THE LAW AND INFORMATION SECURITY:
Legal Protections, Obligations and the Protection of Information

Judge David Harvey

This paper considers the way in which the law approaches behaviours that impact upon the security of information

There are four main areas which will be discussed:

(a) The regulation of the way in which information can be used.
(b) The prescription of penalties for intrusions or activities involving information systems, particularly which compromise the security of those systems or the information contained therein, for the protection of trade secrets and the criminal law protections for the security of personal information.
(c) The creation by the law of exceptions for law enforcement and security agencies who access information and the way in which the competing interests of law enforcement, security and the individual interact.
(d) The provision of protection for systems that are designed to protect information.

In this paper, I propose to consider briefly the provisions of the Privacy Act in considering the regulation of the way in which information can be used, the provisions of the Crimes Act, particularly in relation to computer crimes, which deal with the nature of intrusions into or activities involving information systems and the penalties prescribed therefor; the provisions of various information interception procedures which are prescribed by law and which are present in the Crimes Act, legislation involving the Government Communications Security Bureau (GCSB) and the Security Intelligence Service (SIS) and also legislation dealing with the circumstances under which searches may be carried out or activities monitored in the Summary Proceedings Act, together with the way in which communications organisations may be required to facilitate such information access and monitoring procedures.

Finally, I shall consider the provisions of the Copyright Act, which provide for the protection of technological protection measures which are designed to limit or restrict the ability of the user of digital systems to access or copy information contained within those systems.

(a) Regulation of the Way in which Information Can be Used.
(b) The Prescription of Offences and Penalties for Intrusions Into or Activties Involving Information Systems.
(c) The Creation of Exceptions for Law Enforcement and Security Agencies to Access Information.
(d) The Protection for Systems that are Designed to Protect Information.

Regulation of the Way in which Information Can be Used.

The Privacy Act has as a general objective "to promote and protect individual privacy". That privacy relates to information about individuals that are held by both public and private sector agencies.

The legislation recognises that it is important "to balance the protection of individual rights against what was feasible, what would not cause a completely negative reaction within the business community and what would not completely overturn the way in which a legitimate commercial activity proceeded". The legislation has been characterised as both a human rights statute and a freedom of information statute.

Information is not defined and this appears to be deliberate. Once a word is defined, particularly in legislation, the definition itself imposes boundaries upon the concept. In *Commissioner of Police v Ombudsman*[1], it was noted that the word "information" is not confined to the written word but embraces any knowledge, however gained or held. On appeal[2], McMullin J held that the word denotes "that which informs, instructs, tells or makes aware". The Act regulates the way in which information may be collected, held or used by an agency. An agency is the term that is used to describe individuals and organisations in both the public and private sectors that are subject to the requirements of the Act. In practice, virtually every individual and organisation in New Zealand today may fall under the definition of agency.

The core of the Act is contained in 12 Information Privacy Principles[3], setting out the broad rules with limited exceptions that deal with the following matters:

1. The purpose of collection of personal information.
2. The source of personal information.
3. The collection of information from subject.
4. The manner of collection of personal information.
5. The storage and security of personal information.
6. Access to personal information.
7. Correction of personal information.
8. Accuracy, etc, of personal information be checked before use.
9. Agency not to keep personal information for longer than necessary.
10. Limits on use of personal information.
11. Limits on disclosure of personal information.
12. Unique identifiers.

Principles 1 to 4 apply only to information collected after 1 July 1993.

The Principles that relate to security, access, correction, accuracy, retention and disclosure of personal information – Principles 5 to 9 and Principle 11 – apply to personal information collected both before and after 1 July 1993. Principle 10, which relates to the use of personal information, applies only to information obtained after 1 July 1993. Principle 12, regulating the assigning of unique identifiers, applies to such an assignment after 1 July 1993.

The full force of the enforcement provisions of the Act are presently available only for breaches of Principles 5 (storage and security of personal information), 6 (access to personal information), 7 (correction of personal information) and 12 (unique identifiers).

[1] [1985] 1 NZLR 578
[2] [1988] 1 NZLR 385
[3] s. 6 Privacy Act

The legislation is aimed at the behaviour modification of agencies that hold information about individuals. Thus, a significant portion of the Act is structured around the Information Privacy Principles establishing norms of conduct in relation to collection, handling and use of personal information. Compliance with these Principles is assisted by the rights granted to individuals to have access to information about themselves and to seek correction of it. The Act also contains a complaints' procedure, which places emphasis upon conciliation and the reaching of voluntary settlements. Only as a last resort, where there are unresolved complaints, are these to be determined by the Complaints Review Tribunal.

The Minister of Justice of the time, the Hon Douglas Graham, made the following remarks when moving the third reading of the Privacy Bill:

> "The legislation is not designed to be used as a sledge hammer. It is not designed to be used to drag people screaming off to jail if they do something wrong under the privacy law. The legislation aims to encourage those agencies and organisations that are holding personal data to use that data for the purposes for which it was obtained, and to recognise that people's personal information is precious to them. This legislation is a persuasive type of legislation, rather like the human rights laws. It is not meant to be punitive.[4]

Storage and Security of Personal Information

In this discussion, I should like to focus more upon Information Privacy Principles and particularly Principle 5 dealing with the storage and security of personal information.

The Information Privacy Principles are based on the recommendations from the Organisation for Economic Co-operation and Development concerning Guidelines on the protection of privacy of personal data 1980[5]. The Information Privacy Principles in the Privacy Act have been developed in accordance with the Guidelines recommended by the OECD and also modelled upon the Information Privacy Principles contained in s 7 of the Privacy Act 1988 (Australia).

Principle 5 provides that an agency that holds personal information must ensure that the information is protected by reasonable security to safeguard it against loss and unauthorised access, use, modification, disclosure and other misuse. If it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use of disclosure of the information.

Principle 5 is not necessarily breached as a result of mistake or accident. The Principle, in fact, is directed to the quality of the particular security measures in place and not to whether a breach of these measures has, in fact, occurred.

Security measures do not have to be foolproof, so long as they are reasonable in the circumstances.

---

[4] 1993, 76 New Zealand Parliamentary Debates 15210

[5] The OECD Guidelines

Liability for a failure to comply with the Principle is not absolute. Human error may be factored into the equation.

In one case, correspondence was incorrectly addressed and delivered to a neighbour. This person opened it. The person who should have received the item complained to the Privacy Commissioner. The Privacy Commissioner formed the view that the Inland Revenue Department had not failed to take reasonable steps to protect the information. IRD had policies and training in place to make it clear to staff of the importance of care in handling information. It was held that one mistake by an employee did not necessarily mean that the security measures were inadequate[6].

In another case, a life insurance company developed a sample plan for marketing purposes. This was, in fact, based upon an actual financial plan. The individuals, whose personal information formed the basis for the sample plan, could be identified from it. They complained to the Privacy Commissioner.

Although there had been a breach of Principle 11 (Limits on the Disclosure of Personal Information), Principle 5 had not been breached. Principle 5 does not require that safeguards are failsafe but that they are reasonable in the circumstances. In the case in question, the safeguards were reasonable and there was a one-off error of judgement. Errors of judgement were not covered under Principle 5 unless there was some kind of systemic failure in relation to security safeguards.[7]
As long as safeguards are reasonable, they do not have to be perfect and aspects of human error are factored in. This seems to be a consistent thread throughout the cases.

However, Principle 5 requires more than the existence of a procedure and training programme. These do not guarantee that the procedure will be followed. The Privacy Commissioner emphasised the importance not only of having a procedure and training programme but also an implementation procedure, which must be effective in respect of which steps need to be taken to ensure that it is followed. Such steps could include re-training on procedures following the development of the problem, as well as regular training and refresher courses. It was considered that it may be proper to include a disciplinary provision, so that staff would know there would be consequences for failure to follow a procedure[8].

Under Principle 5, information must be protected “by such security safeguards as it is reasonable in the circumstances to take”. What does “reasonable in the circumstances” mean? The OECD Guidelines have developed a "Proportionality Principle" and the concept of standard of reasonableness “in the circumstances” is consistent with that. Clause 16 of the OECD Guidelines states

> “security levels, measures in cost should be appropriate and proportionate to the value of and degree of reliance on the information systems and the severity, probability and extent of potential harm, as the requirements of security vary depending upon the particular information systems”.

[6] Case No 14982 1988, NZ Privacy Commissioner 15
[7] Case No 26280, 2002, NZ Privacy Commissioner 2 (2002)
[8] Case No 10668, 1997

It has been observed that the following matters may be relevant in assessing reasonableness:

(a) The workability of the safeguard.
(b) The cost of the safeguard.
(c) The risks involved.
(d) The sensitivity of the information, and
(e) The other safeguards that are already in place.

In one case, a bank had a procedure of sending communications in window envelopes. In the complaint in question, a window envelope was not used resulting in the mis-addressing of financial information. The nature of the information required protection by fairly stringent safeguards. It was necessary, following the complaint, for the bank to issue written instructions to staff concerning correspondence with customers. All correspondence had to be sent in window envelopes. In the instant case if a window envelope had been used, the information would not have been mis-addressed. In addition, staff were instructed to use unique customer numbers, in order to ensure that the person requesting the information was, in fact, actually entitled to it. This was considered to be a satisfactory assurance against the repetition of the action which led to the complaint.

Paragraph 11 of the OECD Guidelines, dealing with security and safety, provides that personal data should be protected by reasonable security safeguards against such risk as loss or unauthorised access, destruction, use, modification or disclosure of data.

It is important to note that security and privacy issues are not identical but privacy limitations on data use and disclosure must be in force by security safeguards. These safeguards include the following:

(a) Physical measures, such as locked doors and identification cards.
(b) Organisational measures, such as authority levels with regard to access to data.
(c) Informational measures, particularly in computer systems, such as enciphering and threat monitoring of unusual activities and responses to them.

Organisational measures include obligations for data processing personnel to maintain confidentiality.

Within the context of information security, those who are responsible for maintaining systems which contain personal information would do well, therefore, to take consideration of their obligations under the Privacy Act, which should be read in tandem with the OECD Guidelines. From the very brief discussion undertaken in this paper – which by no means should be considered to be even approaching a comprehensive level – it appears that whilst systems were not seen to be absolute and exceptions may be made for human error, nevertheless it is incumbent upon those responsible for information security systems to ensure that a proper system is in place initially and that continual monitoring, training and supervision should be undertaken.

The Prescription of Offences and Penalties for Intrusions Into or Activities Involving Information Systems.

The computer crimes provisions of the Crimes Act create offences and provide penalties for intrusions or activities involving information systems or, as they are defined in the legislation, computer systems.

There are a number of different heads of criminal activity regarding computers.

(a) Accessing Offences (s 249 and 252)
(b) Damaging or Interfering Offences (s 250), and
(c) Ancillary or Preparative Offences dealing with the provision and possession of software for committing crimes and the provision of information which would assist in computer criminal activity (s.251).

The precise wording of the legislation is contained in the appendix. In this section I propose to discuss, first, the elements of computer offences, secondly, some anomalies that are presented by the way in which the legislation came into being and thirdly, some cases that have been decided regarding computer crime.

(1) Accessing Offences

The accessing offences are contained in ss 249 and 252 of the Crimes Act.

I shall deal firstly with the offence of simple access. The offence of simple access, without authorisation, is created by s 252. The elements of the offence are as follows:

(a) There must be intentional access[9]
(b) The access must be to any computer system.
(c) The access must be without authorisation.
(d) The access must be direct or indirect.
(e) The accused must either:
    (i) Know that he or she is not authorised to access the computer system or
    (ii) Is reckless as to whether or not he or she is authorised to access the computer system.

It is to be noted that the offence is complete upon the proof of those elements. It matters not that the accused did no damage nor even opened any document or programme on the computer system. The offence is directed towards access.

This section was, perhaps, one of the most controversial of all of the computer crimes sections of the Crimes Act. The Law Commission, in its Report No 54, Computer Misuse 1999, observed that the main argument against creating criminal offences in relation to unauthorised access was that it would create an anomaly in terms of existing criminal law which does not punished unauthorised access to information. Gaining unauthorised access to information should be an offence only if, in the process of gaining the access to the information, some other specified offence, such as trespass or theft, is committed. If unauthorised access was gained to information without committing a trespass or theft, an offence would generally not have been committed. The Law Commission gave the example of taking a photograph of a document sitting on another's desk from an adjacent building or reading a document over the shoulder of another passenger in an aeroplane.

[9] Access is defined in s.248 and means "instruct, communicate with, stoare data in, receive from, or otherwise make use of the resources of a computer system. Computer system is also defined in s.248

The Law Commission observed that if gaining unauthorised access to computer data was to be a criminal offence, the person who gained such access would be liable to criminal sanctions, whereas the person who gains unauthorised access to exactly the same information without using a computer and without committing a trespass or theft, will not have committed an offence. This presented an anomalous situation. It was also noted that the Law Commission was assuming that the unauthorised access would be to data stored in a computer, whereas the way in which the legislation has been passed is that the offence is complete upon unauthorised access to the computer system absent any access to data contained therein.

However, the Law Commission was of the view that the public interest in encouraging the use of computers and protecting the community from the misuse of computers outweighed the problems created by the anomaly. The Commission pointed out that there were differences between unauthorised access to information achieved via a computer and access to information achieved by other means. These differences were stated as follows:

(1) Information stored on a computer system is not protected by physical barriers to access or by the law of trespass or theft, as is the case with information recorded in hard copy.

(2) Once a person has obtained access to a computer, vast amounts of information become available, which may otherwise have been stored in a multitude of locations. The computer, itself, may be used to search for, select and process specific data at very high speeds.

(3) The consequences of unauthorised access in the digital age go beyond what was possible with paper-based or manual systems. Not only can access to information be obtained but that information may be amended or otherwise used.

(4) A knowledge-based economy is reliant on information stored on a computer. In this respect it is recognised that computer systems are becoming the norm for the storage of data rather than filing cabinets.

Section 252(2) contains what used to be called a proviso to the offence but which is an exception. The offence created under s.252(1) does not apply to people who are authorised to access a computer system for one purpose, yet access it for another purpose.

Thus, if a person has limited access rights to a computer system – say for the purposes of word processing or document creation – and obtains access to that part of the computer system that deals with the payroll, pursuant to the provisions of s.252(2), that person has not committed an offence.

This sub-section was introduced at behest of the trade union movement, who were concerned that the criminalising of unauthorised access to a computer system in the circumstances that I have just described, could give automatic grounds for dismissal rather than having recourse to normal employment law principles. It was considered that if an employee did exercise unauthorised access to another part of an employer's computer system and, subsequently, caused damage or altered records to that part of the computer system, other offences would be available, in particular those created under s 250 relating to damaging or interfering with a computer system or, depending upon the circumstances, s.249 relating to accessing a computer system for dishonest

purposes. However, we shall see in the case of *Police v Robb*[10], proving damage to a computer system may not be as easy as it seems.

Again, to be abundantly clear, the offence created in sub-section 1 of s 252 does not apply where access to the computer system is gained by a law enforcement agency under the execution of interception warrant or a search warrant, or under the authority of any act or rule of common law. This is to make it clear that the provisions of s.252(1) do not exclude existing statutory or common law law enforcement procedures[11].

Finally, s 252 does not apply in the circumstances specified in ss 253 and 254, which creates a qualified exemption to access without authorisation if a person is acting pursuant to an interception warrant in the case of the New Zealand Security Intelligence Service, or if a person is accessing the system pursuant to the provisions of the Government Communications Security Bureau Act 2003. In addition, as far as the SIS is concerned, those who are requested to give assistance in the execution of an SIS warrant are exempt from criminal liability.

The other access offence is created by s 249 of the Act creates offences involving the access of computer systems for dishonest purposes. There are two major offences. One is the actual dishonest access to a computer system, where something is obtained. The other involves an attempted dishonest access with the intention of obtaining something of value but clearly in circumstances where the attempt has been unsuccessful.

The important element in both offences is the dishonest intention accompanying the access.

For the first offence, the elements are as follows:

(a) Access to a computer system
(b) The access must be direct or indirect
(c) Dishonestly, by deception and without claim of right
(d) The obtaining of any property, privilege, service, pecuniary advantage, benefit or valuable consideration, or a cause of loss to any other person.

It is to be noted that the benefits obtained are very wide or, alternatively, loss may be caused to another person where a benefit does not accrue to the offender. Thus, for example, a person may dishonestly access a computer system, say of a bank, and transfer funds out of the victim's account into the account of another person – not that of the offender. In such a circumstance, loss would be caused to another person, although the offender would not, himself, have obtained the property, privilege, service, pecuniary advantage, benefit or valuable consideration.

It is also interesting to note that the offence created under s 249(1) is utilised in cases of copyright piracy, where offenders use computer systems to copy DVDs or CDs.

[10] To be discussed below
[11] s.252(2)

The maximum penalty imposed for actual dishonest access to a computer system where something is gained or loss is caused is seven years imprisonment.

The second offence – the attempt offence has the following elements:

(a) Access to a computer system
(b) Direct or indirect
(c) With the intention dishonestly or by deception and without claim of right
(d) To obtain any property, privilege, service, pecuniary advantage, benefit, valuable consideration or an intention to cause loss to any other person.

Thus, it is not necessary for any actual loss to be caused to the victim or any actual obtaining of the property, privilege, service, pecuniary advantage, benefit, or valuable consideration. All that is required is a specific intent to dishonestly, or by deception and without claim of right, to achieve the particular goals.

The lesser nature of that offence is recognised by the maximum penalty, which is set at five years imprisonment.

Those, therefore, are the offences involving access to computer systems.

(2) Damaging or Interfering Offences

Section 250 creates the offence of damaging or interfering with a computer system. Under normal circumstances, of course, access would be necessary for this particular offence but the Section is directed towards the consequences of access. Two major categories of offence are created. One involves damage to computer system where a danger to life is likely to result and the elements that are required for proof are substantially less than the second category of offence, which relates to damaging the system itself where there is no danger to life.

Section 250(1) is the offence relating to damaging or interfering with the computer system where a danger to life is likely to result. The elements are as follows:

(a) Destruction, damage or alteration of a computer system
(b) The destruction, damage or alteration must be intentional or reckless
(c) There must be knowledge, either expressed or implied, that danger to life is likely to result.

The seriousness of this office is reflected by the maximum penalty, which is set at 10 years imprisonment.

The elements of offences under s 250, sub-section 2, are a little more complex.

I shall commence with the elements in terms of consequence:

(a) There must be damage, deletion, modification or otherwise some form of interference with or impairment of data or software in a computer system, or
(b) The causing of data or sofware in a computer system to be damaged, deleted, modified or otherwise interfered with or impaired, or

(c) That the computer system be caused to fail or to have service denied to any authorised users.

All of these have to be done:

(a) Intentionally or recklessly; and
(b) Without authorisation
(c) With a specific knowledge that the person charged is not authorised or is reckless as to whether or not they are authorised.

Thus, the offences created under sub-section 2 require proof of a number of prohibited activities relating to the computer system involving some form of damage or alteration akin to damage, along with a lack of authorisation to do those acts, coupled with a knowledge of lack of authorisation or recklessness as to whether or not authorisation is granted.

The element of intention may be critical, as was the case in the recent decision in *Police v Robb.*

One of the charges that Mr Robb faced was laid under s250(2) relating to damaging or interfering with the computer system by the deletion of files.

Mr Robb worked for a company and, in the course of time, his employment was terminated. He had come to the company with data in the form of a contact list, which he incorporated with other data on his employer's computer. Following the termination of his employment, an examination of the computer suggested that important data, including the contact list, had been irrecoverably deleted. This gave the impression that by virtue of that fact, the deletion was intentional. It later transpired that the data was, in fact, in the unallocated space on the hard drive and could be recovered.

The Court's approach was that data could be accidentally deleted from where it was originally placed on a computer system and could be capable of being located in some other part of the system.

In such circumstances, the intent of the individual who deleted the file is important to know, so that further investigation was required to prove beyond doubt as to whether or not the file was, in fact, wiped. Expert evidence revealed that wiping a file required an additional conscious decision over and above simple deletion and the Judge held that for the prosecution to establish a criminal offence of damaging or interfering with a computer system by deletion, it was necessary to exclude the innocent deletion of data.

A distinction was made between wiping and deleting. Wiping was to render data irrecoverable. Deleting was to remove data by pushing the delete key. To wipe data required a certain level of sophistication on the part of the user.

The distinction between wiping and deleting was held to lie in assessing the inference that may be drawn from the act to assess the mental element of the charge – intentional recklessness.

The charge in Robb was a specific one and alleged deletion of data. The Judge's suggestion effectively is that the prosecution is required to establish what the level of competence in terms of computer use of the user was. If the user had a sophisticated knowledge of computers, he or she may know that pushing the delete key only removed a directory reference rather than remove the data entire. A sophisticated user would know that the only way in which the data could be removed was to write over the sectors in which it was contained. An unsophisticated user may well conclude that by pressing the delete key, the material was thereby removed and could not be recovered.

Two matters arise for consideration. The first is that it would appear to be unwise to lay a charge for deletion of data when a more general charge of damaging a computer system might be easier to prove. Damage has a much wider definition and encompasses functional derangement of a computer system. Functional derangement of a computer system may mean simply that the normal expectations of a user are not fulfilled as a result of the actions of the accused. It was the expectation of Robb's employers that he would not remove important data. He frustrated those expectations by pressing the delete key. In that respect, he effected the normal expectations of his employers by his functional derangement in pressing the delete key.

The second point is that, in my respectful view, the Judge has imposed an additional layer of complexity to what should be a relatively simple exercise. What was not addressed was the fact that the data that was still available on the sectors of the hard drive could not be accessed in the normal course of computer use. Special software is required to recover data that has been the subject of a deletion. A number of specific steps must be undertaken to recover data. In the hard copy world and analogy can be drawn with a document that is placed in a shredder. That document can be reconstructed if all of its elements are removed from the shredder bin in the shredded state and laboriously and carefully re-assembled with the utilisation of sellotape or glue. This does not mean that an act intentional damage of the document has not taken place. It most certainly has. And the intention of the person in placing the document in the shredder is abundantly clear. The analogy can be drawn between the shredder and the delete key. Certainly, the material or data can be recovered or reconstituted. But a considerable amount of effort is required. And the actions of the person in pressing the delete key and the intentions that are associated with that action are still abundantly clear.

(3) Ancillary or Preparative Offences

The final series of offences covered by the computer crimes section of the Crimes Act involve activities associated with the commission of computer crimes. Section 251 creates an offence of supplying software or other information that would enable the recipient of the software or other information to access a computer system without authorisation. Again, specific intentions are required. The supplier has got to be aware that the sole or principle use of the software or information is for the commission of a crime or that it is promoted as being useful for the commission of a crime, even although it may be promoted for another purpose. The first offence created by s 251 therefore criminalises the provision of or distribution of software information that may be used to commit crimes.

The second offence created by s 251 involves the person who possesses the software or information. A person must have:

(a) Possession of any software information
(b) That would enable him or her to access a computer system without authorisation, and
(c) Must intend to use that software or other information to commit a crime.

Thus a person who has a hacking programme that he or she does not intend to use for the purposes of the commission of a crime but wishes to examine, study and understand how it works, for the purposes of devising a security system to prevent an attack using that software, has not committed an offence pursuant to s 251(2) because there is no associated intention to use the software or other information to commit a crime. This may bring some comfort to computer scientists and investigators.

Both offences contained in s 251 carry with them a maximum of two years imprisonment.

Anomalies in the Legislation

There are a couple of anomalies in the computer crimes section of the Crimes Act which arise from the way in which the legislative process was undertaken. It may be of interest to know that in 1989 the offences contained in s 249 and 250 were the subject of a significant package of amendments proposed to the Crimes Act. For a number of reasons, those amendments were not effected. New Zealand seemed to manage without any computer crimes provisions to its Crimes Act for 13 years until the 2003 amendments came into force. The way in which those amendments came to pass arose as a result of two highly-publicised incidents that occurred in the late 1990s, one which culminated in the case of *R v Garrett*, where the accused was charged with a number of offences under the provisions of the Crimes Act then in force. The other did not involve a prosecution because there were jurisdictional questions (which were not difficult to answer iof investigating authorities had applied their minds to seeking an answer), where a 17 year old was alleged to have deleted a number of web pages on a web server located in the United States. By this time, of course, the Internet had been commercialised, the dot com boom was underway and computer use was expanding, both in the home and in businesses. The Law Commission was urgently asked to consider issues of computer misuse, culminating in their report in 1999, which was swiftly followed by the introduction of amendments to the Crimes Act. The initial Bill contained the present s 248 (the definition section), s249 (access for dishonest purposes) and s 250, damaging or interfering with a computer system.

The definitions section proposed in the initial Bill defined access in the computer system and the specific wording of that section was to apply to the two substantive sections which were the subject of the initial Bill.

A Supplementary Order Paper subsequently introduced and proposed s252 (Access Without Authorisation), which was added into the Bill. No consequential amendment was made to the Definitions section, so a proposed section that dealt specifically with unauthorised access to computer systems without any issue of damage/access to data or dishonest purposes was not cross-referenced to the Definitions section 248 which specifically defined principal elements of the offence, namely computer system and

access. The anomaly was further complicated after the Select Committee hearing, when s251 was introduced at the behest of the Telcos Once again, as a result of a legislative drafting oversight, the provisions of s248 did not apply to s251. Elements of access and computer systems were again incorporated in that section.

This may not mean much to the lay person and may be seen to be a lawyers' exercise in nit-picking. There are ways by which lawyers and Judges can get around what amounts to a legislative oversight. What it does demonstrate is a certain lack of care in the legislative process. It is presumed that when Parliament creates a criminal offence, the consequences of which involve potential interference with the liberty of the subject, it does so by clear and plain words. Clumsy and careless draftsmanship simply cannot be tolerated and demonstrates, in my view, something of a cavalier disregard for fundamental principles involving the creation of criminal offences.

The second problem which arises involves the way in which offences may be brought before the Court and, once again, arises as a result of the way in which the legislative process was undertaken.

Once again, the problem is one which could be described as lawyers' law but makes the process of bringing a case to trial excessively complicated.

All the crimes in the Crimes Act can be dealt with by way of trial by jury. Because of the seriousness of certain crimes, like murder, manslaughter, aggravated robbery and the like, Parliament has decreed that those offences can be dealt with by trial by jury only. However, a large number of lesser offences, including burglary, theft, fraud and the like, may be dealt with before a Judge alone. These are charges which are deemed to be indictable but triable summarily. The accused person can elect whether or not he or she wished to be dealt with by a jury or by Judge alone. The charges which are indictable but triable summarily are contained in a schedule to the Summary Proceedings Act. When the computer crimes legislation was introduced, section 249 and 250 were deemed to be crimes that were indictable but triable summarily. Thus, an accused person can elect to be dealt with by Judge alone or by a jury. And it will be remembered that the penalties for offences under ss 249 and 250 are quite significant. In the case of the offence under s 250(1), the maximum penalty is ten years imprisonment.

Sections 251 and 252 contain a maximum penalty of two years imprisonment. One would have thought that they would, as a matter of course, be included in that schedule to the Summary Proceedings Act which would make them indictable triable summarily. However, this is not the case. Once again, as a result of legislative oversight or, perhaps, even carelessness, these charges are purely indictable. That means that an accused person has no choice as to whether or not he or she may elect to be dealt with by a Judge alone. Any of these cases under ss251 and 252 **MUST** be dealt with before a jury. This adds a level of complexity to what should be a relatively straightforward procedure. An accused person must go through two hearings before liability is established – a preliminary hearing to determine whether or not there is a case to answer and, then, the trial before a jury. One would have thought that for offences carrying a lesser penalty than those specified in Sections 249 and 250 that a trial before Judge alone would be available. But it is not.

Applying Other Crimes Act Principles to Computer Crime - A Case Study

If, however, one were to consider that the computer crimes provisions of the Crimes Act was the only way in which computer offences could be dealt with, one would be mistaken. The case of *Police v Davies* illustrates this. Davies was employed by a web design company and had Internet access as part of his job. He used this access to download music and pornographic videos which he stored in a hidden directory on his employer's server. He had been warned that such private downloading was not permitted. His employer had Internet access which they were charged on a monthly basis by Telecom. They were required to estimate their megabyte usage each month.

Davies continued to download music and illicit videos, which he continued to store on his server contrary to his employer's instructions. When he was found out, he was dismissed and he was charged with theft. He was not charged with any offences under the computer crimes provision of the Crimes Act. The reason for this was that for the value of the "property" that he derived – and I shall discuss property in a moment – to charge him under the computer crimes provisions of the Crimes Act would clearly be overcharging.

How then did he fall within the concept of theft, which relates to unlawfully and without claim of right taking somebody else's property. The Judge held that Internet access in the megabyte cap was a form of property and that it fell within the definition of property and words "any other right or interest". The private use of this access by Davies deprived or interfered with his employer's right or interest in the Internet access and megabyte cap. Guilty knowledge was established because he knew he was not allowed to do what he was doing and although the megabyte cap may not have been exceeded, it was still an interference with the employer's property right because what, in fact, had occurred was that usage had taken place which, if followed by the employer's legitimate usage, could well have pushed them over their megabyte cap.

This was a case which could have been dealt with under the computer crimes provisions of the Crimes Act but demonstrates that as a result of some of the amendments that took place in 2003 to other parts of the Crimes Act, other offences are available.

Effectiveness of Criminal Sanctions

What affect have the computer crimes provisions had on information security? The computer crimes provisions of the Crimes Act do not automatically mean that computer misuse is going to be prevented. What they do is to provide that where computer misuse has taken place, consequences will follow. The criminal law contains a significant moral element to it. People know what the law is. They know that certain conduct is required of them. They may choose whether or not to abide by the law or embark upon illicit conduct. The definition and the consequences of illicit conduct are what the criminal law provides. In addition, with the exception of s250(2) the computer crimes provisions of the Crimes Act are directed towards the protection of computer systems rather than the information contained therein. Only s250(2) specifically deals with interference with data or software in computer systems. I have already noted that the elements to be proven to s250(2) are somewhat complex and as a result of the decision in *Police v Robb*, which is only of persuasive authority, a further layer of difficulty has been added.

Protection of Trade Secrets

The information security provisions of the Crimes Act go beyond those contained in the computer crimes' sections. Section 230 provides protection for trade secrets. It is to be noted that this goes beyond the protection that is provided by the Copyright Act, the Patents Act, the Designs Act 1953 or the Layout Designs Act 1994.

The definition of a trade secret, in fact, gives wider protection than the copyright and associated intellectual property provisions of the law. A trade secret means any information that:

(a) Is or has the potential to be used industrially or commercially, and
(b) Is not generally available in industrial or commercial use, and
(c) Has economic value or potential economic value to the possessor of the information, and
(d) Is the subject of all reasonable efforts to preserve its secrecy.

A person who, with intent to obtain a pecuniary advantage or to cause loss to another person dishonestly and without claim of right, takes, obtains or copies the document or a model or other depiction of anything or process containing or embodying a trade secret, knowing that it contains or embodies a trade secret, commits an offence punishable by up to five years imprisonment. The offence applies equally to taking or obtaining a copy of such document, model or other depiction.

There are a number of hurdles that have to be cleared before the offence can be established. There has to be a specific intent either to obtain a pecuniary advantage or, alternatively, to cause loss to another person. The activity must be done dishonestly and without a claim of right – that is a belief that one is entitled to do what they are doing. In addition, the person has got to know that the document, model or other depiction of anything or process containing or embodying a trade secret actually contains that information.

It is to be noted that the Section of the Act does not apply only to employees, although clearly employees or members of an organisation which has developed the trade secret would be those most likely to have access to it and benefit from its further exploitation.

What the Section does is that it applies to a trade secret an element of property and creates a specific offence in relation to that property. It is also interesting to note that it specifically applies to the *copying* of the trade secret, or alternatively obtaining a copy or taking a copy of the trade secret.

Security of Personal Privacy Information

The provisions are contained in Part 9A of the Crimes Act address the protection of personal privacy and the creation of certain offences where there are breaches of those protections by use of interception devices. Part 9A must be balanced against the provisions of Part 11A. The reason for this is that the overall scheme of the legislation provides firstly a prohibition on the use of interception devices for the intentional interception of private communications. There are exceptions provided where the person intercepting the private communication is a party to it or does so pursuant to any authority conferred upon him by provisions of Part 11A, the New Zealand Security Intelligence Service Act, the Government Communications Security

Bureau Act, the Misuse of Drugs Amendment Act or the International Terrorism Emergency Powers Act 1987. The provisions of these various pieces of legislation all relate to the utilisation, in some shape or form, of interception devices. The way in which the utilisation of interception devices may be obtained has varying levels of ease or difficulty, depending upon the particular legislation.

In addition, Part 11A deals with obtaining evidence with listening devices rather than just obtaining information. The importance is that evidence can be used in a criminal prosecution or civil proceeding. There are certain requirements for that evidence to be admissible. If the evidence has been obtained in a manner that is not authorised by part 11A, it is inadmissible and cannot be presented. Nevertheless, it still remains as information, which can be utilised as a lead in an ongoing investigation. Problems may arise as to whether or not evidence derived from that information is admissible but that is not within the ambit of this discussion.

What is commonly understood as telephone tapping and bugging is covered by Part 9A. Equally, it is clear that listening to a conversation on CB radio is not an offence. No-one could reasonably expect the communication to be confined to the parties. So, too, is the use of a scanner to listen to emergency service and police frequencies.

Difficulties arise with the interception of conversations carried on over a mobile or cellular phone. The answer might appear to lie not in the awareness by one or more of the parties to the communication that an interception is technically possible, but in the likelihood that it is assigned to the interception of the communication in the circumstances in which it is made.

In earlier legislation, the prohibition related to the interception of oral communications only. Thus, it was not an offence to use a device to intercept other forms of communication, such as a facsimile machine transmission or telephone pager messages. The landscape has changed with the introduction of the Computer Crimes Section, so that consequential amendments were required to legitimise interception in certain cases and criminalise it in others. New provisions in Part 9A recognise the importance of modern communication systems, including the internet. They provide for specific exceptions to the interception rules for the maintenance of communication systems. Privacy concerns are met by the requirement for the destruction of the information once it is no longer needed. There is no reference to a period within which the need to retain may have abated and the wording of the Section is so wide that the information may be retained indefinitely.

The disclosure of private communications that are unlawfully intercepted is prohibited.

Of interest to IT professionals, however, are the provisions of Section 216F. This contains prohibitions against certain types of unlawful disclosure. An unlawful disclosure is defined as:

(a) The intentional and unauthorised disclosure of the existence of an interception warrant to be exercised by a member of the police if the disclosure would, or is likely to, prejudice an investigation, or

(b) The intentional and unauthorised disclosure of:

(i) Any information gained when undertaking maintenance of a communication service, or
(ii) Any information gained when assisting with the execution of an interception warrant other than to the agency executing the warrant.

There must be intentional and unauthorised disclosure of
(a) the existence of an interception warrant and/or
(b) something that is likely to prejudice an investigation.

However, the aspect of the legislation that would be of interest to IT professionals is covered by 216F(1)(b), which deals with the disclosure of any information gained when assisting with the execution of an interception warrant other than to the agency executing the warrant – which clearly applies to technical experts who may assist investigative agencies in their interception activities. It is becoming a practice to obtain assistance from technical experts in the course of an investigation. This provision could also encompass ISP employees who assist in investigation. There are requirements in a number of pieces of legislation, including the Security Intelligence Service Act, the Government Communications Security Bureau Act and the Telecommunications (Interception Capability) Act of 2004. All these pieces of legislation provide, in some shape or form, for the requirement of assistance by members of organisations to assist in the execution of warrants for the carrying out of interception activities.

Under s216F(1)(b), it is necessary to prove that the disclosure is intentional and unauthorised. However, the provisions of sub-paragraph (i) are very wide and extend to any information, not just to information, for example, that may comprise the operation of the service. Thus, a cone of silence is placed over the release of any information gained while maintaining the service. This has interesting implications if a person felt that something unethical (but not necessarily unlawful) was taking place. There is provision for the disclosure of information obtained while monitoring a communication service if that information appears to relate to the commission of a crime, or it has caused serious harm to any person.

The Creation of Exceptions for Law Enforcement and Security Agencies

This is the third theme that I should like to consider.

Part 9A of the Crimes Act 1961 relates to the unauthorised use of interception devices and associated matters. Part 11A of the Crimes Act, together with provisions of the Misuse of Drugs Act, authorise the utilisation of interception devices in certain circumstances by police and customs for the purposes of obtaining evidence relating to serious crimes or drug dealing offences.

The circumstances under which interception devices can be used is rigorously circumscribed. Application has to been made to a High Court Judge for the issue of an interception warrant. The interception warrant is of limited duration. If it is necessary to continue the utilisation of the interception warrant, a fresh application has to be made. Once the interception activity has taken place, a report must be forwarded to the High Court Judge issuing the warrant. In addition, the utilisation of interception warrants is reported to Parliament. A high level of proof is required.

Prior to 2003, the only communications that could be intercepted were telephone communications and “real time” communications, using a bugging device on a physical location. Following the 2003 amendments, interception of information in transit through electronic network systems may also take place. This has been done by the utilisation of the concept of a "facility". The effect of this is to extend interception activities beyond that directed at people and places and to communication systems themselves. A facility is defined[12] as an electronic address, 'phone number or a similar facility that enables private communication to

(a) take place between individuals or

(b) to be sent to or from an identified individual.

Electronic address and 'phone numbers are referred to but there are a couple of significant points:

1. Electronic address is not defined. This could mean an email address, a static IP number or even a temporarily assigned IP number for the duration of an on-line session. Thus, this aspect of the definition could be very wide. A 'phone number is easily understood and more limited in scope than an electronic address.
2. The definition is widened by reference to a similar facility that enables private communication to take place between individuals or to be sent to or from an identified individual.

The addition of a facility, therefore, extends the scope to electronic communication systems such as the internet. Thus, the extent of interception warrants has been extended from personal warrants and premises warrants to facility warrants.

Of particular importance is the care that must be undertaken by those who may be called upon to assist investigative authorities to ensure that information is not disclosed.

It is also important to note that the proper compliance with the provisions of the legislation allows the information obtained by the interception to be admitted as evidence in Court. The importance of this cannot be over-estimated. What investigating authorities are authorised to do by statutory exception is to access computer systems to obtain information and also utilise listening devices or interception devices in circumstances that, for private citizens, is clearly illegal. The legislative power of Parliament of course enables investigative authorities to undertake these activities for the successful prosecution of criminal activity, which is in the public interest and part of the balancing of interests that are so important in the social contract.

The Government Communications Security Bureau and the SIS

Other investigative agencies, such as the Security Intelligence Service and the Government Communications Security Bureau have powers to carry out interception activities as well. They also may require assistance in carrying out their interception activities. I do not intend to go into any great detail about the processes by which interception activities may be carried out by these organisations other than to observe that it is not necessary for the approval of a High Court Judge or any other judicial

[12] s312A(1) Crimes Act 1961

officer to issue interception warrants to SIS investigators or to GCSB investigators. Essentially, the process is an internal one requiring interaction between members of the SIS or GCSB and members of government. There are no review provisions by the Court and, of course, the justification that may be advanced for the "softness" of the provisions is the interest of national security. The GCSB Act, for example, provides that an application for an interception warrant must be made by the Director, in writing, to the Minister in charge of the GCSB for the issue of an interception warrant to authorise the use of interception devices. The SIS Act provides that the Minister and Commissioner may jointly issue an interception warrant.

GCSB warrants authorise the interception only of foreign communication, whereas SIS interception warrants may relate to domestic communications or foreign communications as well.

The GCSB Act provides for specific authorisation to access computer systems and authorisation to engage in this activity may be made by application by the Director to the Minister.

Anti-Terrorism Legislation

The International Terrorism (Emergency Powers) Act of 1987 is a little-known piece of legislation designed to deal with international terrorist emergencies. The process of determining the existence of an international terrorist emergency is set out in ss5 and 6 of the legislation. A meeting of Ministers may authorise the exercise of emergency powers in certain circumstances. Ministerial authorisation of the exercise of emergency powers may endure for a limited period. The House of Representatives may extend the authority to exercise emergency powers pursuant to s7 of the legislation.

The legislation specifically relates to interception. The police may, for the purposes of preserving life threatened by any emergency connect any additional apparatus to, or otherwise interfere with, the operation of any part of the telecommunication system and intercept private communications in the area in which the emergency is occurring. That power may be exercised only by or with the authority of a commissioned officer of the police, who must believe, on reasonable grounds, that the exercise of the power will facilitate the preservation of life threatened by the emergency. That pre-condition is essential but the powers are at the discretion of the commissioned officer. He must have reasonable grounds for belief that the exercise of the power will facilitate the preservation of life. There is no monitoring system as set out in the interception provisions in the Crimes Act or the provisions of the Summary Proceedings Act covering tracking devices.

Tracking Devices, Call Data Warrants and Search Warrants

It is apposite at this point to mention two other aspects of information security that have recently become part of our legal landscape. One is the introduction of warrants authorising the utilisation of tracking devices.

Recently, there was before Parliament a piece of proposed legislation called The Counter Terrorism Bill. This legislation provided a number of provisions dealing with legislative steps that could be taken to deal with counter terrorist activities. It involved, for example, the utilisation of tracking devices and circumstances under

which compelled disclosure of information allowing access to computer systems could be required. When the legislation was finally passed, however, it did not pass in the form of a Counter Terrorism Act. What happened was that a number of other pieces of legislation, which had nothing to do with counter-terrorism, were amended. Once such piece of legislation was the Summary Proceedings Act.

The Summary Proceedings Act deals with certain procedures attendant upon the prosecution of crime and the processes and procedures which may be adopted. Specific to our purposes, the legislation deals with the issue of search warrants. The amendments relating to tracking devices have fallen under that general umbrella of search warrant powers. Police or Customs may apply to the Court for an Order authorising the utilisation of a tracking device, so that the movements of a particular object, such as a motor vehicle, a brief case or, in many cases, a package arriving at the international airport may be monitored and traced to its ultimate destination. In my experience, the tracking device provisions have been used in circumstances where a parcel has been found to contain illicit chemicals such as sudafedrine, which is used for making methamphetamine. The package is noted at the airport, opened, found to contain illicit substances, re-wrapped and sent on its way after a tracking warrant has been obtained. It may then be tracked to its ultimate destination and once it is there, investigating authorities are able to identify those who have received it and carry on their investigations further.

Call Data warrants may be applied for under the Telecommunications (Residual Provisions) Act of 1987. A Call Data Warrant authorises a member of the police or a customs officer to connect a telephone analyser or to have one connected to any part of a telephone network that he or she suspects is being used by a person named in the warrant. Call data warrants record or enable the recording of call-associated data. The telephone analyser that is used does not monitor or record the content of any communicational conversation. All it records is the origin, direction, destination and termination of the telecommunication. It establishes the number from which the call was made and the number from which it was made and the duration thereof. Call data warrants are useful frequently in obtaining contextual evidence regarding communications between suspected criminals. In one particular case, call data warrants revealed an unusual amount of telephone activity passing between suspected criminals shortly before the commission of a crime. These criminals were professional burglars who were responsible for a significant number of burglaries in the South Auckland area. It was necessary for the prosecution to rely upon a large amount of circumstantial evidence in establishing guilt and the pattern that was created by significant numbers of telephone calls between identifiable numbers was an element of this circumstantial evidence.

Of further interest to IT professional is the now legal requirement whereby a person who has knowledge of a computer or a computer network may be required to assist access. This takes place when a police constable is executing a search warrant. He may require a specified person to provide information or assistance. It is necessary to allow the constable to access data that is held in or that is accessible from a computer on the premises named in the warrant.

The specified person may be a person who is the owner or lessee of the computer or of who is in possession or control of it and has relative knowledge of the computer or

the network of which it forms a part or, alternatively, whatever measures there may be applied to protect data held in or accessible from the computer th. There is a specific protection whereby that person may not be required to give information which may intend to incriminate him but that does not prevent the constable from requiring the person to provide such information that is reasonable and necessary to allow the constable to access data that is held in or that is accessible from a computer at is on the premises named in the warrant concerned and contains or may contain information tending to incriminate the person but does not, itself, tend to incriminate the person. Basically, the password or the encryption key is not in and of itself incriminatory, even although it may unlock or may make accessible incriminatory information.

Assistance in Investigations by IT Professionals

IT professionals may also be involved in interception activities pursuant to the provisions of the Telecommunications Interception Capability Act 2004. This does not add to the interception powers granted to various organisations by legislation already discussed. It does enhance interception capability. It places a legislative obligation on telecommunications network operators to be technically able to intercept communications going over their network when those interceptions are authorised by warrant. The purpose of the legislation is to ensure that surveillance agencies are able to effectively carry out the lawful interception of telecommunications.

In addition to the duty upon telecommunications network operators to have the technical capability to intercept communications, there is a legislative duty to assist as well. Network operators are required to provide reasonable assistance to surveillance agencies in executing an interception warrant within their technical capability and on a cost recovery basis. Because of the way in which the legislation has been framed, at first flush it might seem that a network operator is one of the large telecommunications organisations. But when one drills down through the definition of a public communications network, a public data network expands the scope of the application of the legislation to internet service providers. To make the matter even clearer, the legislation defines a service provider as any person who provides a telecommunication service within the extent of the meaning of that term as defined to an end user, whether or not as a part of the business undertaking and regardless of the nature of that business undertaking. It does not include a network operator but the service provider role extends to those who provide a public telecommunications service, such as the owners of hotels, motels and internet cafes.

The Protection of Systems Designed to Protect Information

The final matter upon which I wish to touch involves the protection for systems that are designed to protect information. This presents the subtle difference to the matters that have been discussed before. Although many of the information systems to which reference has been made may have incorporated within them systems to protect information such as passwords or encryption, it is in the field of copyright that specific protection for information that has been "locked up" is provided.

The law of copyright provides protection to copyright owners against the unlawful copying of their work. The "right to copy" is vested in a copyright owner. Only the copyright owner can authorise the copying of any work during the copyright period.

The digital paradigm presents new challenges for copyright owners. One of the realities of computer systems is that copying is essential for a computer to work. In addition, much copyright material is now being presented in digital format. Compact discs, DVDs and computer games are three of the most obvious examples and upon which I shall focus in this discussion, although the principles apply to all copyright material. The answer to the copyright problem that is posed by the digital paradigm lies within the machine itself, which gives rise to the problem. As well as making copying extremely easy, the digital paradigm also allows for copyright material to be protected by technological protection measures. Technological protection measures enable copyright owners to restrict the copying of or access to copyright material. A copy protection device will prevent a DVD from being copied or, alternatively, will not allow specially encrypted information to be copied from an authorised copy to an unauthorised one, thus rendering the unauthorised copy useless. Devices within computers, when interacting with software, may also prevent copying and, sometimes, access. An example is the Sony Play Station 2 device.

Access protection may be provided by region coding. Most people are familiar with the region coding of DVDs. This means that (absent multi-region DVD players) a DVD purchased in a Region 1 country like the United States, will not play on a Region 4 DVD player, purchased in New Zealand. Only indirectly does this have anything to do with copying. Of course, it is necessary for the DVD to play for it to be copied or the material therefrom to be copied to the DVD player but the principal function of Region coding is to prevent access to the copyright material. When one purchases a Region 1 DVD in the United States, it is legitimately acquired and may be played to the user's heart's content, as long as it is on a Region 1 DVD player. There is a line of case authority from England that suggests that in such cases the DVD is sold subject to a license that it will only be played on Region 1 DVD players. In this respect, the copyright owner is not only controlling the right to copy but is also controlling where one may view legitimately acquired material. The Courts in England favour the strict construction of a license. Courts in Australia have focussed upon the importance of copyright preventing copying, rather than restricting access.

Copyright owners were enthusiastic to protect digital material using technological protection measures. However, the imposition of a technological protection measure was only part of the story. The mere imposition of technological protection measures would not prevent those who wish to circumventing the technological protection measure to enable to access to or copying of the copyright material. A technological protection measure was only going to be as good as its inherent strength against a hacker. Thus, copyright owners sought protection not only for their copyright material (which they have had for some considerable period of time) but also sought additional protection against those who would circumvent their technological protection measures. As a result anti-circumvention provisions are common in most pieces of copyright legislation.

Anti-circumvention provisions in legislation differ in strength. For example, under the Digital Millennium Copyright Act in the United States, the act of circumvention itself is proscribed. That is not the case in England or in New Zealand. The act of circumvention of a technological protection measure would involve the copying of protected material which, in itself, would be a copyright infringement. In England

and in New Zealand, the protections that have been granted to copy protected material have been in respect of those who make and distribute a device specifically designed or adapted to circumvent a form of copy protection. In addition, those who publish information that is intended to enable or assist people to circumvent a form of copy protection, knowing that the device or information will be used to make infringing copies, has committed a specific form of infringement.

The cases in England and Australia involving the anti-circumvention provisions of the respective pieces of legislation have involved Sony Playstation 2 games consuls. What happened in those cases was that enterprising merchants made available for sale what were called “mod chips” which enabled the copy protection mechanisms that had been incorporated by Sony into their play station devices to be circumvented. This had two effects. One was that if one purchased a Sony Play Station game in, say, the United States, it could be played on a Sony Play Station consul in New Zealand. Rather like the DVD access codes, Sony had divided the world into geographical regions and the games and consuls that were sold in those regions were compatible with one another but incompatible with consuls or games that were sold in another region.

More significantly for Sony, the circumvention of Sony’s technological protection measures allowed pirated copies of Sony Play Station games to be played on the consul. If one simply copied a Sony Play Station disc, one would be unable to copy the specially encrypted coding that was recognised by the machine and that enabled the game to be played. The mod chip dispensed with the necessity for the recognition of this encryption and, thus, infringing copies of games could be played on play stations.

The approaches that had been taken by the Courts in England and Australia are dependent upon the specific wording of their different pieces of legislation. Thus, the result in England, which meant that those merchants who sold mod chips were in breach of the anti-circumvention provisions of the copyright legislation were not obtained in Australia, where a more restrictive interpretation arose as a result of peculiarities present in the Australian legislation.

The wording of the New Zealand legislation is almost identical to that of England. Thus, in terms of information that is subject to copyright, copyright owners have a double protection. If they lock up their material with technological protection measures, not only is the material itself protected by the usual laws of copyright but the technological protection measure itself is protected and those who would attempt to sell devices or provide information that would facilitate circumvention of the technological protection measure for the purpose of copyright infringement may find themselves subject to the enforcement provisions of the copyright legislation.

The matter does not end there. There is available to copyright owners another remedy and that is provided in the Computer Crimes Sections of the Crimes Act.

Copyright and the Criminal Law - The "Law of Unintended Consequences"

There have recently been a number of prosecutions that have been brought under s131 of the Copyright Act, alleging commercial computer infringement. Associated with these offences where there has been copying of compact discs or DVDs, there has

been a charge of accessing a computer system for dishonest purposes under s249 of the Crimes Act. The prosecutions have been brought under s249(1), which provides “Everyone is liable to imprisonment for a term not exceeding seven years who, directly or indirectly, accesses any computer system and thereby dishonestly or by deception and without claim of right obtains any property, privilege, service, pecuniary advantage, benefit or valuable consideration or causes loss to any other person”.

The elements of the offence are that the access to a computer system must be direct or indirect.

Access in relation to a computer system means to "instruct, communicate, store data in and receive data from or otherwise make use of any of the resources of the computer system". Clearly, the action of copying data from a CD or a DVD involves instructing, storing data, receiving data from or otherwise making use of the resources of the computer system. A "computer system" means a number of things, including a computer or two or more interconnected computers or the communication links between those computers to remote terminals or other devices or, finally, two or more interconnected computers combined with any communication links between those computers or to remote terminals or any other device. A computer system also includes any part of the items earlier described in and all related input, output, processing, storage, software or communication facilities and stored data.

"Dishonestly", in relation to an act or omission, means done or omitted without a belief that there was express or implied consent to or authority for the act or omission from a person entitled to give such consent or authority. Therefore, when somebody is copying a copyrighted DVD they must do so without a belief that there was an express or implied consent to or authority for that act. Furthermore, there must be a lack of claim of right, which means a lack of honest belief that they were entitled to do what they were doing and in making the copy, the infringer obtains the property of another.

"Property" is now given a wide definition, which includes real and personal property, money, electricity and any estate or interest in any real or personal property, and any debt and anything in action and any other right or interest.

Thus, the actual physical activity involved in making of a CD or a DVD may covered under s249 and the other offences involved and associated with s131, including possessing infringing copies or making them commercially available, are specific elements of that offence.

However, the provisions of the Crimes Act go further than criminalising the activity of infringement under s249.

Let us pause for a moment and consider the nature of certain technological protection measures. Technological protection measures are put in place by copyright owners primarily to prevent unauthorised copying of digital material. Technological protection measures come in a number of different shapes and forms. Specifically, they may include measures that inhibit or prevent access to material. The cases of

Sony v Ball[13] and *Sony v Owen*[14] in England recognised that prevention of access is a legitimate activity on the part of a copyright owner. In particular, access coding such as region protection for DVDs has been the subject of those cases.

In New Zealand, the act of circumventing a technological protection measure is not provided under s226 of the Copyright Act. In circumventing a technological protection measure, it has been suggested that the act of copyright infringement is sufficient and in circumventing the TPM will constitute an infringement. That may well apply to copying but what about circumventing the technological protection measure to obtain *access*? An unexpected consequence of s.252 of the Crimes Act 1961 covers this situation.

Section 252 criminalises the access of a computer system without authorisation.[15] If a person circumvents region coding on a DVD to view the DVD, I suggest that person has access to computer system, namely the media, which comprises any part of the computer system. That access is without authorisation because the copyright owner has specifically employed a technological protection measure to prevent that very action. Thus, it is my suggestion that s252 provides an unexpected protection for copyright owners. It is unlikely that merely accessing a Region 1 DVD on a Region 4 player, utilising the software that circumvents access, would result in a prosecution. Nevertheless, the remedy is available for copyright owners should they choose to exercise it and at law, it is my suggestion that an offence has been committed**.**

Conclusion

The question that arises from this discussion of some of the legal aspects of information security must be how effective are these measures in ensuring the security of information? The answer must be that the law is only as effective as either the willingness of citizens to abide by it or the enthusiasm for enforcement authorities to engage in the prevention of offending or the investigation and prosecution of those who do offend. The law in and of itself provides nothing. The law is no more and no less than a set of rules that set the boundaries upon human behaviour. The majority of members of a community accept the constraints that the law provides. In some cases, those constraints are accepted enthusiastically. In others, they are accepted grudgingly. Citizens also decide for themselves whether the importance of the offending behaviour that the law regulates warrants strict compliance. Thus, the harm that is caused by overstaying one's welcome in a parking space may provide a basis for offending conduct on the part of a person who would not even contemplate stealing an orange from a supermarket shelf. In many respects, the law is something of a blunt instrument for the protection of information and, as we have seen in terms of the exceptions that are provided for investigative authorities, there are all sorts of exceptions which can well render an erosion of the strength of a legal protection. It is to be noted, of course, that investigative powers are directed towards different objects that the mere protection of information. The exceptions that investigative agencies have to accessing information systems are not necessarily primarily directed towards those who unlawfully would access those information systems with the purposes of comprising the information contained therein.

[13] [2004] EWHC 1730 (Ch)
[14] 2002 WL 346974 (Ch D) [2002] EWHC 45
[15] As we have seen, access and computer system have a wide definition under the legislation, although as a result of a legislative oversight, s248 does not apply to s252.

It is, perhaps, in the field of copyright protection and technological protection measures that we begin to see the glimmerings of a possible solution to information security and the protection of information systems. At the moment there is protection for those who would provide means of circumventing technological protection measures. A question which may be asked arising from this is whether or not similar protections should be advanced for encryption systems or other forms of technological protections that are available to protect information that is not only subject to copyright but in respect of which some form or level of security is required. It is, perhaps, in this direction that the way in which the law may protect information security should move

Appendix 1

The Computer Crime Provisions of the Crimes Act 1961

248 Interpretation

For the purposes of this section and sections 249 and 250—
access, in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system
computer system—

(a) means—

(i) a computer; or

(ii) 2 or more interconnected computers; or

(iii) any communication links between computers or to remote terminals or another device; or

(iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and

(b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data.

249 Accessing computer system for dishonest purpose

(1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,—

(a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or

(b) causes loss to any other person.

(2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,—

(a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or

(b) to cause loss to any other person.

(3) In this section, deception has the same meaning as in section 240(2).

250 Damaging or interfering with computer system

(1) Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.

(2) Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—

(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or

(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or

(c) causes any computer system to—

(i) fail; or

(ii) deny service to any authorised users.

251 Making, selling, or distributing or possessing software for committing crime

(1) Every one is liable to imprisonment for a term not exceeding 2 years who invites any other person to acquire from him or her, or offers or exposes for sale or supply to any other person, or agrees to sell or supply or sells or supplies to any other person, or has in his or her possession for the purpose of sale or supply to any other person, any software or other information that would enable another person to access a computer system without authorisation—

(a) the sole or principal use of which he or she knows to be the commission of a crime; or

(b) that he or she promotes as being useful for the commission of a crime(whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of a crime.

(2) Every one is liable to imprisonment for a term not exceeding 2 years who—

(a) has in his or her possession any software or other information that would enable him or her to access a computer system without authorisation; and

(b) intends to use that software or other information to commit a crime.

252 Accessing computer system without authorisation

(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.

(2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access.

(3) To avoid doubt, subsection (1) does not apply if access to a computer system is gained by a law enforcement agency—

(a) under the execution of an interception warrant or search warrant; or

(b) under the authority of any Act or rule of the common law.

253 Qualified exemption to access without authorisation offence for New Zealand Security Intelligence Service

Section 252 does not apply if—

(a) the person accessing a computer system is—

(i) the person specified in an interception warrant issued under the New Zealand Security Intelligence Service Act 1969; or

(ii) a person, or member of a class of persons, requested to give any assistance that is specified in that warrant; and

(b) the person accessing a computer system is doing so for the purpose of intercepting or seizing any communication, document, or thing of the kind specified in that warrant

254 Qualified exemption to access without authorisation offence for Government Communications Security Bureau

Section 252 does not apply if the person that accesses a computer system—

(a) is authorised to access that computer system under the Government Communications Security Bureau Act 2003; and

(b) accesses that computer system in accordance with that authorisation.

Appendix 2

The Anti-Circumvention Provisons of the Copyright Act 1994

226 Devices designed to circumvent copy-protection

(1) Where copies of a copyright work are issued to the public, by or with the licence of the copyright owner, in an electronic form that is copy-protected,—

(a) The person issuing the copies to the public has the same rights against a person specified in subsection (2) of this section as a copyright owner has in respect of an infringement of copyright; and

(b) The person issuing the copies to the public has the same rights under section 122 or section 132 of this Act in relation to any device or means (of the kind referred to in subsection (2)(a) of this section) that a person has in his or her possession, custody, or control with the intention that it should be used to make infringing copies of copyright works, as a copyright owner has in relation to an infringing copy.

(2) The person referred to in subsection (1) of this section is a person who—

(a) Makes, imports, sells, lets for hire, offers or exposes for sale or hire, or advertises for sale or hire, any device or means specifically designed or adapted to circumvent the form of copy-protection employed; or

(b) Publishes information intended to enable or assist persons to circumvent that form of copy-protection,—

knowing or having reason to believe that the devices, means, or information will be used to make infringing copies.

(3) References in this section to copy-protection include any device or means intended to prevent or restrict copying of a work or to impair the quality of copies made.

(4) Sections 126 to 129 of this Act apply in relation to proceedings under this section.

(5) Section 134 of this Act applies, with all necessary modifications, in relation to the disposal of anything delivered up under subsection (1)(b) of this section.