APPROACHES TO LIABILITY FOR BREACHES IN DATA SECURITY

Liong Lim*

Data security

The term "data security" could potentially refer to any number of issues. In some circumstances, data security refers to information protection through the use of encryption or some other method of anti-hack technology[1]. On other occasions the use of the term "data security" relates to electronic transaction security or privacy issues.

At the moment, much of the existing legal commentary and, for that matter, government regulation, concerning data security has centred on privacy concerns.[2] There has also been debate on civil rights issues such as whether authorities should have the right to inspect stored material[3] and the legitimacy of using encryption technology for protecting data.[4]

So far, however, there has been very little discussion focussing on liability issues. Questions of liability in the case of a computer security system being breached have been largely unanswered. It is generally unclear whether it is the computer hacker who bears sole liability or whether a data storer, such as an Internet Service Provider (ISP), will also be legally responsible. A related question, and one that is also insufficiently addressed to date, is whether there is such a thing as a reasonable standard of security for protecting electronically stored data. These are important questions to which there is still no clear answer. This absence of discussion is a cause for concern. Data security – especially over the Internet – is vital to the successful

* Gadens Lawyers

1 C Kuner, "Legal Aspects of Encryption on the Internet", (1996) *International Business Lawyer* (April) 186, at 188.

2 American Civil Liberties Union, "Cyber Liberties", www.aclu.org/issues/cyber/priv/priv.html (5/9/99).

3 DK Taft, "Encryption In The Federal Spotlight", www.techweb.com/wire/news/aug/0805ecomm.html (5/9/99).

4 RC Thomsen, "Using/Regulating Encryption", www.commerce.net/conference/1996/encryption/sld001.htm (31/8/99).

development of electronic commerce as a major way of doing business and conducting commercial transactions.[5]

This paper will highlight the legal issues that arise out of the use of data protection and computer security systems, and will offer various suggestions as to how liability can be determined in the case of security being breached. One of the issues considered will be whether there is a standard of reasonable data security and, if so, how the law can identify such a standard and then keep up to date with developments in technology.

Data security liability issues

Data security and technology raises new issues and situations and the law has inevitably fallen behind technology. In most jurisdictions, courts still cling to traditional principles of larceny, espionage or trespass when it is clear that they will no longer work in the modern technological environment of the world today.

Complicated Interrelationship of Laws

Data security issues touch on several areas of law. For example, a simple breach of computer security could potentially give rise to claims of trespass or misappropriation. Negligence and duty of care issues may also be relevant when assessing the adequacy of a security system. Furthermore, in relation to parties storing data there may be duties of confidentiality or other forms of legal responsibility, such as contractual obligations or other imputed duties arising under situations such as bailment. Situations involving data protection and security bring all these areas of law into play and their differing principles and rationales have to be balanced.[6]

International Scope of Issues

A further issue is that while technology is international in scope, laws are often confined to particular jurisdictions. For instance, under the rules of public international law, penal laws are not enforceable

---

5 M Rustad & L Eisenschmidt, "The commercial law of Internet security", law.berkeley.edu/journals/btlj/articles/10-2/rustad.html (6/9/99).

6 The operation of each of these particular areas of law will be discussed in detail later in the paper.

outside a country's jurisdiction.[7] Therefore, even if it is an offence in one country to breach another person's security system, this has no application if the wrongdoer is situated in another jurisdiction. With current technology - especially the Internet[8] - data is potentially accessible to offenders from all over the world. So far, there have been no internationally co-ordinated responses to deal with this problem.

The Organisation for Economic Co-operation and Development (OECD) developed guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. While the OECD guidelines have been notable from a privacy law perspective, they have neglected liability issues for unauthorised security breaches.[9] In a similar vein, the United Nations in 1989 put forward Guidelines for the Regulation of Computerised Personal Data Files, which also addressed some privacy issues but left liability questions largely unanswered.[10]

This lack of a consistent international approach has led to differing approaches being adopted by various jurisdictions.

Unique Nature of Electronic Crime

In addition to jurisdictional concerns, electronic offences raise new and unique practical problems. The nature of computer crime makes it extremely difficult to detect breaches in security and to trace perpetrators.[11] For example, in situations where encryption technology is used, security may be compromised without the encryption code actually being broken.[12]

Part VIA of the *Crimes Act 1914* (Cth) and Part 6 of the *Crimes Act 1900* (NSW) both contain provisions prohibiting unlawful access to computer data. However, both acts are inadequate in relation to the determination of liability. The Commonwealth statute is limited to

---

7 Under international law a penal law is a law which makes a penalty recoverable by a state in order to vindicate some public interest: *Loucks v Standard Oil* (1918) 120 NE 198.

8 S Plunkett, "Internet Hits and Misses", (1996) *BRW* (17 June) 50 at 54.

9 O Akindemowo, *Information technology law in Australia*, Sydney, Law Book Co (1999) at 233.

10 O Akindemowo, *Information technology law in Australia*, Sydney, Law Book Co (1999) at 234.

11 SH Nycum, "Computer Crime Legislation in the United States", (1986) 1 *Comp & L* 64 at 69.

12 A Davidson, "Electronic security and encryption with clients" (1999) 19(7) *Proctor* 31, at 31.

data held by Commonwealth agencies and neither piece of legislation contains provisions requiring the data storer to take reasonable precautions. Therefore, if computer data were to be compromised as a result of an inadequate security system there would be no legislative guidance as to whether the party providing the inadequate safety system would be legally responsible.[13]

Some jurisdictions[14] have resorted to existing principles relating to ownership and property in order to deal with a growing computer crime rate. This may not be the most appropriate approach. Computer crimes involving breaches of security are not like traditional larceny situations in that they do not necessarily involve a misappropriation of property. Data security offences are new crimes and authorities must come up with new and innovative responses to successfully counter them.

Current Efforts at Legal Regulation

As discussed above, the lack of international co-operation has meant that existing data security legislation has been developed by countries on a largely individual level. Responses around the world have ranged from intrusive government regulation to complete indifference to the issue.[15] Consistency in approach will be critical for a co-ordinated international response to be achieved.

The United States

In the United States there are a large number of acts dealing with computer-related offences.[16] The *Federal Computer Systems Protection Act* was proposed to Congress in 1977 in order to deal with a rise in computer-related crime. However, the Act does not directly deal with data security liability and has not been adopted at federal level. Only half the states have responded by amending their legislation. At the individual state level there have been some attempts made to expand

---

13 I Davis, "Crime and the 'Net: An Overview of Criminal Liability on the Internet and the Legal Community's Response" <http://www.law.ttu.edu/cyberspc/jour10.htm#tech1> (5/9/99).

14 See for example Australia's *Evidence Act 1995* (Cth) which covers electronic material under references to property or documents.

15 n1 at 188.

16 WC Durham & RC Skousen, "The Law of Computer-Related Crime in the United States", (1990) 38 *Am J Comp L* 557 at 562.

the scope of existing legislation but once again the legislation has not directly considered data security liability.[17]

In July 1997, a White Paper on technology was tabled before Congress.[18] One of the issues covered by the document was the expanding use of encryption in the US marketplace. The Research Committee advised the government to work with the corporate sector in order to standardise encryption. The paper also attempts to identify a national minimum standard of encryption. Unfortunately, its recommendations on this point are inconsistent - in some passages the Committee suggests that 40-bit encryption should be the minimum acceptable level of security and in other passages a 56-bit minimum is advocated.[19] The Paper's inconsistency on this point adds further confusion to any attempt to identify a national encryption standard. The Paper is silent on the issue of liability and gives no indication as to which party should be primarily responsible if a breach should occur.

At the time of writing the US National Institute of Standards and Technology is in the process of updating its encryption standard.[20] NIST is considering encryption key sizes of up to 256 bits. Unfortunately, while such levels of security would be extremely safe, NIST standards are voluntary only and do not have the force of law.

On 1 July 1999, partly as a result of the recommendations contained in the White Paper, the *Computer Security Enhancement Bill* was introduced.[21] One of the purposes of the bill was "to enhance the ability of the National Institute of Standards and Technology to improve computer security". To that purpose, the Bill gives the National Institute of Standards and Technology the power to work

---

17 To toughen the law a number of states - Tennessee, Virginia and Arkansas - have made computer-related offences strict liability offences and have also widened the definition of "computer" under the law. See n15 at 565-566.

18 WF Krasso, "Survey of Telecommunications & the Internet; Technology White Paper" <http://academic.bellevue.edu/^wkrasso/Crypto.html> (7/25/97).

19 The number of bits refers to how complicated the encryption program is. On the topic of encryption bit-complexity, the White Paper may already be out-of-date. In a competition held in early November by the US RSA a world-wide coalition of hackers cracked a 56-bit encryption security program after working at the problem for over 250 days. While 56-bit encryption is still adequate for most data security, the fact remains that it has been shown to be fallible. This recent development highlights once again the accelerated progression of technology and the need for regulation to keep up with its pace to be effective.

20 "US Encryption Finalists Selected", www.nist.gov/public_affairs/update/upd990816.htm#IT (12/9/99).

21 "HR 2413 IH", thomas.loc.gov/cgi-bin/query/C?c106:./temp/~c106nx4mRp (5/9/99)

with the private sector to establish standards and guidelines in relation to encryption, digital signatures, user authentication and data integrity. In addition, the National Institute can also set up implementation programs for data and computer security guidelines and manage training programs.

There are two principle drawbacks with the Bill. Firstly, the National Institute has the power to set mandatory standards and guidelines for federal government agencies only; in relation to the private sector it can merely suggest *voluntary* standards. Furthermore, the Bill provides that the National Institute is only to prepare standards and guidelines for the private sector "upon request", which leaves it in a largely passive role. Therefore, the Bill has little clout when it comes to the private sector, and absolutely no application in relation to state government agencies.

The second problem with the Bill is that it does very little to actually set up a means of determining data security standards. The Bill encourages co-operation between the government and the private sector but does not provide either party with any guidance as to how data security should be regulated or standardised, or by whom.

Despite these drawbacks, the introduction of the Bill is a notable attempt by the US government to confront data security issues.

Germany

In Germany, the *Federal Law to Regulate the Conditions for Information and Communications Services (Multimedia Law)* which was completed in June 1997 places the responsibility of data security squarely on the service provider.[22] Under the Multimedia Law, part of the service provider's duties include ensuring that the computer user can make use of "teleservices" with full protection from third parties. Allocating liability in this way is a bold move by the German legislature. However, it is fraught with problems. First, the Multimedia Law is silent as to what standard of security service providers will be required to provide. Second, by limiting the application of the Multimedia Law to "teleservices" it covers

[22] C Kuner, "Federal Law to Regulate the Conditions for Information and Communication Services (IuKDG) ("Multimedia Law")" <http://ourworld.compuserve.com/homepages/ckuner/multimd3.htm> (7/25/97).

encryption used over the Internet but overlooks offline data security situations.

Working together with the *Multimedia Law* in Germany is the *Federal Data Protection Law*.[23] The Data Protection Law's purpose is "to protect the individual against his right to privacy being impaired through the handling of his personal data". Chapter III of the Law sets up a Federal Commissioner for Data Protection. Unfortunately, this legislation falls short too. It is essentially privacy legislation and protects the personal data of citizens from unauthorised access. It says nothing about data security liability issues.

Spain

One country which identified data security as a concern very early is Spain.[24] Spanish information protection and data security laws are spread over several pieces of legislation.[25]

The principal Act is the LORTAD[26], which Parliament approved in October 1992. The LORTAD contains four important provisions. First, it sets up an Agency for Data Protection. Individuals can register confidential material with the Agency, specifying at the same time the security measure being used to safeguard the material. The Agency has the discretion to inspect the adequacy of those security measures and take action where parties are using sub-standard security measures. Second, the Act provides that liability for security breaches shall lie with the individuals who are responsible for the files. Third, the Act allows anybody who has suffered damage as a result of a security breach to sue for damages. Fourth, the Act provides for a penalty regime that ranges from "serious" to "very serious" sanctions.

The Spanish Penal Code has also been amended to penalise misappropriation of personal data and computer espionage.[27] The Code has widened its approach to expressly include computer hard disks, diskettes and electronic mail in it scope.

---

23 C Macavinta, "US weighs German ISP law", www.news.com/News/Item/0,4,12201,00.html (25/8/99).

24 L Lim, "Encryption Technology Law in Spain – Lessons for Australian Lawmakers" (1998) 1 (8) *International Law Bulletin* 112.

25 E Batalla, "Legal aspects of computer programs security in Spain", (1996) 28 *Comp & L* 28, at 28.

26 In English the *Organic Law of the Protection of Computerised Personal Data.* See n24 at 28.

27 n24 at 30.

Finally, in response to legislative change, there have also been some developments in the common law. Contracts relating to electronic commerce and data transfer are beginning to contain "confidentiality" clauses, which clarify the parties responsible for the security of data.[28]

However, while Spain is to be commended for its efforts in facing data security liability issues, its system contains several flaws.

- The concept of a party being "responsible" for data is vague and invites dispute.
- The effectiveness of the Spanish system is limited by jurisdiction. Security measures can only be regulated if parties register with the Agency for Data Protection.
- The idea of a supervisory body like the Agency for Data Protection may not be appropriate to all countries. In jurisdictions with strong advocates for personal freedoms and privacy, such as the US, there would be a great deal of resistance to such regulatory bodies.
- The LORTAD does not actually specify the guidelines that the Agency for Data Protection will use in determining the adequacy of a security system. Leaving the determination of an adequate standard to the discretion of the government does not give private individuals any indication as to what constitutes an adequate level of security.

Nevertheless, despite these drawbacks, the Spanish system represents one of the more comprehensive attempts so far in dealing with the data security liability issues. Firstly, it sets up an objective arbitrator to determine the standard of a security system. Secondly, it allocates liability to parties who are responsible for data - this is more equitable than, for example, the German approach, which simply places the burden on service providers. Thirdly, it provides for harsh penalties as a deterrent in order to minimise computer crime and allows any party who has suffered damage to bring an action. And finally, while the principal legislative tool of reform is the LORTAD the Spanish law in general, including the common law, has developed provisions to deal with data security.

---

[28] n24 at 30.

England

England has had data protection legislation since the enactment of the *Data Protection Act 1984*. That act dealt largely with the protection of the privacy and confidentiality of information collected by authorities.

A new *Data Protection Act*, 1998 is proposed which will expand the existing regime to cover the collection and storage of data by certain private sector entities.[29] Unfortunately, the new legislation is silent on liability for breaches of security systems. Presumably the party in possession of the data – called the "Data Controller" – will be responsible for the proper storage and protection of any information in their control. The Act, however, does not specifically set out this duty nor does it specify what constitutes an adequate level of security.

At this stage, it appears that England has fallen into that class of countries which have strengthened their privacy regulations[30] but which have failed to extend their laws to cover the related issue of electronic security.

Australia

Australia's approach to data security has been similar to England's in that the legislature and industry bodies have largely focussed on privacy rather than liability issues. The *Privacy Act 1988* (Cth) contains eleven "information privacy principles" one of which is to place responsibility on record-keepers to ensure that records are protected by such security safeguards as are reasonable to prevent loss, unauthorised use, disclosure or misuse.[31] No mention is made of what is "reasonable" and the provision is clearly ill-suited to the use of encryption where the "record-keeper" is only one of a number of relevant parties.

At the time of writing the Federal Office of the Privacy Commissioner is in the process of drafting new privacy legislation implementing various disclosure and data protection obligations onto

---

29 Field Fisher Waterhouse "*Data Protection Act* 1998" (Summer 1999) ffw.

30 For example, Canada (Quebec and Ontario), Sweden, the United Kingdom, Switzerland, the Netherlands and Ireland have all taken this approach. See "Privacy Protections Models for the Private Sector" <http://www.ipc.on.ca/web_site.eng/matters/sun_pap/papers/models-e.htm> (27/10/97).

31 *Privacy Act* 1988 s.14 IPP No.4(1).

the private sector.[32] It is expected that the legislation will apply the information privacy principles from the *Privacy Act* to non-government data collectors and storers. Whether there will also be provisions dealing with the liability of data collectors and storers for security breaches remains to be seen.

Approaches to data security

Contract Law

One solution to the issue of data security issues draws on the principles of contract law. Under this contractual approach, the question of liability for security breaches should be left to contracting parties to decide.[33] Therefore if, for example, a party engaged security expert to put in place a security system, then those parties could decide between themselves who should shoulder liability if the security system proves to be inadequate.

There are two advantages in this approach. There is flexibility in that contract law allows parties the freedom to decide jurisdiction and liability. A typical contract might, for example, assign responsibility for the integrity of the data to the service provider. The contract may also go so far as to set out in detail the parties' duties, such as responsibilities for supervising access of data, or for the transmission and storage of data.

Secondly, contract law is already international in scope - there are existing conflict of law rules that deal with international disputes by determining jurisdictional issues according to accepted principles.[34] Alternatively, a contract could indicate which jurisdiction's laws are to apply, thereby pre-empting any jurisdictional concerns.

Thirdly, contract law is already being used widely on the Internet to govern electronic transactions.[35] The online community is already comfortable with regulating their relationships through the use of

---

[32] Office of the Privacy Commissioner news release, www.privacy.gov.au/news/index.html#6.8 (20/11/99).

[33] M Kaminky, "Getting Up to Speed on Net Law", (1996) *ABA J* (June) 90, at 90.

[34] In Australia there is clear legislation in the form of the *Service Execution and Process Act* 1992 (Cth), as well cross-vesting legislation and various state judicial rules which deal with the application of laws in international situations involving tort and contract.

[35] n5.

contracts and it may be convenient, and also appropriate, that the issue of liability in relation to data security be determined by contractual principles.

However, there are two disadvantages with using contract law to solve data security issues. The most obvious problem arises when parties omit to allocate liability. If the parties fail to enter into terms (for whatever reason) allocating responsibility, what then? How do arbitrators determine where the liability falls and what standard to apply in examining the security system?

The other problem arises because of the contract law doctrine of privity of contract. The doctrine of privity states that only parties to a contract can be bound by its terms.[36] A typical situation involving data security will affect several parties not all of which will be parties to a data security agreement. So, for example, if a data storage company contracted a computer security provider to set up a security system, only those two parties would be able to sue on the contract if the system were breached. The person whose data was actually being protected - and who would most likely suffer the most damage - would be left with no direct recourse under contract law.

Tort Law

Another possible solution is based on the principles of the law of tort. This approach applies the common law of negligence to situations when security systems are breached. Under the law of tort, a person is "negligent" if their conduct falls below a standard that can reasonably be expected of them. In the context of data security, a computer security or encryption expert might owe a duty to their employer to create an adequately secure computer program. The data storer might in turn owe a duty of care to people who entrust it with information to engage a reasonably skilled expert and to provide an adequate level of security.

There are a number of advantages with this negligence-based approach. Firstly, it is submitted, tort law is flexible enough to account for all the parties involved in a data security arrangement. The law of negligence in Australia and England is wide enough to place a duty of care on a computer security or encryption expert as a professional party (with regard to the provision of very specialised security services) or as a manufacturer (for creating the encryption or computer

[36] See *Dunlop Pneumatic Tyre Co Ltd v Selfridge & Co Ltd* [1915] AC 847.

security program).[37] The data storer would also be under a duty of care towards the data owner because of the latter's reliance on the data storer obtaining an adequate security system.

There may be disputes in some cases as to which party is the data storer – for example, whether it is the ISP or an actual collection agency. However, the requirement of a duty of care would overcome such definitional problems by looking more at the issue of which party was responsible for the security of the data.

Furthermore, in judging negligence, tort law has the capacity to take account of current standards and viewpoints.[38] Although this may require calling expert testimony and increase the expense of trials, it does allow the courts to update themselves as to what is currently acceptable with regard to electronic security.

In addition, like the contract law solution, tort law is international.[39] Therefore, if there was a situation involving a security breach extending over two or more countries, the existing conflict of law rules would be able to ascertain which country's negligence laws would apply.

The main disadvantage with this position is the difficulty with identifying a standard of adequate protection. How do courts judge whether a programme created by an encryption technologist provides appropriate security, or that the level of security provided by a party storing information of third parties is adequate? Courts have traditionally had little technological expertise and in certain jurisdictions – particularly the US – the courts have declined to set a standard of care in relation to computer professionals.[40] To compound

---

37 In *Donoghue v Stevenson* [1932] AC 562 and *Jaensch v Coffey (*1984) 155 CLR 549 the bases for recognising a duty of care were enunciated under the "neighbour" principle. Where there was proximity between parties and a level of reliance between them then a duty of care owed by one to the other would be recognised. In the context of encryption, there is arguably a proximate relationship between the encryption expert and data storer. There is also clearly reliance by the data owner on the encryption expert and data storer performing their work adequately.

38 Under negligence law, a person holding themselves out as a specialist is required to perform their occupation with the skill and diligence of a similarly skilled person in the circumstances: *Voli v Inglewood Shire Council* (1963) 110 CLR 74. This would presumably be wide enough to cover parties holding themselves out as encryption specialists.

39 See n33.

40 See generally, *Chatlos Systems, Inc v National Cash Register Corporation* 479 F.Supp 738 (D.N.J. 1979) and *Hospital Computer Systems v Staten Island Hospital* 788 F.Supp 1351 (D.N.J. 1992).

the problem there are very few professional bodies that can determine industry standards for technology professionals as there are, for example, in law or medicine.[41]

Secondly and more importantly, technology improves at such a pace that what is state-of-the-art today will be out-of-date in months. There is a real danger that courts will not be able to keep up with developments in data security technology and will not be able to adequately determine reasonable objective standards.

Confidentiality Principles

A third possible solution is to look to the law of confidentiality for guidance. Under this approach, breach of a security system could be treated as a breach of confidence. To obtain protection under existing principles of the law of confidentiality, parties are required to show that there is information intended to be confidential, that they had taken steps to secure that information and that their security had been breached.[42]

In *Franklin v Giddins*[43] it was held that a person must do all they reasonably can to safeguard their information. Under this principles it was held in *BBC Enterprises Ltd v HiTech Xtravision Ltd*[44] that the use of a security measure (such as encryption) is relevant only in so far as it indicates an intention that the protected information is confidential. It has been suggested that the strength of the security or encryption program used would also indicate the level of confidentiality of the information and would be relevant to the question of whether they had done all that was reasonable to safeguard their information.[45]

The main advantage with this position is in the issue of damages. Liability for breaking confidence is based on unconscionable conduct[46] and damages can be adapted to reflect the degree of unconscionability. Therefore, a wide range of damages is available to compensate for

---

41 n5.

42 S Ricketson, *Intellectual Property: Cases, Materials and Commentary*, Sydney, Butterworths, 1994, ch 3.

43 [1978] Qd R 72.

44 (1989) 18 IPR 63.

45 P McGinnes, "The Internet and privacy - some issues facing the private sector" (1996) 29 *Comp & L* 25 at 26.

46 P McGinnes, "The Internet and privacy - some issues facing the private sector" (1996) 29 *Comp & L* 25 at 26.

financial loss as well as intangible distress such as embarrassment resulting from disclosure.

However, there are two major faults with a confidentiality approach that would make it an inappropriate solution. First, the principles of confidentiality focus on the nature of the protected data rather than on the adequacy of the security system. This means that liability would be determined by the type of information being protected rather than on the competency of the parties. The quality of the security system being used would be judged by the nature of the protected information rather than by technological and expert standards.

The other problem with the law of confidentiality is that if a person chooses to store their information in a medium where there is an inherent risk of compromise - such as the Internet – it may be considered to be failing to take adequate care of the information and may count against claims being brought in the event of a security breach.

Property Law - Bailment

Under a proprietary approach, the law of bailment may offer a solution to liability for breaches of computer security. Under existing principles, a bailment is a delivery of property into the safekeeping of another. The rationale for recognising the existence of a bailment is that possession imposes a duty of care upon the party with possession of the property: *Ashby v Tolhurst*[47]. Is it arguable that by securing data and subjecting the information to special protection, this constitutes a bailment, thus imposing a duty on the data storer to be responsible for the security of the data?

It is unlikely that bailment law would have any operation in situations involving computer data security. The primary reason for this is that the law has never recognised information as property.[48] Accordingly, as bailment law essentially imposes duties in relation to property, being in possession of information could never give rise to bailment obligations.

A further issue is that data security does not actually involve the delivery of property or information. If property or information were

---

47 [1937] 2 KB 242.

48 *Oxford v Moss* [1978] Cr App R 183. See also n9 at 205.

actually delivered or transmitted from one party to another, there is a change of possession. However, when data is secured electronically (for example, by use of encryption) there is no change in possession and so it is hard to see how simply securing information could constitute a bailment. Furthermore, it is highly unlikely that a bailment would be imputed. Traditionally, courts have always assumed a change in possession before imputing a bailment.

Another limitation of the law of bailment is that it only protects material which is in a party's possession. Data security, on the other hand, is often designed to protect the *transmission* of information as well as its storage. Information in transit cannot be said to actually be in anyone's possession; therefore, bailment would not be an appropriate doctrine for determining liability where data is compromised while in transit.

Criminal Law - Larceny

The criminal law approach has been favoured by a number of jurisdictions. The sections of the Commonwealth and NSW Crimes Acts discussed earlier have made it an offence to obtain access to a computer without lawful excuse or authorisation. This approach essentially characterises electronic security breaches as a novel form of larceny.

Under the law of larceny in this country an offence takes place when one party, without the consent of the owner and without claim of right made in good faith, takes and carries away the property of another with the intention to permanently deprive the owner of it. At first glance, the larceny offence seems quite adequate to deal with computer fraud and electronic espionage.

However, there are several reasons why this solution would be inappropriate to deal with situations involving data security. Firstly, like bailment, information is yet to be recognised by courts as a form of property.[49] Secondly, the criminal law relating to larceny protects the possessor of property and not necessarily the owner.[50] Therefore, the party that has suffered the greatest harm is left without redress. Thirdly, the larceny offence does not take security measures into account. Once property has been removed then the adequacy of the

---

[49] *Oxford v Moss* [1978] Cr App R 183.

[50] See *Crimes Act 1900* (NSW) s.94J, *Croton v R* (1967) 117 CLR 326, *Davies* [1970] VR 27 and *Rose v Matt* [1951] 1 KB 142.

property's security is irrelevant to liability.[51] Fourthly, a breach of security does not necessarily mean that information has been appropriated or removed. A security breach may result in a loss of confidentiality without data being stolen. In such situations, then, the law of larceny would have no operation even though there has clearly been an offence committed.

Upgrading the Law

What, then, is the most appropriate approach to data security? Ideally, any solution should contain a few key elements. Firstly and most importantly, it must be up-to-date. This means that the law must be able to take into account current advances in technology and be able to adapt its standards to reflect technological progress.

Secondly, the law must be flexible. Any system must be able to take into account the fact that data security arrangements will typically involve many parties. Allocation of liability under the law must recognise that it is possible for several parties to be responsible for a security breach occurring.

Thirdly, the law must provide certainty. Parties must be able to know what standards of security are considered reasonable. In order to achieve this and provide parties with clear guidelines, the government may need to consider intervening and taking the bold step of identifying acceptable electronic security standards. The obstacles to determining an up-to-date, universally acceptable standard of security have already been encountered in the United States.[52] Nevertheless, it is important that data collectors and data storers have some guide as to what the law considers a minimum level of reasonable protection for data. It may be that an industry-specific response is required or that an agency such as the Office of the Privacy Commissioner is simply given the task of investigating and formulating national guidelines from time to time.

Fourthly, any solution must have principles that are international in scope. The ideal situation would be if the international community could come at an agreement regarding data security technology. This

---

[51] See *Smith v Desmond* (1965) AC 960 and *Kennison v Daire* (1986) 60 ALJR 249. Although the cases do not deal with encryption specifically, they do show the criminal law's approach to larceny – namely that the diligence of a custodian is irrelevant to the larceny offence.

[52] n19.

may not be far off. The United Nations has held several discussions, including a Convention on Secure Internet Transactions in November 1997. It is hoped that these talks will result in some international consensus on data security regulation.

Fifthly, a law regulating data security must be enforceable. There must be mechanisms in place to ensure standards are being met and that wrongdoing is being detected and punished. The United Nations, in a Conference on New Communication Technologies held in September 1997 observed that most issues that arise from the use of technology are regulatory problems and not technological ones.[53] The inadequate response of governments to technological issues does not arise from an inability to comprehend new technology but from a reluctance to set out regulatory guidelines.

Finally, the law must allow freedom. While it is important that there be some form of regulation, it is imperative that there is not over-regulation. Individuals should still be able to do business, transact and communicate freely. Therefore, data security guidelines should allow contracting parties to agree on the allocation of responsibility and liability for security breaches and even standards of service when securing data.

It is important that all these factors be considered when drafting a law to deal with electronic data security. The first step for the Australian government and the judiciary in this country is to recognise that the absence of any guidelines for data security liability issues is a matter of concern. National guidelines relating to data security should be set up and international discussion on the subject must be encouraged. The accelerated use of encryption and other methods of data protection world-wide requires a solution to be reached quickly before the existing shortcomings in the law become even more pronounced.

---

[53] "DPI/NGO Conference Considers New Communication Technologies" <http://www/un.org/plweb-cgi/idoc.pl?4271+...ser_+www.un.org.80+un+un+pr+pr++internet> (29/10/97).