Regulating Damage on The Internet: A Tortious Approach?

DANE MCLEOD*

The aim of this article is to show that a legislative approach to regulating conduct that causes property damage is fraught with difficulties in the context of the Internet environment. Further, the criminalisation of such behaviour may be undesirable given the social costs that will result. It is hard to philosophically justify such criminal regulation of civil wrongs. I will examine the recent proposal of the Standing Committee of Attorneys General regarding the incorporation of computer offences into Chapter 4 of the Model Criminal Code. I will illustrate that, given the inflexibility of a legislative response to both keep pace with technological change, and adequately define the harm, the common law is best equipped to deal with these harms. Further, civil actions and the use of tort law are of even greater utility given both the commercial imperatives involved and the incentive to corporations to protect their own interests. Any legislative response should be more appropriately targeted to (i) recognising that intangible property is capable of being the subject of civil tort actions and (ii) providing a safety net for individual users who may fall victim to corporate abuses of power. The Internet suggests the necessity to legislatively embrace provisions for computer damage in each State's equivalent of the Wrongs Act 1958 (Vic) and further, to extend the traditional notion of property beyond the tangible. The definition of property should be synchronized between the criminal and civil law.

THE MEDIUM AND THE HARM

Introduction

> When the 'persons' in question are not whole people, when their 'property' is intangible and portable, and when all concerned may readily escape a jurisdiction they do not find empowering, the relationship between the 'citizen' and the 'state' changes radically. Law, defined as a thoughtful group conversation about core values, will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically-defined territories. [1]

On 6 May 2000, the Love Bug virus was discovered to have crippled millions of computers, shut down e-mail systems and caused more than $3 billion damage.[2] Almost 90 per cent of Australian companies and 10 million computer users were affected by the virus spread via an anonymous email titled 'ILOVEYOU'. This incident highlighted the world's interconnectedness, the

* Articled Clerk, Clayton Utz Lawyers, Melbourne. This article was written as an Honours thesis as part of the Bachelor of Law, Monash University. The views expressed in this article are those of the author and not necessarily those of the firm by which the author is employed.

1 David Johnson and David Post, 'Law and Borders - The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367 par 113.

2 John Masanauskas and Greg Thom '3 Billion Love Bug' *Herald Sun* (Melbourne) 6 May 2000, 1.

enormous potential for damage in the global environment that is the information superhighway, and the shortcomings in government considerations concerning this threat.

The Internet as a medium does not lend itself readily to regulation. The Standing Committee of Attorneys General (SCAG) has proposed the implementation of a number of computer offences within the Model Criminal Code (Code) to combat any damage caused to computer systems.[3] On 30 May 2001, the Crimes Amendment (Computer Offences) Bill (NSW) 2001, implementing these recommendations passed through both Houses of the New South Wales Parliament.

It is submitted that we rush too quickly to the legislative criminalisation of such conduct and need to consider a number of pertinent factors that may lead us to deny the approach suggested by SCAG. To assist the discussion we need to understand the broad complexities of the Internet and the specific harms that need to be addressed.

Overview of the Internet.

The World Wide Web (WWW) was created as a global online store of knowledge, containing information from a diversity of sources and accessible around the world in the event of a global calamity. The Internet is a unique medium of worldwide communication,[4] which allows wide dissemination of information, delivers freedom of speech for all, and can facilitate true international cooperation. However, it also undermines traditional legal concepts. The Internet's uniqueness appears to demand correspondingly unique laws.

The shift from a tangible physical environment to an intangible electronic environment presents challenges to law enforcement. Previously, the ability to damage property was determined by physical limitations. On the Internet, criminals access information from anywhere in the world and damage systems electronically. Both legislation and the common law need to reflect the increase in criminal behaviour with respect to intangibles. The shift to intangibility means that many existing laws protecting physical property need to be redefined.

What is the Internet?

The Internet is a system of technical protocols that enables all computers to communicate with one another. It allows all information to become part of a single body of knowledge whilst contained in individual computers. Computers provide the architecture of the Internet and can be used as the target of an offence, as a tool to commit an offence; or contain evidence of a crime but be incidental to the offence. An Internet user potentially has a worldwide audience, with the capacity to send and receive information to any other connected network. Packets of information are broken down, sent separately by the best available route at any given time, and reassembled at the receiving end. An Internet Protocol address indicates where to send the packets. Without protocols, there would be simply a series of proprietary networks in isolation from each other. The one-to-many nature of the Internet alters the scope of communications[5] and increases the

3 Model Criminal Code recommended by Model Criminal Code Officers Committee of Attorneys General, *Chapter 4, Damage and Computer Offences*; Report of the Committee issued January 2001.

4 *American Civil Liberties Union v Reno* 929 F Supp 824 (ED Penn, 1996), 872, 887, 883 (Dalzell J).

5 Kent Alexander and Scott Charney, 'Computer Crime' (1996) 45 *Emory Law Journal* 931, para 42.

potential for harm to computer data and property. The Internet as a medium presents many unique difficulties that affect our ability to regulate.

Enforcement Difficulties

The investigation of property damage on the Internet has complex multi-jurisdictional and identification issues. A country seeking to enforce its criminal laws may not have jurisdiction over the perpetrator, and less serious offences may not be investigated because of the impracticalities and costs involved. Communication and cooperation between multiple and disparate law enforcement agencies located in different countries is difficult. Investigators from different agencies may unnecessarily duplicate efforts or, inadvertently interfere with one another. Further, criminals using legitimate user identifications and data encryption technology create problematic issues of proof. A large percentage of computer crimes are neither detected nor reported. Law enforcement personnel may lack the necessary technical competence, which makes prosecutions uncertain.[6] A law enforcement officer may not be familiar with certain hardware and software, the special computer techniques that can be used or the special utilities that may aid his or her enforcement efforts.[7]

The ability of existing laws to sanction Internet conduct that results in property damage is thwarted by technological advances, as the original legislators did not envision such future changes in the way we communicate. An example of this need to draft new legislation is that SCAG believes the virus threat warrants specific legislation. The rapid pace of innovation means the existence of such technological capabilities to cause damage may not fall within the confines of existing statutes, which were drafted many years before. This problem may be multiplied in the future as technological innovation increases exponentially.

The formulation of a regulative framework for the Internet demands further consideration of two specific issues: the anonymity it provides to those with nefarious purposes, and the jurisdictional problems that arise when trying to assert domestic laws upon those located in unascertained jurisdictions. Whilst it is beyond the scope of this paper to consider the intricacies of jurisdiction, it is necessary to briefly highlight the area because, in the Internet context, it is difficult for countries to enforce their domestic criminal laws overseas. It is physical proximity and physical control that enables Australia to impose criminal sanctions. The anonymity of the Internet assists criminals to avoid detection and arrest. Criminals also have access to technologies that enable anonymous communication.

The global nature of the Internet constrains Australia's ability to impose domestic criminal sanctions as users can withdraw from the rule-making jurisdiction of Australia and evade both sanctions and the detection of their illegal

6 Many with technical expertise are also defecting to private enterprise, see Garry Linnell, 'Cybercops: How Australia Lost the War Against Hackers' *The Bulletin*, 10 August 1999, 241.

7 The case of *Steve Jackson Games Inc v US Secret Service*, 816 F Supp 432 (WD Tex1993) is illustrative. The U.S. Secret Service was held civilly liable and ordered to pay damages for damaging the business of the plaintiff by seizing a book entitled *GURPS Cyberpunk*, which they believed to be a handbook for hackers. It was actually a game being developed by the company. In Court, it was said the true nature of the game was self-evident to anyone with even a limited knowledge of Internet technology.

behavior. The Internet enables 'regulatory arbitrage'. [8] It also enables transactions between people who do not know the physical location of the other party. There is no necessary connection between an Internet address and a physical jurisdiction.

There appear to be no clear jurisdictional rules. The case law is often contradictory.[9] On balance, one may come within a court's jurisdiction by repeated actions towards a particular forum. Whether liability is attracted may be a matter of degree, and judged on the particular circumstances of the case.[10] It is also uncertain whether a court should apply the laws of the jurisdiction where the conduct originated,[11] or the laws of the jurisdiction where the damage results.[12] In a case where the applicant had accessed a US bank via the Internet from Russia, the English Court of Appeal said:

> In the case of a virtually instantaneous instruction intended to take effect where the computer is situated it seems to us artificial to regard the insertion of an instruction onto the disk as having been done at the remote place where the keyboard is situated.[13]

Until this is resolved users may be liable in other jurisdictions for conduct that is not prohibited in their own jurisdiction.

As a result of all the novel enforcement difficulties outlined above, the perpetrators of harm in the Internet context may be able to avoid liability for their actions. Similarly, the methods by which a perpetrator facilitates the infliction of harm in Cyberspace, are correspondingly unique and demand our consideration.

Internet Security Threats

Computers control many important and essential utilities and contain copious amounts of private information: ' The modern thief can steal more with a computer than with a gun. The modern terrorist may be able to do more damage with a keyboard than with a bomb'.[14] Criminal damage can be committed over the Internet by a number of methods. Damage is most commonly caused by the

8 Michael Froomkin, 'The Internet as a Source of Regulatory Arbitrage' in Brian Kahin & Charles Nesson (eds), *Borders In Cyberspace* (1997) 129, 129.

9 For a comprehensive listing of US court decisions addressing personal jurisdiction see *Millenium Enterprises Inc v Millenium Music*, 33 F Supp 2d 907 (D Or, 1999); *McDonogouh v Fallon McElligott*, 40 USPQ 2d 1826 (SD Cal, 1996) held that contact with a website in jurisdiction is of itself insufficient to establish jurisdiction; *Pres-Kap Inc v System One Direct Access*, 636 So2d 1351 (Fla App, 1994) held mere contact with intra-state representatives of a supplier whose database is interstate is insufficient; the Supreme Court of British Columbia recently held in *Braintech Inc v Kostiuk* (1999) 171 DLR (4th) 46, cited in *Compulaw Newsletter* Vol 1, No 9, 70, that 'the mere transitory, passive presence in cyberspace of the alleged defamatory material' was insufficient to provide a court in Texas with jurisdiction.

10 In the High Court of Australia, Gaudron, Gummow and Hayne JJ in *Lipohar v The Queen* (1999) 200 CLR 485, 123 held the requirement of nexus for a common law offence between the offence and the country seeking jurisdiction need only be a 'real connection with the jurisdiction'. However, Callinan J in *Lipohar v The Queen* (1999) 200 CLR 485, 269 preferred the Canadian 'real and substantial link' test established in *Libman v The Queen* (1985) 21 CCC (3d) 206; this has also been approved by English Courts: *Solicitor-General v Reid* [1997] 3 NZLR 617.

11 Joanna Zakalik, 'Laws Without Borders in Cyberspace' [1996] 43(1) *Wayne Law Review* 105.

12 In *United States of America v Thomas*, 74 F 3d 701, (1996) the court held the community standard that applies is that of the community where the person is accessing the material.

13 *R v Governor of Brixton Prison; ex parte Levin* [1997] QB 65, 82.

14 US National Research Council Report, *Computers at Risk*, cited in Justice Michael Kirby, 'Information Security - OECD Initiatives' (1992) 3 *Journal of Law & Information Science* 25, 26.

unauthorised access of one's computer system by another person. The transfer of a corrupt file by disc, download or email attachment can attack a computer's files.[15] A virus is a common example of such an attack. Damage may also result from a hacker obtaining remote access to a computer connected to the Internet, and abusing any security weaknesses. An outline of some of the common acts of potential criminal damage follows.

Hacking

A hacker obtains unauthorized access to computer systems.[16] In 1996 the US General Account Office discovered that hackers using the Internet broke into the US Defence Department's computer more than 160,000 times.[17] In a 1995 survey of 200 businesses, 95 per cent admitted to being victims of computer fraud as a result of hackers gaining unauthorised access.[18]

The good intentions of a hacker do not negate the threat to computer systems and users. Hackers can recklessly or negligently cause damage to a computer system and disrupt a nation's security and the public welfare. Even if no damage is caused, a hacker's actions may still require expensive remedial measures to be taken.

Spam

Spam is essentially unsolicited email. It may be junk email, pornography, business opportunities, software, and products.[19] Spammers obtain addresses by harvesting information obtained from people voluntarily, or by automated crawler programs that trawl for strings of text resembling an email address and compile a list. Spam takes up an Internet Service Provider's (ISP's) bandwidth, has significant nuisance value and can jam systems. ISP's can filter spam out of the mail they handle. However, over time the complaints have become too time consuming and wasteful. ISP's need to implement filters, which slows the time and facilities of the provider to others. Spam is a breach of 'netiquette', and increases costs to consumers and ISP's. The Australian Draft Code of Conduct indicates intolerance toward this activity.[20]

ASIC recently charged a 'spammer' with a number of offences including interference with, interruption of, or obstruction of the lawful use of a computer by means of a telephone facility operated by Telstra. The defendant subsequently pleaded guilty.[21] In the U.S. there has been six different attempts to legislate against spam; but each attempt has been constrained by issues of free speech.

15 Tim Roper, 'Internet Business Security - Prudence or Paranoia?'(1996) 29 *Computers and Law* 6, 7.

16 *Steve Jackson Games Inc v US Secret Service* 816 F Supp 432, (WD Tex, 1993).

17 New Zealand Law Reform Commission, *Computer Misuse*, Report No 54 (1999) para 26.

18 David Gripman, 'The Doors Are Locked but the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem' (1997) 16(1) *The John Marshall Journal of Computer & Information Law* 167, 173.

19 Coalition Against Unwanted Commercial Email at <www.cauce.org>.

20 Internet Industry Association of Australia, *Industry Code of Practice*, Third Draft, 2 February 1998

21 *Steven George Hourmousiz v Australian Securities & Investments Commission* (Magistrates Court of Victoria, Magistrate D McLennan, 14 July 2000) committed for trial, Melbourne County Court, 19 October 2000. Hourmousiz was subsequently sentenced to two years imprisonment, 21 months suspended. His co-accused, Wayne John Loughnan, was sentenced on 22 May 2001 to two years jail, wholly suspended.

Cookies

Cookies allow information to be placed on and retrieved from a user's hard drive during the browsing of websites. They are effectively a surveillance tool that allows profiles of browsing behavior to be compiled. The user's hard drive is treated as a storage device for servers to record how they wish to interact with that user. Cookies can determine a profile of a user, what sites are visited, and what the user did when there. The potential of this as an area of criminal damage is increasing because of the use of Java script, which allows for the downloading of executable programs on a user's hard drive. The programs can be utilized commercially to 'webjack' a computer, disabling one's back arrow or cancel button so as to redirect one to another site or cause an inability to prevent unsolicited spam.

Viruses, Worms & Trojan Horses

A computer virus is a program that can insert executable copies of itself into other computer programs. A virus program takes control when downloaded onto a computer and executes its own code when the computer user operates the familiar program to which it is attached. A virus can cause a computer system to crash, by repeatedly replicating itself to the point to which the systems capacity is exhausted and prevents any other information processing. A worm searches for idle resources and disables them by erasing the contents. A Trojan horse contains hidden code and can perform unwanted functions.

Cyber-terrorism

Cyber-terrorism is commonly understood to be unlawful attacks or threatened attacks against computers and the information they contain to intimidate or coerce a government or its people in furtherance of political or social objectives.[22] The disruption of essential services, financial systems or computer breaches that lead to violence (such as aircraft crashes) warrant much more serious legislative sanctions than does the cyber-voyeurism of juvenile hackers. One report suggests that hackers are psychologically and organisationally ill suited to cyber-terrorism.[23]

Spam can also be used for terrorist purposes. In 1996 Spanish protestors jammed the Institute for Global Communications web-site because it hosted a site that supported Basque separatists. In 1998 Tamil guerillas overloaded Sri Lankan embassies with 800 emails a day to disrupt communications. NATO computers were similarly targeted during the Kosovo crisis.[24]

It can be seen by the above discussion that there are multiple issues in the Internet context that demand our attention when we seek to alleviate behavior commonly characterized as criminal. Regulatory decisions must be fully informed by such considerations, not only to allow the healthy unimpeded growth of a new medium of communication, but also to ensure the very effectiveness of the regulation.

22 Dorothy Denning, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives (23 May 2000).

23 Center for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School, Monterey, California (August 1999) cited in Denning, ibid 5.

24 Ibid 2.

THE HARM AND INTANGIBLE DAMAGE

As discussed above, the Internet challenges our ability to enforce the domestic regulation of the medium. Further, the Internet also demands that we reconsider our traditional conceptualisations of what amounts to harm, the objects that are capable of being damaged, and even what constitutes damage in the intangible Internet environment. In attempting to regulate the infliction of damage in the Internet context, it is necessary to consider what constitutes property that is capable of being damaged on the information superhighway.

The Internet Threat

Hacking and the transmission of dangerous entities, such as viruses, threaten private property. The libertarian approach advocated by hackers calls into question the idea of ownership of information. Hackers argue information should be free and able to be accessed equally by anyone. They view information to be common property. Corporations, on the other hand, have vested financial interests and view information as constituting a private property right.

Halbert argues the demonisation of hackers protects private interests.[25] Trespass analogies allow intangibles to become tangible. The very fact people are seeking to protect information signifies it has become a commodity. Criminalisation may be an inappropriate use of State power, as it limits equal access to information. It may be a fairer allocation of costs for corporations to defend their own commercial interests. Extrapolating from Halbert, it is submitted that it is preferable for civil liability to be recognized as the appropriate mechanism to protect the interests at stake. However, legislation may be necessary as a base of minimum standards to protect collective public interests.

Tangible or Intangible Property?

An essential truth has to be acknowledged - a computer cannot function without data. Data constitutes both the information stored within a computer and the programming instructions that allow a computer to function. Legislators have sought to criminalise damage to the storage device, and protect computer integrity rather than the data itself because of the belief the data is intangible.[26] It is unrealistic for SCAG to hold fast to the notion that the proposed legislation is to protect computer integrity and nothing else, as a computer is nothing without data. It is submitted that it is more appropriate to focus on what is actually being damaged, that being the data, than the box wherein it is contained. Regulatory attempts need to acknowledge this reality. The common law has in a number of cases recognised that intangible property is capable of being damaged.

In *HMA v Wilson*,[27] the Scottish High Court, held that whilst there was no familiarly identifiable property damage, a malicious intention to stop the production of electricity which rendered a machine inoperative is as much

[25] Debora Halbert, 'Computer Technology and Legal Discourse: The Potential for Modern Communication Technology to Challenge Legal Discourses of Authorship and Property' <http: www.austlii.edu.au/au/other/elaw/vol1no2/halbert.html>.

[26] *Oxford v Moss* (1978) 68 Cr App R 183.

[27] (1984) SLT 117.

damage to an employer's property as would be a physical act of sabotage.[28] In the English case of *Cox v Riley*,[29] Cox had disabled a computerised saw using a program cancellation facility contained within a printed circuit card. The court rejected the defence argument that the electronic impulses that were affected by Cox's conduct were not capable of being considered property. The court held that Cox's conduct caused the owner to expend time and money in restoring the saw to its original condition; therefore it was incorrect to argue there was no property damage. Stephen Brown LJ stated that as we are living in the age of computers, we must realise that machinery can be operated by 'stimulating, or activating electrical circuits or magnetized contacts[30] Lloyd uses the analogy of a vandal spray painting a wall. The conduct does not weaken the building, but an owner must expend time and money to restore the wall to its original condition.[31] The decision in *R v Zischke*,[32] which actually involved painting slogans on walls, may further assist the conceptualisation of data as tangible property. It was held that it was only necessary under s469 of the *Criminal Code* (Qld) to establish an object had been rendered imperfect by the alleged act.

In *R v Whiteley*,[33] which was an appeal against a conviction for criminal damage caused to a University's computer systems, staff resources were expended in tracking and rectifying the problem, but no damage was caused to any physical part of the relevant computers. The court held that the changes made to the information held on the system constituted criminal damage. Lane CJ said:

> What the Act requires to be proved is that tangible property has been damaged, not necessarily that the damage itself is tangible. There can be no doubt that the magnetic particles upon the metal discs were part of the discs and if the appellant was proved to have intentionally and without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disc to the owner, there would be damage. [34]

In Victoria, it has been held the concept of tangible property should not be restricted to the gross physical entity that can be perceived by human senses, but should also extend to all the characteristics of physical property including electrical characteristics.[35] The judge also ruled that as the magnetism had changed on the disk in question, there was a perceptible change to tangible property.

These cases highlight that the common law may be able to deal with such harms quite competently. There has been a shift from tangible to intangible property as a store of wealth and measure of exchange. Value is found in electronic constructs. Information or data although intangible is potentially the

28 Ibid 119.
29 (1986) 83 Cr App Rep 54.
30 Ibid 58.
31 Ian Lloyd, *Information Technology Law* (1993), 149.
32 [1983] 1 Qd R 240.
33 (1991) 93 Cr App Rep 25.
34 Ibid 28.
35 *Lynn v Barylak* (Unreported, County Court of Victoria, 7 February 1991) as reported in Gordon Hughes 'The First Computer Virus Prosecution' (1991) 61 (4) *Australian Accountant*, 66.

commodity of greatest value in the future.[36] The New Zealand Law Reform Commission believes the importance of information as a business asset in the knowledge economy, may justify definition of information as a property right for both civil and criminal law purposes.[37]

Property Rights?

Huber and Lessig separately argue the creation of property rights in intangible data would assist regulation of the Internet. Huber believes governments should divide the electromagnetic spectrum by frequency and geographic area, sell it like land and create property rights.[38] Courts can then resolve disputes as they would disputes over trespass to real property.[39] Case-by-case adjudication of Internet disputes would generate efficient rules[40] and a unique body of common law.[41] Proven common law principles of property, contract, and tort law could be enforced.[42] The assumption is that the Internet is too large and chaotic 'to be governed wholesale, from the top down'. [43] Huber believes the common law is similar to the Internet in its complexity and decentralization,[44] and is best able to move with technological change and adapt to handle cutting-edge legal issues.[45]

Lessig favours the creation of a property interest in data as it provides an incentive to protect and further develop information technology.[46] If programming code was private property the government would be able to regulate Cyberspace by controlling people's behaviour. Courts in common law deliberations can also factor in shifting public policy concerns. Lessig offers trespass law as an example of an appropriate response to spamming.[47]

However, one must acknowledge that litigation by those with the largest vested interest in protecting their commercial position may not deliver for the greater good. The effectiveness of developing property rights as a solution may be thwarted by the individual autonomy it encourages. The competing demands may be too much, given the sheer volume of individuals and potential conflicts that may arise on the Internet.

Property

The *Crimes Act 1958* (Vic) defines property as including money and all other property, real or personal, including things in action and other intangible property.[48] Despite this recognition of intangible property, it is clear that intangible property poses difficulties for many courts. In *Preddy*,[49] which

36 Alvin Toffler, *Powershift* (1990) cited in David Carter and Andrew Katz 'Computer Crime: An Emergency Challenge for Law Enforcement' *FBI Law Enforcement Bulletin*, December 1996, 1.
37 New Zealand Law Reform Commission, above n 17, 13, para 36.
38 Peter Huber, *Law and Disorder in Cyberspace: Abolish the FCC and Let Common Law Rule the Telecosm* (1997) 73.
39 Ibid 73-74.
40 George Priest, 'The Common Law Process and the Selection of Efficient Rules' (1977) 6 *Journal of Legal Studies* 65.
41 Johnson and Post, above n 1.
42 Huber, above n 38, 4-9.
43 Ibid 6.
44 Ibid 4.
45 Ibid 8.
46 Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501, 521.
47 Ibid 547.
48 Section 71(1).

concerned electronic transfers, the House of Lords held that the common notion of appropriation was thwarted because upon transfer a new chose in action was created in the defendant's favour, and therefore it could never have belonged to another. Goff LJ in obiter suggested that cheques should be treated similarly. In *Parson's case*,[50] the Victorian Court of Appeal categorised cheques, which are a chose in action and thus by nature intangible, as a special form of tangible property possessing inherent value. The tangible piece of paper represented by a cheque was, in this case, said to be deprived of substantial value. The Victorian courts are still to consider the situation of electronic transfers, but it can be seen with the legal gymnastics evident in this case that the future direction is less than certain.

Property is traditionally considered to be a relationship between the subjects of property, that being legal persons, and the things that are the objects of property rights. Property rights can also effectively order relationships between people. The ownership of 'property' confers various rights upon the owner, such as the right to protection from others interfering with one's ownership of the property concerned.[51] The enforceability of a property right is ultimately dependent on society's belief that the property right in question is a moral right.[52] Mosk J in the Supreme Court of California said that:

> The term 'property' is sufficiently comprehensive to include every species of estate, real and personal, and everything which one person can own or transfer to another. It extends to every species of right and interest capable of being enjoyed as such upon which it is practicable to place a money value.[53]

Gray's conceptualisation of property as not a thing, but rather a 'bundle of rights' may assist in tackling the intangibility of computer data. A resource such as information, that is presently not an object of property, theoretically remains in the commons.[54] The philosophy of the commons militates against government regulation as it asserts that any individual can use commons property without seeking permission from anyone else. It necessitates that there is no entity with exclusive control. On Gray's theory, a resource such as the Internet can only become the object of property rights if it is able to be excluded and able to be regulated so as to prevent strangers accessing the benefits inherent in its ownership.

> 'Property' is not about enjoyment of access but about control over access. 'Property' is the power-relation constituted by the state's endorsement of private claims to regulate the access of strangers to the benefits of particular resources. [55]

49 *R v Preddy* [1996] AC 815.
50 *R v Parsons* [1998] 2 VR 478; aff'd (1999) 195 CLR 619.
51 Felix Cohen, 'Dialogue on Private Property' (1954) 9 *Rutgers Law Review* 357, 373.
52 CB MacPherson, *Property: Mainstream and Critical Positions* (1978) in Marcia Neave, Chris Rossiter & Margaret Stone (eds), *Sackville and Neave Property Law: Case and Materials (6th ed, 1999) 12.*
53 *Moore v Regents University of California* 793 P 2d 479 (1990) (Mosk J) cited in Marcia Neave, Chris Rossiter & Margaret Stone, ibid, 34.
55 Ibid 294.
55 Ibid 268.

When referring to intangible property, issues of intellectual property created in, for instance, original software are not being discussed. What is being discussed is whether there should be recognised individual property rights to the information on one's computer. There is no reason why data or information cannot be considered to be property and therefore capable of tortious protection. The difficulties presented by the Internet could be overcome by conceptualizing Cyberspace as bound by a legally unique border separated from the real world. The Internet boundary is definable, entry is dependent on a password and a domain name represents a distinct virtual place. The recognition of information as property would honor both the truth that property rights can structure human interactions, and the reality that that which is property actually reflects what the community regards as valuable.

ATTEMPTS TO ADDRESS CRIMINAL DAMAGE

SCAG proposes criminal legislation as an antidote to damage caused in the Internet context. Their discussion paper makes the point that its proposals are derived to a large extent from the British legislation and the UK Law Reform Commission report. [56] However, Victoria's first computer virus prosecution,[57] and *Bedworth's case*[58] in the UK illustrated the possible ineffectiveness and the potential inflexibility of a legislative response.

Bedworth was acquitted after he raised the defence that he was addicted to computer use, and as a result was unable to form the necessary intent.[59] In the Victorian decision, the County Court acquitted a defendant charged with both computer trespass under s 9A of the *Summary Offences Act 1966* (Vic), and attempted criminal damage to property under the *Crimes Act 1958* (Vic). The offences engendered discussion in court as to what was meant by 'access', a 'computer system', what amounted to lawful authority, and to what extent motive was relevant.[60] The computer trespass charge was dropped because there was no proof the defendant acted with malicious intent; there were innocent explanations for the defendant's behaviour. This indicates the difficulty of securing convictions where specific and technical offences are open to interpretation; the drafting of legislation cannot hit the moving target that is the Internet. Also, the lack of intent thwarted the legislative aim. It is necessary to ask whether the correct target is the requirement of intent or simply the conduct. If it is the conduct that we seek to ameliorate then the lower civil burden of proof may be preferable. The criminal law, because of its coercive nature, requires that intent to engage in the prohibited

[56] Model Criminal Code recommended by Model Criminal Code Officers Committee of Attorneys General, Discussion paper, January 2000, 86.

[57] *Lynn v Barylak* (Unreported, County Court of Victoria, 7 February 1991).

[58] *R v Bedworth* (Unreported, UK, Judge Michael Harris, 17 March 1993).

[59] Reported in *The Independent Newspaper* (18 March 1993) cited in Andrew Charlesworth, 'Legislating Against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990' (1993) 4(1) *Journal of Law and Information Science* 80, 87-93. The author relates that the hacker culture is often compared to the culture of other socially dysfunctional and obsessive groups. Like gaming, hacking can be characterised as repetitious behaviour that offers intermittent reward, where pleasure is derived from beating a system's defenses.

[60] Gordon Hughes, 'First Computer Virus Prosecution' (1991) 61(4) *Australian Accountant* 66, 66-67.

act be proved beyond reasonable doubt.

The Australian Proposal

The main concern of the Australian proposal is protecting the security of computer systems from unauthorized access, corruption or sabotage. The proposed criminal legislation is not directed at protecting from predatory gain, privacy or secret information. However, that distinction between the box that contains the data and the data itself might be too artificial to maintain in the future. When a computer is attacked it is the data, the operating information or programming code that is damaged; there is no familiar tangible damage to the computer itself.

The Code takes a minimalist approach to definition. Data is considered to be information in any form that is entered into a computer. Data held in a computer is considered to extend to impairment of data held on discs or other removable storage devices, and extends to data in a device located outside the computer as long as it is electronically accessible by that computer.[61] This exceeds the British provisions.[62]

The term 'computer' is not defined because SCAG views such statutory definitions to be both over inclusive, because they could apply to common household appliances; and under inclusive, as technological advances may make them obsolete. Judicial interpretation is considered best able to deal with the evolutionary process of technology despite the appearance of over delegation of legislative responsibility to the courts. By contrast, the *Computer Misuse Act 1993* (Singapore) defines key terms. Singapore has formulated definitions which would appear to be sufficiently flexible to accommodate technological advances.[63] SCAG argues that any resulting over-criminalisation cannot be avoided.[64] However, this inability to define terms may support the argument to leave it to the area to the common law, as the Committee seems to be leaving great scope for judicial interpretation.

It is submitted that legislation is required to protect the individual from victimisation by those with greater resources, such as corporations. Legislation should be approached as a base from which the common law can develop, rather than as an Icarus-like attempt to over-reach and pass an all-encompassing act which, despite its breadth, is in danger of being rendered obsolete by technological advances from the moment of its enactment. Civil law must be co-opted to help combat the harm.

The offences proposed by the SCAG are:

- **Part 4.2.4** - Unauthorised access, modification or impairment to commit a serious offence. This is a preparatory offence designed to catch those who engage in unauthorised misuse in order to commit another offence. (s 308C of

61 Model Criminal Code Discussion Paper, above n56, 97.

62 The *Computer Misuse Act 1990* (UK) created three offences: s1 - The act of obtaining unauthorised access to a program or data held on a computer; s2 - The act of obtaining authorised access used in order to facilitate the commission of a further serious criminal offence; s3 - Unauthorised modification of data or programs. The offences are committed when targeted at a storage device. It does not protect against situations where, for example, someone uses their own computer on another's premises to access data on discs.

63 Section 2 (1).

64 Model Criminal Code Report, above n 3, 127.

the Crimes Amendment (Computer Offences) Bill 2001(NSW)) ('the Bill').

- **Part 4.2.5** - Unauthorised modification of data to cause impairment. (s 308D of the Bill).
- **Part 4.2.6** - Unauthorised impairment of electronic communications (s 308E of the Bill).
- **Part 4.2.7** - Possession of data with intent to commit a computer offence (s 308F of the Bill).
- **Part 4.2.8**- Supply of data with intent to commit a computer offence (s 308G of the Bill).
- **Summary Offence** - Unauthorised impairment of data held in a computer disk, credit card & c.
- **Summary Offence** - Unauthorised access to restricted data.[65]

SCAG acknowledges that the proposed offences may overlap with the *Telecommunications (Interception) Act 1979* (Cth) and specifically s7 which deals with the interception of a communication. They argue that because of the uncertainty of the boundary between the computer and telecommunications system it is wiser to provide concurrent operation of the proposed Code with State and Territory offences.[66] It is submitted that this leads to potentially unjust over-criminalisation. SCAG's acknowledgement that existing law may overlap and that the technological boundary is uncertain, demonstrates that it would be preferable to leave developments to the common law. The following section of this article considers some specific issues raised by the individual offences proposed.

Unauthorised access, modification or impairment to commit a serious offence

Part 4.2.4 (1) of SCAG's proposal states that access, modification or impairment is limited to access, modification or impairment caused (whether directly or indirectly) by the unauthorised execution of a function of a computer. It is unclear what this provision is directed at - is it the conduct of the person, or the activating of the processes of the computer? Former Deputy FBI Director Walton advised of the difficulty in proving intent and damage to obtain successful prosecutions.[67] The remote causation of virus damage presents particular difficulties. The 'execute a function' terminology[68] was designed to cover viruses, but in practice it may not. The recipient of an infected email who opens and releases it may be held responsible rather than the original creator of the virus.

An access requirement, rather than a conduct requirement, in legislation may allow virus creators to escape prosecution as damage by a virus attack may be caused by one system accessing another already infected system. If the program itself accesses a given computer system then any actus reus requirement of criminal law may not be met.[69] Due to a virus' replicating nature, a particular

65 Model Criminal Code Report, above n3, 91-92.

66 Ibid 97.

67 United States, *Hearing on Legislative Vaccine to Counter Computer Viruses*, Senate Judiciary Subcommittee on Technology and the Law, 15 May 1989 SD-226.

68 Model Criminal Code Report, above n 3, 133.

69 The conduct elements of Part 4.2.4 are: Cause unauthorized access to data; Cause unauthorized modification of date; Cause unauthorized impairment of electronic communication to or from a computer.

computer can be affected without the specific intention of the virus' creator. Software can be distributed to an innocent who themselves actually accesses the computer in question. The original perpetrator can be situated remotely in distance and time from the subsequent harm. Thus it is arguable viruses need to be specifically distinguished by not requiring access as an element of the crime. It is necessary to provide for criminal damage caused when the creator did not access the computer affected.

The comment is made that; 'the potential scope of the offences in this part will depend on the development of case law jurisprudence which determines the limits of what can and cannot amount to a "computer"'. [70] Arguably, this questions the very need to legislate.

Unauthorised modification of data to cause impairment

The Part 4.2.5 offence of unauthorised modification of data requires proof of an impairment of access to data. Impairment is not defined and includes intangible harms, and disputes 'akin to the undefined concept of causing damage to property'.[71] Is this a potential legislative recognition of intangible property rights? The comment is made that: 'British case law on criminal damage suggests that the concept of damage is sufficiently flexible to cover impairment of data'.[72] The discussion paper further states:

> [t]hough it is possible that any conduct worth catching in a specially drafted offence already falls within the scope of criminal damage legislation it is preferable, in principle, if distinctive kinds of wrongdoing...are made the subject of specific legislative provision.[73]

Can this preference be sustained on principle or effectiveness? The New Zealand Law Reform Commission advocates criminal legislation rather than a piecemeal approach because new offences would make the area clear and certain.[74] However, the existence of multiple and overlapping legislation in fact delivers the opposite.

SCAG believes the *Whiteley* decision[75] to be an impracticable and ingenious fiction, and deems it preferable to make specific reference to computer damage.[76] Chapter 4 of the Code avoids imposing criminal liability for mere misuse of data or computers. The offence requires proof of modification with intent to impair data, or recklessness as to such impairment. This indicates a distinction between mere misuse and the intent to damage. Mere unauthorised access will not amount to an offence. Access is defined exhaustively to cover conduct which causes data output or display, execution of a computer program, and the copying or moving of data.[77] The English Law Reform Commission, on the other hand, took the view that system owners had to expend considerable resources on becoming aware of unauthorised access even where there was no damage.[78] Lloyd, however, queries

70 Model Criminal Code Report, above n3, 135.
71 Ibid 137.
72 Ibid 157.
73 Ibid 159.
74 New Zealand Law Reform Commission, above n 17, Ch 5, par 88.
75 (1991) Cr App Rep 25.
76 Model Criminal Code Report, above n3, 159.
77 s308A of Model Criminal Code, above n 3.
78 UK Law Reform Commission, Criminal Law: Computer Misuse, Report No 186 (1989) par 18.2.

whether this peace of mind offered to those who own computers is evident in any other criminal law.[79] It is arguable the cost of protecting their own systems should be borne by the computer owners.

The offence of unauthorised modification to cause impairment is intended to cover:

- A person with limited authorisation who impairs data by an unauthorised operation.
- Hackers who cause damage by modifying data or programs after obtaining unauthorised access.
- Damage or impairment caused by a worm or virus circulated on a disk and executed by an innocent agent.[80]

The Code proposals are wider than the *Computer Misuse Act 1990* (UK), which requires proof of an intention to impair data. The Code imposes liability for intentional and reckless impairment. Part 4.2.5 does not require proof of impairment. It is sufficient if done with the intention to impair or recklessness as to the risk. This would cover the discovery of logic bombs before they were activated.

There may be courtroom debates in the future as to the meaning of 'modification'. The drafters of the UK Act indicate their equivalent offence may be committed when data is added, not only deleted. The NSW Bill also specifically includes the addition of data in its definitions section s308A. This clarification ensures the creator of a virus will be responsible when any computer is modified, although they cannot be considered directly responsible for the infection of a particular machine.[81]

Some commentators argue that it is the creation of the virus program that should be prohibited.[82] There can be no beneficial purpose to which such a program can be justified. Complementary offences suggested include: knowingly distributing virus programs and knowingly inserting them.[83] There may not be an identifiable correlation between a virus creator's intentions and the actual effect of the virus created. The intent of conduct may be diametrically opposed to its effect. Some argue the emphasis should be on the conduct and not the effect, as even a benign virus causes substantial recovery costs to be incurred.[84]

Unauthorised impairment of electronic communication

The Part 4.2.6 offence of impairment of data and electronic communications is designed to stop tactics such as spamming. The offence amongst other things is directed at conduct resulting in serious economic loss or serious disruption of business, government or community activities.[85] An argument can be made that costs may be more appropriately allocated if private rights owners, who are better positioned to protect their own interests, are able to litigate civilly for damage to

79 Lloyd, above n31, 172.
80 Model Criminal Code Report, above n3, 163.
81 Section 3(3).
82 James Tramontana, 'Computer Viruses: Is there a Legal "Antibiotic?"' (1990) 16 *Rutgers Computer & Technology Law Journal* 253, 260.
83 Ibid 260-261.
84 Roper, above n 15, 530.
85 Model Criminal Code Report, above n3, 171.

intangible property.

The Part 4.2.6 offence of unauthorised impairment of electronic communications also includes the intentional impairment of electronic information that may impair the capacity to transmit or receive information. Part 4.2.6 has liability for reckless impairment, however unlike Part 4.25 it requires proof the communication was impaired.

Parts 4.2.7 and 4.2.8 were added as a result of submissions after the release of the original Discussion Paper.[86] Part 4.2.7 is a preparatory offence relating to an individual who has possession of data or program and intends to use them. The offence requires proof of an intention to commit a further offence. Part 4.2.8 was formulated to catch those propagating computer programs intended for use in the commission of an offence.

Unauthorised access to or modification of restricted data

This summary offence protects data secured by an access control system such as a password. The Scottish Law Reform Commission rejected this distinction.[87] The offence requires proof that the person accused knew that access was unauthorised. There is no negligence or recklessness liability. The *Computer Misuse Act 1993* (Singapore) goes further in its s 7 by making the abetting of any of the offences in s 7 an offence, and this covers, for instance, the giving of passwords to third parties.

Whilst the unauthorised access offences are targeted at hackers, the proposed summary offence further extends to insiders. The summary offence is restricted to conduct which provides access to data by means of a programmed function of the computer. Merely to inspect data on a computer screen without permission is no offence, unless shown to another. The offence is justified by the need to ensure security and integrity of systems, rather than privacy. It is believed private information should not have special protection because it is stored in a computer.[88] It is submitted that this provision ignores the great potential for employee abuse that has been recognised by law enforcement agencies. Damage can be caused negligently whilst browsing. Remedial costs are still incurred. Tort law may be able to step into the breach, as it is rare for criminal liability to be imposed for temporary use of another's chattels without permission.

The Problem with 'Access'

The Scottish Law Reform Commission suggested that unauthorised access should not be criminalised. They suggested that legislation should be phrased in terms such as: condemning the unauthorised access, inspection or acquisition of knowledge of data or programs, or the addition, erasure or alteration of them with the intention of advantaging oneself or of causing damage. This proposal was based on a consideration of the undesirability of criminalising juvenile hackers.[89]

The New Zealand Law Reform Commission makes the point that one argument against criminalising unauthorised access to data is that the existing

86 Standing Committee of Attorneys General, Chapter 4 Model Criminal Code, Damage and Computer Offences; and Amendments to Chapter 2: Jurisdiction (January 2000).

87 Scottish Law Reform Commission, *Report on Computer Crime*, No 106 (1987) par 4.15: 'just because a door is open does not justify walking through it'.

88 Model Criminal Code Discussion Paper, above n 56, 145.

89 Scottish Law Reform Commission, above n 87, par 4.4.

criminal law does not punish unauthorised access to information without a criminal purpose.[90] People may access the same information without using a computer and not be criminally liable.[91]

Further overlooked issues in most discussions concerning the implementation of an 'access' requirement are that it is technically possible to intercept electronic data without having to physically attach anything to a network,[92] and that data may be modified only on a computer's memory and not in permanent storage. In addition, if the hacking process is wholly automated, authority suggests that there may be no offence, as a machine does not have a state of mind.[93]

The issue of unauthorised access as it pertains to the proposed summary offence becomes difficult when a user has limited access rights. It is necessary to establish the user was aware of exceeding their rights. This is problematic when a user is authorised, but the purpose for which the access is utilized is unauthorised. Establishing intent may be difficult in this situation where knowledge of the unauthorised status is necessary. In the situation where A passes on a password to B, B may not have the necessary mens rea.

In *DPP v Murdoch*,[94] Hayne J suggested that entry to a computer system would not be trespassory if the person had a general permission to use the system, even though they had an improper purpose. Hayne J held that s 9A of the *Summary Offences Act 1966* (Vic) did not distinguish between hackers or insiders, it was only concerned if access was not within the scope of permission.[95] This may support the need for a legislative response.

Employees and Authorised Access

The issues of what is authorised access, and whether access is authorised for some purposes and not for others, are recurring themes in the discussion of computer misuse. Employees are an unacknowledged source of criminal damage, and may in fact be the most significant source.[96] The Code needs to address the reality that a person may have authorisation for one purpose but not for another. In *Australian Municipal Administrative Clerical & Services Union v Ansett Australia*,[97] the court held distribution of a union bulletin via email by an employee union official was an authorised lawful business activity of the employer Ansett. This may open a Pandora's box as to what may be considered authorised use. It is necessary to be aware that the requirement for access to be unauthorised may lead to a situation where for example, employees with authorisation can cause damage without incurring liability. The House of Lords in *R v Bow Street Metropolitan Stipendiary Magistrate; Ex parte Government of the United States of America*,[98] affirming the correctness of the decision in *DPP v Bignell*,[99] acknowledged that misuse of authorised access for ulterior purposes

90 New Zealand Law Reform Commission, above n 17, par 40.
91 Ibid par 41.
92 Ibid par 52.
93 *Kennison v Daire* (1985) 38 SASR 404, 406 (King CJ).
94 [1993] 1 VR 406; applied and followed in *Gilmour v Director of Public Prosecutions* (1995) 43 NSWLR 243.
95 Ibid 406.
96 David Carter & Andra Katz, 'Computer Crime: An Emerging Challenge for Law Enforcement; (1996) FBI *Law Enforcement Bulletin* 1, 2-3.
97 (2000) 175 ALR 173.
98 [2000] 2 AC 216.
99 [1998] 1 Cr App. Rep 1

would not fall within the scope of prohibitions against unauthorised access. SCAG has recommended that there should be no liability for access where a person has authorisation, but an ulterior intent. The belief is that other criminal laws can handle such breaches, the purpose of the Code is to merely protect computer integrity.[100] SCAG considers it undesirable that mere programming errors are criminalised. They believe that imposition of liability on insiders who exceed their authority is not justified unless one can prove the accused knew that access was unauthorised.[101] Conversely, Denning in a recent submission to the US House of Representatives highlighted that 'there is always the possibility of insiders, acting alone or in concert with other terrorists, misusing their access capabilities.'[102]

The FBI highlighted that conduct which could be characterized as criminal trespass may be no more than cyber-voyeurism. It is difficult to correctly determine whether the infringement is of a company policy, a law, merely a breach of ethical netiquette standards or the result of poor judgement.[103] However, hackers may not originally have malicious intent, but the temptation once gaining access may be too great and lead to other crimes. It is submitted that there needs to be consideration of damage done to systems where there is an ulterior motive such as theft. The FBI believes the most common computer crime to be theft of information.[104] The Code provisions may be avoided in a situation where there is authorised access, an ulterior motive, no intention to commit damage but damage results.

It is hoped the foregoing discussion of SCAG's proposal demonstrates that, given the fluidity and continuing change in the medium, the Internet denies the ability of legislation to define the harm to an extent sufficient to provide future clarity and certainty in the law. Further difficulties inherent in a legislative approach are discussed below.

STATUTE OR A COMMON LAW APPROACH?

Is legislation the appropriate way to control damage to private computer systems?

Libertarian ideals have, until now, shaped the Internet. Libertarians prefer the common law as it is developed by individuals interacting on a case by case basis, and does not come from a single, central source. Hayek argues that law must be generally applicable, and should not aim at some particular social goal.[105] It is argued that the state should not make value judgements as to particular behaviours, as this favours one social group over another. This can be problematic though, as allowing individuals to have a right to do anything so long as no harm is inflicted creates a debate about what is 'harm'. The common law can equally consist of value judgements and political choices, and has many instances of directed state intervention, and of judges who had very definite goals in

100 Model Criminal Code Discussion Paper, above n 56, 115.
101 Ibid 147.
102 Denning, above n 22, par 12.
103 Carter and Katz, above n 97, 4.
104 Ibid 1-2.
105 Friedrich Hayek, *The Road to Serfdom* (1994) and *Law, Legislation and Liberty* (1981).

mind.[106] The discussion below examines the difficulties of a legislative approach.

Legislative Difficulties

Lord Williams said that criminal offences should only be created when absolutely necessary. Among the factors to be considered he listed: whether the behavior sufficiently warrants intervention, if it could be remedied by another means or under existing legislation, whether the offence is enforceable, tightly drawn and legally sound; and whether the penalty is commensurate with the seriousness of the offence.[107]

Loundy[108] indicates some other drafting difficulties one may encounter in formulating legislation. The liability for illegal activities in Cyberspace may be affected by how we view the Internet's delivery of information. Does it act like a publisher, a common carrier, or a broadcaster? Information systems may even be analogous to traditional public fora, such as street corners or community bulletin boards. Conversely, the Internet may be seen as unique and novel. The perception affects legislative purpose.

Judicial Aptitudes

Advocates of the necessity for new legislation assume that the existing law is unable to keep pace with technological advancement.[109] The Internet, they argue, usurps the common law's ability to deal with disputes as they arise. The U.K. Law Commission believed the meaning of 'damage' was problematic in the electronic context and supported the necessity for new legislation.[110] The Commission believed it was difficult to explain to judges and juries how the law of criminal damage applied to the factual situation of unauthorized access to data. This inspired the *Computer Misuse Act 1990* (UK). Yet judges, as a matter of practice, commonly adapt legal rules to social changes. I would argue legislation might not be the only alternative. Judges determine conflicts when necessary, and as they arise. The law is sufficiently broad in most cases to apply to circumstances unforeseen by the original legislators. The statement in *Cox v Riley*[111] indicates the ability of judges via the common law to mould the law to reflect social change. In our adversarial system a judge is also dependent on the opposing arguments presented by the parties, and it is here that a lack of understanding of technological issues may impact on judgement.

Inflexibility

Despite the perception that Parliament is better equipped to respond quickly to technological change, the legislative process in reality hinders quick responses.[112] Legislative change depends on the commissioning of reports, committee

[106] Professor James Boyle, 'Libertarianism, Property & Harm' *Net Total: Law, Politics and Property in Cyberspace* (unpublished manuscript) Chapter 2.
[107] Written reply to question by L Dholakia, H.L. Deb Vol 602 WA 57 (18 June 1999).
[108] David Loundy, 'E-Law 2.0: Legal Issues Affecting Computer Information Systems and System Operator Liability' (1992) 3 *Albany Law Journal of Science & Technology* 1, Parts III and IV.
[109] Colin Tapper, 'Judicial Attitudes, Aptitudes and Abilities in the Field of High Technology' (1989) 15 *Monash University Law Review* 219, 219-220.
[110] UK Law Reform Commission, above n 78, par 2.31.
[111] (1986) 83 Cr App Rep 54.
[112] Tapper, above n 109, 223-225.

considerations of submissions, the drafting of legislation and its approval in parliament. The result is often a political compromise. The political process, and the resulting debate that ensues as to the merits of the legislation, can hamper the passage of legislation. Another problem with a legislative response is that it is enshrined in inflexible terms, and fixed in time. Legislation directed at particular computer hardware or software may become obsolete due to technological advances. The legislative focus should be on the criminal conduct, the intent and the result. Tapper further comments that legislative changes occur intermittently whilst the common law allows fluid judicial extensions of the law, and matters not considered by the legislators or missed by imprecise drafting can easily be embraced within the common law.[113] However, it is submitted that this may appear to be a circular argument because if the judiciary can overcome drafting difficulties, there should be no problem in legislating to begin with; the common law and legislation may be complementary.

One's theoretical perspective determines if one prefers the creation of new legislation or not. The common law property rights approach, as argued above, can be seen to present particular advantages in regulating the Internet. The argument in favour of criminalising Internet conduct that causes damage may be equally appealing.

IS CRIMINALISATION APPROPRIATE?

Distinct from the common law versus statute argument, there is a further issue of whether criminal legislation as opposed to civil legislation is more appropriate to regulate conduct that causes damage on the Internet. Crime is commonly associated with violence and as having a direct impact on individuals. However, the increased interconnectedness and dependence on computer systems means there is greater potential for the impairment of financial systems and people's health and safety. Technological advances have caused a conceptual shift in the type of activities considered criminal. The Internet focuses attention on the economic consequences of crime.

The decision to impose criminal liability is effectively a reflection of the condemnation of a particular course of conduct by society. The criminalisation of particular conduct denies the social validity of that conduct, punishes its performance, and deters those who may contemplate it.[114] This use of the coercive power by the State against individual subjects typically requires justification. However, Ashworth believes the criminal law is increasingly developing in a chaotic and unprincipled manner.[115] It is becoming more difficult to differentiate between civil and criminal law on the basis of the content of the law alone, or by the subject matter it seeks to regulate. The proliferation of purely regulatory offences makes it hard to identify the specific attributes of criminal law. Many of such regulatory offences are implemented on a basis diametrically opposed to the traditional justifications for the criminal law. An increasing number of criminal laws are minimally antisocial and have a non-existent social stigma. Such minor offences are in effect no more than civil wrongs. The increased use of strict

[113] Ibid 225.
[114] Andrew Ashworth, *Principles of Criminal Law* (2nd ed, 1995) 1- 4, 22 -57.
[115] Andrew Ashworth, 'Is the Criminal Law a Lost Cause?' (2000) 116 *Law Quarterly Review* 225, 225.

liability, omission liability and reverse onus provisions denies the traditional necessity of a mens rea requirement in criminal law. The 'one golden thread' that the prosecution bears the burden of proving guilt is disavowed.[116]

Marshall and Duff conversely argue that crimes are differentiated from civil actions because, although they comprise actions against individual property or persons, they can also be characterized as wrongs against the community.[117] However, the boundaries between civil and criminal law are becoming hazy as public authorities are bringing both civil and criminal actions with increased frequency. It is only the procedure and not the content of the law that distinguishes civil from criminal law. The decision to criminalise certain behaviours may be no more than a political act on the part of government so they are seen to be responding to issues. The decision is generally a response to particular change phases in contemporary social history.[118]

The emerging Internet globalization is an example of such a societal growth phase. We must ask, in relation to the Internet, the extent to which the crimes are serious in relation to other crimes, and identify the purposes of regulating by statute. Is this the most effective way to prevent criminal damage via the Internet? Are we in fact trying to criminally regulate civil wrongs?

Philosophical Justifications for Criminalisation

Criminal liability is typically founded on the preservation of individual autonomy, but has grown to protect both individual autonomy and collective welfare. The criminal law is said to give offenders notice and the opportunity to curb criminal actions, thus allowing individuals to make their own decisions.[119] The state's role, it is argued, is simply to telegraph the consequences of the choice to engage in socially undesired conduct. However, this theory denies the social reality in which we live. Society by definition restricts. The pursuit of individual ends, as expressed in the freedom of choice, is socially impossible without qualification. Raz believes the state's obligation is to create the social conditions necessary for the exercise of individual autonomy.[120] This may demand the rights of certain individuals be protected against the majority. This could well be the appropriate philosophical model for Internet regulation.

Minimalists argue the state is only justified in criminalising conduct that causes harm to others; they emphasize the need to protect individuals from the abuse of power. [121] On this view, the criminal law should only be used as a last resort to punish and prevent 'the most reprehensible types of wrongdoing'.[122] Individuals are able to pursue their choices to the point at which they cease to be compatible with the freedom of others to do likewise.[123] It is argued that simple

116 Ibid 228.

117 SE Marshall and RA Duff, 'Criminalization and Sharing Wrongs' (1998) XI *Canadian Journal of Law and Jurisprudence* 7, 7.

118 Ashworth, above n114, 1.

119 Herbert Hart, *Punishment and Responsibility* (1970): individuals should not be held criminally liable unless they have the capacity and a fair opportunity to do otherwise.

120 Joseph Raz, *The Morality of Freedom* (1986), 425.

121 John Stuart Mill, *On Liberty* (1992) Chapter 1, par 9: 'the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others'.

122 Nils Jareborg, 'What Kind of Criminal Law Do We Want?' (1995) *Scandinavian Studies of Criminology* 19.

123 DAJ Richards, 'Rights, Utility and Crime' (1981) 3 *Crime and Justice* 247.

cost-effectiveness or political expediency is insufficient to justify the criminalisation of conduct, and that the use of criminal law for minor wrongs leads to over-criminalisation.

The contrary argument, the welfare principle, is that an individual also owes obligations to greater society. This principle favours the use of criminal law to reinforce collective rather than private interests. The welfare argument is that criminalising behaviour may be in the interests of the community, in a time of limited resources. The proposed Chapter 4 of the Model Criminal Code may be seen as a trend toward the protection of collective interests.

The definition of what constitutes harm and whether it demands the attention of the criminal law varies with a society's morality, culture, and political ideology. The interests protected by law reflect which interests are seen as legitimate in the eyes of society. The nature of property is such that when a court exercises its jurisdiction against a third party to prevent what might be considered a wrong, it is in fact granting a subject an entitlement in an object of property.[124] The decision to criminalise behaviour on the Internet may unconsciously confirm a property right in intangible data that can be more effectively regulated by other areas of law.

The decision to criminalise certain conduct on the Internet is not justified by arguments founded on morality. It is essentially a utilitarian decision made to protect certain rights and interests for the public good. The criminal law is utilised here because it is seen to be the most efficient and cost-effective means of effectively controlling the conduct that causes damage on the Internet. The criminalisation of this conduct would be denied by this theory if the resulting social consequences were the same or worse than the situation the law is aimed at remedying. [125]

Merits of Criminalisation

Criminal punishment can actively promote ethical standards and educate new users.

Alternative arguments commonly characterise hackers as rebellious youth;[126] or an elite group exploring the potential of computer systems; and motivated by intellectual curiosity, not malevolence. However, society's tolerance of hackers is dwindling as the average citizen is faced more frequently with the damage that is done in the pursuit of supposed 'electronic good samaritanism'.[127]

In the U.S. Senate, Senator Leahy stated that:

> Just as a kid who enters another's property is trespassing, or who goes into another's home is breaking and entering, or who takes another's apple is stealing, so too, a hacker who manipulates or destroys the computer program of another - or who renders it inoperable - is breaking the law.[128]

[124] The court acknowledged this in *Foster v Mountford* (1976) 14 ALR 71, where the court awarded an injunction to prevent publication of Aboriginal tribal secrets.

[125] Jeremy Bentham, *Introduction to the Principles of Morals and Legislation* (1986) 19. Society must not punish 'where it must be inefficacious: where it cannot act so as to prevent the mischief... where the mischief may be prevented... without it: that is, at a cheaper rate'.

[126] Benjamin Fox, 'Hackers & The U.S. Secret Service', (1997) *The UCLA Online Institute for Cyberspace Law and Policy*, <http://www.gseis.ucla.edu/iclp/bfox.html>.

[127] Ibid Part IV par 2.

[128] US Senate Judiciary Subcommittee, above n 67.

It is said beneficial experimentation and free information flow must be balanced against the prevention of criminal activity. However, it is submitted that the criminal law alone may not be sufficient to achieve the legislative aims.

The fact that current criminal regulation in other areas does not stop every harm from eventuating does not necessarily deny the merits of criminalisation. The reach and speed of Internet technology exponentially increases the number of door handles that can be tested, and the number of people able to test whether the door is open.[129] Criminal legislation may be seen as effective if it prevents the great majority of harm from being inflicted.

A privatised technological approach to regulation, facilitated by changing the architecture of the system, is often suggested as an alternative to legislation. However, this is effectively industry self-regulation, and is insufficient to provide equal and efficient control of the Internet. Criminal legislation may be more effective given the fact that corporations control the Internet, and the very essence of the corporate world is competition, not cooperation. Architectural mechanisms such as trusted systems, encryption and protective technology are effectively privatised law that can be utilized by the creators for their own ends.[130] Corporations who own the programming code will favour their private interests. There must be recognition of public values. Whilst it is true that both government and corporate entities must combine to stop criminal activity,[131] technology and self regulation are only useful to regulate the Internet at a subordinate level. Any regulatory regime must provide for a uniformity of approach.

Easterbrook J believes the Internet is no more than a 'souped up telephone'[132] and argues that a separate law of Cyberspace would muddle rather than clarify.[133] The law is best served by the application of general rules to specialised situations. An unregulated Internet, as advocated by libertarians, is misguided because it artificially separates the private and public spheres, ignoring the vast influence private entities have on Internet traffic, and over-rating the government's power to regulate. [134] Legislation is required to ensure the protection of collective public interests because of the fact Internet networks are privately owned. To take the argument one step further, it is not difficult to imagine a scenario where a private company sends a virus in retaliation for unpaid fees or jams a recipient's computer with unwanted spam for a perceived slight. An individual's right of uninterrupted access needs to also be protected.

Problems Associated with Criminalisation

It is said criminalisation can drive behaviours underground where they are incapable of being controlled,[135] and damages the potential of the next generation of leaders and policy makers.[136] In addition, the resulting social costs in terms of enforcement and imprisonment may be disproportionate to the offence or

[129] Roper, above n 15, 12.
[130] Lessig, above n 46.
[131] Victorian Law Reform Committee, *Technology and the Law* (May 1999) 114, Par 8.8.
[132] Justice Frank Easterbrook, 'Cyberspace and the Law of the Horse' (1996) *The University of Chicago Legal Forum* cited in Lessig, above n 46, 501.
[133] Ibid.
[134] Harley Wright, 'Law, Convergence and Communicative Values on the Net", (1996) 7(1) *Journal of Law and Information Science* 54, 65.
[135] Jim Thomas, 'Review of the Cuckoo's Egg' (1990) *Computer Underground Digest*, Issue No 1.06.
[136] Fox, above n126, 10.

increase evasive criminal behaviour. The ability of Internet users to choose the regulatory regimes and jurisdiction they desire exacerbates the problem.

The deterrent effect seen as necessary in criminal damage legislation may result in the punishment of a few individuals in a disproportionately unjust manner. A juvenile hacker may be sacrificed in order to send a strong message of deterrence. Considerations of deterrence are inappropriate and ineffective in relation to criminal prosecutions against companies, yet crime on the Internet predominantly impacts on the interests of the corporations who currently control it. Criminals are exploiting the current gap between corporate control of technology and the State's capacity to regulate it.[137] Commercial spammers or 'webjackers' may escape liability because of the inability to prove the requisite criminal intent.

To use the criminal law is inappropriate as this distorts the system; actions should be criminalised because of their seriousness. Ashworth argues governments overestimate the preventive effect of the criminal law in their pursuit for a politically symbolic fix.[138] Legislation alone will not solve virus and hacking problems; the opportunity structure must be changed.[139] Criminalisation cannot be justified on the basis of economic efficiency alone. The criminal law should be kept to a minimum and reserved for the most anti-social forms of behaviour out of respect for individual autonomy. There may be more acceptable and effective informal means of control such as the common law and civil liability.

In assessing the seriousness of the wrongdoing involved in Internet offences one must look to the interests affected, the remoteness of the harm from the conduct, and culpability. The harm must be sufficiently serious to justify criminalisation; and the form of regulation chosen must be effective to counter the harm. Seriousness should not vary with the social context in which the wrongdoing occurs. Criminal laws may differ markedly depending on the jurisdiction.

Different criminal statutes in different jurisdictions may fragment the global marketplace by imposing differing standards, causing Internet gridlock rather than protecting users.[140] Multiple domestic laws, and issues such as varying degrees of proof, have the potential to paralyze Internet interactions. It is impossible for users to be expected to have knowledge of all the laws applying in the multiple jurisdictions they interact with in such a packet switching network. The Singapore Act is illustrative. It has harsher penalties, and grants wider powers of investigation that may infringe human rights. The interests of business and society are placed above the rights of defendants. This undermines the foundations of the criminal law, and the concepts that one is innocent until proven guilty and that the state needs to prove guilt.

Justice Michael Kirby, in a speech concerning data protection, stated that to the extent that different regulations existed in different countries, regulatory attempts

[137] Louise Shelley, 'Crime and Corruption in the Digital Age' (1998) 51(2) *Journal of International Affairs* 605, 606-607.

[138] Ashworth, above n 115, 250.

[139] Cynthia Nicholson, 'Computer Viruses: Information Age Vulnerability and the Technopath' (1990) 27 *American Criminal Law Review* 525, 540.

[140] The Singapore *Computer Misuse Act 1993* for example in ss 6-7 makes it clear its goal is the protection of victims. It goes further than the Australian and British Acts, and requires in s 3 (3) that a person 'knowingly' commit an offence rather than require proof of intent.

would be ineffective and diminish participation as no user could possibly comply with many disparate legal regimes.[141] Justice Kirby stressed the need for global collaboration to provide international solutions to information security. He believes information should be protected by reference to several principles: *availability* of it to authorised persons, *confidentiality* to protect against unauthorised use, *integrity* to protect from alteration or destruction of data once accessed, *authenticity* and *utility*.[142] SCAG's recommendations focus only on the integrity of computer systems. It is submitted that the threat to computer integrity may be small compared to the economic loss or the productivity costs that a virus may cause.

Tortious Regulation?

As the harm inflicted in the Internet context predominantly results in damage to data, that damage can be remedied more reliably and efficiently by tort law. The common law has distinct advantages over the statute approach. Statutes fix one's notion of 'harm' and damage at a particular time and in particular language, and inhibit the flexible application of law to changing circumstances.

Quite apart from the statute versus common law argument, civil tort law may be of even greater utility than criminal law given the commercial interests at stake, the impractical workings of criminal law in this context, and the developing recognition within society that information can constitute property. The approach in the US when issues of damage first emerged on the Internet was to utilise tortious doctrines such as trespass and conversion. At the outset, it is acknowledged that traditionally torts have not protected intangible interests. However, this discussion endeavours to illustrate that this hurdle is not insurmountable and that in fact it is desirable we do so.

APPLICABLE TORTS

A tort has been judicially defined, as a breach of duty owed generally to one's fellow citizens. This duty is imposed by law, and not as a consequence of duties fixed by the parties themselves.[143] Tortious duties protect rights and interests, and are owed to persons generally and not to specific individuals. Courts initially resorted to tort law when faced with remedying damage to property caused via the Internet. Several torts were eminently suitable and able to be adapted to the new medium. I believe torts such as conversion, trespass and negligence are best suited to remedying property damage on the Internet.

The Merits of Tort Law

Tort law is equally as capable of discouraging wrongdoing as is criminal law. Cane argues that tort law is partly a system that furthers certain social goals.[144] Tort law can deter wrongful conduct, encourage socially responsible behaviour, and restore injured parties to their original condition by compensation.[145]

[141] Justice Michael Kirby, 'Information Security - OECD Initiatives' (1992) 3 *Journal of Law and Information Science* 25, 34.
[142] Ibid 43-44.
[143] *Macpherson & Kelley v Kevin J Prunty & Associates* [1983] 1 VR 573, 587 (Murphy J).
[144] Peter Cane, *The Anatomy of Tort Law* (1997) Chapter 7.
[145] Gripman above n18, 176.

Similarly, Weinrib postulates tort law is a system of responsibility for human conduct based on corrective justice.[146] Civil proceedings in tort provide for the recovery of compensatory damages or other remedies (such as injunctions), for injuries or losses caused by the acts of another in breach of a right or duty imposed by law. Monetary awards can equally deter, and exemplary damages can be punitive in nature. Tort law can operate in a more commercial context to compensate losses caused to economic interests when a right is breached or a duty is not performed. In the Internet context, state sanctions are irrelevant to commercial operators who are concerned with private property rights.[147] Tortious remedies such as injunctions may be of greater utility. Private operators are best able to protect their own rights and interests as they have greater resources than the state and they have a financial incentive in obtaining a satisfactory outcome. The counter argument is that they may not recognise the validity of any collective public goods in the protection of their own interests.

Tort law historically has also imposed lower standards of care when a minor is involved.[148] This may assist to combat the potential for over-criminalisation that legislation would suggest. I would argue that the laws of trespass and conversion are also more readily transferable to other jurisdictions than are domestic criminal statutes.

Trindade and Cane highlight there is currently controversy as to whether the law of torts is an appropriate mechanism of adaptation to reflect changing expectations in relation to protecting what people value. Their view is that the law of torts should adapt its principles as new circumstances arise.[149] Tort law has not been stagnant, new torts have developed to address social needs as society changes. *Donoghue v Stevenson*,[150] one of the most well known tort cases, is illustrative. This case addressed what was then the novel method of modern packaging and distribution.[151] As society has evolved other torts have been created to protect against harassment[152] and the invasion of privacy.[153] The New Zealand Law Reform Commission recognised that there might also exist a duty not to spread computer viruses based on a 1965 decision, which held the existence of a duty not to allow a biological virus to be transmitted.[154]

The Burden of Proof

As has been touched on above, another pertinent consideration is that the criminal burden of proof demands that the offence be proved beyond reasonable doubt. In addition, most criminal offences, strict liability aside, demand that the intention to engage in the prohibited conduct be proved; the mens rea element. Professor Michel Vivant[155] asserts that it is not clear what reasonable behavior is on the Internet. This thwarts the use of legal standards based on the reasonable person.

146 Ernest Weinrib, *The Idea of Private Law* (1995) 233.
147 William Cornish, *Intellectual Property Law* (4th ed, 1999) par 2.19.
148 *Mullin v Richards* [1998] 1 WLR 1304.
149 Francis Trindade and Peter Cane, *The Law of Torts in Australia* (3rd ed, 2000), 4.
150 [1932] AC 562.
151 New Zealand Law Reform Commission, above n 17, Appendix C, par 141.
152 *Khorasandjian v Bush* [1993] QB 727.
153 *Bradley v Wingnut Films Ltd* [1993] 1 NZLR 415.
154 *Weller v Foot & Mouth Disease Research Institute* [1966] 1 QB 569.
155 Professor Michel Vivant, 'OECD Forum: Internet Content Self-Regulation' (Paris, 25 March 1998).

The civil burden may make prosecutions easier to obtain.

Conversion and Trespass

Conversion

Conversion is when a defendant by intentional conduct, and without lawful justification, deals with goods in a manner repugnant to a plaintiff's possession or immediate right to possession.[156] Conversion is dependent on actual possession or an immediate right to possession, not a right of ownership. A deliberate and wilful dealing in a manner inconsistent with the rights of the true owner, or reckless dealing resulting in depriving the owner constitutes conversion. An indirect action by a defendant can be conversion, all that is required is the taking of goods out of the possession of anyone with the intention of exercising dominion over them. Neither dishonesty nor a positive act of misconduct is necessary. Persons can be liable for conversion by abusing the possession of goods even if they were rightfully acquired,[157] or by transferring possession from the plaintiff to a third person.

Traditionally, conversion was inapplicable to things incapable of being property. The subject matter was required to be a tangible movable object capable of being in actual possession. Courts have overcome the potential problem that intangible rights, such as cheques, insurance policies and shares, cannot be converted by treating the documents that evidence those rights as the goods converted. The conversion of the goods is treated as the conversion of that which they represent. It is submitted that it would not be too long a bow to draw to include computer data under such an umbrella. The decisions of *Cox v Riley*[158] and *Whiteley's* case[159] have already been considered above and support a move to converting the intangibility of data into tangible property, which is capable of protection by the law.

In *America Online v IMS et al*,[160] unsolicited spam emails were considered to constitute actionable conversion and trespass. It was viewed as appropriating computer facilities without authorisation for their own purposes. Junk email overloads the system causing malfunctions and deprives other users of legitimate use of the system. In *Mundy v Decker*[161] an employee's deletion of email was held to constitute conversion. On appeal the issue was whether the computer directory and the individual file that were deleted had proprietary value aside from the tangible forms that could be printed. Decker's actions in deleting the entire contents of the directory were held to be wrongful exercise of dominion over Mundy's property, thereby establishing a cause of action in conversion.

Conversion may be helpful in the Internet context to overcome the difficulty where there is a temporary derangement of the property. If there is only a temporary derangement of magnetic or electronic impulses it might be argued there was no damage. In such situations, torts such as conversion may assist in

156 Trindade and Cane, above n 149.
157 *Moorgate Mercantile Co Ltd v Finch and Read* [1962] 1 QB 701.
158 (1986) 83 Cr App Rep 54.
159 (1991) 93 Cr App Rep 25.
160 24 Fsupp 2d 548 (ED Va, 1998).
161 1999 WL 14479 (Unreported, Nebraska Court of Appeal, 5 January 1999).

the recovery of any productivity losses that result. In *Samuel v Stubbs*,[162] a case that involved the defendant jumping on a policeman's hat, it was held that for property to be damaged, it was unnecessary for it to be prevented from serving its normal function. It is sufficient if there is a temporary functional derangement of it.

However, the remedy for conversion may be unsuitable if the remedy sought was the delivery up of information rather than the usual payment of damages.

Trespass to goods

Trespass to property is a wrongful interference with goods in the possession of another. The interference must be wrongful and intentional, although actions for reckless and careless interference are possible.[163] A plaintiff must be able to show actual, constructive or a legal right to immediate possession at the time of interference. [164] The defendant's act must be voluntary, intentional or negligent, and must directly occasion the trespass. Any act that sets in motion an unbroken series of continuing consequences, the last of which ultimately causes contact with the goods of the plaintiff, will be sufficiently direct. This could adequately encompass actions for damage caused by viruses where the causation is remote. Whilst the interference must be direct and physical; the defendant need not make personal contact with the goods. This addresses the problematic issues of remoteness on the Internet. In *Kirk v Gregory*,[165] the mere moving from one place to another of a good was sufficient for trespass. The fact there is no material damage does not prevent a cause of action. Trespass is actionable per se without proof of damage. This may silence debates based on the intangibility of property.

To be able to compensate for damage caused by hacking or computer viruses via an action in trespass, it would be necessary to conclude that such conduct is an interference with goods, that there is liability for unintentionally transmitting a virus and that intangible property can be actually damaged. The deliberate transmission of a computer virus with the intention of damaging the recipient's computer is an action directed at the plaintiff's property. Consequently, the plaintiff may be prevented from using their computer. It is clear that liability for trespass could arise if the defendant should have known of the existence of the virus and failed to prevent its transmission. There is no need to show the damage suffered was foreseeable. Thus, tort law may remedy what criminal damage statutes cannot. The actual computer itself may not be damaged in any physical sense. A virus may cause costs in restoring the computer to an operational state, loss to the value of data, loss of profits and productivity in downtime, or loss of reputation.[166]

For example, the court in *CompuServe Inc. v Cyberpromotions*,[167] held that Cyberpromotions committed the tort of trespass on personal property by using CompuServe's computer system without permission. In *America Online v LCGM*

[162] (1972) 4 SASR 200.
[163] *Penfolds Wines Pty Ltd v Elliott* (1946) 74 CLR 204, 214 gives examples of acts constituting trespass.
[164] *Johnson v Diprose* [1893] 1 QB 512, 515.
[165] (1876) 1 Ex D 55.
[166] New Zealand Law Reform Commission, above n 17, 62, par 154.
[167] 962 F Supp 1015 (SD Ohio, 1998).

Inc. et al,[168] unsolicited email was held to constitute a trespass to chattels, based on the terms and conditions that applied to America Online accounts. A permanent injunction was granted to prevent abuse.

A trespass action may not be possible if the situation was merely one where files are copied as the owner's property is not damaged, unless the court invokes the *Cox*[169] and *Whiteley*[170] approaches whereby the magnetic impulses are seen to be affected. In this scenario, conversion could also be denied, as the owner is not deprived of possession. However, this may not be a problem as SCAG's stated aim is to preserve computer system integrity and the proposed provisions do not extend to such situations.

In the above cases, conversion and trespass are readily applicable to the Internet context. Existing tort law can be seen to give satisfaction to plaintiffs for damage to their operating systems and business. To allow the use of tort law there needs to be a general acceptance that data can be a good possessed, and that intangible property is equally capable of being converted and trespassed against.

Negligence

A negligence action may cover damage caused where there was no intent. However, in Cyberspace, negligence may be precluded because the court believes it has the potential to expose defendants to 'liability in an indeterminate amount for an indeterminate time to an indeterminate class.'[171]

To establish liability for a negligent act or omission it is necessary to establish the defendant owed a duty of care to the plaintiff. If the case is outside the scope of the established duties, one considers if there is a sufficient relationship of proximity to establish a duty of care. Is it reasonable that the defendant's carelessness would cause damage to the plaintiff? Do any considerations limit the scope of the duty to the class of person to whom it is owed?[172] On the Internet, one user may have a relationship of proximity with any other user whenever information is transferred from one computer to another. Gripman suggests a negligence duty of care should be imposed on commercial interests.[173] It is submitted that this could assist enforcement. A duty of care would create a legal obligation to exercise a reasonable standard of care.[174] In assessing what is a reasonable standard of care courts may consider current industry practice. The risk of a virus could be balanced against the cost and difficulty of taking precautions.[175]

The remoteness of damage may be an issue for negligence actions as the sheer number of intermediaries may mean either the number or the fact they acted in a severing way breaks the chain of causation. Liability will be limited when the harm is considered too remote.[176]

168 46 F Supp 2d 444 (ED Va, 1998).
169 (1986) 83 Cr App Rep 54.
170 (1991) 93 Cr App Rep 25.
171 *Ultramares Corporation v Touche*, 255 NY Rep 170, 174 (Ct App, 1931).
172 *Anns v London Borough of Merton* [1978] AC 728.
173 Gripman, above n 18, 172.
174 *Blyth v Birmingham Waterworks Co* (1856) 11 Exch 781,784; 156 ER 1047.
175 New Zealand Law Reform Commission, above n 17, 69, par 173.
176 *Overseas Tankship (UK) Ltd v Morts Dock and Engineering Co Ltd*, The Wagon Mound (No1) [1961] AC 388.

Against Torts

To litigate an action as a civil wrong may deny a defendant certain rights. Especially relevant is that fault be proved beyond reasonable doubt. It may be necessary to gauge whether the harm is serious enough to require proof of fault. Intention and culpability are integral parts of the criminal law.

The lack of resources of some defendants may militate against tort actions. A computer vandal may have little money to pay a compensation claim and thus civil liability may not be a deterrent. In addition, it may be more difficult for a victim to pursue a civil action because of the costs and inability to obtain evidence as they lack the investigative and search and seizure powers of the state.[177]

Recommendations

The *Wrongs Act 1958* (Vic) currently makes provision for such diverse and obscure actions as damage by aircraft[178] and animals straying on to a highway.[179] It may be that the uniqueness of the Internet similarly demands consideration. This need is exacerbated by the fact that the medium's uniqueness will be transcended by its ordinariness as much of society rushes to capitalise on the economic and distribution virtues of the medium.

The NSW Parliament has recently decided to implement SCAG's proposal.[180] It is suggested the criminal law needs to be supplemented by the civil law to change the opportunity structure and provide further disincentive to engage in such conduct. The fact that corporations are not effectively deterred militates in favour of civil remedies. The Love Bug incident also indicates that civil remedies may be the only redress open to victims as the criminal law is too inflexible to define and thwart all behaviours on the Internet that can cause damage. Each State's equivalent of the *Wrongs Act 1958* (Vic) should include a definition of property which, like the *Crimes Act 1958* (Vic), includes intangible property. Any criminal legislation should specifically not preclude the ability to pursue civil action. Given that the judiciary may follow centuries of precedent and deny the ability of torts, such as trespass and conversion, to be applicable to intangible property, legislation may need to make it clear that such torts are capable of being used in relation to information systems. A computer offences section, comparable to the criminal proposals, may similarly be inserted into each State's equivalent of the *Wrongs Act 1958* (Vic). It may be necessary to enshrine in statute the concept that a temporary derangement of data is as equally capable of representing damage as is a policeman's hat. Further clarity would be provided by provisions that state that interference with computer systems and the data they contain constitutes interference with goods for the purpose of civil actions.

[177] Gripman, above n 18.
[178] Part VI.
[179] Part VIII.
[180] Crimes Amendment (Computer Offences) Bill 2001.

CONCLUSION

The Internet is a novel and multifaceted medium of communication, which is becoming an integral part of our day-to-day social interactions. It presents a number of enforcement difficulties arising from its design and nature as it allows anonymous interactions between people in spatially distinct jurisdictions. Individual nation states are unable to enforce their domestic criminal laws. The types of security threats and ways in which criminals can facilitate property damage are also novel; and such technological innovations create problematic issues of proof.

Conduct that has the potential to cause damage in the Internet context is essentially a threat to private property. The legal system appears to be reluctant to remedy damage caused to computer data because of the belief that data is of an intangible nature. Legislative attempts are overly concerned with protecting the integrity of computer systems; the box rather, than the data. Yet, it is the data that is of value; without it a computer system is merely a plastic box and silicon chips. There are cases that illustrate that the common law has been able to adequately adapt to technological innovation, recognise the value in electronic constructs and the need to provide remedy for interference with intangible goods. Some commentators argue that the recognition of property rights in information or data would assist the regulation of the Internet. I would suggest that the medium is sufficiently excludable to be the object of property rights. Property rights attach to that which society deems valuable and worthy of protection. The Internet is socially valuable.

The proposal by SCAG is to be applauded for its considerations. However, there are a number of pertinent questions unanswered that militate against the success of legislation that attempts to be an all-encompassing antidote to our Internet ills. In addition, statute by its very nature is less flexible than the common law and fixed in time and space. This has a disadvantage in regulating an area concerned with technological evolution. The fluidity and continuing change on the Internet denies the ability of legislation to define the harm to an extent sufficient to provide clarity and certainty in the law.

The decision to criminalise certain Internet conduct is a utilitarian decision based on the belief it is the most efficient and cost effective way to regulate it. It can also be seen to be a decision based on a concern for society's collective welfare and interests. In this regard, legislation serves a purpose as a base of minimum standards to protect individuals from the abuses of corporations. However, there is also a philosophical argument that we should not criminalise what are effectively civil wrongs; that the criminal law should be saved for the most heinous of crimes and individual autonomy should be sacrosanct. To use the criminal law simply because it is effective distorts the system; actions should be criminalised because of their seriousness. Raz's construct, where the state's role is to create the conditions necessary for the exercise of individual autonomy, demands individual rights be protected against the majority and may be the appropriate philosophical model for Internet regulation.

As the harm inflicted in the Internet context predominantly results in damage to data, that damage can be remedied more reliably and efficiently by tort law. Given the commercial interests at stake, the impractical workings of the criminal

law in this context, and the developing recognition within society that data can constitute property, tort law is of greater utility. In the United States, tort law was initially used to remedy damage inflicted via the Internet, and torts such as conversion and trespass were eminently suitable. On the one hand, the criminal law is no deterrent to corporations when one considers the difficulty in holding a corporation criminally liable, together with the great commercial temptations on offer. On the other hand, commercial operators that fall victim are more concerned with property rights and compensation rather than State sanctions. Tort law can equally deter wrongful conduct and operate as corrective justice, as well as more fairly allocate costs.

An action in trespass offers the advantage of being actionable *per se* and thus able to overcome any intangibility debate. Conversion may assist if the law insists that interference with electronic goods is merely a temporary derangement. Negligence actions may overcome the necessity to prove intent if a duty of care can be shown. In addition, all civil actions have the added advantage of a lesser burden of proof than the criminal law. General tort law is also better able to transcend jurisdictions than idiosyncratic criminal laws, especially in the common law jurisdictions.

Any legislative response should be directed to synchronizing the understanding of property between both the criminal and civil law; and transcending the anachronistic and increasingly irrelevant historical doctrines that fixate on tangible property and the need for actual possession in order for the law's protection. If this is not addressed then the law may find itself superfluous to the majority of society's future interactions. Embracing civil law in our regulatory attempts would assist in changing the opportunity structure to engage in conduct that causes damage.

The appropriate legislative response is to speed up the judicial recognition of two major issues: that data has value in society; and it deserves protection and compensation when damaged. The compensation for costs, such as lost productivity and repairs, should be justifiable on the basis of the same utilitarian arguments presented to justify criminalisation. There are social advantages to civil actions in this area; it would provide a more efficient allocation of costs, and compensate both corporations and individuals for damage caused through no fault of their own. The potential for large-scale economic disruption to society increases everyday as the Internet becomes more prevalent. Protecting the integrity of computer systems alone is misguided, as it is not the box that is precious, it is what it contains.