the damage. This is because a virus acts automatically once it is introduced into a computer.

---

380 See supra notes 110 and 371, and infra note 430.
381 Cross, supra note 21 at 565.
382 As defined by J. Vargo and R. Hunt, Telecommunications in Business: Strategy and Application (Boston: Irwin, 1996), at 417, "A virus is a segment of code that, when inserted in an otherwise harmless program, converts the program into a Trojan horse [defined infra, at note 383]."
383 A "Trojan horse", in computer terminology, is, "a malicious program that performs some useful task, such as sorting a directory, while at the same time carrying out some secret activity, such as introducing errors into data files, erasing files, or erasing the entire hard disk itself" (ibid.).
384 "Worms and bacteria refer to programs that infect computer networks. Although not as destructive as Trojan horses and viruses, they can force a network to shut down until all copies of the hostile program have been removed" (ibid., at 418).
system, with no direct control being exerted by the human counterpart. However, it seems that the introduction of the virus alone will be enough, and the use of viruses and other such programs is prohibited by the offence\textsuperscript{385}.

\textit{(c) Telecommunication Protections}

In the previous chapter, the provisions relating to the protection of telecommunications were discussed, and it was noted that Section 184 prohibits the interception of many forms of private communication\textsuperscript{386}. In the computer age, the integrity of communication networks with regards to protecting information is crucial for two reasons. First, because computer and telecommunication technologies are converging, which means that much information is now stored "on-line" and would be vulnerable if a telecommunication network was compromised; and second, because the computer itself is now heavily involved in a communications role, and computer data transmissions must also be protected if information is to be adequately secured.

The problem of information being stored "on-line" was outlined above, and it was mentioned that much data now subsists in a twilight zone somewhere between communication and storage. In this way, the interception of telecommunications could capture information not only during transmission but also during storage. Additionally,

\textsuperscript{385}See Davis, \textit{supra} note 55 at 107-113.
the "on-line" nature of computer networks means that the boundary between communication and storage is being blurred. As such, where an interception of communications ends and an unauthorised accessing of a computer system begins is becoming increasingly more difficult to determine. To this end, computer networks must be secured if information stored in them is to be protected.

The fact that computers themselves are engaged in communication creates other problems. The wide-spread use of electronic mail (e-mail) and other electronic data interchanges (EDI) has provided new sources for interception. Such mediums are extremely insecure, as e-mails for example, can be read by system administrators, employers387 and by anyone possessing the requisite technology to "capture" messages en route to their destination388.

The question then arises as to whether computer data transmissions can be regarded as private communications for the purposes of Section 184, and hence, whether they will be protected from interception. It was noted, in the last chapter, that Section 184 will almost certainly protect all forms of voice telephony, facsimile, and data

---

386See Specific Communications Protections section, Chapter 2.
387See infra note 565.
388The computer programmes which allow e-mails to be captured in this way are referred to as "sniffers" (see supra note 324). The success of these programmes depends on the data being uncoded, as if it is encrypted it could not be read upon capture (see encryption in the Target Removal section, Chapter 4). To this end, e-mails should be viewed like postcards, in that they can be read by anyone en route (Coyle, supra note 256 at 151). It should also be borne in mind that automated computer back-ups will store copies of your e-mails, even after you have erased them (Coyle, supra note 256 at 152-153). In addition,
transmissions, and it is likely that computer transmitted faxes and Internet telephony will be protected in this way. However, the situation in relation to e-mail is more tenuous. In some cases it seems that e-mail will not be regarded as secure enough to meet the "reasonable expectation of privacy" requirement, and hence will not be protected, whereas in other cases it will. For example, encrypted e-mail transmitted over private networks will be regarded as private, whereas un-coded e-mail sent over public networks will not.

The real difficulty, however, arises in relation to computer communications conducted solely between two or more computers with no human intermediary. In these cases it seems likely that Section 184 will not apply. As Takach notes, "the wiretap provision in section 184 arguably is limited to person to person communications and

---

389 See supra note 141.
390 M. Rotenberg, Director, Electronic Privacy Information Center (<http://www.epic.org>) notes that "E-mail is more like a postcard than a sealed letter".
391 There is no Canadian authority on this matter, however in the U.S., the case of United States v. Maxwell 42 M.J. 568 (U.S.) (U.S.C.A. Armed Forces 1996) upheld the privacy of such communications. This case should be compared with Smyth v. Pillsbury Co. Below (see infra note 392).
392 There is no Canadian authority on this matter, however in the U.S., the case of Smyth v. Pillsbury Co. 914 F. Supp. 97 (U.S.) (E.D.Pa. 1996) determined the unprotectability of this form of e-mail transmission. This case should be compared with United States v. Maxwell above (see supra note 391). Indeed, sending unencrypted e-mail is similar in effect to sending a postcard through the public mail system. Although most e-mail requires a password to access, and is hence marginally protected in storage, it is unprotected during transmission. However, as noted in the text, the boundary between storage and communication is becoming increasingly more difficult to determine.
393 In the U.S., the Electronic Communications Privacy Act (U.S.) 18 U.S.C. 2511, states that it is unlawful for anyone to read or disclose the contents of an electronic communication unless harm is being done to the system (in which case the system administrator is permitted to view the e-mails), or consent to view the message is given by either the recipient or the sender. It should be noted that such consent is often required as part of employment agreements (See ECPA 18 U.S.C. 2516-2518, and 2703). See also infra note 565.
therefore may not be adequate to cover computer to computer communications".

Fortunately, however, the new Unauthorised Use of a Computer provision, discussed below, will protect such communications.

(d) Computer Specific Protections

In addition to the peripheral protections outlined above, Section 342.1 of the Criminal Code protects computer networks, and the information which they contain. Otherwise known as the Unauthorised Use of a Computer offence, the provision states that:

SECTION 342.1

(1) Every one, who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer, or

\[394\] It is also unclear whether computer messages which are not actually in transmission, but which are stored or queued "on-line", ready for delivery, are covered by this provision.

\[395\] Takach, supra note 32 at 159.

\[396\] This section came into effect in 1986, through the passing into law of the 1985 amendments of the Criminal Code. Criminal Code of Canada, R.S.C. 1985, c. C-46, s.342. Subsection (d) however was added in April 1997, when An Act to Amend the Criminal Code and Certain Other Acts (Bill C-17) (S.C. 1997, c.18 (s.18)) passed into law. Bill C-17 was originally introduced on December 14, 1995, and re-introduced on March 7, and was part of the Criminal Code Improvement Act, 1996. See “Report of the Sub-Committee on Computer Crime”, supra note 332.
(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Subsection (a) is similar in effect to the theft of computer time and services offence outlined above, and would protect private information by preventing any unauthorised use and access to the computer system in which it resides\textsuperscript{397}. Subsection (b) prohibits the interception of any function of a computer\textsuperscript{398}, and as such, not only protects any information in either on or “off-line”\textsuperscript{399} storage, but also any information which is communicated by computer or which is in transmission between two or more automated devices\textsuperscript{400}. In this way, the ambiguities of Section 184 become irrelevant, as computer communication is protected independently of that provision\textsuperscript{401}. Interestingly, the use of

\begin{footnotesize}
\textsuperscript{397}This subsection is a prohibition against service, however, and is undoubtedly geared more towards prohibiting the free acquisition of an otherwise costly, or “charged” service. Service is defined in s.342.1(2) as including “\textit{data processing, and the storage or retrieval of data}”.

\textsuperscript{398}The use of any computer or computer programme, or any intervention by a human actor, would seem to be proscribed, and the use of “\textit{sniffers}” would be prohibited in this way (see \textit{supra} note 324).

\textsuperscript{399}“Off-line” storage refers to data which is stored on a computer which “stands alone”, and is not connected to a network. In order to access such a system it is necessary to have physical access to the terminal and its interface.

\textsuperscript{400}This is dependent on the categorisation of “communication” as a computer function, which it is pursuant to s.342.1(2) (see \textit{infra} note 401).

\textsuperscript{401}This is because s.342.1(1)(b) prohibits the interception of any function of a computer, which under s.342.1(2) defines a computer function as including, “\textit{logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer system}”.
\end{footnotesize}
automatic programmes to intercept communications, such as "sniffers"\(^{402}\), is also prohibited under subsection (b).

Subsection (c) is of particular interest. This is because it prohibits even an attempt to commit an offence under parts (a) and (b), and as such creates a strong defensive barrier against unauthorised access; especially since any indirect interference is also regarded as criminal. This provision would clearly protect against any hacking activity, and would also criminalise many infringing acts before the target computer could even be reached. For example, it is likely under this subsection, that an offence would be committed as soon as the target computer's network connection was accessed. This subsection allows for the easier prosecution of more remote offences, or offences with a greater degree of ambiguity, and can include such things as, "encouraging others to use computers to ... prohibited ends"\(^{403}\). It is clearly the intention of Section 342.1 to prevent all unauthorised access to computer networks, regardless of how such entry may be attempted. As Davis and Hutchinson note, the inclusion of subsection (c) is undoubtedly, "intended to capture individuals acting through several computer devices or by way of a programme or virus acting at some time after the person has ended direct manipulation of the device"\(^{404}\).

\(^{402}\)See supra note 324.

\(^{403}\)Davis and Hutchinson, supra note 55 at 167.

\(^{404}\)Ibid.
The Trafficking in Passwords provision contained in subsection (d) was added in April 1997, and serves as a useful early defence barrier to unauthorised use. It also provides additional protection for private information which is stored in these computer systems. The origin of this subsection was Bill C-17, and under Section 19 of this Bill, another offence to aid in the protection of computer networks was proposed. This is the Possession of a Device to Obtain Computer Services offence, which if introduced would prohibit the possession of any device, "the design of which renders it primarily useful for committing an offence under section 342.1(1), under circumstances that give rise to a reasonable inference that the ... device ... has been used or is or was intended to be used to commit an offence contrary to that section." Similar, in effect, to Section 327 discussed above, this provision would increase the defensibility of computer networks, because not only would unauthorised access be prohibited, but also the means by which such access could be perpetrated. It is likely for example, that such a provision would not only prohibit the use or possession of any device which could directly obtain an unauthorised service, but also any device, such as a "sniffer" program which could be used to "capture" a password which could used to obtain an unauthorised service. It is important to note however, that in preventing the ownership of devices

---

405 Interestingly, "traffic" includes both import and export, and will include encryption technologies. See the Target Removal section, Chapter 4.
406 See supra note 396.
407 See A Proactive Approach to Protecting Information section, below.
408 See supra note 396.
409 This new provision is similar to subsections 191(1), 327(1) and 351, which makes it an offence to possess scanning devices, and other instruments which can be used to tap telecommunication transmissions or break and enter into a house. See Takach, supra note 32 at 160, A Proactive Approach to Protecting Information section, below, and supra notes 413-418.
which can be used to affect unauthorised entry, the provision would not prevent the possession of devices which could be used to inflict harm on a computer system. For example, it would not outlaw the possession of viruses or other malicious programs, even though their actual deployment is prohibited under Section 430.

It should be noted, however, that Section 342.1 does not protect information directly, and although unauthorised access to data is open to prosecution, no remedy exists for the disclosure of any information which was obtained in this prohibited manner411. This has implications for the protection of private information, which will be discussed below.

E. A PROACTIVE APPROACH TO PROTECTING INFORMATION

It has been repeatedly noted throughout the course of this thesis that information must be protected if exclusivity is to be maintained. It has also been noted that, in the computer age, the most important area requiring protection is acquisition, and we have discussed the many laws which serve this end. By far the best way of protecting against

410 Section 19 of Bill C-17. See Davis and Hutchinson, supra note 55 at 168.
411 In R. v. Forsythe (1991), 137 A.R. 321 (Prov. Ct.), the accused was found not guilty under this section of the Criminal Code, because he was found not to have obtained a computer service, either directly or indirectly. In the case, other persons, although under his direction, had obtained the computer service, and he was simply the recipient of the information which was gleaned. From this case it appears that the recipients of computer information are not prosecutable under the offence. On the basis of remoteness this seems a reasonable restriction, however, it may be better in the realm of computer data to protect the
the acquisition of information is by preventing access to it, and not all of the laws mentioned take this approach. For example, theft, fraud and mischief, although proscribing against the taking of or tampering with information, only provide reactive remedy rather than proactive defence; and the nature of information means that this is an unsuitable path to take.\footnote{Of course, all law is reactive and can only provide remedy to a crime or civil wrong. However, certain laws prohibit activities which cause, or enable, other crimes to be committed, and these can be deemed as proactive in effect. An example from the physical world which helps protect private information, is the prohibition of breaking and entering\footnote{In order to prevent theft, and the criminalisation of the “tools” which enable breaking and entering to occur\footnote{Indeed, two levels of proaction are evident here. The first level being the direct prevention of theft through the prohibition of breaking and entering, and the second level being the indirect prevention of theft through the prohibition of the devices used to break and enter and commit theft.}. Indeed, two levels of proaction are evident here. The first level being the direct prevention of theft through the prohibition of breaking and entering, and the second level being the indirect prevention of theft through the prohibition of the devices used to break and enter and commit theft.}.

Of course, all law is reactive and can only provide remedy to a crime or civil wrong. However, certain laws prohibit activities which cause, or enable, other crimes to be committed, and these can be deemed as proactive in effect. An example from the physical world which helps protect private information, is the prohibition of breaking and entering\footnote{In order to prevent theft, and the criminalisation of the “tools” which enable breaking and entering to occur\footnote{Indeed, two levels of proaction are evident here. The first level being the direct prevention of theft through the prohibition of breaking and entering, and the second level being the indirect prevention of theft through the prohibition of the devices used to break and enter and commit theft.}. Indeed, two levels of proaction are evident here. The first level being the direct prevention of theft through the prohibition of breaking and entering, and the second level being the indirect prevention of theft through the prohibition of the devices used to break and enter and commit theft.} in order to prevent theft, and the criminalisation of the “tools” which enable breaking and entering to occur\footnote{Indeed, two levels of proaction are evident here. The first level being the direct prevention of theft through the prohibition of breaking and entering, and the second level being the indirect prevention of theft through the prohibition of the devices used to break and enter and commit theft.}. Indeed, two levels of proaction are evident here. The first level being the direct prevention of theft through the prohibition of breaking and entering, and the second level being the indirect prevention of theft through the prohibition of the devices used to break and enter and commit theft.\footnote{In order to prevent theft, and the criminalisation of the “tools” which enable breaking and entering to occur\footnote{Indeed, two levels of proaction are evident here. The first level being the direct prevention of theft through the prohibition of breaking and entering, and the second level being the indirect prevention of theft through the prohibition of the devices used to break and enter and commit theft.}. Indeed, two levels of proaction are evident here. The first level being the direct prevention of theft through the prohibition of breaking and entering, and the second level being the indirect prevention of theft through the prohibition of the devices used to break and enter and commit theft.}.

---

\footnote{A proactive approach is always better than a reactive one. It is far easier to prevent your information becoming known in the first place, than it is to erase the memories of those who have acquired the knowledge (see supra note 99). Indeed, it is this capability of information to be universally possessed which makes it so difficult to control (see The Nature of Information section, Chapter 2, and The Inadequacy of Law section, Chapter 4). In the computer age, D.H. Slavik and T.M. Peters, “Computer Network Insecurity: How to Defend Your Confidential Files”, Trial, March 1995, 80, at 85, note that, “A kilobyte of protection is worth a gigabyte of cure”.}

\footnote{Supra note 165.}

\footnote{Supra note 409.}
Another example is the interception of radio-communications. As discussed in the previous chapter, the disclosure of intercepted radio-communications is illegal\textsuperscript{415}. However, preventing disclosure alone is akin to shutting the stable door once the horse has bolted; the damage has already been done, exclusivity has been lost, and privacy infringed. As a proactive solution to this problem, interception must be banned\textsuperscript{416}, and as a further measure, the devices which can be used to intercept such communications should also be banned\textsuperscript{417}. In addition, to increase the number of defensive walls which surround the target of the protection, radio-communications should be encrypted, unauthorised decryption prohibited, and finally, the possession of devices which allow unauthorised decryption to take place should be outlawed\textsuperscript{418}.

These "proactive laws" are crucial in defending information, because although no law can ever prevent a crime occurring, the existence of provisions and associated penalties creates a deterrent effect, which raises an internal psychological barrier to committing the offence\textsuperscript{419}. Deterrence theory\textsuperscript{420} suggests that individuals weigh the advantages and disadvantages, or pleasure and pain accruing from committing an illegal

\textsuperscript{415}\textit{Supra} note 135.
\textsuperscript{416}This is the proposition under \textit{Bill C-109}. See \textit{infra} notes 416 and 417.
\textsuperscript{417}Alter, \textit{supra} note 121 at 7-8. This is similar to Sections 326 and 327 of the \textit{Criminal Code}, where the theft of telecommunications is illegal, as well as the possession of any device which enables such theft. See also Section 342.1. See \textit{Theft of Telecommunications and Computer Specific Protections} section, above.
\textsuperscript{418}\textit{Ibid.} See also, \textit{Target Removal} section, \textit{Chapter 4}.
In order to deter criminal activity, therefore, the punishment must outweigh the psychological or practical gain achieved from committing an offence. Although more recent studies suggest that the likelihood of detection and apprehension, and the celerity and certainty of punishment, are more important than the severity, it is clear that the deterrent effect will increase in proportion to the number of additional offences which have to be committed. This is because, as the number of offences increase, so does the chance and fear of detection, as well as the severity of the punishment. In this way, "proactive laws" provide a forward defence in the protection of information by reducing the number of interception attempts, and decreasing the success rate of those attempts which are made.

In addition, by legally prohibiting the possession of the tools and devices which can be used to perpetrate the target offence, the ability and chance of successfully committing the principal offence are reduced in very real terms. This is a legal extension of the usual criminal law concept of "proactive laws." These "proactive laws" provide a forward defence in the protection of information by reducing the number of interception attempts, and decreasing the success rate of those attempts which are made.

---

420 See Norrie, supra note 265 at 17-35.
423 This is an application of the twelfth principle of Situational Crime Prevention, "Rule Setting" (see Rule Setting section, Chapter 4). It is also a psychological extension of Defensible Space Theory (see Natural Surveillance section, Chapter 4).
424 This is a legal extension of the fourth principle of Situational Crime Prevention, "Controlling Facilitators" (see Controlling Facilitators section, Chapter 4).
of the "facilitator control" principle of *Situational Crime Prevention*\textsuperscript{425} theory, which will be discussed in greater detail in the next chapter\textsuperscript{426}.

These rationales and theories also apply to the protection of private information in the computer age. The situation has already been outlined with regards to communication, where interception as well as the possession of devices which enable interception are prohibited\textsuperscript{427}. However, the situation in relation to the storage of information on computer networks is slightly different. This is because the target of the criminal activity is not actually protected in law\textsuperscript{428}. In discussing theft, both the theft and the breaking and entering were illegal, whereas here only the breaking and entering is unlawful. There is no underlying criminal activity, because the acquisition of information is not, in itself, illegal. Such an approach is useful for legal consistency because no discrepancies arise in the treatment of information stored in computer media compared to information stored in traditional media\textsuperscript{429}. However, proaction is still the best method of defence in relation to information, and following the discussion above, the more proactive measures which can be applied, the better.

\textsuperscript{425}See *Theoretical and Practical Protections* section, *Chapter 4*, and *infra* notes 444, 450 and 452.

\textsuperscript{426}See *Theoretical and Practical Protections* section, *Chapter 4*.

\textsuperscript{427}See the *Theft of Telecommunications* and *Telecommunications Protections* sections, above.

\textsuperscript{428}See *Theft* section, *Chapter 2*.

\textsuperscript{429}Indeed, the "Report of the Sub-Committee on Computer Crime", *supra* note 332 at paras. 29-32 at 15-16, recommended that information in the computer realm should not be treated any differently from that stored in more traditional media. See also Piragoff, *supra* note 6 at 116. This is not an approach taken by all jurisdictions, however. For example in England, the *Data Protection Act*, (U.K.) 1984, only applies to computer stored and transmitted information. See also, the *Ontario Information Technology Security Directive*, discussed in Management Board of Cabinet. Province of Ontario, *Information Technology Security* (Toronto: Queen's Printer for Ontario, 1986, revised February 1991).
As noted, controlling access is the key to securing information in the computer age, and “access control”, which is itself another Situational Crime Prevention measure, will be discussed in greater depth in the final chapter. Fortunately, blanket access control, which is in effect a prohibition against network trespass\(^{430}\), is the approach taken by the Canadian legislatures in defending computer networks\(^{431}\). Indeed, many levels of proactive defence are evident. Six levels, to be precise: (1) Section 342.1(1)(a) prohibits unauthorised use; (2) Section 342.1(1)(b) prohibits unauthorised access; (3) Section 342.1(1)(d) prohibits the use or possession of passwords which allow unauthorised access; (4) the Possession of a Device to Obtain Computer Services offence prohibits the use or possession of any devices which can be used to obtain unauthorised access, or which can be used to obtain passwords to effect unauthorised entry; (5) the Theft of Telecommunications offence prohibits the use of telecommunications services which can

\(^{430}\)See Wasik, supra note 347 at 75-81, and G.D. Baker, “Trespassers Will Be Prosecuted: Computer Crime in the 1990s”, Computer Law Journal (1993) Vol.12:61. In protecting computer networks, it is important to understand exactly what is being sought to be protected. Is it simply hostile presence in the network which is the reason for protection, or the fear of privacy infringements and the loss of information exclusivity. When an intruder trespasses through our home, is it the fact that he or she is in our home which is our concern, or the fear of what he or she may find or take away? As noted in the case of R. v. Plant (supra note 112), per McLachlin J. at 303-304, “Computers may and should be private places, where information they contain is subject to the legal protection arising from a reasonable expectation of privacy. Computers may contain a wealth of personal information. Depending on its character, that information may be as private as any found in a dwelling house or hotel room”. See infra note 521.

\(^{431}\)In England however, a bifurcated approach is taken. Under the Computer Misuse Act (U.K.), 1990, s.1(1) creates an initial offence where unauthorised access to a computer system is affected, and s.2(1) creates a second tier “ulterior motive offence” with more severe penalties, where access is perpetrated for the purposes of committing a further misdeed such as data manipulation or erasure (see also the English Law Commission (U.K.), Working Paper No. 110: Computer Misuse (London: HMSO, 1988)). Conversely, it is also interesting to note that Massachusetts has, so far, not enacted any computer specific legislation, because it believes traditional law will be adequate for protecting computer networks and the information which they contain. See E.F. Patch, “Addressing Computer Crime in Massachusetts: The Problems with Comprehensive New Criminal Statutes - The Advantages to a Multifaceted Approach”, New England Law Review (1985-1986) Vol.21(4):759. See also, B.J. George Jr., “Contemporary Legislation Governing Computer Crimes”, Criminal Law Bulletin (1985) Vol.21:389.
be used as the pathway to obtaining unauthorised access; and, (6) Section 342.1(1)(c) prohibits even the attempt to effect entry, either directly or indirectly432.

Although it is important to note that these protective shields are in place primarily to prevent computer crime433, it is clear that they also provide exceptional protection for computer stored information. Indeed, the disadvantage of not protecting information directly is more than outweighed by the advantages gained in not upsetting the balance or getting embroiled in debates regarding the protection of information in general434.

432The situation is analogous to the protection of a castle strongbox in medieval times. The strongbox, which contained the castle treasure, and which, in our case, can be regarded as the computer network containing the private information, would be kept in the “keep” of the castle behind locked doors. Surrounding the keep, would be the castle ramparts, and surrounding these, a steep slope and a moat to slow the advance of aggressors. Finally, access to the keep and strongbox would be controlled by the use of keys, and access to the castle itself would be controlled by means of the barbican, drawbridge and portcullis. See Theoretical and Practical Protections, Chapter 4, and infra note 500.


434See supra notes 152, 273-281 and 429 and infra notes 569-573 and 698-703.
CHAPTER 4

A PRACTICAL APPROACH

A. THE INADEQUACY OF LAW

Throughout the course of this thesis, many legal protections used to secure private information have been discussed. Both traditional and computer-specific legal regimes were outlined, and their effectiveness analysed. In relation to traditional mediums, protections against acquisition and dissemination were discussed, and in the computer age, it was concluded that the best method of protection was a proactive one, with private information being secured through the creation of several defensive barriers which prevent and deter access.

However, it is unlikely that law alone will be adequate in protecting private information. Securing information is very different from remedying its loss, and the
nature of information\textsuperscript{435}, and the essence of privacy, mean that once exclusivity is lost, that no amount of legal compensation can make amends\textsuperscript{436}. Information is so ephemeral in value and dynamic in nature, that reactive legal suits are futile in providing any kind of solution. Information moves extremely quickly, and in comparison, legal mechanisms move extremely slowly\textsuperscript{437}. This dichotomy means that, by the time the matter gets to court, the information being fought over is usually obsolete and not worth the fight.

In addition, extreme jurisdictional difficulties arise. Once information is transmitted into or through another country or even another province, it becomes impossible to trace, protect or redeem. Legal redress may not be available in many countries through which the information passes, and even if it is, the tracking and prosecution of the perpetrators would be too physically, economically, and legally problematic\textsuperscript{438}. This transborder flow of data and the untraceable multi-jurisdictional

\textsuperscript{435}Information is capable of universal possession, and in the computer age it can be reproduced and transmitted around the world at virtually no cost. This makes it difficult to control, especially as it can exist in people’s minds in the form of knowledge, even when the “data carrier” (i.e., the paper or computer file which contains the information) is removed or re-appropriated by the owner. Once information is disseminated, its exclusivity is forever lost and can never be regained. Information is, hence, very different from tangible assets, except such things as air and fish in the ocean which are also migratory and “un-ownable”. See supra notes 96-101.

\textsuperscript{436}This is especially the case with personal information which causes embarrassment or upset, as once someone possesses the knowledge, it will be forever in their mind until they forget it through the natural course of time. The damage caused by personal information exclusivity loss is hence irreparable. See supra notes 99.

\textsuperscript{437}For a discussion of the civil and criminal remedies, see Davis and Hutchinson, supra note 55 at 127-137.

\textsuperscript{438}Consider, for example, the dissemination of sensitive and confidential national security information. It would be impossible to order a foreign power to “forget” what it had heard, both practically and legally. See supra note 435. See also “Report of the Sub-Committee on Computer Crime”, supra note 332, para.46 at 18.
routing of telecommunications\textsuperscript{439} is of key concern to all players in the information age, and as legal protection is futile, other courses of action must be taken.

**B. THEORETICAL AND PRACTICAL PROTECTIONS**

In order to secure information in the computer age, it will be necessary to apply both theoretical and practical protections. Theoretical protections refer to psychological principles which can be applied, or ideologies which can be created, to help secure information. Practical protection can be sub-divided into two categories, physical protection and electronic protection\textsuperscript{440}. The first is geared more toward the protection of an individual computer system from physical theft, and defending against "intimate"\textsuperscript{441} access on "stand-alone"\textsuperscript{442} machines; and the second is geared more toward the protection of computer networks and defending against remote access. Of course, physical and electronic protections will overlap in many instances, because electronic

\textsuperscript{439}By which I am referring to the packet-switching of information, such as on the Internet. Such technology routes "packeted-information" around the globe randomly, and one unit of data could be split up and sent through many different jurisdictions. This causes immense problems for regulation, especially with regards to such things as encryption technologies (see infra note 629). See especially, Asynchronous Transfer Mode (ATM) technology, Steinberg, supra note 323, Werbach, supra note 359 at 17-18, and Vargo and Hunt, supra note 382 at 439-442.

\textsuperscript{440}Technology can be used to protect information, just as it can be used to unlawfully intercept and acquire it. See Cross, supra note 21 at 527-529.

\textsuperscript{441}By which I mean actual access to the computer system through the use of the keyboard or other direct interface attached to the individual machine, or access to the network from an "inside" connection.

\textsuperscript{442}These are computer systems which are not attached to a network, with the only way of accessing the system being through the physical access of the system through "intimate" interface (ibid.).
protections can be used to physically safeguard machine access, and physical protections can be used to secure electronic access.

In discussing these protection techniques, a Situational Crime Prevention (SCP) framework can be applied. SCP arose as a criminological theory in the late 1960s and early 1970s, stimulated by research conducted at the British Home Office. The basic premise of the theory is that the intensity and severity of crime can be reduced through manipulating the situation in which the crime occurs. SCP measures are very specific in scope and application, and generally either seek to eliminate crime in an extremely localised area, such as an apartment building, or an individual street; or to eliminate one very specific sub-category of crime, such as public telephone box vandalism, or transit robbery.

---

445 See infra note 469.
446 Neighbourhoods can also be protected by employing SCP measures however. See Natural Surveillance section, below.
447 See infra note 459.
448 See infra note 554.
To elaborate, Clarke\textsuperscript{449} outlined SCP as, "comprising measures directed at highly specific forms of crime that involve the management, design, or manipulation of the immediate environment in as systematic and permanent a way as possible so as to reduce the possibilities for crime and increase its risks as perceived by a wide range of offenders"\textsuperscript{450}. Murray\textsuperscript{451} expressed the goals of SCP as, "simply to reduce the opportunities for crime by increasing the effort that the offender must invest, increasing the risks he must take, and reducing the rewards"\textsuperscript{452}. It should be noted that SCP does not simply relate to the manipulation of the physical environment, but includes the control of any factors relevant to the situation of a crime. These are discussed in greater depth below, but influencing the psyche or "mind-set" of the potential malefactor is one important measure, as is the awareness of potential victims\textsuperscript{453}.

In the computer sphere, SCP can be used to manipulate the virtual environment to deter criminal activity, with psychological principles being used to intimidate potential

\textsuperscript{452}Ibid., at 358.
\textsuperscript{453}SCP also requires an evaluation of other factors, many of which cannot be controlled. Such as time of day, weather, and the number of people in the vicinity. This last factor, although largely dependent on the time of day can be influenced by physical planning, and the incorporation of night-time facilities into daytime regions, i.e., placing cinemas and restaurants near office blocks and housing. See J. Jacobs, The Death and Life of Great American Cities (New York: Random House, 1961). See also Natural Surveillance section, below.
offenders, and awareness of computer security being raised in the minds of potential victims.

*The Twelve Techniques of Situational Crime Prevention*

In looking at the actual practical and psychological defences which SCP can provide, twelve “opportunity reducing techniques” can be highlighted, and these can be separated into three sub-categories:

**Table 1: The Twelve Techniques of Situational Crime Prevention**

<table>
<thead>
<tr>
<th>A. Increasing the Effort</th>
<th>B. Increasing the Risks</th>
<th>C. Reducing the Reward</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Target Hardening</td>
<td>5. Entry/Exit Screening</td>
<td>9. Target Removal</td>
</tr>
</tbody>
</table>

---

454 Table adapted from R.V. Clarke, *Situational Crime Prevention: Successful Case Studies* (Albany: Harrow and Heston, 1992). Category 7, “Employee Surveillance”, was originally entitled “Surveillance by Employees”. It has been altered in this context to cover a broader field of protections. See Employee Surveillance section, below.
Each technique protects computer systems and networks in different ways, and these will be addressed in turn. Before we begin, it should be noted that many of these techniques focus specifically on the security of computer networks, which are more likely to be used by commercial enterprises and government agencies than by individuals. At first glance, this would seem to shift the focus away from individual privacy and on to the protection of business data and state information. However, as discussed in previous chapters, much personal information is held by commercial enterprises and government agencies, and this information will be stored and transmitted over public and private networks. Therefore, the security of computer networks is equally as important for the protection of privacy and information exclusivity, as is the security of “stand-alone” computer systems. In any event, it should be borne in mind that the protection of privacy is only being used as an example of private information security, and general matters of commercial and state information protection are not exempt from discussion.

A. Increasing the Effort

1. Target Hardening

As the title suggests, this technique involves hardening the target to make it more difficult for perpetrators to succeed in committing the intended offence. In the tangible world, this includes the erection of physical barriers and the use of defensive mechanisms
which obstruct the malefactor from accomplishing their goal. Examples include the use of steering locks\textsuperscript{455}, safes, toughened glass bandit screens in post offices\textsuperscript{456}, banks\textsuperscript{457}, taxis, and buses\textsuperscript{458}, and the use of reinforced doors, locks\textsuperscript{459} and other materials in general.

This is the oldest and most obvious of the twelve SCP techniques, and many of the "real-world" examples are also of application in the protection of information in the computer age. Intimate access to computer systems, especially stand-alone units, can also be prevented by reinforcing doors and locks, and by installing physical, electronic and biometric "locks" on the computer itself. These measures would prevent both unauthorised access to private information, and the physical removal of the information through the taking of the computer\textsuperscript{460}.

The same techniques can be employed in relation to network target hardening, where the modems, servers, bridges, switches, and wiring can all be locked away\textsuperscript{461}. In addition, the difficulty and detectability of wire-tapping can be increased through the use

\begin{thebibliography}{9}
\end{thebibliography}
of fibre-optic cable or double-walled conduits containing pressurised gas. Also, all network cabling and electronic devices, including VDUs, emit electromagnetic radiation either through conduction or radiation, and this can be "picked up" or captured by relatively simple scanning and eavesdropping equipment. In order to prevent computer data from being acquired during use or transmission either between networks or inside a network, it is necessary to carefully place network cabling so that its broadcasting effect is minimised. Cables should be physically and electronically shielded to prevent this kind of eavesdropping, and the TEMPEST electromagnetic emanation standards should be strictly adhered to. VDUs should also be physically screened to prevent direct optical surveillance.

---

461 Vargo and Hunt, supra note 382 at 406.
462 Davis and Hutchinson, supra note 55 at 121.
463 An abbreviation for Visual Display Units, used to avoid confusion between scanners which can monitor information, and VDUs which display it.
464 The Dutch scientist Win van Eck, conducted an experiment in 1985 to show how easy it was to monitor computer emanations. With relatively simple and inexpensive equipment, he was able to read information from VDUs from up to three miles away, and even select which VDU to read in a crowded office environment containing many computer screens. See I. Beale, “Computer Eavesdropping - Fact or Fantasy”, (1988) 3 EDP Auditor J. 39 (taken from Davis and Hutchinson, supra 55 at 119-121). See also infra note 467.
465 For example, if cabling is in contact with water or gas pipes, the conduction will be increased, rendering network data more susceptible to detection and interception. See Potts, “Emissions Security”, Computer Law and Security, Vol.3 (1988) 27, at 41.
466 For example, if cabling is laid in certain formations, it can act like a giant antenna, transmitting data over great distances and strengthening any signal which may be captured. Ibid.
467 TEMPEST is an abbreviation for Transient Electromagnetic Pulse Emanation Standard. Developed in the 1980s, this standard rates the susceptibility of computer equipment to monitoring. Digital transmissions and processing emanations are even easier to isolate and reconstruct than analogue communications. See C.J. Selim, Eavesdropping on the Electromagnetic Emanations of Digital Equipment (1990) <cjs@curu.curu.edu>.
Many other target hardening techniques also exist in the computer age, including the use of complex passwording, user identification and authentication, and encryption and firewalling. However, the nature of these protections means that they are more appropriately discussed under later headings\(^468\).

2. Access Control

This technique refers to controlling the access of persons to certain buildings or areas, or facilities within that building or area. More specifically, in the tangible world, this technique aims to exclude potential offenders from the physical location in which an offence could be committed. Examples include fenced yards, parking lot barriers, entry phones\(^469\), identification badges, personal identification numbers (PINs) and coded entry doors, all of which prevent trespassing and keep criminals away from property which could be stolen. Indeed, examples of access control go back to medieval times, where castles were protected through the use of portcullises, drawbridges, and moats\(^470\). Although the overlap between “Access Control” and “Target Hardening” is clear to see, in the computer sphere, access control is geared more towards preventing access to

\(^{468}\) Passwording will be discussed under Access Control, Identification and Authentication under Access Control, Entry/Exit Screening and Employee Surveillance, Encryption under Target Removal, and Firewalling under Entry/Exit Screening.


\(^{470}\) Clarke, supra note 444 at 110. See also the analogy, supra note 432.
certain files and data stored within computer systems, than it is with preventing physical access to the computer terminal or storage medium.

The four key goals of network security and access control are outlined by Vargo and Hunt\(^{471}\) as consisting of four components:

(1) \[\text{To}\] maintain the confidentiality of data as they are stored, processed, or transmitted;

(2) \[\text{To}\] maintain the integrity of data as they are stored, processed, or transmitted;

(3) \[\text{To}\] maintain the availability of stored data, and;

(4) \[\text{To}\] ensure the identity of the sender and the receiver of a communication. \(^{472}\)

Slavik and Peters\(^{473}\) describe good computer security as being:

Like a lock on your computer system. It is designed to admit everyone you designate, with a minimum of complications, and exclude everyone else. Computer system security is no more than a dynamic delaying technique. It cannot keep all intruders out forever, but it can make breaking in difficult and time-consuming enough that potential invaders are motivated to look elsewhere. \(^{474}\)

\(^{471}\)\textit{Supra} note 382.
\(^{472}\)\textit{Ibid.}, at 404.
\(^{473}\)\textit{Supra} note 412.
\(^{474}\)\textit{Ibid.}, at 80.
The most important method of access control in the computer realm is passwording. Passwords\textsuperscript{475} or “pass-phrases” only allow those persons who know the code to access a computer system, or certain protected files within that system. They prevent unauthorised “network trespassers” from accessing data, and in this way provide an extremely simple and effective way of protecting private information, both from intimate and remote access. Unfortunately, simple passwords can be easily guessed, acquired or otherwise by-passed. Studies show that many people use passwords which are easy to remember, and consequently, easy to guess. Examples include family and pet names, dates of birth and even the term “password” itself. Widely available computer programmes exist which can “crack” passwords\textsuperscript{476}, or enter every recognisable word in the English language in a few minutes\textsuperscript{477}. This means that any password consisting of any English word, name or geographical location would provide absolutely no security\textsuperscript{478}. However, the success of these hacking techniques can be significantly reduced by changing the login attempt rate, or instituting a user lock-out or system shut-down protocol if more than a specified number of unsuccessful attempts are made.


\textsuperscript{477}This is presumably the case for any language other than English. Science fiction passwords such as “Skywalker”, “Spock”, “Bilbo”, etc., should also be avoided, as these are frequent target words for hackers. See Slavik and Peters, supra note 412 at 84.

\textsuperscript{478}Most passwords are based on the user identification, or some variation of the user or login name. Vargo and Hunt, supra note 382 at 410, suggest upto 30%. Indeed, dictionary attacks are very successful,
It should also be noted that even non-sensical letter chains can be broken in seconds. For example, a three letter character chain, consisting of any of the 26 letters of the alphabet\textsuperscript{479} can be cracked in two seconds, with a four letter chain being broken in one minute, a six letter chain in nine hours and a seven letter chain in nine days\textsuperscript{480}. To this end, it has been advised that any password should consist of at least a six length key chain, utilising any of the 256 ASCII characters available on a standard computer keyboard. A random, non-sensical character chain consisting of numbers, upper and lower case letters, and special characters should be created, for example, “M%3jK&”. Proactive programmes exist which will enforce the creation of such a password\textsuperscript{481}, and a character chain of this length and format would take 891 years to crack, and a ten key length chain of this nature would take 8,308,861,211 centuries to break\textsuperscript{482}.

In addition, surreptitious computer programmes exist, called “spoofs”\textsuperscript{483}, which hoodwink authorised users into entering their passwords into an artificial login procedure, which instead of granting access to the computer system, records and transmits the

\textsuperscript{479}This is based on lower case letters only. To include upper case letters in the combination would greatly increase the number of permutations, and would, hence, increase the time required to crack a password.


\textsuperscript{481}Such as “PASSWD”, available on the Internet from \texttt{<http://www.dartmouth.edu>}.  

\textsuperscript{482}Supra note 480.

password to a potential hacker for later use in attempting unauthorised access. Spoofs which imitate other computer servers can also be used, and make it appear that a request for access has come from a legitimate sub-system or server, when in fact an unauthorised system is making the request. However, spoofs can be defeated through the use of message authentication or non-repudiation programmes, which allow the user to determine, "(1) whether a received message is identical to the one transmitted from the origin, (2) if errors were introduced by accident or design, and (3) that no messages have disappeared and no new ones have been introduced." Protection against the use of "spoofed" passwords can also be achieved through the use of date/time stamps, message authentication codes and real-time verification mechanisms.

The vulnerability of standard password systems has led to a shift towards more complex validation procedures. The use of biometric identification and token authentication is now becoming widespread, and in conjunction with traditional password protections, these techniques should offer extremely high levels of security. Biometric

---

484 This is referred to as "IP Spoofing". See Vargo and Hunt, supra note 382 at 411.
485 Ibid., at 410.
486 Ibid., at 411. See also, supra note 483.
487 This is especially the case if biometric identification, through its authentication process, can determine the immediacy of the sample, or the "life" of the scanned anatomical part. For example, breath or blood could be used to determine identity, and these could be tested for "freshness", to ensure that the sample came from the authorised individual and was not a bottled sample which could be used by an interloper. Testing for the "life" of an anatomical part, such as an eye or finger in retinal scans and fingerprint authentication would negate the possibility of an artificial finger or retinal print being used, and would also prevent access being achieved through the maiming or murder of the authorised user to acquire the relevant body part for use against the biometric scan. Of course, even with these safeguards, the authorised user could still be forced, under duress, to access the system (see infra notes 662 and 687). In addition, unauthorised access could still be achieved through tampering with the files which contain the cross-referencing data. For example, the retinal scan contained in the authentication database as belonging to a
identification consists of determining the identity of an individual by measuring and assessing his or her unique physical characteristics, including, analysing keystroke timing patterns to determine the user\textsuperscript{488}, and the use of fingerprint recognition, retinal scans, or digital signatures. Token authentication involves the authorised user carrying a device which verifies his or her identity\textsuperscript{489}, including, magnetic swipe cards, smart cards, and active badge readers\textsuperscript{490}. It should be noted, however, that token authentication also possesses a serious weakness. Namely, that the token can be stolen\textsuperscript{491}. In this light, a combination of password, biometric, and token access systems should be utilised\textsuperscript{492}.

\textsuperscript{488}Interesting privacy issues arise here, as the individual would be under constant supervision because everything they typed would be under observation. See infra note 565.

\textsuperscript{489}Token authenticators are used instead of conventional physical and software-controlled locks on hardware connectors or interface cables. The detection of a token is what enables access. See Vargo and Hunt, supra note 382 at 411. and infra note 490.

\textsuperscript{490}Ibid., "Active badge readers operate by use of an infrared transmitter and receiver that operate from the wearer's badge (or pager) and the workstation. Encrypted challenge/responses are handed between the two. Active badge systems have other advantages as well. They can provide hands-free access through security doors, activate secure printing [or faxing] only when the wearer is near the printer, provide a link to the UNIX finger command to assist with an individual's location, provide workstation lockout when the wearer leaves the room, and assist in the general location of personnel in or around a building".

Although Vargo and Hunt note the advantages of active badge systems in assisting in the location of personnel in a building, it should be understood that this could infringe employee privacy in the workplace. See infra notes 565, 619 and 620.

\textsuperscript{491}For example, a library card or driving licence which does not possess a photograph, can be stolen and used by anybody, and can in no way authenticate a person's identity.

\textsuperscript{492}According to the U.S. National Security Agency and National Computer Security Center (B. Keller, INFOSEC Awareness Division, Attn: X711/IOAC, and the NSA “Red Book”, “Orange Book” and “Green Book”, Security Directives), there are three classifications of authentication: “Authentication by Knowledge”, “Authentication by Ownership” and “Authentication by Characteristic”. Simply put, authentication by something known, by something held, or by something that we are. The implementation of security measures, which require at least two forms of authentication, and preferably all three, will provide extremely high levels of protection. A common example of a security measure which requires two forms of authentication, is the Automated Teller Machine (ATM) bank-card. When withdrawing money from an ATM, the card must be inserted into the machine and a password entered. This involves both “Authentication by Knowledge” and “Authentication by Ownership”. See also Simonds, supra note 475 at 86-87.
Indeed, passwords which activate tokens, or tokens which are necessary to activate the password "login" procedure are likely to be extremely effective\textsuperscript{493}.

An advanced access control measure is the "Kerberos Security Access Server"\textsuperscript{494}, which adds an additional level of security to those offered by passwords and other access control systems. "Kerberos" validates each user for each application, and relies on three components to watch over network security\textsuperscript{495}: a database, an authentication server, and a ticket-granting server. The actual operations of this system are extremely complex, but briefly, a request is made by the user to access an application, and the user’s credentials are authenticated by the Kerberos database. Then, a doubly-encrypted ticket is issued, which is valid for only a short time, and this ticket is then decrypted by the user’s password which allows access to the application server\textsuperscript{496}. As the ticket is time restricted and the password is never transmitted, hackers do not have any opportunity to acquire anything of use, even if they do intercept Kerberos communications or acquire a Kerberos ticket.

\textsuperscript{493}This is the approach taken by the Racal "DynPass" and the Guardata "WatchWord II Token". token authentication systems. A channel is opened by the token, for a short period of time, ranging from seconds to minutes, and this channel allows the wearer to enter a password. If the correct password is inputted then access is granted, and if the incorrect password is entered, the token closes the channel so that subsequent attempts cannot be made. See Vargo and Hunt, supra note 382 at 411.


\textsuperscript{495}Kerberos is the three-headed watchdog which guards the gates of Hades in Greek Mythology. The Access Server was named as such because it has three heads of attack, a database, an authentication server and a ticket-granting server (see text).

\textsuperscript{496}See Vargo, supra note 382 at 412-413, for a detailed explanation of how the Kerberos system works.
However, it must be borne in mind that system security is an equilibrium between security and usability. As Vargo and Hunt note, "The most secure system is unusable, and the most useable system is insecure". As such, the appropriate level of security must be balanced against efficiency, which will involve detailed risk assessment calculations based on vulnerability and level of risk. It is, however, probably more effective to invoke a "layered" security environment with the most important files and applications at the centre of the security process, with less crucial data being stored on the periphery. A problem-oriented policing approach should also be adopted, with the most highly targeted servers, information files and access points being the most heavily protected. In addition, it should be noted that maintenance port and "back door" access refers to access protocols which do not require user identification or authentication.

---

497 Ibid., at 403.
498 Ibid., at 403.
499 Ibid., at 421-425.
500 Simonds, supra note 475 at 131, outlines a "Perimeter Approach to Security and Access Control". The first level of defence is "Security by Obscurity"; second, "Physical Security"; third, "Workstation Access Control"; fourth, "Network Access Control"; and fifth, "Application and File Restrictions". All of these levels of defence are geared around protecting sensitive applications and files. As P.G. Neumann, "Computer Insecurity Issues", Science and Technology, Fall 1994, 50, at 50, notes, "Each element in the 'network of networks' requires appropriate levels of password protection, tiered, partitioned access according to the sensitivity of files, and rigorously enforced operating procedures and physical controls". See Royal Canadian Mounted Police, Small Systems Security Guidelines (Ottawa: Supply and Services Canada, 1982). See also A Proactive Approach to Protecting Information section, Chapter 3, and supra note 432.
502 Supra note 500.
503 Unaltered system defaults frequently lead to this kind of security breach.
504 "Back door" access refers to access protocols which do not require user identification or authentication.
access should also be restricted if access control is to be adequately secured\textsuperscript{505}. Also, employee access to on-line files and services should be structured, with employee lists and system privileges being regularly reviewed and updated\textsuperscript{506}. Other access control measures will be discussed under “Entry/Exit Control”.

3. \textit{Deflecting Offenders}

This technique refers to the manipulation of the physical environment, the channelling of behaviour, and controlling circumstances in order to avoid situations where crimes are likely to occur, or where the effects of a crime are likely to be exacerbated. In the tangible world, examples include decreasing the density of taverns to avoid drunken conflicts and assaults\textsuperscript{507}, swiftly dissipating football crowds to avoid hooligans\textsuperscript{508}, and reducing overcrowding in shopping malls to reduce the likelihood of pick-pocketing\textsuperscript{509}.

In the computer sphere, this technique is relatively hard to employ, as it would be meaningless to virtually re-address a server, and physical relocation would achieve

\footnotesize{\textsuperscript{505}Davis and Hutchinson, \textit{supra} note 55 at 95.}
\footnotesize{\textsuperscript{506}Ibid.}
\footnotesize{\textsuperscript{507}T. Hope, \textit{Implementing Crime Prevention Measures}. Home Office Research Study No.86 (London: HMSO, 1985).}
\footnotesize{\textsuperscript{508}Clarke, \textit{supra} note 450.}
nothing in the networked world. Indeed, a consistent physical and virtual IP address is desirable in the commercial world to increase trade and create a conception of reliability, faith and dependency. A reduction in traffic, or the dispersal of computer systems and network connections would also be counter-productive as networking costs would increase and outside connections would be harder to police and protect.

Indeed, the only useful applications of this particular SCP technique would be in the removal or closure of web-sites which post acquired passwords for other hackers to use, or the actual removal and off-line storage of vital information and computer data. Of course, this last measure would cause great inconvenience and negate the purpose for using a computer system and network in the first place. This matter will be discussed in more depth under the category of “Target Removal”.

4. Controlling Facilitators

This technique refers to the physical control or removal of items which will reduce the incidence and severity of crime. In the tangible world, examples include the provision of plastic instead of glass containers in bars to prevent serious injury occurring from drunken brawls510, “Caller ID” to reduce the number of obscene telephone calls511,
and breathalyser ignition control systems built into the cars of recidivist drunk drivers\textsuperscript{512}. Indeed, controlling facilitators is also a measure of some vintage, and examples stretch back to the days of the "Wild West", where patrons of a bar would be required to check in their weapons to avoid the potentially fatal consequences of an intoxicated conflict\textsuperscript{513}.

It is important to note, however, that facilitators usually consist of items which are in common and lawful everyday use, such as automobiles, alcohol, and telephones, but which under certain circumstances can be used to commit, facilitate or increase the severity of a criminal act. For example, automobiles can be used in bank-robbery "getaways" or driven by drunk drivers; telephones, in certain areas, can be used for drug-dealing; and, alcohol, which disinhibits many potential offenders, facilitates the commission of many offences.

In the computer sphere, facilitator control can be used to ensure privacy and secure private information in a number of ways. Many of these measures were covered in the previous chapter, where the legal prohibitions against using or possessing scanners,
and other eavesdropping and interception equipment was discussed\textsuperscript{514}. It was noted that such prohibitions create an additional defensive shield against unauthorised access, and that metaphorically speaking, this prevents the criminal not only from entering through the door, but also from walking up the garden path\textsuperscript{515}. However, the focus of this chapter is upon the inadequacy of law, and indeed if facilitators such as scanners are to be adequately controlled and information successfully protected, much more than law would be required. Extremely strict controls, or even bans on the import, use, and manufacture of all eavesdropping devices would be required, with the confiscation of all infringing products. Of course, this too involves the application and administration of law, but at a far more proactive level\textsuperscript{516}.

\textbf{B. Increasing the Risks}

\textbf{5. Entry/Exit Screening}

This technique refers to the detection of the entry of intruders or malefactors, or the exit of escapees and other wrongdoers. This measure differs from “Access Control”, \textit{“in that the purpose [of entry/exit screening] is less to exclude potential offenders than to increase the risk of detecting those who are not in conformity with entry...”\textsuperscript{517}}

\textsuperscript{514}Sections 327 and 342.1(1)(d) of the \textit{Criminal Code}, and the \textit{Possession of a Device to Obtain Computer Services} offence. See the \textit{Theft of Telecommunications} and \textit{Computer Specific Protections} sections, \textit{Chapter 3}.

\textsuperscript{515}See \textit{Analysis} section, \textit{Chapter 3}.
Examples include the use of baggage and passenger screening at airports to reduce the number of successful hijacking attempts, the use of electronic book detection screens in libraries to prevent book theft, and the installation of automatic ticket barriers to avoid fare evasion. All of these measures allow persons in conformity with entry and exit requirements to pass relatively unhindered, whilst preventing the passage of those who are in violation of the requirements.

In the computer sphere, this method of screening can be used to determine valid requests for service from those which are invalid or unauthorised. Just as passwording prevents unauthorised access, other techniques, systems, and devices exist which permit certain activities whilst prohibiting others. Screening is necessary because many people access the computer systems of other individuals and organisations for a variety of legitimate purposes every day, and it is essential that these activities continue unhindered: Internet web-sites are frequently accessed to obtain information, e-mails are transmitted, and electronic transactions take place. All these functions require free and easy external access to company computer systems, and the existence of blanket access control

---

516 *Ibid.* See also *Concluding Thoughts* section, *Conclusion.*
517 Clarke, supra note 444 at 113.
protocols which would prohibit all access to a company's computer system would be undesirable and counter-productive, if not economically damaging.

The difficulty is that, once access is gained to these legitimate services, they can be used as platforms for accessing unauthorised areas of the system. Indeed, the mere existence of the network connection means that it can be used to effect entry into prohibited areas. For example, a bank computer system can be accessed to conduct on-line banking, transfer electronic funds or perform a variety of transactions. However, it is crucial for the bank that access to this area of the system does not permit access to bank accounts, reserve funds, or confidential information. In receiving e-mail, it is important that the addressee's e-mail account not be vulnerable to perusal by the sender, and in allowing Internet access it is important that outsiders not be able to access a company's private files and resources, as this would lead to serious economic and competitive losses. Indeed, the situation is akin to inviting someone into your home, as Clarke notes, "You might invite me into your living room, but not into your bedroom"\textsuperscript{521}.

The most effective way to confine authorised external access only to legitimate areas of a system, and to ensure that all requests for service are authentic, is through the use of "firewalls"\textsuperscript{522}. Vargo and Hunt define a firewall as, "a dedicated gateway machine

\textsuperscript{521}Clarke, supra note 444 at 107. See also supra note 430.
\textsuperscript{522}Additional protections include the use of Address Filtering, which allows routers to control remote logins, file transfers, and other activities; Application Layer Security, which can operate user/host authentication, organisation identification, and IP packet encryption, and; Emergency Disconnection,
with special security precautions used to provide security from outside network connections and dial-in lines. The idea is to protect a cluster of more loosely administered machines hidden behind it from intruders"\(^{523}\).

A firewall\(^{524}\) is a small, closely guarded portal which, by forcing all incoming and outgoing traffic to pass through it, allows for the easy detection of unauthorised transmissions. As the traffic passes through, it is screened for its validity and authenticity, and if successful, the packet of data scanned will be allowed to proceed to another sub-network server, or to the outside world, depending on the direction of the transmission. Without a firewall, the entire LAN\(^{525}\) would be vulnerable to Internet users. The firewall limits contact with outside networks, and decreases the "zone of risk" which exists where the LAN interfaces with the Internet\(^{526}\).

Many varieties of firewall exist\(^{527}\), but their application generally takes one of two forms; either they prohibit access to all services which are not explicitly permitted, or

\(^{523}\)Defined by Vargo and Hunt, supra note 382 at 117.

\(^{524}\)Which can consist of software and hardware, or software alone.

\(^{525}\)Local Area Network.

\(^{526}\)See Vargo and Hunt, supra note 382 at 117.

\(^{527}\)See Simonds, supra note 475 at 215-268. Firewalls come in many varieties: Packet-Filtering, Application and Circuit-Level Firewalls; Bastion Host, Screened-Host, Screened-Subnet, Proxy, Dual-Homed and Hybrid Gateways, and; Screening and Dial-Up Screening Routers.
permit access to all servers unless expressly prohibited\textsuperscript{528}. One of the "strongest" varieties is the "bastion host", otherwise known as a "proxy gateway" or "application-level gateway". The bastion host is akin to a public space within a private building, and is a virtual area on the periphery of a LAN which is predominantly used to allow Internet access, whilst preventing further access into the private network; the problem discussed above. Interestingly, just as the use of drawbridges, moats, and portcullises were discussed as examples of medieval access control techniques, another castle defence is analogous to entry/exit screening and firewalls. This was the "barbican", a small area just inside the castle walls which acted as an "air lock" between the interior of the fortress and the outer world\textsuperscript{529}. Similar, in effect, to modern day penitentiary entry/exit systems, visitors and patrons were screened for the validity of their passage before any damage or loss could be inflicted\textsuperscript{530}.

A related protection measure, which can be employed, is "router filtering". This method of protection acts as a reception for incoming service requests and as a forwarder for outgoing data transmissions\textsuperscript{531}. The router filter, often referred to as a "screening router", is a router or hub on the boundary of the private network which lies between the internal LAN and the public network. Routers operate similar to baggage scanners at airports, except that data packets can be screened not only for their content, but also for

\textsuperscript{528}Vargo and Hunt, supra note 382 at 117.
\textsuperscript{529}An example of a barbican still exists in the Ancient City of York, in England.
\textsuperscript{530}In addition, if any malefactor was caught in the barbican, they were trapped and were, hence, easy to dispatch.
their source, destination, and service type. Their operation is very similar to the bastion host variety of firewall outlined above, except that routers of this nature divert all incoming and outgoing traffic through security procedures such as firewalls, rather than acting as firewalls themselves. Routers can also be used to prevent all dangerous activities, such as remote printing or file transfers, altogether. In addition, requests from unknown or unexpected servers and devices can be ignored or disconnected. In this way, information security is enhanced, because any communication received from an unrecognised or unauthenticated source will not be accepted, and any outgoing information destined for such a source will be captured and prevented from release.

In performing this dual entry and exit screening role, private information is doubly protected. A strong deterrent effect is also created, because would-be intruders can be traced through their IP address, and the fear of such detection should reduce the confidence, determination, and success of hackers who wish to gain access to the system.

It should also be noted that protection can be increased through the use of many firewalls and routers placed at key points within the private network. In this way, even if periphery access is effected, the damage will be limited to a small area, and key information files

---

531 The best routers support packet-filtering at the host, network and service (protocol) levels.
532 See Vargo and Hunt, supra note 382 at 118.
533 Ibid., at 408-409.
534 A dual-role bastion host such as this is known as a "hybrid gateway". Another method of firewalling is to install two network boards on a computer, one for LAN access and the other for Internet access. This is known as a "dual-homed gateway", and in this way the computer controls any connection between the private internal, and public external networks. See Simonds, supra note 475 at 222.
and applications will remain secure.\textsuperscript{535} Such precautions will also help defend against employee discrepancies, as discussed under the "Employee Surveillance" category below. In addition, screening routers and bastion hosts\textsuperscript{536} should be used in conjunction with one another to enhance network security, and increase the protection of private information.

6. \textit{Formal Surveillance}

This technique refers to surveillance by state officials and private personnel who are employed specifically to conduct surveillance, and provide a deterrent through their presence. Examples include police officers\textsuperscript{537}, security guards\textsuperscript{538}, and store detectives, and electronic counter-measures such as intruder alarms, "red light" and speed cameras\textsuperscript{539}, and closed-circuit television (CCTV)\textsuperscript{540}. In the computer sphere, this technique involves the employment of computer security personnel, whose specific function is to monitor and audit system security, to control password distribution and

\textsuperscript{535}A "layered" approach to security should be adopted. See Simonds, \textit{supra} note 475 at 131, \textit{Access Control} section, above, \textit{A Proactive Approach to Protecting Information section, Chapter 3}, and \textit{supra} notes 432 and 500.

\textsuperscript{536}When these applications are used in conjunction with one another, the device becomes known as a "Screened-host gateway".


system access privileges, and to prevent and detect unauthorised access and use\textsuperscript{541}. System security does not necessarily have to be carried out “in-house”, and can be contracted out to a third party, or carried out remotely by a network service provider\textsuperscript{542}. In addition, many automatic security and audit functions can be installed on computer networks which enable the computer to police itself. Also, many computer programs exist which facilitate system administration and remote server auditing by human actors\textsuperscript{543} including, SATAN\textsuperscript{544}, COPS\textsuperscript{545}, Tripwire\textsuperscript{546}, NADIR\textsuperscript{547}, DIDS\textsuperscript{548}, NSM\textsuperscript{549}, ISOA\textsuperscript{550} and IDES\textsuperscript{551}.

\textsuperscript{541}Such as audit trail analysis, including manual review, statistical and expert system analysis; command and object monitoring, including biometrics and system activity; and, network monitoring, which includes the utilisation of products and devices as SATAN (see infra note 543).

\textsuperscript{542}Predominantly, Internet Service Providers (ISPs).

\textsuperscript{543}In addition, many government and commercial computer security agencies exist, including, in Canada, the Security Evaluation and Inspection Team (SEIT); in New Zealand, Catalyst (the Government Communications Security Bureau); and in the U.S., the Computer Emergency Response Team (CERT, <ftp://info.cert.org>), the National Computer Security Association (NCSA), Computer Incident Advisory Capability (CIAC, <ftp://ciac.llnl.gov.pub.ciac>), and the Forum of Incident Response and Security Teams (FIRST). Other risk-analysis and network security agencies include the Central Computer and Telecommunications Agency Risk Analysis and Management Methodology (CRAMM), and the Los Alamos Vulnerability and Risk Assessment Methodology (LAVA).

\textsuperscript{544}Security Administrator Tool for Analysing Networks.

\textsuperscript{545}Computerised Orical and Password System.

\textsuperscript{546}A utility program for checking integrity on UNIX systems.

\textsuperscript{547}Network Anomaly Detection and Intrusion Reporter.

\textsuperscript{548}Distributed Intrusion Detection System.

\textsuperscript{549}Network Security Monitor.

\textsuperscript{550}Information Security Officer's Assistant.

\textsuperscript{551}Intrusion Detection Expert System.
7. **Employee Surveillance**

This technique refers to surveillance which is provided by employees as a secondary function of their job. Many employees, including receptionists, parking lot attendants, hotel and apartment block doormen\textsuperscript{552}, train and bus conductors\textsuperscript{553}, and shop assistants are in a position to conduct surveillance through the natural course of their work. Employee surveillance also covers such things as the location of payphones in places where they are under "subconscious" supervision. For example, public telephones placed in bars, shopping malls, and railway stations generally suffer fewer attacks than those located in more secluded areas\textsuperscript{554} because of the aura of surveillance\textsuperscript{555}.

However, in the computer sphere, such employee surveillance is unlikely to be feasible. Although physical supervision of equipment, to prevent theft, may be possible, network surveillance could not occur naturally or as a secondary function. The only direct application of this technique in the virtual world would be the reporting of anything suspicious, untoward, or unexpected to a systems administrator.

\textsuperscript{552}I. Waller and N. Okihiro, *Burglary: The Victim and the Public* (Toronto: University of Toronto Press, 1978).


\textsuperscript{555}See Natural Surveillance section, below.
The term “employee surveillance” can be manipulated and extended beyond its original meaning, to cover another form of protection. This is surveillance of employees. Many security breaches and information exclusivity losses today occur because of employee incompetence or dishonesty. Problems arise, for example, when employees learn of their imminent termination, and as a result maliciously attempt to destroy computer files or network efficiency by introducing a Trojan horse, worm, or virus; or when they are bribed, blackmailed, or compromised by competing companies to acquire confidential information. If an employee has access to all system files and applications, then damage to the company from such activity is maximised.

The extent of this damage can be significantly reduced through the use of internal security protocols and compartmentalised operation. Firewalls can be installed between servers and different databases and applications, and data in storage can be differentially encrypted so that one “key” does not decrypt all information on the network. Managed bridges and structured cabling can be used to control access from individual hubs and servers to the private network backbone, and thus restrict traffic between different network components and user groups. Unfortunately, however, most LAN architecture

---

556Sieber, supra note 433 at 11, suggests that up to 90% of computer crime is conducted by employees. However, Davis and Hutchinson, supra note 55 at 55, note the opposite, with up to 90% of computer crime conducted by outside hackers. See supra note 332.
557See Davis, supra note 55 at 51-72.
558See Target Removal section, below. In addition, employment contracts should strictly prohibit unauthorised computer activity and threaten the prosecution of any employee who “steals”, sells, or otherwise compromises the exclusivity of company information.
559Vargo and Hunt, supra note 382 at 406.
employed at present broadcasts information to all stations on a network560, and this is catastrophic for security. "Need to know" is a fundamental principle of security, and in order for network information to be adequately protected, intelligent hubs must be used to transmit information only to the device and person to which the information is addressed561. Finally, "Closed User Groups" (CUGs) which enhance internal security by limiting application server access562, can also be used. This means that traffic is not only controlled between hubs but also between individual groups of users563. The delivery and sending addresses of each device can be checked to ensure that each request or data packet is part of the CUG, and any illegitimate packet would be rejected or disregarded. In these ways, network data-flow can be restricted so that only small amounts of information are available to employees, and hence internal security risks can be reduced to a minimum.

Another area of employee surveillance is e-mail monitoring. With the current level of technology, it is possible for company executives and system administrators to record and read employee e-mail accounts. Although this is an extremely controversial

560Ibid., at 405. This is the case with Ethernet networks. However, if they are wired in a star topography, it is possible to implement "intelligent hubbing" (see text and infra note 561).
561Ibid., at 408. If an intelligent hub is used, each computer's IP address can be checked before the data is transmitted. Technically speaking, the data is still transmitted to all computers on the network, but information sent to all terminals except the specified one will be overwritten so that the data is unintelligible.
562Ibid., at 409. For example, if there is an accounts server, a personnel server, and an inventory server, users may only be allowed access to one or two of these servers and not all three. For instance, one user may have access only to the accounts server, another only to the personnel server, and yet another to both the personnel and inventory servers, but not to the accounts server. This is what is meant by a "Closed User Group".
matters, it seems that such surveillance will be condoned, at least in the United States. E-mail monitoring would clearly be a valuable tool in the protection of private information and the maintenance of internal security. However, in permitting the circumvention of protective measures which would allow for such surveillance, security is being compromised. A “back door” is, in effect, being created, and as discussed above, would facilitate external hacking which is likely to be a much greater risk than information leaks perpetrated through e-mail transmissions.

One final protection measure, which can be discussed under this heading, is the use of incentive schemes. In relation to SCP, an incentive scheme is a method by which employees are encouraged to remain vigilant to the perpetration of crime, and are rewarded for its detection. This situation is no different with regards to computer crime, where a further psychological extension of this technique can be employed. By

563Closed User Groups also help protect the entrances to individual departments.
564E-mail surveillance constitutes a grave infringement of privacy for employees. However, employee privacy is not a focus of discussion in this thesis. See infra note 565.
565Branscomb, supra note 22 at 92-105 discusses the issue of e-mail privacy in the workplace. She notes that, in the U.S., employers do have a right to view employee e-mail due to the fact that they own the computer system on which the e-mail is written, received, or transmitted: "Michael Simmons, chief information officer at the Bank of Boston, has stated what many believe to be the correct corporate policy: 'If the corporation owns the equipment and pays for the network, that asset belongs to the company, and it has a right to look and see if people are using it for purposes other than running the business'" (Branscomb, at 100). See also W. Eckerson, "Privacy Suit Forces Users to Examine E-mail Policies: Case Against Epson Raises Troubling Questions", Network World, 17 September, 1990, 1, and Cavoukian and Tapscott, supra note 241 at 115-127. It is also interesting to note, in passing, that e-mails will not be regarded as being published, and hence are not open to libel actions. E-mails are viewed as a private communication under the U.S. federal Electronic Communication Privacy Act (U.S.) 1986, 18 U.S.C. 2511. See also, the California Penal Code, 631. See supra note 393.
566See Access Control section, above, and supra note at 504.
567Murray, supra note 451 at 360.
568Examples include such schemes and initiatives as “Crime Stoppers”.
assigning rights to information\textsuperscript{569}, and creating a royalty system for certain units of data\textsuperscript{570}, the individual would have an economic, as well as an emotional incentive, to protect their private information. Indeed, as Branscomb\textsuperscript{571} notes, "If... information has economic value, we should receive something of value in return for its use by others"\textsuperscript{572}. The fear of pecuniary loss, through free-riders\textsuperscript{573} obtaining their information, would increase the individual's level of scrutiny and vigilance over their computer network, and hence, would automatically increase the level of protection for private information\textsuperscript{574}.

8. Natural Surveillance

In the tangible world, this technique refers to surveillance performed by individuals incidentally, as they go about their everyday lives. It differs from both formal

\textsuperscript{569}Indeed, A.R. Miller ("Personal Privacy in the Computer Age: The Challenge of New Technology in an Information-oriented Society", Michigan Law Review (April 1969) 67, and A. Westin (supra note 83), suggest that the best way to solve the privacy problem may be through ascribing property rights in personal information. Miller states, at 1224-1225, that, "Perhaps the most facile approach to safeguarding privacy is the suggestion that control over personal information be considered a property right vested in the subject of the data and eligible for the full range of constitutional and legal protection that attach to property", and Westin notes at, 324-325, that, "Personal information, thought of as the right of decisions over one's private personality, should be defined as a property right with all the restraints on interference by public or private authorities and due process guarantees that our law of property has been so skillful in devising". See Branscomb, supra note 22 at 180-181. See also supra notes 152 and 273-281, and infra notes 570-573 and 698-703.


\textsuperscript{571}Supra note 22.


\textsuperscript{573}See Neumann, supra note 500 at 50-54.
and employee surveillance, because the surveillance is conducted by "passers-by", and other people who have no professional relationship with the owner of the object or building under supervision. The aim of this SCP measure is to increase the visibility of objects under surveillance without reducing their security. Examples include, pruning hedges and removing high walls to enhance the "observability" of property, and using internal and external lighting to raise the likelihood of criminal activity being seen. Additional measures include implementing "Neighbourhood Watch" programmes and other initiatives to increase the number of "eyes on the street".

Of more importance for our purposes, however, is the protection of smaller items such as computer terminals, printers, floppy disks, and VDUs which may all contain or

---

574 See Traditional Privacy Problems Exacerbated section, Chapter 3, and supra note 280.
575 Of course, high walls prevent access, and knocking these down may reduce the defensibility of the property, and be in direct conflict with the principles of Target Hardening and Access Control discussed above. However, these high walls could be replaced with equally high vertically barred fences, which would provide Natural Surveillance, without reducing the effects of target hardening or access control.
576 Internal lighting also creates an added deterrent effect, through the perception, true or false, that there is someone in the building. The use of automatic timers to switch lights on and off in the home to create the illusion that the house is occupied, for example, is a frequently used burglar deterrent, as is leaving lights on in shops, offices, and banks in the evening.
578 Of course, the fear of being seen in the mind of the criminal should also act as an increased deterrent. See R. D. Hunter and C. Ray Jeffery, "Preventing Convenience Store Robbery through Environmental Design", in R.V. Clarke, ed., Situational Crime Prevention: Successful Case Studies (Albany: Harrow and Heston, 1992).
display private information. Of course, increasing the visibility of these items is more likely to increase their chances of being stolen, or of information being acquired. This is especially the case with regards to computer VDUs and keyboards, because by increasing natural surveillance, information could be more easily read from the monitor, and passwords more easily obtained from observation of the keystroke sequence. In these ways, this SCP technique would not appear to be very helpful in the protection of information or computer networks.

However, natural surveillance is only one aspect of a much larger strategy known as Crime Prevention Through Environmental Design, or CPTED\textsuperscript{580}. This initiative is based in Defensible Space Theory (DST)\textsuperscript{581}, which consists of three principles including natural surveillance, “territoriality”, and “image and milieu”\textsuperscript{582}. The strategy is based on the premise that crime can be reduced by increasing natural surveillance, increasing the territoriality of a physical place, and enhancing its image and milieu\textsuperscript{583}. The most important principle with regards to protecting information and computer networks, is territoriality. By fiercely defending a system access point or gateway, or a network


\textsuperscript{582}Murray, \textit{supra} note 451 at 350-351.
connection, security can be reinforced, and information protection strengthened. These matters have already been discussed in relation to access control and entry/exit screening, where the use of passwords and firewalls were discussed.

Other ways of increasing territoriality also exist, however. For example, the boundary of the computer network can be psychologically and legally extended, so that the initial connection to the private telecommunication line at the LEC or ISP can be regarded as a trespass on company or individual property. This increases personal vigilance of the network due to the allocation of responsibility and the human instinctual desire to protect property and defend territory. If the property boundary is moved further away, the defensive reaction is invoked earlier, and this increases the protection of information. The deterrent effect will also be increased if the hacker is aware that he or she is encroaching on hostile territory or is under observation from an earlier point in time.

This was discussed in chapter three, where it was noted that the deterrent effect will increase as the chances and fear of detection and apprehension increase. Moving the boundary further away means that the real or virtual distance which must be travelled under surveillance is increased, and this not only means that the intruder has a greater

---

583 Ibid.
chance of being detected, but also that the psychological fear of being detected is increased. Combined, these factors greatly increase the deterrent effect, and should deter all but the most determined network intruders. In the physical world, this is analogous to creating a strong territorial boundary at the edge of one’s garden, because this means that a perpetrator will feel like a trespasser under observation, and be intimidated, long before he or she ever reaches your front door\textsuperscript{585}.

Finally, image and milieu. By enhancing the image and milieu of a physical place it is possible to deter intruders, and in the virtual world this means enhancing the functionality or appearance of a network. Although, at first glance, such a measure would appear ineffective, the deterrent effect can in fact be increased through enhancing the appearance and operation of a network. This is because an efficient and effective network will make perpetrators feel that they are encroaching in well organised, and hence well-protected territory. This will increase their belief that they are under observation, and that their intrusion will be detected. Thus, enhancing the image and milieu of a network will increase the psychological defence level, and reduce the number of successful system attacks.

\textsuperscript{585}As discussed above, and in the previous chapter.
C. Reducing the Rewards

9. Target Removal

This technique refers to the removal of the target of criminal activity. This can involve removing property or other items entirely, removing a component of them, or restructuring their design and use. Examples from the physical world include the removal of telephone kiosks to prevent vandalism, and the use of pre-paid phonecards to eliminate the storage of cash within the phone to prevent theft. Other examples include the removal of car radios, the use of time-locked safes, and the implementation of exact change fares on bus and transit systems.

In the computer sphere, this technique can be employed in a number of ways. Most obviously, the information itself can be removed. By storing data off-line, the incentive to break into a private network is greatly reduced, because no information can be gleaned, even if unauthorised access is effected. In addition, the information

\[ 586 \text{Markus, supra note 554.} \]
\[ 590 \text{Another technique which can be employed is the use of “ephemeral e-mail”. This is a form of electronic evaporating ink, where the e-mail erases itself from all files after a certain period of time has elapsed. See A. Cortese and K. Holland, “E-cash”, Business Week, May 29, 1995; A. Cortese and K. Holland, “What’s the Color of Cyber-money?”, Business Week, February 27, 1995; and Tapscott, supra note 16 at 281.} \]
exclusivity losses incurred through the physical taking of data\textsuperscript{591}, could be reduced by removing the hard disk and tape drives from computer systems and storing them at remote, and preferably anonymous, locations\textsuperscript{592}. This measure could be enhanced by removing floppy disks and printouts. Also, floppy drives, VDUs, CD "burners"\textsuperscript{593}, and printers could be disconnected or electronically deactivated to prevent information from being displayed, downloaded, copied, or printed. The only problem with removing information and prohibiting its acquisition in these ways, is that the entire purpose of the computer system is negated\textsuperscript{594}. Indeed, the network would be very secure, but completely unusable\textsuperscript{595}.

By far the best way of removing information, is not to remove it at all. This, at first, seems counter-intuitive, but it is possible to transmit, store and disseminate information without it being of use to anyone who might intercept or acquire it. This is through the use of encryption. Encryption removes the target, because the information which is obtained is unreadable, and hence useless\textsuperscript{596}.

\textsuperscript{591}Through breaking and entering or employee theft for example.
\textsuperscript{592}This also reduces the risk of data being destroyed by freak accidents, especially if the data is stored at more than one location. Combined with frequent “back-ups”, the remote storage of data should also reduce the risk of damage caused by viruses and other malicious data deletion programs. See J. Rothfeder, “Hacked! Are Your Company Files Safe?”, PC World, November 1996.
\textsuperscript{593}This is a device which records onto compact discs, to be compared with CD-ROM (Compact Disc - Read Only Memory) drives, which only allow data to be downloaded from compact discs, and do not permit recording.
\textsuperscript{594}See Deflecting Offenders section, above.
\textsuperscript{595}Supra note 497.
\textsuperscript{596}As Vargo and Hunt, supra note 382 at 413, state, “Data encryption devices secure sensitive information while it is electronically transmitted, stored, or processed. Encryption systems, which include both hardware devices and software packages, employ a mathematical algorithm to scramble plaintext, rendering it unintelligible until it is unscrambled through the use of a special key”.
Indeed, if encryption was employed in all aspects of data processing, many of the other techniques such as target hardening, access control, or entry/exit screening would become irrelevant. As Rothfeder noted, "If encryption were universally used, it wouldn't matter how secure firewalls, [or passwords] ... were. Nobody would be able to read what they stole." However, the other protections still have their place, because encrypted information could be intercepted, deciphered, and read at a later date, or the decryption key itself could be captured.

Encryption works by scrambling a "plaintext" or "in-clear" message by feeding it into an encryption algorithm, which is "seeded" by an encrypting key. This creates a "cryptogram" or "cyphertext" which should be completely unintelligible to both human actors and computers alike. The only way to reconvert this cyphertext back into plaintext, is to "reseed" the cryptogram with a decrypting key; which may or may not be the same as the encrypting key, depending on the system used.

\[597\] For example, differential encryption could be employed, utilising different "keys" and codes, so that individual units of data would only be available to certain employees. See Employee Surveillance section, above.

\[598\] Supra note 592.

\[599\] Ibid., at 180.

\[600\] The easiest way to think of encryption algorithms and keys, is to view the algorithm as the rules of conversion and the key as the enabling device. An extremely simple encryption algorithm would be one which replaced each letter of the alphabet with the one immediately following it, for example A would become B, B would become C and Z would become A. An encryption key is required to enable the conversion process. Hence MARC SENIOR, the plaintext, would become NBSD TFOJPS, the cyphertext. To return the cyphertext to its plaintext form, a decrypting algorithm is required, which once again can only be activated by the use of a decrypting key. In this case, the decrypting algorithm will replace each letter of the alphabet with the one immediately preceding it, for example B would become A, C would become B and Z would become A. The decrypting key could be the same as the encrypting key, or it could be different. This is because they are simply the "activators", and as with a physical door operated by an electronic lock, the code may be different to go from the outside to the inside, than from the inside to the
Many data encryption technologies and standards exist, including DES\textsuperscript{601}, RSA\textsuperscript{602}, Lucas\textsuperscript{603}, PGP\textsuperscript{604}, IDEA\textsuperscript{605}, Seneca\textsuperscript{606}, RC4\textsuperscript{607}, ROT13\textsuperscript{608}, and CRYPT(1)\textsuperscript{609}. Encryption technology can be both hardware or software based\textsuperscript{610}, be symmetric or asymmetric in nature, and can consist of either public or private keys. Symmetric cryptography is where the same “key”\textsuperscript{611} is used to both encrypt and decrypt data, and asymmetric cryptography is where a different key is required to encrypt or decrypt. A private key encryption system is where the keys to both encrypt and decrypt are kept secret, and public key encryption involves keeping one key secret, whilst publicly disseminating the other. For security in communication, the public key is the encrypting
one, with the decrypting key being kept secret, whereas for authentication, the encrypting key is the secret one, with the decrypting key being publicly known\textsuperscript{612}.

With regards to voice encryption, many chips and algorithms also exist, including, "shipjack" technology employed in "clipper chip"\textsuperscript{613} and "capstone"\textsuperscript{614} technologies, MYK-7\textsuperscript{615} and STU-3\textsuperscript{616}. Facsimile encryption usually involves the use of built in encryption algorithms or the use of an EIA-232 DTE\textsuperscript{617} port to allow for the attachment of hardware encryption devices\textsuperscript{618}. In discussing facsimile encryption however, it should be noted that the printout at the end of the process is not encrypted, otherwise it would be unreadable and effectively useless\textsuperscript{619}. To this end, in order to ensure that the process of encryption was not in vain, the fax machine should be placed in a secure environment so that the information does not fall into the wrong hands upon arrival\textsuperscript{620}.

\textsuperscript{612}In this way, a message will only decrypt properly if it is authentic, and is sent from the person claimed. This is because, for a message to decrypt, it must have been encrypted using the private key which is known only to the individual in question.

\textsuperscript{613}This is achieved through the use of clipper chips, which employ a proprietary 80-bit split-key algorithm called "shipjack". See Vargo, supra note 382 at 413.

\textsuperscript{614}Simonds, supra note 475 at 118-127.

\textsuperscript{615}This is Mykotronx's standard clipper chip encryption designation, the design and production of which is supervised by the U.S. Government's National Security Agency (NSA).

\textsuperscript{616}This is the code number for Motorola's voice encryption chip.

\textsuperscript{617}Data Terminal Equipment Port.

\textsuperscript{618}Simonds, supra note 475 at 118.

\textsuperscript{619}This is because the facsimile must be "readable" by the addressee. If the fax printout was encrypted, it would be unreadable to everyone, including the addressee, which would be futile. The encryption key could also be faxed, but this would allow anyone to decrypt the message. In addition, the amount of labour involved in manually decoding and transcribing the information would be likely to outweigh any of the advantages gained from encrypting the fax in the first place.
The level of security which encryption provides is dependent on several factors. Perhaps the most important is the key length. The longer the key, the harder is the code to crack, and the harder the information to decipher. However, weak encryption, employing short key lengths, can be substantially strengthened through triply-encrypting the plaintext by passing it through the encrypting algorithm three times, and using a different key for each encryption. Another security factor is the secrecy of the keys. If the decryption key is obtained, free access to the data is acquired, and key management is crucial in ensuring secure encryption. Also, similar to password protection, the ability to guess or by-pass the encrypting algorithm, or to try all possible keys, will also effect the level of security which encryption provides.

It should be noted, however, that the use of encryption is not without its difficulties. Encryption demands extremely large amounts of system capacity, and greatly increases the time taken to process, store and transmit data. In addition, many

---

620 To this end, many companies, especially law firms, are installing secure fax rooms. In addition, "tokens" can be carried by employees which only allow the fax machine to print out the message when the wearer of the "token" is in close proximity to it. See supra note 490.

621 This can be ensured through the use of so-called "one time pads", decryption keys which can only be used once and are as long in key-bit length as the message itself. They are however, extremely inefficient and should only be used if security is of extreme importance. See supra notes 497 and 498.

622 It should be noted here, that the encryption algorithm is generally common knowledge. It is the control over the keys which ensures the success of encryption. For example, the DES encryption algorithm is public knowledge, but the keys are strictly controlled. Public knowledge is indeed the general principle behind asymmetric public encryption systems, although here even the encrypting key is public. A prime example of public dissemination of encryption technology is the PGP (Pretty Good Privacy) software designed and freely distributed by Philip Zimmerman to combat the U.S. government prohibitions and controls over encryption technology (see infra note 635).
countries regard encryption technology as a munition\(^{623}\), or dual-purpose good\(^{624}\). The unbreakable coding and transmission of information by foreign powers is regarded as a threat to national security\(^{625}\), and as a result the import and export of encryption technology is strictly controlled\(^{626}\).


\(^{624}\)Such as Canada, and many of the countries of the European Union. In Canada, the export of goods is controlled both by restrictions placed on the export of certain goods to any country, and the export of any goods to certain countries. Controlling Acts include the Export and Import Permits Act, R.S.C. 1985, c.E-19, and the United Nations Act, R.S.C. 1985, c.U-2. The export of goods is restricted if they appear on any Area Control List, SOR/81-543 or Export Control List, SOR/89-202. It should be noted that interesting problems arise in relation to U.S. “origin” goods which are exported from Canada. In the computer hardware and software fields, advances in technology are constantly being made, which means that export lists must be constantly updated if they are to remain reasonable and effective in scope. The \textit{General Software and Technology} notes which are of application to encryption technologies are covered by Item 1000 of the Export Control List. However, encryption technologies specifically are covered by Items 1150-1155. See Takach, \textit{supra} note 32 at 224-238. In Europe, C.J. Millard, D. Griffith and V. Marsland, \textit{The Internet: Identifying and Managing Legal Risks Online} (London: Clifford Chance, 1997), note at 21. “In Europe the export of encryption technologies is governed by a European Council Regulation setting up a Community regime for the control of exports of dual-use goods [European Council Regulation, No. 338/94]. Dual-use goods are defined as goods which can be used for both civil and military purposes. Encryption software is classified as a dual-use good and is therefore subject to export controls [European Council Decision, 94/942/CFSP, as amended by Council Decision 96/613/CFSP].” In the U.K., the EC Regulation has been implemented as the Dual-Use and Related Goods (Export Control) Regulations 1996 (SI 1996/2721). See Bacard, \textit{supra} note 322 at 70-123.

\(^{625}\)Indeed, encryption, and the ability to decrypt enemy transmissions, was key in the Second World War. It is a legitimate concern that strong encryption technology (or the ability to decrypt friendly communications) should not fall into enemy, or potential enemy, hands. Of course, once one begins second-guessing who will be a “friend” and who will be a “foe” in the future, the selective export of encryption becomes a gamble. For example, Iraq was supplied with arms by the U.S. and the U.K. to fight Iran; a few years later, Iraq invaded Kuwait and Operation Desert Storm began.

\(^{626}\)The status of encryption technology as a munition or a dual purpose good, means that it is controlled by the \textit{International Traffic in Arms Regulations} (ITAR) (22 CFR 120.1). In the U.S., no encryption technology with a key-length of more than 56 bits may be exported from the U.S. (this was recently increased from 40 bits). Many other countries control encryption however, including China and Russia, and it should be noted that some countries are more concerned with the import of encryption technology than with its export, for example France. See G.W. Fresen, “Summary of Discussion on Encryption and Export/Import Controls”, Baker and McKenzie: A World Without Borders, Annual Client Seminar Day, Toronto, October 14, 1997 (CD publication); Millard, Griffith and Marsland, \textit{supra} note 624 at 18-23 and 78-84; and Barth and Smith, \textit{supra} note 621 at 286-290. See also, \textit{supra} notes 623-625.
It is unlikely, in this day and age, that such controls will be effective. This is because many encryption algorithms have already been disseminated\textsuperscript{627}, and because some governments\textsuperscript{628} do not restrict encryption and are developing their own extremely strong keys and technologies; and these algorithms will undoubtedly find their way into countries which do restrict encryption technology, due to the international nature of computer and telecommunications networks\textsuperscript{629}. Indeed, the structure of the Internet means that even encryption exported to listed or unrestricted countries is likely to pass through many prohibited countries \textit{en route}\textsuperscript{630}.

Law-enforcement agencies are also keen to control encryption technologies, so that they may continue to eavesdrop on criminal communications\textsuperscript{631}. To this end, there are currently proposals, in the U.S., to introduce "clipper-chips" into telephone equipment\textsuperscript{632}. These chips would encrypt all voice conversation, however, the FBI and

\begin{notes}
\begin{enumerate}
\item For example, in Japan, private companies are developing extremely strong encryption technologies, with key lengths of over 1,024 bits, the distribution of which will be unconstrained by the Japanese government. This technology will be distributed throughout the world, and will undoubtedly destroy U.S. plans to control strong encryption. See Barth and Smith, \textit{supra} note 623 at 289-290.
\item This is due to the "packet-switched" nature of Internet communications. See "Privacy on the Internet: Plans to Control Encryption Software are Futile and Misguided", The Economist, March 7-13. 1998, 18-19, and \textit{supra} note 439.
\item There is concern that encryption technologies are used by criminals, such as terrorists, child pornographers, drug-dealers and other organised crime groups. See Millard, Griffith and Marsland, \textit{supra} note 624 at 20.
\end{enumerate}
\end{notes}
other law-enforcement agencies would maintain “back door” access with which to listen in on selected communications. Needless to say, this has caused a great deal of controversy due to the privacy concerns which arise. The schema is also likely to prove unworkable, because any individuals who do wish to keep their conversations secret from the state, will simply privately re-encrypt their messages over the clipper-chip encryption algorithm. Trusted third-party or escrow retention of decryption keys is a possible solution to this dilemma, however, it is difficult to know who to entrust with this responsibility.

Simonds, supra note 475 at 121-126.
633 The problems of “back door” access have already been discussed in the Access Control section, above. See supra note 504.
634 See Cavoukian and Tapscott, supra note 241 at 142-144, and Bacard, supra note 322 at 45-48 and 99-123.
635 Indeed, the FBI under the Digital Telephony Wiretap Bill 1994, has mandated telecommunication exchanges and carriers to allow for 1% of all phone conversations in the U.S. to be monitored at one time, which, in addition to the “clipper chip” controversy will have a significant impact on privacy. See ibid., P.R. Zimmerman, Phil’s Pretty Good Software Presents: PGPfone Pretty Good Privacy Phone Owner’s Manual Version 1.0 (Beta 7-8 July 1996), at 7-10, and J. Nelson, “Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and Its Effect on Free Flow of Information and Privacy”, UCLA Law Review 1139 (1994).
636 However, the cryptography policy of the O.E.C.D. (Recommendation of the Council concerning Guidelines for Cryptography Policy, March 27, 1997) states that the protection of data and personal privacy is paramount, with escrow and key recovery a secondary matter. This is the reverse of the position taken by the United States.
637 Privacy proponents argue that government cannot be trusted with the “keys”, because they would use them themselves. In addition, third-party escrow by commercial entities would seem to offer no solution. They would still be heavily influenced by government, and could be forced to hand over the “keys”. It is clear that there is an extremely difficult balance to strike between government and public interest. The question would seem to become one of whom do you prefer knows your secrets, hackers or the government? This creates an interesting dilemma. In March 1997, the U.K. Department of Trade and Industry issued a public consultation paper concerning these issues, entitled, “Detailed Proposals for Legislation for the Licensing of Trusted Third Parties for the Provision of Encryption Services”. See Millard, Griffith and Marsland, supra note 624 at 22-23.
10. Identifying Property

This technique is self-explanatory, and involves deterring crime and increasing the facilitation of property return, through its identification. Examples include cattle branding, vehicle licensing638, parts and property marking639, PINs for car radios640 and hidden transmitters which allow property to be traced641.

In the computer sphere, this technique can clearly be used to mark and identify computer equipment including, floppy disks, through the use of serial numbers and printouts through the use of headed and water-marked paper. However, this is unlikely to protect the information contained within computer systems, unless units can be found and returned before any information is downloaded. This point is crucial, because as noted in previous chapters, the exclusivity of the information is the important element, with the retrieval of the lost information being secondary. Of course, another measure which could be employed would be to mark information as “confidential”, as this might deter the morally-minded from reading the information; although this is an extremely marginal

---

protection, especially considering that it is thieves who are likely to have taken the information in the first place\textsuperscript{642}.

With regards to computer networks, property identification can be employed to deter crime in another way. This is through making it clear to users, and intruders, that they are in your network, and on your territory. This matter was discussed earlier under the category of “Natural Surveillance”, where it was noted that an efficiently run network would deter offenders through the increased perception and intimidation of surveillance. These issues do not here need reiterating\textsuperscript{643}.

\textit{11. Removing Inducements}

This technique refers to the removal of circumstances which induce criminal activity. It differs from “Controlling Facilitators”, because the focus is not on preventing the availability of items which can be used to perpetrate crime, but instead on the prevention of situations and conditions arising which stimulate or catalyse criminal activity. Examples include, keeping money and expensive jewellery and automobiles out

\textsuperscript{642}This is not to say that all thieves are immoral. It could, of course, be claimed that property rights are immoral and that thieves are acting with justification. In addition, some theft, such as for survival, may not be regarded as immoral, and may not even be regarded as criminal. The crux of the point being made, however, is that persons who are willing to violate property rights are unlikely to adhere to confidentiality notices. In addition, it is entirely possible that the thieves who stole the computer system did so purposefully for the information which it contains, and so are especially unlikely not to read or assimilate the information which they have taken.

\textsuperscript{643}See the \textit{Rule Setting} section, below.
of sight, removing weapons to reduce the propensity for violence\textsuperscript{644}, rapidly repairing property damage\textsuperscript{645}, and immediately cleaning graffiti from walls and public transit vehicles\textsuperscript{646}. The swift reparation of damage is important, because research suggests that minimal decay and the perception of a disorganised and badly kept area or facility, leads to further decay which promotes crime\textsuperscript{647}.

The situation in the computer sphere is similar. If a network breach occurs and a security loophole is found, it is likely that other hackers will exploit this weakness and the network will soon become over-run with intruders. It is, therefore, imperative that any network security breaches be immediately discovered and rectified. Another measure which could be employed under this category would be to reduce the attractiveness of the network to hackers. This could be accomplished by removing the information or encrypting it, and relaxing security precautions. Although a bizarre precaution to take, evidence suggests that many hackers are attracted to complex, devious and hard to crack security systems. As such, many hackers would lose interest if a system was easy to

break into, and hence access violations would decrease. However, this idea is only of theoretical interest, because it is in direct contravention to the other SCP measures discussed, and is also likely to be counter-productive in protecting information from instrumental hackers, who are likely to pose the greatest threat.

12. Rule Setting

This technique refers to the regulation of conduct by the imposition and posting of rules, policies, and conditions, which must be followed by all persons in a certain organisation, or by all those using a certain facility. For example, transit systems, hospitals, schools, hotels, and restaurants all have guidelines which regulate the conduct of the clientele they serve, and all retail and commercial enterprises have strict operating procedures which must be adhered to by all employees. Additional examples include the setting of rules regarding customs declarations, income tax returns and library book check-out procedures. The principal aim of this technique is to remove all

648 In the physical world, this is analogous to painting murals on walls to prevent graffiti. The wall is in effect already "graftified", and is hence of no interest to vandals. See J. Wise, "A Gentle Deterrent to Vandalism", Psychology Today, September 16, 1982, 31-38.

649 See infra notes 663-668.


ambiguity regarding conduct in any situation which may arise, and so even such things as employee telephone use should be subject to "legislation".

In the computer sphere, many of these techniques are of direct application. Rules regarding the use of e-mail, and specifically its content, can be employed to protect information. In addition, rules regarding passwords can be enforced so that they are changed frequently, and not divulged to others. Also, system usage could be regulated so that employees know exactly which areas of the system they are authorised to access and which areas are "off-limit". This would aid in the detection of unauthorised access, and remove any doubt as to culpability. In these ways rule setting is crucial in maintaining internal system security652.

However, rule setting is also crucial in maintaining external network security. This is because, by clearly defining territorial boundaries, and posting virtual notices to inform trespassers of their intrusion653, potential hackers are deterred due to the additional psychological barriers they must overcome in breaking the rules654. As Clarke points out, "The existence of these rules means that offenders must be prepared to incur higher costs in terms of fear or conscience"655.

652As Clarke, supra note 444 at 188 states, "Such rules would not normally require the backing of law, but some highly specific laws and local ordinances have the character of situational measures".
653Such as the popular "Trespassers will be prosecuted" signs, which are in many cases a legal fiction due to the civil nature of trespass.
654See the Natural Surveillance and Identifying Property sections, above.
655Clarke, supra note 444 at 118.
C. ANALYSIS

The use of SCP techniques, to defend computer networks and stand alone systems, raises a number of interesting questions. These include such matters as, will the protection of computer systems ensure the security of information; will SCP measures be effective in protecting computer networks; and, should practical protections be employed at all? These questions will be addressed in turn.

(a) Can Information be Protected by Ensuring Computer Network Security?

This matter can be dealt with relatively summarily, because it has been the focus of discussion throughout the whole course of this thesis. It has been noted repeatedly, that the protection of information is crucial in controlling its dissemination, use and accuracy, and that this is necessary for the maintenance of privacy\cite{footnote1}. As has also been discussed, information must be prevented from unauthorised acquisition and from unauthorised disclosure, if it is to protected\cite{footnote2}. With regards to private information specifically, prevention of unauthorised acquisition was found to be the crucial element, and the best way of defending against acquisition is to prevent access to the

\footnotetext[1]{See Chapter 1.}
\footnotetext[2]{See Chapter 2.}
information\textsuperscript{658}. In the computer sphere, this means controlling access to the computer system, or to the computer network in which the information resides\textsuperscript{659}. The protection of computer systems, will therefore, most definitely secure network information and its exclusivity.

\textit{(b) Can SCP Protect Computer Networks?}

In answering this question, a deeper understanding of SCP theory is required. The effectiveness of any crime prevention or defensive measure is entirely dependent upon its ability to prevent criminals from successfully completing their objectives. This in turn is dependent upon correctly analysing the psychology, motivation and rationale of the potential offender. As with all criminological theories, SCP makes certain assumptions about the mentality of criminals, and the model created will only work if these assumptions are correct. SCP assumes that humans are rational actors whose decisions to commit crime are guided by immediate and practical stimuli\textsuperscript{660}. If this assumption is

\textsuperscript{658}See the \textit{Private Information in the Computer Age} and \textit{A Proactive Approach to Protecting Information} sections, \textit{Chapter 3}.

\textsuperscript{659}See \textit{Theoretical and Practical Protections} section, above.

correct SCP will indeed work, but if criminals are in fact driven by deeply emotional pressures, then SCP will fail. The failure will come on two fronts, first because the criminal is likely to possess enough motivation to overcome any defences which may be mounted, and second, because if one target is too difficult, another will be attacked in its place.

The situation in relation to hackers and the protection of computer networks is extremely complex. This is because there are many different types of hacker, all of whom have different motivation levels, and different reasons for breaking into computer networks. The two main varieties are “instrumental” hackers, and “expressive”


662 In SCP theory, this is referred to as the “displacement of crime”. The extent to which displacement occurs after the implementation of an SCP measure is unknown. Some argue that there is no displacement, and others that it simply goes undetected, with criminal activity either being diffused into many other fields and thus disappearing amongst background figures, or being diverted into areas so disrelated from the prevented activity that it is not measured or detected. It should also be noted that displacement is likely to occur in some instances such as robberies, but not in others such as suicide. See T. Gabor, “The Crime Displacement Hypothesis: An Empirical Examination”, Crime and Delinquency (1981) 26:390-404; T. Gabor, “Crime Displacement and Situational Prevention: Toward the Development of Some Principles”, Canadian Journal of Criminology (1990) 32:41-74. See also R. Barr and K. Pease, “Crime Placement, Displacement, and Deflection”, in M. Tonry and N. Morris, eds., Crime and Justice: A Review of Research, Vol. 12 (Chicago: University of Chicago, 1990); and R.V. Clarke and P.M. Mayhew, “The British Gas Suicide Story and Its Criminological Implications”, in M. Tonry and N. Morris, eds., Crime and Justice: A Review of Research, Vol. 10 (Chicago: University of Chicago Press, 1988). See infra notes 679 and 689.

hackers. Instrumental hackers include all those who break into computer systems to accomplish a further goal, such as to retrieve information for personal use or for sale to competing companies; and all those who maliciously destroy data for revenge, or because they have been hired to do so by a third party. By comparison, expressive hackers include all those who break into computer systems purely for the joy of doing, or for the thrill of the challenge.

Instrumental hackers will, in some cases, act according to the SCP model, basing their actions on practical stimuli, and will therefore be easily deterred by a complex network defence system. These hackers will usually be breaking into computer systems opportunistically, to find what they can of value, and will quickly transfer their energies to breaking into less secure systems. However, others will be attacking specific systems to gain particular units of data, or acquire information of a certain type.

A. Bequai, Technocrimes (Toronto: Lexington Books, 1987), at c.3-4; and Davis, supra note 55 at 7-10 and 84-85. Internal crime committed by current, or ex-employees, is not being discussed here. However, the significant threat posed by these groups should not be overlooked (see supra notes 556 and 557).

These classifications are taken from studies involving violent offences, such as assault, rape and murder. For example, in the case of murder, the victim may be killed for pure pleasure, which would be "expressive" in nature, or in order to inherit under the terms of a will, in which case the murder would be "instrumental". See R. Sampson and J. Lauritsen, "Violent Victimisation and Offending: Individual, Situational and Community-Level Risk Factors", in A.J. Reiss and J. Roth, eds., Understanding and Preventing Violence, Vol.3 (Washington D.C.: National Academy Press, 1994); and N. Weiner, "Violent Criminal Careers and Violent Career Criminals: Overview of the Research Literature", in N. Weiner and M. Wolfgang, eds., Violent Crime, Violent Criminals (Newbury Park: Sage Publications, 1989).

Instrumental hackers are generally regarded as the true "computer criminals", with expressive hackers being seen as petty or recreational "crackers" (see text).

Revenge is a difficult motive to classify. In some ways it is "expressive", as it serves no other purpose than to satisfy an emotional need. Conversely, however, destroying data can be argued to be "instrumental" in satisfying this need. For our purposes, revenge will be classified as an instrumental act, because it includes selling data to a competitor, which is an instrumental motivation.

This sub-set of instrumental hacker can be labelled the "opportunistic instrumental hacker".

Similar in nature to an opportunistic thief in the physical world.
and these hackers are unlikely to follow the criminal model proposed in SCP. This sub-set of non-opportunistic hacker\textsuperscript{668} will be highly motivated, and will focus purely on one specific computer system, or on the databases of one particular type of industry. They will not be easily deterred, but comparatively, they will have little interest in attacking other systems.

Expressive hackers, on the other hand, will act in direct contravention to SCP theory in all cases. They are driven by addiction, and as such are extremely highly motivated. They are both opportunistic and focused. They will attack any system, although once a system is targeted they are extremely unlikely to be deterred by a strong defence. In fact, as the thrill of the challenge is the sole motivation behind an attack, a strongly protected computer system will make a more attractive target than a weakly protected one.

In creating a defensive strategy, it is essential to determine which variety of hacker you are seeking to deter. As Poyner and Webb\textsuperscript{669} point out, in relation to residential burglary, if you wish to prevent jewellery theft, then shrubs and bushes should be cut down, whereas to prevent the theft of electrical goods, other houses should

\textsuperscript{668}This sub-set of instrumental hacker can be labelled the "non-opportunistic instrumental hacker".
overlook the access points to your home\textsuperscript{670}. In protecting a network from instrumental hackers, a strong defence will be the best strategy, whereas in defending against expressive hackers, a weak defence, or no defence at all will be the best approach\textsuperscript{671}. An SCP strategy geared towards instrumental hackers is not guaranteed to work against expressive hackers, and vice versa. In deciding upon a course of action, the individual or organisation must determine which variety of hacker poses the greatest threat\textsuperscript{672}. This will depend largely on the losses incurred by the person or company from an attack by each kind of hacker.

Following our discussion above, it is clear that instrumental hackers constitute the greatest threat, and any defences should be directed towards their deterrence. The implementation of extremely strong security measures, and the combined application of many of the SCP opportunity reducing techniques outlined above, will prove the most effective approach\textsuperscript{673}. This is because both opportunistic and non-opportunistic instrumental hackers, are likely to fail against very stringent protections, and will either

\textsuperscript{670}See \textit{Natural Surveillance} section, above. It should also be noted that the best approach to preventing commercial burglary will be very different from the approach needed to prevent residential burglary. See Clarke, \textit{supra} note 444 at 98-99.

\textsuperscript{671}The idea of deterring or preventing computer crime through abandoning all security is only suggested as a theoretical solution to the problem of expressive hackers. In practice, such an approach would be ludicrous. It would be akin to a bank leaving its money on the street in order to deter criminals addicted to safe-breaking.

\textsuperscript{672}See Vargo and Hunt, \textit{supra} note 382 at 421-425. The internal threats posed by employees should not be forgotten, however (see \textit{Employee Surveillance} section, above, and \textit{supra} notes 556 and 557).

\textsuperscript{673}Even if expressive hackers did pose the most serious threat, it is still likely that stringent security would be the best approach. If security was strong enough, no access could be gained, regardless of the number of attempts, and this would clearly be the best all-round solution.
give up completely or divert their efforts into breaking into other computer systems674. On the other hand, expressive hackers, who are likely to have the highest motivation, may fail against strong counter-measures, but even if they succeed, will do relatively little damage in comparison to instrumental hackers675. Of course, there are exceptions, for example, even an innocent trespass into an air traffic control computer would constitute a serious threat to life.

(c) Should Practical Protections be Employed?

In answer to this question, two aspects must be considered. First, theory and morality, and second, practicality. Theoretically and morally speaking, the considerations are whether individuals should have to protect themselves against computer network trespass, and whether such an individualistic approach is a correct or beneficial one.

In response to the first part, it can be argued that crime prevention is the responsibility of the state, and that citizens have no place taking matters into their own hands676. It can certainly be suggested that they should not have to protect themselves, even if they are permitted to so do. Additionally, it can be argued that self-protection

674 See supra notes 662 and 663.
675 Of course, there are exceptions, such as when an expressive hacker wishes to try out a new virus or when he or she accidentally destroys data.
degrades and disrespects the law, because it becomes superfluous as a protection mechanism\textsuperscript{677}. Vigilantism would be promoted, and a self-centred and individualistic approach encouraged. These ideals can quickly lead to a breakdown in social cohesion, which in the physical world promotes a lack of care over the environment, an increase in decay and the stimulation of crime\textsuperscript{678}. This was discussed above, and the same situation would be likely to occur in the virtual realm. In this light, SCP measures would actually appear to increase crime\textsuperscript{679}.

However, in counter-argument, it has been suggested, through the neo-realist approach, that even if the state should protect, it is incapable of so doing, and that as such, citizens are left with no alternative but to protect themselves\textsuperscript{680}. Following this line of thought, there would appear to be nothing wrong with protecting oneself, and indeed many government bodies and law-enforcement agencies promote such self-protection\textsuperscript{681}. Individualistic schemes are evident in many aspects of society today\textsuperscript{682}, and with the current climate of privatisation their prevalence is likely to increase.

\footnotesize


\textsuperscript{678}See \textit{Removing Inducements} section, above, and \textit{supra} notes 645-647.

\textsuperscript{679}At the very least, crime would displace and attacks on less secure networks would increase. For example, Mayhew et al., \textit{supra} note 553, note that the reduction in theft rates of vehicles fitted with steering locks was accompanied by a proportionate increase in the theft of vehicles not fitted with steering locks. See \textit{supra} note 662, and \textit{infra} note 685.

\textsuperscript{680}See \textit{supra} note 676.

\textsuperscript{681}The "Report of the Sub-Committee on Computer Crime" (\textit{supra} note 332 at paras.49-51 and 69, at 18-19 and 22), recommended that the implimentation of network security measures was the best approach to take in defending against computer crime.

\textsuperscript{682}Examples include the implementation of Neighbourhood Watch programs, the use of burglar alarms and the employment of private security personnel.
Practically speaking, it is unlikely that SCP measures will be effective in reducing computer system attacks. This, of course, depends on the ratio of instrumental hackers to expressive hackers, as the balance of this ratio will effect the general level of motivation, and therefore the effects of deterrence and displacement. It is probable that individually highly secure computer systems will displace offenders and promote attacks on less secure systems\textsuperscript{683}. Thus, the individualistic approach will actually increase attacks and data confidentiality loss for certain network users\textsuperscript{684}. For example, it has been found that the implementation of “Neighbourhood Watch” programmes simply transfers crime; decreasing it in the Neighbourhood Watch area, but increasing it in the surrounding vicinity, as the displaced offenders are absorbed\textsuperscript{685}.

If information is truly to be protected in the computer age, hacking must be prevented, not simply shifted from one virtual location to another. The only way SCP will be effective in reducing hacking on a wide-scale, is by implementing the measures across the whole network\textsuperscript{686}. Interestingly, however, this may have the effect of

\textsuperscript{683}See supra notes 662 and 679.

\textsuperscript{684}Of course, this problem could be solved by introducing nation-wide or international SCP initiatives. It is possible that minimum standards of security could be set and their implementation enforced by law (see “Report of the Sub-Committee on Computer Crime”, supra note 332, paras.49-51 at 18-19). Victims of computer attacks could be held contributarily negligent if they do not possess adequate network security protection. However, it could be argued that protection against computer crime is a state responsibility and not a private one (see Nelken, supra note 676). Also, it is unlikely that such a scheme could be introduced at a general level, and even if it could, it would probably prove more efficient to tackle the problem in other ways.

\textsuperscript{685}See Rosenbaum, supra note 579. Houses in the area surrounding the Neighbourhood Watch zone are attacked at an increased rate which coincides with the reduction in attacks experienced inside the Neighbourhood Watch area. Thus, the crime rate does not actually increase overall, just in the area surrounding the Neighbourhood Watch zone.

\textsuperscript{686}See supra note 684.
increasing crime, or exacerbating its effects. For example, in New York City, bandit screens were introduced in ticket booths on the subway system to reduce robberies committed with knives, or other non-projectile weapons. The effect was that armed robbery with firearms increased, and instead of being wounded transit system employees were killed. To halt this problem, the transit authority introduced bullet-proof kiosks, to which end, robbers began to use incendiary or explosive devices which increased the death toll\textsuperscript{687}.

In the computer sphere, this may mean that employees of companies may be physically threatened, blackmailed, or otherwise coerced to break into files, and physical breaking and entering to retrieve information may increase if access cannot be achieved through network connections. Indeed, the highly-motivated nature of hacking may make this a reality. However, it is unlikely that most hackers\textsuperscript{688} would turn to such extreme and physical measures if their traditional methods failed\textsuperscript{689}.

\textsuperscript{687}See J. Dwyer, \textit{Subway Lives} (New York: Crown, 1991), Ekblom, \textit{supra} note 456, Clarke, Field and McGrath, \textit{supra} note 457, and Poyner et al., \textit{supra} note 458. This is similar to the current debate in England regarding the arming of the police. It is hypothesised that arming the police would encourage thieves and other malefactors to become better armed, and thus result in a higher death toll both of civilians and police officers.

\textsuperscript{688}Especially expressive hackers.

\textsuperscript{689}For example, when people in England were no longer able to commit suicide due to the detoxification of the gas supply, suicide decreased by 40% due to the lack of any other appropriate methods. The substitution of more violent or courageous means of suicide did not occur. See Clarke and Mayhew, \textit{supra} note 662.
Conversely, it is also feasible that an equal number of incidental benefits may occur through the use of SCP measures. In the computer sphere, it is possible that increased security on some systems and networks may produce a "halo effect", whereby all computer based infringements are reduced or halted. This would be primarily due to a psychological deterrent effect created through the aura of protection and vigilance, as explained above, and it is certainly likely that some less secure networks would benefit from the introduction of SCP measures on other networks. In short, the general effects of SCP are as of yet unknown, and the balance could tip either way; SCP could reduce crime, displace it or exacerbate it.

In any event, the implementation of SCP techniques on an individual computer system, would be certain to increase the protection of the information contained within that system, regardless of the effect on other networks; and the greater the security differential, the better will be the protection.

690 In SCP theory, this is known as the "diffusion of benefits". See Clarke, supra note 444 at 129-132. Examples of diffusion include, a police crackdown which reduces crime long after the crackdown has ended (L.W. Sherman, "Police Crackdowns: Initial and Residual Deterrence", in M. Tonry and N. Morris, eds., Crime and Justice: A Review of Research, Vol.12 (Chicago: University of Chicago Press, 1990)); a library book detection screen which prevents the theft of all library books, not only those which have been "tagged" (Scherdin, supra note 519); and, CCTV installed on buses which reduces damage and misbehaviour on buses without CCTV (B. Poyner, "Video Cameras and Bus Vandalism", Security Administration (1988) 11:44-51). In many ways, the protection of information can itself be viewed as an additional benefit. This is because the primary function of the law and of SCP measures is to prevent computer trespass and unauthorised access. Another benefit which may arise is a reduction in telecommunications fraud, due to less hackers stealing communications to perpetrate their crimes. See A Proactive Approach to Protecting Information and Theft of Telecommunications sections, Chapter 3, and supra notes 360, 368, 429 and 430.

691 This was the term used by Scherdin, supra note 519, in explaining the "diffusion of benefits" (see ibid.). Also termed the "free rider", "drip feed" or "bonus" effect.

692 See supra note 590.
CONCLUSION

LAW AND PRACTICALITY

A. SUMMARY

Throughout the course of this thesis, a number of related issues have been discussed. It was noted that individuals, organisations, and governments wish to maintain exclusivity in information for many reasons, and the value of this exclusivity was examined. The discussion focused around privacy, where control over the dissemination, use and accuracy of information was found to be crucial. It was concluded that information must be prevented both from unauthorised acquisition and from unauthorised dissemination, if it is to be protected in any meaningful way.

In discussing prevention against acquisition, it was noted that protection must exist in all stages of information development; during its creation, transmission and storage. It was also noted that some control must be exerted over those who possess

\[69^3\text{See Natural Surveillance section, above.}\]
knowledge of your private information, so that they may be prevented from disclosing it. To this end, many traditional legal protections were discussed, including privacy, surveillance, interception of private communications, theft, fraud, data protection, breach of confidence and public disclosure.

In the computer age, many old privacy problems were found to be exacerbated, and new ones created, due to the increased difficulties of controlling information both in its acquisition and disclosure. In focusing on private information, the protection of exclusivity was found to be far more viable, primarily because the protection of private information is far more concerned with prevention against acquisition than it is with dissemination. In defending information on computer networks, the application of traditional law was discussed, including theft, mischief, and interception of communications. In addition, the protection afforded by more specific legislation, such as the unauthorised use of a computer provisions, was also examined. Each was found to be useful to differing degrees, although in general, proactive laws were found to be the most effective.

In the last chapter, it was suggested that the law was inadequate for the purposes of protecting information, no matter how proactive the approach. The reasons for this being the elusive nature of information, and the associated jurisdictional difficulties arising, from the international flow of data over telecommunication and computer networks. To this end, the application of Situational Crime Prevention techniques was
discussed, and the employment of theoretical, practical and psychological protections was found to be the best approach to take in securing private information in the computer age.

B. CONCLUDING THOUGHTS

The premise of this thesis has been that practical measures are necessary to protect information because law alone will be insufficient. Indeed, reactive legal redress and information security are two very different things. However, it is important to note that law cannot, and should not, be ignored in protecting information. Not only does the law provide indirect psychological protection by way of creating an aura of privacy, but it also protects information directly through a deterrent effect. The presence of proactive laws is also important for reinforcing practical measures, and for highlighting the culpability of hacking and unauthorised entry694.

In addition, law cannot be separated from the regulation of information, nor from the technologies which protect it. As we have seen, the law regulates the export of encryption technologies and helps control the use of devices which can be used to illegally acquire information. The level of technology is closely related to law, because the security provided by a device directly effects the “reasonable expectation of privacy”.

694See von Hirsch, supra note 677.
which in turn alters the extent of the legal protection which is afforded. It should also be noted that the law could be employed to enforce the use of network security measures, and the doctrine of contributory negligence could be applied to those who do not adequately protected themselves against hackers.

One final issue which should be addressed, however, is whether the law should protect information or privacy at all. It has been assumed, throughout the course of this thesis, that information exclusivity should be protected, although this is in fact a matter of great controversy. Indeed, suggestions have been made that it is socially

---

695 See The Acquisition of Information during its Communication section, Chapter 2, and Telecommunication Protections section, Chapter 3.
696 See "Report of the Sub-Committee on Computer Crime", supra note 332. See also supra notes 676 and 684.
697 It is questionable, however, whether it should be the duty of citizens to protect themselves from crime, and even more so, whether they should be held responsible for their own victimisation. See ibid.
698 The issue is especially contentious with regards to commercial information, especially regarding patents. As Hammond states in "Quantum Physics", supra note 24 at 52, two challenges arise with regards to commercial information, "The first relates to the ability of the profession and the commercial community to devise new social arrangements that will ensure both the creation and the effective and profitable utilisation of new information and technology. The second challenges a liberal society to protect its basic political and human values from unwise applications or withdrawals of that new knowledge. The real question is whether the institution of property is an appropriate vehicle for addressing those challenges". However, this thesis is more concerned with private information, especially that of a personal nature, and the protections afforded such information were discussed in Chapter 2. Regardless of the theoretical justifications and moral quandaries, it was noted that even though privacy is not regarded as a right, that it is protected under many individual Acts and common law principles. See Surveillance and General Privacy Protections section, Chapter 2, and supra notes 106-109.
699 The debate regarding the theory and justification for protecting privacy is especially heated. See S. Warren and L. Brandeis, "The Right to Privacy" (1890) 4 Harv. L. Rev. 193, at 205; Prosser, supra note 71 at 389; E. Bloustein, "Privacy as an Aspect of Human Dignity: An answer to Dean Prosser" (1964) 39 NYU Law Rev. 962, at 973; S. Benn, "Privacy, Freedom and Respect for Persons" (1971) Nomos XIII 1; H. Gross, "The Concept of Privacy" (1967) 42 NYU Law Rev. 34; and Posner, "The Right to Privacy", supra note 572. See also The Essence of Privacy and Privacy as Control over the Dissemination of Information sections, Chapter 1, and infra notes 700-706.
damaging to restrict the flow of information\textsuperscript{700}, and that privacy and information exclusivity are economically inefficient\textsuperscript{701}. The crux of the argument is whether privacy should be regarded as a basic human right, or whether it should be considered a luxury left to market forces to provide\textsuperscript{702}. This matter is of the utmost theoretical importance, because it affects the political justifications behind the legal protection of privacy. If privacy is to be regarded as a right, the state alone should uphold it, and the market should have no place in its protection\textsuperscript{703}. Conversely, if privacy is regarded as a luxury, the state should relinquish its control and the market should have sole dominion over its provision\textsuperscript{704}.

In practice however, the theoretical implications are limited\textsuperscript{705}, because individuals, organisations and governments will always desire secrecy regardless of legal provisions, and given the inability of law to protect information, the application of

\textsuperscript{700}As noted by the National Telecommunications and Information Administration, in “Privacy and the NII”, supra note 309, “The free flow of information - even personal information - promotes a dynamic economic marketplace, which produces substantial benefits for individual consumers and society as a whole”. See infra notes 701-706.

\textsuperscript{701}See R.A. Posner, An Economic Analysis of Law (Boston: Little, Brown & Co., 1986), and Posner, supra note 572. See also, Laudon, supra note 570, Hunter and Rule, supra note 570, and supra notes 152, 273-281 and 571-573.

\textsuperscript{702}See supra note 699, and infra notes 703 and 704.

\textsuperscript{703}As stated, in “Privacy and the Canadian Information Highway”, supra note 136, “Should privacy be an optional extra, for which only some Canadians can afford to pay, or should privacy be cost-neutral and considered an essential part of service offerings”. See also Nelken, supra note 676.

\textsuperscript{704}Of course, there is no reason why both the public and private sectors cannot protect privacy in collaboration with one another. However, theoretically speaking, if the protection of privacy is to be regarded as a public duty, then the private sector should not engage in its maintenance. Although, if the state cannot adequately protect privacy, then it would seem that individuals are left with no alternative but to protect themselves, regardless of the theoretical or moral quandaries. See Nelken, \textit{ibid}.

\textsuperscript{705}The theoretical implications are also limited because many of these issues have already been resolved. See supra notes 698 and 699.
practical security measures will always be necessary.\footnote{Indeed, vibrant markets are likely to exist for the provision of security devices, and many techniques exist for stimulating these markets. Examples include provoking fear and paranoia regarding privacy infringements, and highlighting the disadvantages and dangers of exclusivity loss. This marketing technique is widely used, for instance, in the sale of automobiles based on their safety features after highlighting the dangers of road accidents, and the sale of security devices for personal safety and property protection after highlighting the dangers of personal victimisation and burglary. For an outline of the motivation of fear, and its very real effects, see Murray, supra note 451 at 352-355. Additionally, C.L. Schultze, The Public Use of Private Interest (Washington D.C.: Brookings Institution, 1977), notes that a market can be constructed and a public goal fulfilled by creating an individual private demand for a good.}
BIBLIOGRAPHY

BOOKS


**JOURNAL AND INTERNET ARTICLES**


Bloustein, E., "Privacy as an Aspect of Human Dignity: An answer to Dean Prosser" (1964) 39 NYU Law Rev. 962.


GOVERNMENT PUBLICATIONS AND INTERNATIONAL DOCUMENTS


Government of Canada (Department of Justice), *The Steps Ahead* (Ottawa: Department of Justice, 1987).


House of Commons, Standing Committee on Justice and Solicitor-General, *Open and Shut: Enhancing the Right to Know and the Right to Privacy* (Ottawa: Supply and Services Canada, 1987).


CONFERENCE PAPERS, UNPUBLISHED PAPERS AND IN-HOUSE PUBLICATIONS


Bennett, C.J., Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association (Rexdale: CSA, 1995).


Public Interest Advocacy Centre, Surveying Boundaries: Canadians and their Personal Information (Ottawa and Montreal: PIAC and FNACQ, 1995).


NEWSPAPER AND MAGAZINE ARTICLES


Eckerson, W., “Privacy Suit Forces Users to Examine E-mail Policies: Case Against Epson Raises Troubling Questions”, Network World, 17 September, 1990, 1.


INTERNET AND SECURITY RESOURCES


<http://www.wizvax.net/kevinmca>.

Catalyst (The New Zealand Government Communications Security Bureau).


Central Computer and Telecommunications Agency Risk Analysis and Management Methodology (CRAMM).


Forum of Incident Response and Security Teams (FIRST).


Los Alamos Vulnerability and Risk Assessment Methodology (LAVA).

Machado, R., Paradigm Shift Research, <romana@apple.com>.

National Computer Security Association (NCSA).


Security Evaluation and Inspection Team (SEIT).