reciprocal payment agreement was reached between Telstra and the last of the three IAPs which had complained about Telstra's conduct.

As a consequence, the ACCC withdrew the competition notice. In the view of the ACCC, its objectives had been achieved. The remedy it had sought, viz the signing of reciprocal payment arrangements among the parties, was in place. Incidentally, the ACCC was not, and did not seek to be, privy to the details of those arrangements.

One way of characterising this episode might be to say that the effect of the competition notice was to redress Telstra's market power. Because of the competition notice, and the threat of substantial pecuniary penalties on Telstra, the other IAPs were put in a position where Telstra more actively and urgently wanted to reach reciprocal payment agreements with them.

It is interesting to contemplate the possibility that one or more of these complainants, armed with the suddenly greater bargaining power given it by the issuing of this competition notice, might have tried to force Telstra into an unreasonable payment arrangement. In that case, and had Telstra raised the matter with the ACCC, the ACCC might have had to become closely involved in the details of a reciprocal payment arrangement and even in the negotiating process. That would have been undesirable, given the primacy of commercial negotiation between parties underlying much of the thinking behind Australia's telecommunications competition regulatory regime.

Competition notices are fairly blunt instruments, as is perhaps most clear when the analogy is made with "cease and desist" orders. The challenge for the ACCC has been to sharpen the blunt instrument. The regulator's aim, when faced with what it considers to be anti-competitive conduct by a powerful incumbent, is often not to have that conduct cease in the normal sense, but rather to have the conduct change. In the Internet case the ACCC's objective was for reciprocal payment arrangements to be put in place. However, a competition notice is necessarily stated in terms of what a carrier is doing wrong. Stating what the carrier needs to do to cease being in contravention of the competition rule may involve setting out a whole different course of behaviour and thus be similar to drafting a mandatory injunction.

It is hoped that the outcome of this regulatory intervention will be vigorous competition among Internet backbone providers, and that this will flow through in benefit to end-users. There is encouragement for this hope in the fact that one of Telstra's rival IAPs reduced its wholesale rates by 20 per cent shortly after seeking a reciprocal payment agreement with Telstra. Nevertheless, the ACCC is monitoring the situation.

Liability Issues in Encryption Technology

Liong Lim

Keeping Secrets

Encryption is perhaps the ultimate way to keep secrets.[1] The accepted method of security has been to limit access to information. For example, documents might be placed in a safe with a combination lock, or valuables might be locked in a drawer for which only a few have the key. The disadvantage with such forms of security is that once access is achieved then those secrets are compromised.

Encryption, on the other hand, is a method of security which scrambles information so that only parties with a particular formula can unscramble it. Therefore, even if someone were to obtain access to confidential information, that information would be incomprehensible without the unscrambling formula.[2] Encryption offers this added level of security and accounts for its increased use worldwide.[3]

However, using encryption does not come without problems. What happens when the inevitable occurs and security is breached? It is this point - the legal issues arising out of breaches of encryption - which this paper will deal with. Some of the issues canvassed will be how liability can be determined, whether some standard of care should apply to parties making use of encryption and how the law can keep up to date with developments in technology.

Problems with Existing Legal Discussion

So far, legal discussion about encryption technology has been fairly narrow, focussing mostly on the privacy implications of encryption.[4] Debate has centred around issues such as whether authorities should have the right to inspect encrypted material[5] and the constantly increasing uses for encryption.[6]

There has been very little legal commentary or government regulation which deals directly with the consequences of encryption failing. However, encryption is becoming so central to our current use of technology that this absence of

discussion is a cause for concern. Encryption technology presents situations which the existing law has never had to face.

1. Complex Number of Parties Involved

Encryption typically involves a number of parties. For example, a common situation might concern a company which employs an encryption expert to create a security system to safeguard the company's clients.

If encryption was not a consideration, then if the company client's information were somehow compromised, the client would have a possible remedy under the law of bailment. The company as the storer of the data would be liable as bailee and the client could sue them as bailor. The company as the data storer would then be left to pursue a separate claim against the wrongdoer.

Now, with the use of encryption another party is thrown in. The data storer depends on the quality of the encryption programme provided by the encryption expert in order to fulfil its duties to the data owner. It is arguable, then, that the encryption expert owes a legal duty to the data storer to provide an adequate security system and also owes an ultimate duty to the data user who suffers damage as the result of an inadequate security system. Would this duty be framed under the law of tort? Is it contractual? Or is it an extended bailor's duty? The insertion of the encryption expert as a participant in commercial transaction necessitates the recognition and formulation of new duties.

2. Complicated Interrelationship of Laws

The nature of encryption liability covers several areas of law. In formulating duties for parties using encryption, all those relevant areas of law need to be taken account of. The unauthorised decrypting of confidential information could potentially give rise to liability under the law of larceny on the part of the party breaching the security system on the grounds that they have wrongfully appropriated another's property. There is also potential liability under the principles of negligence if an encryption expert creates a substandard security system. Furthermore, there may be liability under the law of personal property, especially the rules relating to bailment, against the party responsible for storing and holding the information. Situations involving encryption touches on all these areas of law and their differing principles and rationales have to be considered.[7]

3. International Scope of Issues

Modern technology has given people world-wide access to data and information. However, 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 outside a country's jurisdiction.[8] Therefore, even if it is an offence in one country to break another person's encryption system, this has no application if the wrongdoer is situated in another jurisdiction. With current technology - especially the Internet[9] - 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.

4. Unique Nature of Electronic Crime

Electronic offences raise new and unique practical problems. The nature of computer crime makes it extremely difficult for authorities to detect breaches in security and to trace perpetrators.[10] Without specific regulations relating to electronic wrongdoing authorities will continue to encounter problems both at the crime-detection stage and at the prosecution stage.[11]

Some jurisdictions[12] have expanded existing principles relating to ownership and property in order to cover computer data under the statutory definition of property but this is not enough. Computer crime, especially breaking encryption, is not a new variant on industrial espionage or larceny - there is no misappropriation of property. There is simply a breach of security resulting in confidential information being compromised. Encryption offences are a new crime and authorities must come up with new and innovative responses to successfully counter them.

5. The Law is Behind Technology

Perhaps the ultimate concern, which gives rise to all the problems above, is that the law has fallen behind technology.[13] 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. The law must begin to accept that the concept of secrecy has evolved.

As a consequence, there are very few laws about encryption in particular. There have been isolated efforts to amend and improve laws by a few countries. However, these developments essentially expand existing offences and regulations.[14] With the exception of Spain, no country has adequately responded to the unique concerns raised by encryption. This will be discussed below.

Current Efforts at Legal Regulation

It is important that the law takes an active approach to encryption technology issues. A legal framework must be set up to regulate security in the technology market. The law can protect users by providing objective guidelines of what standards of security are acceptable or unacceptable.

Furthermore, involving the law would offer a better chance of reaching a workable international solution with regard to encryption. Currently, countries have been dealing with encryption issues on an individual level without much international co-operation. Responses

around the world have ranged from intrusive government regulation to complete indifference to the issue.[15] It is only through the law that a co-ordinated international response can be achieved. Legal regulation has been essential in achieving international consensus on other issues such as human rights and trade tariffs; an attempt should be made on the issue of data protection as well.[16]

The real issue is not whether there should be laws regulating encryption, but rather what should be their content. A few jurisdictions have recognised the potential problems involved with increased use of encryption and have made moves to develop regulatory structures to counter those issues.

1. *The United States*

In the United States there are a large number of acts dealing with computer-related offences.[17] 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 encryption and has not been adopted at federal level. Only half the states have responded by amending their legislation. At state level there have not been any enactments of note. Instead, the approach has been to expand the scope of existing legislation by widening liability and by redefining terms.[18] Unfortunately, this also fails to directly deal with encryption issues.

In July 1997, a White Paper on technology was tabled before Congress.[19] 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.[20] 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 is primarily responsible should breach occur. As yet there has been no indication to what extent Congress will follow the recommendations contained in the Paper. However, even if the Paper were to become the basis for an encrpytion law, its failure to deal with the issue of encryption liability would cause problems.

2. *Europe*

In Europe, the European Union released a document earlier this year entitled "Principles of Global Cryptographic Policy".[21] In Article 1 the Policy recognises that all businesses and individuals have the right to keep their information confidential. Article 19 on liability provides that allocation of liability in the use of encryption should be left to individual parties to decide. The language of the Policy is overly broad and its recommendations - while noteworthy - are impractical. The most useful aspect of the Policy is its recommendation that governments co-operate and find a common solution to encryption issues in Europe.

3. *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 protection squarely on the service provider.[22] Under the Law, part of the service provider's duties include insuring 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, it is silent as to what standard of security service providers will be required to provide. Second, by limiting the application of the Law to "teleservices" it covers encryption used over the Internet but overlooks general data security situations.

Working together with the *Multimedia Law* in Germany is the *Federal Data Protection Law*.[23] The Law's purpose was "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 security issues.

4. *Australia*

The Australian Parliament has recently taken a bold step towards regulating the use of encryption within government agencies. In May 1998 the Office of Government Information Technology announced Project GATEKEEPER.[24] The project aims to create a regulatory structure encompassing several elements: an authentication system facilitating the use of digital signatures and other forms of electronic identification, an authority to oversee the standards of security used by agencies and a certification body to grant accreditation to parties using an approved level of security. The regime will be administered by a Government Public Key Authority (GPKA).

The scheme is a commendable initiative. However, it suffers from one major drawback - the standards set by the GPKA will only apply to those government agencies which choose to participate. This means GATEKEEPER will not apply to all government departments nor will it apply to the private sector.

Nevertheless, despite GATEKEEPER's limited jurisdiction, it represents an important step. Previously, Australia like many other countries had only addressed the issue of encryption in the context of privacy.[25] The *Privacy Act 1988 (Cth)*

placed responsibilities on record-keepers to ensure that data was protected by such security safeguards as were reasonable to prevent loss, unauthorised use, disclosure or misuse.[26] No mention was made of encryption and no clarification given for what constituted "reasonable" security.

Now GATEKEEPER attempts to set up a supervisory body to regulate the use of encryption and, more importantly, provide guidelines as to what is acceptable security. Users of encryption will finally have an accredited standard by which to judge the service-provider's liability. However, the scheme is as yet untested and of very limited application. Furthermore, there is no indication of any legislative support for the GATEKEEPER strategies. The Australian government has yet to commit to legislative regulation of encryption.[27]

A Co-ordinated Approach - Spain

One country which has been refreshingly proactive in dealing with the use of encryption is Spain. The government in Spain has spread its information protection laws over several pieces of legislation.[28] The principal Act is the LORTAD[29] which Parliament approved in October 1992. In dealing with encryption technology concerns in Spain, the LORTAD contains four important provisions. First, it sets up an Agency for Data Protection. Individuals can register their confidential files with the Agency, specifying at the same time the security measure being used to safe guard the file. The Agency has the discretion to inspect the adequacy of those security measures and take action where parties are using sub-standard encryption technology. 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 which ranges from "serious" to "very serious" sanctions. The Spanish Penall Code has also been amended to penalise misappropriatiom of personal data and computer espionage.[30] The Code has widened its approach to expressly include computer hard disks, diskettes and electronic mail in it scope. 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.[31]

However, while Spain is to be commended for its efforts in tackling the problems of using encryption technology, its system contains fundamental 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. Encryption technology, however, is international in scope.
- 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 which 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 encryption security.

Nevertheless, despite these drawbacks, the Spanish system represents the most comprehensive attempt so far in dealing with the encryption technology 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 recognised the need to deal with encryption as a part of modern technological society. In short, Spain has realised that new measures need to be taken to make sure secrets are kept.

Other Solutions

1. Contract Law

One solution to the issue of encryption technology draws on the principles of contract law. Under this contractual approach the question of liability for encryption should be left to contracting parties to decide.[32] Therefore if, for example, a data storer engaged an encryption expert, 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. Further, contract law is already international in scope - there are existing conflict of law rules which deal with international disputes by determining which jurisdictions' laws apply.[33]

Some German service providers have already developed standard form contracts for use in local and international data protection.[34] A typical contract would assign responsibility for the integrity of the data to the service provider (in accordance with German law) and set

out in detail the service provider's duties.[35] These might include duties to supervise access of data, transmission of data and storage of data. Furthermore, the contract would clearly indicate which jurisdiction's laws are to apply, so the problem of inter-jurisdictional commerce is answered.

However, there are two disadvantages with using contract law to solve encryption technology issues. The most obvious problem arises when parties omit to allocate liability. If the parties fail to enter into terms (either by omission or design) specifying their agreement as to the use of encryption, 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] As mentioned earlier in the essay, encryption involves several possible parties not all of which will be parties to a contract. So, for example, if a data storage company agreed with an encryption service provider that the latter would be responsible for the integrity of the encryption, only those two parties would be able to sue on the contract. Therefore, if the contract law approach applied, the party who actually owned the data - and who would most likely suffer the most damage - would be left with no direct recourse!

2. *Tort Law*

Another possible solution is based on the fundamental principles of tort law. This approach applies the civil law of negligence to situations when encryption systems are breached. A party or parties will be fixed with a duty of care owed to another party or parties. For example, in situations involving encryption the encryption expert might owe a duty to the data storer to create an adequately secure system. The data storer might in turn owe a duty of care to the owner of the information to engage a reasonably skilled encryption expert. There are a number of advantages with this negligence-based approach.

Tort law is flexible enough to account for all parties involved when encryption is used. The law of negligence in Australia and England is wide enough to fix a duty of care on the encryption expert as a professional party (with regard to the provision of very specialised encryption services) or as a manufacturer (for creating the encryption program).[37] The data storer would also be under a duty of care towards a data owner because of the latter's reliance on the data storer obtaining an adequate security system.

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.

Furthermore, 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 the encryption technologist provides appropriate security? In the first place, courts have traditionally had little technological expertise and would have to rely on expert witnesses, raising the costs of trial.

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 the progress in the field of encryption technology. The result will be that they will penalise encryptors for old programmes when those programmes should have been discarded long ago. Until the law recognises the speed of technological progress, they will always be behind.

3. *Confidentiality Principles*

A third possible solution is to subsume encryption under the law of confidentiality. Under this approach, breach of an encryption system should be treated as a betrayal 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.[40]

In *Franklin v Giddins*[41] 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*[42] that the use of encryption is relevant only in so far as it indicates an intention that the encrypted information is confidential. It has been suggested that the strength of the encryption program used would also indicate the level of confidentiality of the encrypted information and would be relevant to the question of whether they had done all that was reasonable to safeguard their information.[43]

One of the advantages with the confidentiality approach is the issue of damages. Liability for breaking confidence is based on unconscionable conduct[44] and damages can be adapted to reflect the degree of unconscionability. Therefore, a wide range of damages are available to compensate for financial loss as well as intangible distress such as embarrassment resulting from disclosure.

The other advantage with a solution based on confidentiality principles is that there are already international treaties and guidelines in existence. The OECD has had Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data since 1980.[45] Although the Guidelines are principally concerned with privacy

as opposed to security, at least they provide a starting point for an eventual international encryption standard.

However, there are two major faults with a confidentiality approach which 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 encryption system. This means that encryption technologists would be liable for the type of information they are encrypting rather than on the quality of their encryption skills. The quality of the encryption system being used would be judged by the nature of the encrypted 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 - then that may prevent any action being brought because of a failure to take care. However, encryption is designed for the express purpose of allowing information to be stored and transmitted in mediums which would otherwise be dangerous. Therefore, the law of confidence could possibly create injustice by denying claims to persons who take risks, even though they have used encryption in order to overcome those risks.

4. Property Law - Bailment

Under a proprietary approach the law of bailment seeks to offer a solution to liability for breaches of encryption. 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*[46]. Is it arguable that by encrypting data and subjecting the information to special security programs, this constitutes a bailment, thus imposing a duty on the encryptor to be responsible for the security of the encrypted data?

It is unlikely that bailment law would have any operation in situations involving the use off encryption. The primary reason for this is that there is no actual delivery of property or information. When data is encrypted there is no change in possession and so it is hard to see how simply encrypting 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.

5. Criminal Law - Larceny

The criminal law approach has been favoured by a number of jurisdictions. Australian criminal legislation makes 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 encryption. Firstly, the criminal law relating to larceny protects the possessor of property and not necessarily the owner.[47] Therefore, the party which has suffered the greatest harm is left without redress. Secondly, the larceny offence does not take encryption into account. Once property has been removed then the adequacy of the property's security is irrelevant to liability.[48] Thirdly, a breach of encryption 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.

6. Business and Commerce

Under a commercial and economic approach, the absence of regulation of encryption technology is best solved by implementing strong regulation. The solution is attractive to authorities because it allows them to retain control in the emerging area of e-commerce.

In Germany the government has taken an interventionist approach on the grounds that the issue of data protection has constitutional significance - it is a basic right of citizens that their personal data be protected.[49] In the US, the Research Committee for the Technology White Paper[50] advised the government to intervene and set national minimum standards for encryption. Their argument to support intervention was that encryption had become too big for the government to control or monopolise, the best alternative was to ensure a uniform standard in the market. The most extreme proponents of the interventionist approach are France, China and Israel where encryption is banned except under licence.[51]

In Australia there are indications that some government regulation is needed for practical reasons. However, encryption is not out of control in this country yet so government regulation would be very effective without the need to resort to the extremes of other countries.[52]

However, while there may be a number of reasons to support government intervention and regulation, the fact remains that the effectiveness of any regulatory structure will depend on the quality of the legislation which that government action implements.

Upgrading the Law

What, then, is the best way to protect secrets? Ideally, any solution to the issues raised by the use of encryption should contain a few key elements. Firstly and most importantly, any

solution to the issues raised by the use of encryption 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 situations where encryption is used 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 standard of encryption is considered reasonable. In order to achieve this and provide parties with clear guidelines, the government must step in and take the bold step of identifying acceptable standards of encryption security.

Fourthly, a solution must have principles which are international in scope. The ideal situation would be if the international community could come at an agreement over the use of encryption technology. This may not be far off.[53] Various committees in the United Nations, such as the Department of Public Information (DPI), have called for international regulation of the use of encryption.[54] The United Nations has also scheduled a series of discussions and conferences, beginning in November 1997, to debate the issue of Secure Internet Transactions. The outcome of these talks will not be known for several months but they do evidence a growing awareness of encryption technology as a genuine issue. It is expected that the issue of data security and transmission will be discussed. If formal international consensus does not eventuate, the next best solution would be for individual countries to incorporate existing conflict of law rules into their regulatory regimes.

Fifthly, a law regulating encryption 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 which arise from the use of technology are regulatory problems and not technological ones.[55] 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, encryption guidelines should allow contracting parties to agree on liability and even standards of service when dealing with encryption, as long as such intentions are sufficiently clear.

It is important that all these factors be considered when drafting a law to deal with encryption technology. The first step for the Australian government and the judiciary in this country is to recognise that encryption is a matter of concern. National guidelines relating to encryption should be set up and international discussion on the subject must be encouraged. The accelerated use of encryption world-wide requires a solution to be reached quickly before the current gap in the law grows even larger.

1 Kuner C, 'Legal Aspects of Encryption on the Internet', (1996) *Int Bus Lawy* (April) 186, at 188.
2 Conference, 'Internet and the Law', (1996) 46 *Am Univ L Rev* 327, at 427.
3 For example, Australia will soon begin encrypting its military and naval communications with the HF-Mod system (High Frequency Modernisation). Encryption is already standard practice with Sydney Water and the NSW State Transit Authority, both of which protect their geographical data with GIS security (Geographic Information System). Furthermore, Master Card is currently in the process of implementing the SET encryption system (Secure Electronic Transactions) for its credit card transactions in Australia as well as world-wide.
4 American Civil Liberties Union, 'Cyber Liberties' <http://www.aclu.org/issues/cyber/priv/priv.html> (30/10/97).
5 Taft D K, 'Encryption In The Federal Spotlight' <http://www.techweb.com/wire/news/aug/0805ecomm.html> (30/10/97).
6 Thomsen R C, 'Using/Regulating Encrpytion' <http://www.commerce.net/conference/1996/ encryption/sld001.htm > (30/10/97).
7 The operation of each of these particular areas of law will be discussed in detail later in the paper.
8 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.*
9 Plunkett S, 'Internet Hits and Misses', (1996) *BRW* (17 June) 50, at 54.
10 Nycum S H, 'Computer Crime Legislation in the United States', (1986) 1 *Comp & L* 64, at 69.
11 Davis I, '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> (7/25/97).
12 See for example Australia's *Evidence Act 1995 (Cth)* which covers electronic material under references to property or documents and the current *Electronic Commerce Bill.*
13 See above n.2 at 417.
14 In NSW Australia, for example, the *Crimes Act 1900 (NSW)* was recently amended. Part 6 was added which dealt with offences relating to computers and made it a crime to obtain access to a computer without lawful excuse or authorisation. However, Part 6 is only 3 sections long and runs for just over one page. No mention is made of breach of security systems and nothing is said about encryption.
15 See above n.1 at 188.
16 With respect to human rights, for example, United Nations covenants on Crimes Against Humanity which were implemented in Rwanda and, to a lesser extent, in the former Yugoslavia. And with respect to trade see the GATT Treaty.
17 Durham W C and Skousen R C, 'The Law of Computer-Related Crime in the United States', (1990) 38 *Am J Comp L* 557, at 562.
18 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 above n.17, at 565-566.
19 Krasso W F, 'Survey of Telecommunications & the Internet; Technology White Paper' <http://academic.bellevue.edu/~wkrasso/Crypto.html> (7/25/97).
20 The number of bits refers to how complicated the encryption program is. On the topic of encrpytion bit-complexity, the White Paper may already be out-of-date. In a competition held in November 1997 by the US authorities a world-wide coalition of hackers cracked a 56-bit encryption RSA 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.
21 'Principles of Global Cryptographic Policy' <http://www.cosc.georgetown.edu/~...rypto/EUROBIT-ITAC-ITI-JEIDA.txt> (7/25/97).
22 Kuner C, '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).
23 Macavinta C, 'US weighs German ISP law'

<http://www.news.com/News/Item/0,4,12201,00.html> (25/7/97).
24 'About GATEKEEPER' <http://www.ogit.gov.au/gatekeeper/aboutgatekeeper.html> (15/6/98)
25 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).
26 *Privacy Act 1988* s.14 IPP No.4(1).
27 'The Wallis Report' <http://www.law.usyd.edu.au/~alant/wallis-report.html> (22/5/98)
28 Batalla E, 'Legal aspects of computer programs security in Spain', (1996) 28 *Comp & L* 28, at 28.
29 In English the *Organic Law of the Protection of Computerised Personal Data*. See above n.28, at 28.
30 Above n.28, at 30.
31 Ibid.
32 Kaminky M, 'Getting Up to Speed on Net Law', (1996) *ABA J* (June) 90, at 90.
33 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.
34 'Agreement on Interterritorial Data Protection' <http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex1.htm> (27/10/97).
35 Ibid.
36 See *Dunlop Pneumatic Tyre Co Ltd v Selfridge & Co Ltd [1915] AC 847*
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 above n.33.
40 Ricketson S, *Intellectual Property: Cases, Materials and Commentary* (Sydney: Butterworths, 1994), ch 3.
41 [1978] Qd R 72.
42 (1989) 18 IPR 63.
43 McGinnes P, 'The Internet and privacy - some issues facing the private sector' (1996) 29 *Comp & L* 25, at 26.
44 Ibid.
45 Greenleaf G, 'Europe '92 - Implications of the European Commission Draft Directive on Data Protection in Australia' (1991) *NSW Society for Computers and the Law Yearbook* 207, at 210.
46 [1937] 2 KB 242.
47 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*
48 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.
49 'Data protection' <http://www.bundesregierung.de/ausland/system/sys60.html> (27/10/97).
50 See above n.19.
51 'Cryptography - The Current Policy Debate' *Compulaw Newsletter* Vol 4, No 1 p.2, at 2.
52 Hughes H and Cosgrave D, 'The Internet - legal questions' (1995) *L Inst J* (April) 326, at 326.
53 Above n.45, at 207.
54 'Joint DPI/Columbia Roundtable' <http://www.un.org/plweb-cgi/idoc...+un+un+pr1997+pr1997++encryption> (22/6/98)
55 '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).

Casenote—Flyde Microsystems Limited v Radio Systems Ltd (Laddie J 11 February 1998)

John Lambert, Barrister, Lanasttter Buildings Manchester, UK

In this case Laddie J had to construe section 10 (1) of the *Copyright, Designs and Patents Act 1988*. The sub-section defines *"a work of joint ownership"* as *"a work produced by the collaboration of two or more authors in which the contribution of each author is not distinct from that of the other author or authors."*

Facts

The defendant had asked the plaintiff to develop and supply printed circuit boards ("PCBs") for a sophisticated mobile radio system capable of tuning to a frequency in response to a signal from a base station known as "trunked radio". The main component of the PCBs was an EPROM chip loaded with special software. That software was written by the plaintiff, but the defendant had been in close contact with the plaintiff during its development. The plaintiff did not charge for developing the software but made a handsome return on the sale of PCBs to the defendant. Initially it supplied PCBs fitted with the EPROM chips to the defendant, but the parties found it convenient for the defendant to install the software onto blank chips and fit those chips to the plaintiff's PCBs at its premises. Over the years the plaintiff did more than £3 million worth of business with the defendant. Things went wrong only when the defendant began to buy PCBs elsewhere to which it fitted EPROM chips loaded with the software. The defendant claimed to be entitled to do that on the grounds that it was a joint owner of the copyright subsisting in the software and that it had a free licence to make such use of the software. The plaintiff disputed that claim and contended that it was the exclusive proprietor of the copyright. The parties were unable to come to terms: the plaintiff sued the defendant, and the defendant counterclaimed against the plaintiff, for infringement of copyright.

The Preliminary Issues

The parties had agreed that two questions should be tried as preliminary issues:

- whether the copyright in the software belonged to the plaintiff alone or to the plaintiff and defendant jointly; and