THE INTERNET AND THE LAW

Benedict Dugan* ***and Bob Dugan****

I INTRODUCTION

The Internet and related technologies are impacting on the law like no other phenomenon in our lifetime. The impact is felt from the basic institutions of contract and tort to the remote corners of competition law and securities law. The legislative system is not coping with the challenge, as demonstrated by the paralysis over the Electronic Transactions Bill and the Crimes Amendment Bill (No 6). This article opens with some background material about the Internet, proceeds to consider its impact on eight areas of the law and concludes with some observations about the feasibility and direction of regulation.

A History

The Internet traces its history to the ARPAnet, a United States Department of Defence project in the late 1960's to establish a communication system capable of withstanding catastrophic attack. The Internet was confined to military and university purposes until 1987 when it was made available for commercial use.[1] Internet use exploded in the early 1990s after invention of the browser/server combination that we associate with the Worldwide Web. The number of connected persons has risen from 242 million in the year 2000 to over 500 million in 2002. The phenomenon known as electronic commerce has grown from $0 in 1990 to $500 billion in the year 2000 and is predicted to top one trillion dollars by the end of this year.[2]

** Computer Science Department, University of Washington, Seattle.

* Reader in Law, Faculty of Law, Victoria University of Wellington.

Editor's Note: This paper was prepared before the passage of the Electronic Transactions Bill as the Electronic Transactions Act 2002. The points that the authors make, they believe, about the Bill remain true of the Act.

1 <http://www.netvalley.com/archives/mirrors/dave/marsh-timline-1.htm>.

2 <http://www.epaynews.com/statistics> and <http://www.internettrafficreporter.com>.

B What's the Internet?

For some of us, it is a faster, cheaper alternative to the postal service. For others, it's a new way to shop; for others it's a library, or a public forum; and for an increasing number of us, it's a job. From the user's view, the Internet is a universal machine, a machine that can, from one instant to the next, morph into other machines. A toaster can only do one thing. Today the Internet serves as a postal system, a school, a library, a shopping mall, a bank and much more. Tomorrow, it will be a word-processor, a cinema and a parliament. Very soon, it will be an omniscient and intelligent presence that knows our every secret and that can devise solutions to heretofore unfathomable problems. The Internet is, in short, reshaping our world from one day to the next.

C Principal regulatory impact

The main regulatory impact of the Internet does not concern the Internet as such. It concerns reshaped real-world institutions. For almost 100 years, the lack of library resources alone relegated the law faculty where I work to the status of a third rate institution in a remote island nation. Three months ago, with the stroke of a pen and at a cost less than that of a new car, our students gained instantaneous access to library facilities superior in many ways to the combined hardcopy holdings of Oxford and Harvard. While this happened overnight, it will take us the better part of a decade to adjust. The object of regulation here will not be the Internet but rather the education industry.

D Nature of the Internet

Intelligent regulation requires an understanding of the nature of the Internet. Though the Internet is everywhere, its character remains elusive. In many contexts, it is simply referred to as a cloud. For the web surfer, it is an interconnected collection of over two billion documents. Many lay persons probably view it as a more complex version of the telephone system or cable television. Programmers view the Internet as a collection of conventions or standards, largely ones without any legislative sanction. The character question is important. If the Internet is an electromagnetic cloud like the radio spectrum, this invites regulation by auction and/or user restrictions. A quite different approach is indicated by the view that the Internet is a collection of conventions or protocols. As implemented, this collection has four specific features that must inform any attempt at regulation. The Internet is digital, distributed, packet-switched and open.

E Internet as Digital

All information stored, processed and communicated on the Internet is in digital format, represented by sequences of binary values. This contrasts with the analog information perceived and processed by the human senses that can assume any of an

infinite number of values within and outside the perceptible range. Digital format has a peculiar, universal capability. In the off-line world, different sorts of analog information are associated with particular instantiation-text with paper, sound with vinyl or magnetic tape, etc. This physical nexus constrains the processing, transmission and, importantly, the reproduction of the artefact. In the on-line environment, songs, text and photos can be stored, processed and transmitted in digital format over a wide variety of media. The reproduction of information in analog formats – for example, by photocopy or tape-deck - requires a significant financial investment and results in successive deterioration. No such constraint applies to digital records. Thousands of copies can be made at virtually no cost. The thousandth copy of a copy cannot be distinguished from the original.[3]

F Internet as Distributed

The classical telephone network resembles a bike wheel without the rim. A single path connects each spoke end with a central hub. There is only one path between any two spoke ends and that path passes through the hub. In contrast, the Internet resembles a sponge, spider web or a rabbit warren. Each node is connected with multiple other nodes each of which is similarly connected. There are multiple paths between any two nodes. There is no central hub. This redundancy feature underlies the resilience of the Internet to calamity as well as to regulation.

G Internet as Packet-Switched

The classical telephone network is also circuit switched. At the central hub, each customer's wire is connected to a switching unit. When one customer rings another, this causes the switch to connect the hub ends of their two wires. Once the circuit is established, it provides a medium for continuous and two-way communication to which only the two customers and the hub are privy. In the Internet, the information is first broken into packets labelled with the addresses of sender and recipient. The movement of a packet through the warren of networks is determined by these addresses. In effect, they provide instructions to routing computers located at the nodes where the networks intersect. The several packets comprising a given message may take quite different routes from the sender to the recipient. The telephone allows simultaneous two-way communication, Internet communication involves one-way exchanges of data packets. Yet such is the speed of the exchange that there is the impression of duplex communication.

---

3 On the furious search for copy-proof CdROMs, see <http://www.heise.de/newsticker/data/ghi-a30.08.02-000/> [JVC product].

Also see, <http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/sha-07.08.02-000/default.shtml&words=Wasserzeichen> [Frauenhofer Institute watermark technology].

H Internet as Open

The Internet is open in several distinct senses. The most obvious is that associated with use of the Ethernet protocol, a set of standards that addresses the physical interconnection and operation of computers connected in the local area network. Packet transmission is by way of public broadcast. As the packet moves from one network to another, it is perceived by every node within the particular network. However, the packet is picked off only by routers and that node having the recipient's address. With appropriate software, freely available and easily used, the packet can be read by any machine connected on any of the networks through which the packet passes. The Internet is open in a second sense that relates to its constituent conventions or protocols. These protocols are accessible by the public, free for use and not, in general, the subject of property rights. The Internet is open in a third sense. Unlike an automobile, the Internet can be used without government permission.

I Sovereignty

These four features have fundamental implications for regulation. The most obvious relates to sovereignty. In an off-line environment, regulation is predicated ultimately on geographical location and political borders. Traffic in hard copy pornography can be regulated by a prohibition enforced against producers and distributors within a country and by guards at its borders. With the advent of the Internet, the local porn dealer simply closes shop and moves the material on to a web site in a jurisdiction that does not prohibit pornography. The web site can deliver material to local residents far more cheaply and efficiently than a single local shop. However, the facilities used in the dissemination now lie largely beyond the reach of local enforcement authorities. The local ban must be implemented, if at all, against the recipients or the local ISP. Under the present state of technology, ISP's cannot accurately distinguish between a porn page and an email. Experience with drugs and gambling shows that user-based enforcement is not cost-effective.

J Security

As a second fundamental regulatory peculiarity, the Internet is a very insecure place. A packet broadcast under the Ethernet protocol can be intercepted and perceived by anybody connected to the network or networks through which the packet passes. The open protocols provide public information required for effective hacking. Unlike its analog counterpart, digital information can be perfectly copied and/or altered without detection. Security issues figure significantly in computer crime, privacy invasion and copyright violation. Whilst encryption can solve many of the security problems, its widespread deployment greatly complicates law enforcement.

K Internet as the New Commons

The tragedy of the commons drives much modern regulation. The lesson of that story is that private property rights are necessary to preserve the resource and maximise its value. There is increasing acceptance for the view that the Internet, as presently constituted, represents a commons. It is a freely accessible resource used to produce goods and services.[4] However, unlike the off-line commons, the Internet resource is non-exhaustive and non-rivalous. Economists appear sharply divided as to the efficiency consequences of a partial closure of such a peculiar commons.[5]

L Specific Impact

The following pages consider the impact of the Internet on eight areas of the law. Three foundation areas are examined first: contract, tort, and crimes. Consideration is then given to its impact on the law of civil liberties, banking, company and securities, taxation, and competition. The Internet and related technologies are also causing upheavals in the law relating to privacy, employment, agency, property and intellectual property. The individual topics are surveyed by reference to principal themes, most of which have, in the last five years, become the subject of rich litigation and academic discussion. Much of the material is drawn from the United States, the jurisdiction with the most experience in using and regulating the Internet.

II IMPACT ON SPECIFIC AREAS OF THE LAW

A Contracts

1 New contracting environment

From a legal point of view, the institution of contract lies at the heart of electronic commerce. Contracting practices on the Internet bear only a superficial resemblance to scenarios presumed by traditional rules. Those involve the face-to-face transaction or the exchange of documents generally between parties within the same jurisdiction. In both scenarios, the parties have the opportunity to verify each other's credentials before they commit themselves contractually. In contrast, the typical Internet contract is a real time encounter between complete strangers, often in different jurisdictions. Most transactions have a computing machine on one or both sides of the deal. This scenario stresses both the substance of contracts as well as the rules for their formation.

---

4 Lawrence Lessig *The Future of Ideas* (Random House, New York, 2001) 19-85.

5 See generally Carol Rose "The Comedy of the Commons" (1986) 53 U Chi L Rev 53.

*2 Issue*s

In digital commerce, contracts are generally packaged as box wraps, shrink wraps, browse wraps and click wraps. Performance and assent are inter-layered. In many situations, the purchaser is not confronted with the terms of the transaction until long after payment for the goods. Another formation issue concerns compliance with writing and signature requirements.[6] The needs of digital commerce have also impacted on contract substance. The licence has replaced the sale as the favoured transaction vehicle, largely as an attempt to deal with the replicability of digital information. In relation to digital products, it is unclear whether performance involves the delivery of goods, the rendering of services or the exchange of information. The characterisation of performance controls the applicability and operation the Sale of Goods Act 1908, the Consumer Guarantees Act 1993 and the Fair Trading Act 1986.

3 Regulation

In view of their significance for electronic commerce, it comes as no surprise that these matters have been the subject of the first wave of Internet regulation. In 1995, shortly after the dawn of the e-commerce age, Utah enacted what appears to be the first digital signature statute.[7] This was a technology-specific measure pursuant to which a valid electronic signature could only be affixed by use of public key encryption. In 1997, Germany enacted a digital signature statute along the same lines.[8] In 1996, UNCITRAL approved the broader scoped and more technology-neutral Model Law on Electronic Commerce (MLEC).[9] The measure provides a framework for electronic compliance with requirements for writing and signatures as well as ones for notice and document retention. The UNCITRAL model has served as the basis for legislation in the United States, Australia and Canada.[10] In the United States, the Uniform Electronic Transaction Act

---

6 The search string "writing or written" yielded 3,299 hits in one electronic version of the New Zealand statutes; the string "sign or signed or signature" yielded 2,875 hits.

7 Utah Code Ann 46-3-101 to 504 (Michie l996).

8 See Signaturgesetz of 22 July 1997 (BGB1. IS. 1870, 1872) replaced by Gesetz über Rahmenbedingungen für elektronische Signaturen of 16 May 2001 (BGB1. I 2001, 876); these can be found at <http://jurcom5.juris.de/bundesrecht/>.

9 UNCITRAL Model Law on Electronic Commerce with Guide to enactment, < http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

10 See Electronic Transactions Act 1999 (Cth); Uniform Electronic Commerce Act 1*999* (Can) (this model act has been enacted in most of the provinces and influenced the federal Canadian Personal Information Protection and Electronic Documents Act SC 2000, c 5). In the United States of America, see the Uniform Electronic Transactions Act 1999 <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>, is supplemented at federal level by Electronic Signatures in Global and National Commerce Act 2000, 15 USCA 7001-7006 (West Supp 2001) US.

[UETA], which has been enacted in all but a few states, also deals with contracting by electronic agents and transferable instruments.[11]

4 Developments in New Zealand

New Zealand remains one of the few English-speaking jurisdictions without a legislative framework for electronic compliance with contract formalities. In 1998, in its first report on the impact of electronic technology, the Law Commission recommended legislation along the lines of the MLEC.[12] In 1999, the definition of *writing* in the Interpretation Act 1924 was amended to acknowledge the possibility of electronic compliance.[13] A year later, the Electronic Transactions Bill patterned on the MLEC was introduced in Parliament. The Bill received its second reading in April 2002 and was well down the agenda at the close of the legislative session.

5 The Electronic Transactions Bill

The Electronic Transactions Bill is a plain language version of the MLEC. The plain language thrust eliminates much of the technical specificity which provides certainty in the overseas statutes. Test-driving typical transactions through the Electronic Transactions Bill does not lead to predictable destinations.[14] For instance, it is unclear:

- whether the writing requirement is satisfied by a record on a CD Rom or by a human memory;
- whether the signature requirement can be satisfied by an email letter heading or a ticked box on a web page; or
- how the document retention requirement applies in common situations involving system migration or format conversion.

It is precisely such issues that should lead to certain results under the statute. The Bill raises serious questions concerning plain language drafting as well as the sufficiency of this country's law-making resources.

---

11 Uniform Electronic Transactions Act 1999) ss 14 and 16 (dealing with electronic agents and transferable records). As of June 2002, it had been adopted by 41 states; see < http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp>.

12 New Zealand Law Commission *Electronic Commerce Part One: A Guide for the Business Community* (NZLC R50, Wellington, 1998) 119.

13 Interpretation Act 1999, s 29.

14 For a critical discussion, see Benedict Dugan and Robert Dugan "Electronic transactions" [2001] NZLJ 483.

6 Other issues

The law remains unsettled in relation to the enforceability of wrap contracts and the sales/licence distinction. The cases continue to roil through and divide the appellate courts in the United States. Driven by Judge Easterbrook's controversial decision in *Pro CD*, the doctrine of "layered contracting" appears to be gradually replacing the traditional approach based on offer-and-acceptance.[15] It has been adopted by the Uniform Computer Information Transaction Act 2000 (UCITA).[16] That model statute-which regulates the formation, terms, performance and remedies in computer information transactions-was originally designed for inclusion in the Uniform Commercial Code. However, strongly opposed by both academics and consumer groups, it was ultimately approved for enactment as a separate statute. The UCITA has, at the time of this writing, been adopted in only two jurisdictions (Maryland and Virginia).[17]

B Torts

1 Tort-prone environment

Involving millions of strangers interacting with each other in a fast-moving and complex environment, the Internet is a particularly fertile ground for tort law. To make matters more interesting, the Internet environment is filled with new forms of valuable property. Domain names, registered less than a decade for under $100, sell today for millions.[18] Similar values attach to commercial web sites, an intellectual construct unknown a decade ago. The shopping routines that guide customers through these sites are themselves the subject of patent rights.[19] The new property also includes an ever increasing volume of entertainment products and, at the periphery, the very protocols comprising the Internet itself. Finally, many Internet participants have very deep pockets.[20] In many respects, the Internet resembles motorway traffic, the accident-prone environment which, at least in the United States, generated much modern tort law.

---

15 *ProCD Inc v Zeidenberg* (1976) 86 F 3d 1447 (7th Cir).

16 The Uniform Computer Information Transaction Act can be found at <http://www.law.upenn.edu/bll/ulc/ucita/ucita1200.htm>.

17 See Md Code Ann. [Com Law II] 22-101 to 22-816 (2001); Va Code Ann. 59.1-501.1 to -509.2 (Michie Supp 2000); at time of writing, sixteen other states were considering adoption of the UCITA; see <http://www.bmck.com/ecommerce/ucitacomp.htm> (last accessed 14 June 2002).

18 See "Dot-cc Domain Name Fetches $1 Million" (13 July 2000) *Newsbytes*, Los Angeles.

19 See *State Street & Trust Co v Signature Financial Group Inc* (1998) 149 F 3d 1368 (Fed Cir); Anders and Quick "Technology Journal: Amazon 2001 Barnesandnoble.com" (25 October 1999) *Wall St J*, New York.

20 See, for example, *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 (SC).

2 New types of interference

Almost daily, the Internet generates new instances of perceived objectionable conduct. Occurring between strangers, these fall to be remedied, if at all, through the law of tort and crimes. Particularly in the United States, where Internet use is most widespread and well established, the pressure on tort law is fuelled by that jurisdiction's unique cost rules. The result is a veritable flood of litigation involving most of the nominate torts. In every case, the court must adapt the elements of the particular tort to the peculiar features of the Internet environment, an exercise which raises difficult issues of both law and policy.

3 Defamation

In the off-line world defamation was a tort generally reserved for those with access to the public media, ie politicians, movie stars, journalists and publishers. Today, any PC user can, for nothing or a few cents, place a message on a bulletin board or establish a web site which will reach far more people than accessible by all the hard copy publishers in this country. But, whereas traditional defamation generally involved only a single intermediary publisher, the Internet presents the offended plaintiff with several financially substantial intermediaries including the local ISP, the communication service, and the web portal. The threshold issue is whether these intermediaries qualify as a publisher—a matter that divided the courts in the United States and finally resulted in broad statutory immunity.[21] In view of the boundary-less nature of the Internet, it is not surprising that another issue to divide the courts involves the place of defamation. That issue lies at the heart of the *Gutnick* case in Australia which pits an Australian businessman against the Wall Street Journal. The defamatory statement appeared in a newspaper article mounted on a web site in New Jersey. Given the differences in defamation law in Australia and the United States, the place of defamation is outcome-determinative.[22]

4 Trespass to chattels

After a century of insignificance, the tort of trespass to chattels has become the flavour of the day. It is being applied to a wide range of conduct at the heart of Internet commerce, including the use of search robots and spiders, framing and deep linking, cybersquatting, spam, web site defacement, and denial of service attacks.[23] Illustrative is

---

21 Compare *Chubby Inc v Compuserve Inc* (1991) 776 F Supp 135 (SD NY) with *Stratton Oakmont Inc v Prodigy Services Inc* (1995) 23 Media L Rep 1794 (Sup Ct NY); immunity conferred by 47 USCA s 230 and applied in *Zeran v America Online* (1997) 129 F 3d 327 (4th Cir) cert den 524 US 937.

22 *Gutnick v Dow Jones*, above. The appeal has been heard by the High Court and has attracted significant attention in the press; see Michael Pelly "Web Site Of Libel Puts Publishing On The Spot" (12 June 2002) *Sydney Morning Herald*, Sydney.

the *Ebay* case brought by the largest Internet auction site.[24] The plaintiff's site was being accessed several thousand times an hour by the defendant aggregator's spider. Bargain hunters visited the aggregator's site rather than the many individual auction sites, with a diversion of advertising revenues. Ebay convinced the Court that the marginal additional load on its server constituted a trespass to chattels. AOL successfully invoked the same tort against a commercial spammer that was emailing AOL members over its servers.[25] In extending this long moribund tort to the new environment, the courts have had to re-jig all of its elements including tangibility, intentionality, interference and quantification of injury.

5 Other torts

The economic torts of misappropriation, unfair competition and interference with contract have also experienced a significant resurgence in the Internet environment. They are invoked as a ground for relief in situations where protection is not available under the law of intellectual property. The key issue is often one of pre-emption.[26] As a last resort, there is always the tort of negligence. In *Lunney*, the plaintiff invoked the tort against an ISP which allowed a stranger to register and send defamatory emails in the plaintiff's name.[27] In *Doe*, an irate parent sued another ISP in negligence for allowing a subscriber to distribute pornographic photos of her minor son.[28] Liability turns principally on whether the ISP's duty of care extends to these plaintiffs, an issue ultimately laid to rest in the United States by federal statute.[29] The next wave of negligence cases will focus on security issues. Where a denial of service attack brings down the site of your web broker, you will invoke the tort against the manufacturer of the server software.

---

23 See *Rfor exampleister.com Inc v Verio Inc* (2000) 126 F Supp 2d 238 (SD NY)(robots/spiders), *Ticketmaster Corp v Tickets.com Inc* (2000) 2000 US Dist LEXIS 4553 (CD Cal)(framing/deep linking), *Panavision International v Toeppen* (1998) 141 F 3d 1316 (9th Cir)(cybersquatting), *America Online Inc v IMS* (1998) 1998 US Dist LEXIS 20645 (ED Va)(spam), *America Online Inc v National Health Care Discount Inc* (1974) 174 F Supp 2d 890 (ND Io 2001)(denial of service), *Internet Doorway Inc v Parks* (2001) 138 F Supp 2d 773 (SD Miss)(appropriation of email address).

24 *eBay Inc v Bidder's Edge Inc* (2000) 100 F Supp 2d 1058 (ND Cal).

25 *America Online Inc v IMS* (1998) 1998 US Dist LEXIS 20645 (ED Va).

26 See, for example, *Pollstar v Gigmania Ltd* (2000) 170 F Supp. 2d 974, 2000 US Dist LEXIS 21035 (ED Calif).

27 *Alexander G Lunney v Prodigy Services Co* (1999) 94 NY 2d 242 (Ct App).

28 *Jane Doe v America Online Inc* (2001) 783 So 2d 1010 (Fla).

29 See 47 USCA s 230.

6 Regulation

As compared to contract law, tort law has not engendered the same pressure for regulation, except where the issue involves the essential structure and operation of the Internet. Several jurisdictions have addressed the liability of intermediaries such as ISPs, portals and telecommunications systems. The federal United States statute confers a wide immunity, whereas the German statute takes a much more conservative approach.[30] The United States has also enacted federal legislation regulating cybersquatting, and a number of states have regulated spam.[31] Apart from a few cases involving domain name disputes and defamation, there has been little tort litigation in New Zealand.[32] This is not because such incidents have not occurred, but probably because the local cost rule deters their litigation.

C Crimes

Not surprisingly, it is the aberrant use of computers that makes the biggest headlines. The extent of the problem is difficult to gauge. On the one hand, nervous about negative publicity, commercial enterprises are reluctant to report computer-related offences and to detail the extent of their losses. On the other hand, many reports do not clearly distinguish between conduct that is clearly criminal (for example, unauthorized network access or data destruction) and conduct giving rise to only civil liability (for example, auction fraud and copyright infringement). Nevertheless, it seems likely that the amounts at stake are substantial.[33] What is certain, however, is that regulation of computer crime poses some very difficult issues.

---

30 Gesetz ueber die Nutzung von Teledienste n (BGBl I 1997, 1870) <http://jurcom5.juris.de/bundesrecht/tdg/index.html>.

31 See Anticyberquatting Consumer Protection Act 1999 15 USCS s 1051. The anti-spam for example, legislation from United States and Europe is collected at www.spamlaws.com.

32 *O'Brien v Brown* [2001] DCR 1065 [defamation over the Internet], *Oggi Advertising Ltd v McKenzie* [1999] 1 NZLR 631 (HC) and *Lewis v Wilson & Horton Ltd* [2000] 3 NZLR 546, (HC) (domain name disputes).

33 *Accountancy Age* 11 Oct 2001 p 21 [PricewaterhouseCoopers estimates the global cost of cybercrime at $1.4 trillion annually]; *CSI/FBI 2002 Computer Crime and Security Survey* at http://www.gocsi.com/press/20020407.html (in a survey of 503 large companies, 34% reported losses estimated at around half billion dollars).

1 Types of computer crimes

Computer crimes are commonly classified according to the involvement of computers. In many instances, the objectionable conduct simply uses the Internet as a medium and clearly constitutes an offence under existing statutory provisions for, eg, fraud, gambling and pornography. The FBI's operation Cyberloss in the year 2000 involved prosecution of over 200 individuals associated with various Internet scams affecting over 67,000 victims.[34] Over half the cases involved auction fraud. The problem in these cases is largely one of enforcement. The other type of computer crime includes a wide range of exploits that target a computer or a computer system. These generally involve unauthorised access, destruction and theft of data. At the one extreme are bank frauds and denial of service attacks which cause high six-figure losses.[35] At the other extreme are web site graffitti and viruses, the majority of which have at most a nuisance value. This conduct eludes easy subsumption under traditional criminal offences. Illustrative is the local case of *Garrett*.[36] By means of an email attachment, the defendant installed malicious code into the victim's computer. This code caused the victim's computer to transmit to the defendant the victim's log-in and password for their ISP. The defendant then used this information to obtain services on the victim's account.

2 Features of computer crime

Most off-line crimes require physical proximity of the offender and victim. Many crimes — for example, pornography, gambling, copyright piracy — also require a significant initial investment and physical infrastructure. These features both facilitate enforcement and pose a barrier to entry. In most computer crime, the victim neither sights the offender nor knows where the offender is located. The exploit can be mounted as easily from inside as outside the victim's jurisdiction, preferably from one where the conduct is legal. Offenders commonly employ readily available software to disguise the origin of the exploit. Internet piracy and fraud can be mounted on-line at a fraction of the cost of similar operations in the off-line environment. Often, the victim is situated alone in the security of their home-a fact which is thought to make them particularly susceptible to fraud. But a few things remain reassuringly the same. Most of the serious economic

---

34 <http://www.fbi.gov/pressrel/pressrel01/ifcc052301.htm>.

35 In the survey cited at note 33 above, 62 firms quantified losses from DOS attacks, with highest reported loss of $50m and average loss of $18m.

36 *R v Garrett* (2001) 2001 NZDCR LEXIS 103 (DC), *R v Garrett (No 2)* (2001) 2001 NZDCR LEXIS 157 (DC).

crimes - such as account manipulation and credit card theft-are committed by insiders, or more recently, by organised criminal groups, rather than the bearded computer geek.[37]

3 Regulatory response

Prosecution of computer crime requires new law enforcement measures, many of which can be put in place without special legislation. These include on-line complaint centres, specially designed equipment, trained personnel and international co-operation.[38] Other measures, however, such as Internet surveillance, require statutory intervention that usually bumps against privacy concerns and civil liberties.[39] In OECD jurisdictions, it is generally recognised that new offences need to be defined for cases like *Garrett*. The first such measure was proposed in 1977 in the United States, followed a few years later by enactment of the Computer Fraud and Abuse Act 1984.[40] Since then, that statute has been revised on six occasions to accommodate technical advances and innovative hacking. During the same period, specific computer crime legislation has been put in place in all but four of the OECD jurisdictions, one of which is New Zealand.[41] But this is not for want of trying.

4 Crimes Amendment Bill (No 6) 1999

A computer crimes Bill was presented to Parliament in 1998 as the currently pending Crimes Act Amendment Bill (No 6). Whilst the Bill has sparked lively debate, this has largely centred on its privacy implications. There has been relatively little discussion of the four substantive offences proposed by the Bill. The offences part of the Bill suffers the same general infirmity as the Electronic Transactions Bill. The plain language provisions, whilst concise and with an obvious thrust, fail to respect the underlying technical reality. As a result, the proposed offences potentially criminalise a wide range of completely innocuous conduct, some of which is essential to the functioning of the Internet, including the use of cookies, installation of Ethernet cards, and publication of academic articles on Internet security.[42]

---

37 See *Computer Intrusion Cases* at <http://www.usdoj.gov/criminal/cybercrime/cccases.html>.

38 See the FBI's Internet Fraud Complaint Center at <http://www1.ifccfbi,gov/index.asp>.

39 See for example, the controversy over the FBIs Carnivore, a system for monitoring email; Peter Young "The Case Against Carnivore: Preventing Law Enforcement from Devouring Privacy" (2001) 35 Ind L Rev 303.

40 18 USC s 1030.

41 For a survey of OECD legislation, see <http://www.mossbyrett.of.no/info/legal.html>.

42 See Benedict Dugan and Robert Dugan "Cookies and Electronic Crime" [2001] NZLJ 439.

5 Garrett

Until legislation is enacted, individuals like Garrett must be prosecuted, if at all, under the existing property offences and fraud offences in the Crimes Act 1961. In *Garrett,* the Crown alleged that the installation of the Trojan code constituted wilful damage to property, and the use of the information constituted fraud and forgery.[43] Determined to fit the statute to cover the facts, the Court held that the magnetic particles and software residing on the victim's computer qualified as property, the passwords qualified as documents, and the infestation of the Trojan code constituted damage. More rigorous consideration of the offences' elements in view of the technical reality would likely lead to a different result. Divorced from this reality, the judgment can potentially capture a variety of non-criminal conduct. It is this possibility that has driven enactment of special legislation in overseas jurisdictions.

6 Cross-border problems

Much of the objectionable conduct perceived by local users originates offshore. This includes pornography, gambling, securities fraud, hate speech and software piracy. The cross-border feature greatly complicates law enforcement. As the conduct is often legal in the jurisdiction of origin, enforcement must proceed on a catch-as-catch-can basis. On a research trip in Europe, an Australian academic was arrested and imprisoned in Germany on account of Nazi-related but otherwise legal content on his Australian web page.[44] Shortly after delivering a paper to a security conference in Las Vegas, a Russian programmer was arrested by the FBI for decryption activities legal in Russia.[45] These enforcement measures, while they make for good press, do little to protect local users. Extradition is an answer only in the event that both jurisdictions have similar criminal statutes. However, the enactment of uniform legislation flounders on the differing national views on the conduct involved. Whereas English-speaking jurisdictions generally find pornography criminally objectionable, the European jurisdictions are more concerned about hate speech.

---

43 The defendant was charged under Crimes Act l961 ss 229A [taking and using documents with intent to defraud], 264 [forgery], 266A [altering or reproducing document with intent to defraud] and 298(4) [wilful destruction of property].

44 Clennell "Nazi Law: SA Doctor Charged" (10 April 1999) *Sydney Morning Herald*, Sydney.

45 See <http://www.usdoj.gov/usao/can/press/html/2001_08_28_skyarov.html>; and <http://www.freeskylarov.org>; Millar "Hackers plan to hit back as FBI detains Russian: Copyright crackdown provokes worldwide protests" (28 July 2001) *The Guardian* London.

D Civil Liberties

1 Singular challenge

The Internet is testing civil liberties in a manner unmatched by any event since the Second World War. The pressure is coming principally from the needs of law enforcement agencies dealing with computer crime, the tension between intellectual property and the freedom of expression, and the perceived flood of Internet hate speech and pornography.

2 Freedom of expression

The multi-levelled openness of the Internet makes it a public forum like no other. We can all connect to the Internet and, once connected, communicate with millions of users. Any attempt at regulating the Internet must, sooner rather than later, collide with the protections for free speech. The matter was first brought before the United States Supreme Court in *Reno,* a First Amendment challenge to the federal Internet porn statute.[46] The statute criminalised distribution of pornographic content unless the supplier provided a means of adult access. The Court, acknowledging the Internet as a unique medium for expression, held that the statute imposed an unreasonable burden on speech under the American local-standards definition of pornography.[47]

3 Filters

Filters are, of course, the code answer to objectionable content. A filter is an application which can block content by reference to specific words and/or packet addresses. Courts and commentators in the United States are divided on the application of the First Amendment to such technology. In the first, and most celebrated case, a Virginia federal court struck down a local library policy which required use of a filter to screen pornographic and indecent material.[48] The Court held that freedom of expression included the right to access information. In another Virginia case, the Court upheld use of a filter to implement a statute which forbade public employees from accessing pornographic materials from office computers.[49] The Court reasoned that, as the filter operated only in the workplace, it did not affect the employees' freedom to express

---

46 *Reno v American Civil Liberties Union* (1997) 521 US 844; for Communications Decency Act 1996, see 47 USCS s 609.

47 After the decision in *Reno*, above, Congress enacted the Child Online Protection Act 1998, Pub L No 105-277, 112 Stat 2681 (1998), in hopes that it would withstand a First Amendment challenge. However, before the effective date, enforcement was enjoined on First Amendment grounds. See *American Civil Liberties Union v Reno* (2000) 217 F 3d 162 (3rd Cir).

48 *Mainstream Loudon v Board of Trustees of Loudon County Library* (1998) 24 F Supp 2d 552 (ED Va).

49 *Urofsky v Gilmore* (2000) 216 F 3d 401 (4th Cir).

themselves in their capacity as private citizens. More recently, the federal district court in Pennsylvania struck down on First Amendment grounds a federal statute that requires public schools, as a condition of receiving federal funding, to install filters to screen out pornographic and indecent material.[50] Even the most accurate filters tend to be grossly over-inclusive. In my own workplace, the filter blocks a site—that is largely a collection of articles from national press concerning topics of interest to the punk community. It is presumably triggered by the occurrence of words such as 'sex', 'pornography', 'drugs' and so on.

4 The Australian statute

In the year 2001, contrary to the recommendations of an extensive review, Australia enacted an Internet porn measure linked to its scheme for movies.[51] In relation to local providers, the statute forbids the dissemination of any X-rated material and requires provision of an adult access arrangement for R-rated material. For content coming from overseas, the local access provider must make available to users a means to filter the material. The scheme would not withstand challenge under the United States constitution.[52] Its principal effect will be to drive the supply of pornographic material offshore. Most recently, the statute has also been criticised as secret law enforcement. The Australian Broadcasting Authority has refused to comply with an Official Information Act request for a list of local sites which have incurred an X-rating.[53]

Sovereignty issues as illustrated by the Yahoo litigation, the regulation of Internet content often involves sovereignty issues. Acting under France's hate speech statute, a French court enjoined Yahoo from serving the French audience any of its auction sites that carry Nazi memorabilia or relics.[54] When Yahoo refused to comply, the plaintiff threatened enforcement proceedings in the United States. Yahoo sought and obtained a

---

50 *American Library Association v United States* (2002) 2002 US District LEXIS 9537 (ED Pa); Children's Internet Protection Act 1999, Pub L No 106-554.

51 Broadcasting Services Amendment (Online Services) Act 1999 (Cth).

52 Meghan Wharton "Pornography and the International Internet: Internet Content Regulation in Australia and the United States" (2000) 31 Hastings Comm & Ent L J 121.

53 See <http://www.aba.gov.au/abanews/news-releases/2002/25ur02.htm> and <http://www.efa.org.au/Campaigns/99.html>.

54 *LICRA et UEJF v Yahoo! Inc and Yahoo France* (Superior Court of Paris), <http://www.gigalaw.com/library/france-yahoo-2000-11-20-lapres.html>; <http://www.canevet.com/jurisp/textes/000522.htm>.

declaratory judgment from a federal court that the French judgment was unenforceable in the United States on First Amendment grounds.[55]

5 Code as speech

Whilst regulation of Internet content raises constitutional questions, these are largely confined, on the one hand, to a narrow slice of information and, on the other, largely to Anglo-American jurisdictions. An issue with larger ramifications is whether code qualifies as protected speech. The issue was first raised in relation to the United States restrictions on the export of encryption software.[56] The regulation was challenged by an academic who wished to place on his web-site class materials that included a discussion of encryption software. In view of the international reach of the web-site, the academic sought a declaratory judgment concerning liability under the export regulations. The federal district court held that code qualified as speech and the regulation was unconstitutional.[57]

6 The DeCSS litigation

The same issue was raised in a quite different context by the DeCSS litigation. In order to view DVD's on his Linux operating system, a Norwegian teenager decrypted the digital rights scheme used to prevent DVD's being viewed on an unlicensed player application. The decryption code was reproduced on the web-site of the defendant, the publisher of *2600*, a publication devoted to hacking. An association representing several Hollywood studios sought injunctive and declaratory relief under the recently enacted Digital Millennium Copyright Act. That statute imposes civil and criminal liability for the supply and use of software designed to provide unauthorised access to digitally-protected copyright material.[58] The defendants argued that, as applied, the statute contravened the First Amendment. The case was argued on behalf of the defendants by civil rights luminaries including the American Civil Liberties Union, the Electronic Freedom Foundation, and the Dean of the Stanford Law School. Rejecting the constitutional challenge, the Court held that the statute affected speech as an instrument but not speech

---

55 *Yahoo! Inc v La Ligue Contre le Racisme et L'Antisemitisme* (2001) 169 F Supp 2d 1181; 2001 US Dist LEXIS 18378 (ND Cal).

56 Export Administration Regulations, 15 CFR Parts 730-74.

57 *Junger v Daley* (2000) 209 F 3d 481; 2000 US App. LEXIS 6161 (6th Cir).

58 Digital Millennium Copyright Act 1998, 17 USCS s 120l *et seq*, see the US Copyright Office summary at <http://www.loc.gov/copyright/lfor exampleislation/dmca.pdf>.

as expression.[59] Shortly afterwards, a California court came to the opposite conclusion in relation to the same software.[60]

7 Search and seizure

Freedom of expression is not the only civil liberty affected by the use of digital technology. Law enforcement activities have recently raised questions concerning the protections against unreasonable search and seizure. The recent *Scarfo* case involved a suspected loan shark who had used software to encrypt all of his communications. The FBI installed on the defendant's computer a keyboard logger which caught the encryption passwords as they were entered on the keyboard and transmitted them to the FBI. In addressing the defendant's objection to use of the evidence, the Court had to decide whether the application constituted a wire-tap or a general search, the two practices being subject to different criteria.[61] Privacy and search and seizure objections have also been raised against the government's use of Carnivore. This network sniffer application enables the FBI to intercept and collect communicatons which are the subject of an interception order.[62] Its use is facilitated by a 1994 statute requiring telephone companies to provide a port on their facilities through which the law enforcement authorities can monitor digital communications.[63] The provision of such a port is also mandatory under German statute.[64] It is reported that private organisations are employing spiders and spyware to access and search private computers for illegally copied material.[65]

8 Other issues

Due process (natural justice) objections have been raised against the take-down provisions of the DMCA. As the take-down order must be complied with prior to any court hearing, the provision raises the applicability of that line of cases dealing with pre-

---

59 *Universal City Studios Inc v Reimerdes* (2001) 111 F Supp 2d 294 (SD NY) affd sub nom *Universal City Studios Inc v Corley* (2002) 273 F 3d 429; 2001 US App LEXIS 25330 (2d Cir).

60 *DVD Copy Control Association v Andrew Bunner* (2001) 93 Cal App 4th 648 (Cal Ct App).

61 *United States v Nicodemo S Scarfo* (2001) 180 F Supp 2d 572; 2001 US Dist LEXIS 21561 (D NJ).

62 For a description of Carnivore, see <http://www.fbi.gov/hq/lab/carnivore/carnivore.htm>; see *Carnivore Eats Your Privacy* at <http://www.wired.com/news/politics/0,1283,37503,00.html>.

63 Communications Assistance for Law Enforcement Act 1994 (CALEA), PL 103-414, 47 USCS §§ 1001.

64 Gesetz ueber die Nutzung von Telediensten (BGBl I 1997, 1870) at < http://jurcom5.juris.de/bundesrecht/tdg/index.html>.

65 In the United States, Congress is considering legislation which would legitimise the practice. See <http://www.eff.org/IP/P2P/20020802_eff_berman_p2p_bill.html>.

judgment seizures.[66] In a novel twist, the use of filters in public libraries has been justified by the prohibition against sex discrimination, the filters being viewed as necessary to prevent harassment of female employees.[67] As noted above, the Crimes Amendment Bill (No 6) would catch publications dealing with computer security and encryption software. The controversies over pornography and code-as-speech impact at or very close to the application level of the Internet. Freedom of expression issues are also arising further down the protocol stack. First Amendment challenges have been successfully mounted against statutes which require open access to cable facilities and the scrambling of adult movies broadcast over cable.[68]

E Banking

Around 20% of the households in the United States currently use Internet banking, the figure being expected to rise to 33 % in 2005.[69] Most banks simply use the Internet—alongside branch banking, telephone banking and ATM banking—as another vehicle to deliver their services. There are a few but notable Internet-only banks, for example, WingspanBank, owned by BankOne, the fifth largest US bank. The expansion of Internet banking is driven by cost economies. It is reported that an Internet transaction costs around 1¢ (United States) as compared to around $1 for a branch transaction and 27¢ for an ATM transaction.[70] Internet banks pass these savings on to their customers. For instance, Internet cheque accounts often carry interest and provide direct payment schemes free of charge. The digital economy presents some interesting challenges for payment and lending services.

1 Payments

Payment mechanisms have always been one of the core services offered by banks. The obvious examples are cheques and, in European countries, giro accounts. These were joined in the late 50's by credit cards which rely heavily on telephone technology. In the

---

66 See Elizabeth Thornburg "Going Private: Technology, Due Process, and Internet Dispute Resolution" (2000) 34 UC Davis L Rev 151, 191.

67 For an account of the librarians' successful complaint before the Equal Employment Opportunities commission, see *American Libraries* (1 August 2001) No 7, Vol 32; 23 (available on <http://www.lexis.com>).

68 *Advanced Cable v Broward County* (2000) 124 F Supp 2d 685 (SD Fla) (cable access), *United States v Playboy Entertainment Group* (2000) 529 US 803; 2000 US LEXIS 3427 (scrambling of sexually oriented programming).

69 <http://www.onlinebankingreport.com/resources/sr7.html>.

70 Christian Watson "The Growth of Internet-only Banks: Brick and Mortar Branches are Feeling the Byte" (2000) 4 NC Banking Inst 345, 349.

mid-60's, the banks seized upon digital technology to expand their cash-dispensing role through the use of ATM's. In the mid-80's, the same technology served as the basis for direct debit systems including EFTPOS and more recently SmartCards. The available payment mechanisms vary considerably in relation to unauthorised use, reversability, credit, float, privacy, costs, security and, in most jurisdictions, the basis of regulation. None is wholly suitable for Internet transactions. The Internet seller is unwilling to wear the credit risk and clearing delay associated with taking a cheque from an unknown purchaser who often resides in a different jurisdiction. EFTPOS runs on local area networks that have yet to be integrated with the Internet. The credit card is the most popular Internet payment device particularly in the United States where the customer enjoys a right of charge-back against the bank in the event of a dispute with the merchant.[71] However, credit cards cannot be used in person-to-person (P2P) transactions and are not cost-effective in the increasingly common small-charge transactions on the internet. As regards privacy, an increasingly paramount concern, cash payment does not leave a digital trail like that associated with credit cards or EFTPOS. Concerns about the security of Internet payments have been largely addressed by robust encryption techniques.[72] Most payment frauds involve unauthorised access to account information held by merchants or banks.

2 Alternative payment mechanisms

The last five years has witnessed a furious search for better payment mechanisms for Internet transactions. Currently, there are a number of contenders. These include digital money, adaptation of SmartCard technology, electronic cheques, independent payment services, and secure credit card systems. Their developers seek to capture income streams similar to those enjoyed by the banks with their ATM's. Consider digital money. The customer purchases digital tokens and pays by means of a credit card or direct debit. The tokens are stored in a "wallet" file on the customer's desktop. The customer transfers these tokens out of the wallet to a merchant in payment of the Internet transaction. The merchant can store the tokens in its own wallet or cash them with the token supplier. The mechanism leaves no digital trail and works as between private persons. At present, the most popular of the alternatives are the payment services which have emerged to deal with private party transactions over auction sites. PayPal, the leading such service, has over 7,000,000 users and operates in 26 countries.[73] An Internet seller can register with

---

71 15 USCA s 1666i.

72 For recent developments in credit card security, see < http://www.epaynews.com/index.cgi?survey=&ref=browse&f=view&id=1030704757622215212&block=>.

73 See <http://www.paypal.com>.

PayPal and designate its services as a payment mechanism. The customer/purchaser requests PayPal to make the payment to the registered seller. The payment is funded either out of the purchaser's account with PayPal or their credit card. The service enables payment between private persons and also prevents sellers learning the details of a purchaser's bank account or credit card.

3 New collateral

In the lending area, the principal issue raised by digital technology concerns the use of information products as collateral. The creation and marketing of software has, in the last three decades, grown from virtually nothing to a multi-billion dollar business employing millions of skilled workers. The development, distribution and acquisition of this product must be financed either by lenders or equity investors. As the principal source of debt finance, banks will be concerned with the availability of effective collateral.

4 Example

Consider what is probably the most common software financing transaction. A small business seeks to borrow the funds needed to purchase a server application and back-office support. The suite is manufactured overseas, distributed by a local vendor under a non-exclusive end-user licence and delivered on one or more shrink-wrapped CD Roms. The non-digital counterpart to this transaction is the financed acquisition of equipment, for example the computing hardware used in the debtor's office. Under the Personal Property Security Act 1999 (PPSA), the security for hardware financing is easily documented and plays out in a predictable and commercially acceptable manner. The bank would take over the equipment a purchase money security interest that enjoys priority over any pre-existing security interest given by the manufacturer or any distributor.[74] When the financed purchase involves a software application, the operation of the PPSA is anything but certain.

5 Software as collateral

The threshold issue under the PPSA involves identification and classification of the collateral. Does the collateral comprise the CD Roms, the digital information on that medium, the end-user licence, the contract rights conferred by that licence or the limited copyright in the information contained on the CD Roms? The CD Roms clearly qualify as "equipment", under the definition in s 16(1), but they are of relatively little value. The real value resides in the digital information which probably does not even qualify as personal property under s 16(1), in which case the PPSA does not apply. Another value compromises the rights obtained under the licence which qualify as property in the nature

---

74 Personal Property Security Act 1999, s 73.

of an intangible. However, this possibility raises the anterior question whether the licence creates a security interest in favour of the local distributor or manufacturer. The more often one reads the definition in of security interest s 17 against the terms of the typical non-exclusive end-user licence, the less certain one is of the answer to this question. If the licence constitutes a security interest, then upstream parties are subject to the registration requirements and enforcement rules of the PPSA. Also, taking the licence as collateral is problematic from the lending bank's viewpoint. Under the usual covenants the user right, the principal value conferred by the licence, is subject to the licensor's power of termination, and covenants, the security transfer requires the licensor's approval. For a variety of reasons, that approval may not be forthcoming. The termination right complicates, if not precludes, enforcement of the security interest in the event of default. The real leverage under the licence lies in the termination right, control over which the bank could, theoretically, obtain by means of an authorisation or assignment from the licensor. Apart from the commercial impediments to such an arrangement, it is unclear whether such an arrangement would trigger the PPSA. Many of these problems have been clarified by the 1991 revision of UCC Article 9,[75] a development that was deliberately ignored by the New Zealand reformers. It is likely that the local adoption of the pre-revision model will result in more uncertainty than if the matter had been left for regulation under the pre-PPSA common law.[76]

6 Digitalised instruments

The final topic concerns digitalisation of instruments. Account balances were one of the first forms of wealth to be subject to digitalisation. This was likely a by-product of the digitalisation of double entry accounting. With the networking of computers, it was natural that inter-account adjustments evolve into a means of payment and wealth transfer. Digitalisation has largely bypassed the traditional means of payment effectuated through transfers of instruments. There is no direct digital counterpart to the dollar bill or promissory note. This is quite surprising in view of the plasticity of digital information and the Internet. The hiatus affects both the payment side and security side of commercial transactions. On the payment side, there is, as noted earlier, a growing need for a digital equivalent of anonymous cash, a need counterbalanced by the law enforcement concern with money laundering. On the security side, some of the most awkward rules in the PPSA are those related to security over instruments. In recognition of these concerns, lawmakers in the United States have provided a statutory framework for digital

---

75 Revised UCC Article 9 can be accessed at <http://www.law.upenn.edu/bll/ulc/ulc.htm>. For a discussion, see Steven O Weise "The financing of intellectual property under revised UCC article 9" (1999) 74 Chi -Kent L Rev 1077.

76 Robert Dugan "Personal Property Securities Act - Price of Certainty" [2000] NZLJ 241.

instruments. The 1991 revision of UCC Article 9 provides for the possibility of electronic chattel paper and the UETA provides more generally for digitalised instruments.[77]

F Company and Securities

The Internet and related technologies are also driving significant changes in company and securities practice. As the most obvious, electronic compliance can replace paperwork for a wide range of requirements including those for incorporation, shareholder communications, annual returns and reports, document retention, share issues, and secondary trading.[78] In New Zealand, full implementation of electronic compliance awaits enactment of the Electronics Transaction Bill. Whilst electronic compliance reduces the cost of using the corporate form, many of the requirements can, as demonstrated by the North American experience with limited liability companies, be abolished without a reduction in investor protection.[79]

1 Information costs lowered

The principal benefit of electronic compliance probably occurs at the investor level. Ordinary investors can now access, free of charge, basic and secondary investment information that, ten years ago, would have only be available to professionals in hard copy. Since 1993, filings under the United States securities statutes are available on a same-day basis over the Web on the EDGAR database.[80] Much of the same data now also appears on corporate web sites. This primary information facilitates secondary analysis, much of which is also distributed on-line through brokers and financial advisors. The increased availability of timely and high quality information both empowers investors and enhances the efficiency of the share markets.

2 On line share issues

Paper-based regulations continue to prevent the Internet from realising its full potential as a medium for new issues. In the United States, there appear to have been only two regular issues over the Internet under the Securities Act 1933. The most notable was that of Spring Street Brewing in March 1996. The issue was not underwritten, involved 900

---

77 See UCC 9-102(a)(31)("electronic chattel paper"), 9-105[control of electronic chattel paper], 9-203(b)(3)(D)(attachment of security interest in electronic chattel paper); 9-314(a)(perfection of security interest in electronic chattel paper); Uniform Electronic Transactions Act s 16 (transferable records).

78 See, for example, on-line incorporation at <http://www.companies.co.nz>.

79 Robert Dugan, Peter McKenzie and David Patterson *Closely Held Companies-Legal and Tax Issues* (CCH 2000) 700-701.

80 See <http://www.sec.gov/edgar/aboutedgar.htm>.

000 shares and raised $1.6m. Several no-action letters were necessary to excuse non-compliance with various registration and prospectus requirements that were not compatible with the on-line environment.[81] In contrast, no-action letters have made the Internet a popular medium for private placements under Regulation D.[82] This regulation frees from the registration requirements of the 1933 Act offers to accredited investors that are not accompanied by general solicitation or advertising. Many on-line brokers provide qualifying customers access to exempt offerings. The prospective investor first establishes compliance with financial criteria for accreditation and then receives password access to the offer documents.[83]

3 Secondary market

The secondary market is also increasingly going on-line. There are hundreds of on-line brokers. The number of on-line trading accounts is estimated to grow in the United States from 3m in 1997 to 14.4m by the end of 2002.[84] This reflects the fact that fees for on-line services are significantly cheaper than for comparable off-line services.[85] The ancillary services provided by on-line brokers are generally no less and, in many cases, greater and more convenient than those available from the traditional off-line broker. Activity in the secondary market is undoubtedly stimulated by the economies associated with Internet communication and advertising. Information can be delivered via chat room, newsgroup or web site to an indefinitely large audience for a cost of pennies per prospective investor.

4 Abuse facilitated

The same features of the new technology that expedite compliance and transacting also facilitate abuse. In 2000, the SEC received and responded to 81,500 complaints, an increase of ten per cent over 1999.[86] The cases involve virtually every type of investment scam, including phony offerings, market manipulations, affinity frauds and pyramid schemes. The so-called *pump and dump* is probably the most serious abuse. A person holding or

---

81 Daniel M Weisenfeld "IPOs on the Internet: The Need for the Next Step" (2000) 22 Hastings Comm & Ent LJ 529.

82 Regulation D is found at 17 CFR 230.501 et seq (http://www.sec.gov/divisions/corpfin/forms/regd.htm).

83 See for example <http://www.harrisdirect.com/pre/ps_ipos.htm>.

84 "The ABCs of online investing--An introduction to investing in mutual funds through an electronic broker" at http://www.globefund.com/centre/onlineinvesting/online_home.html. The New York Stock Exchange estimates that at the end of the l990's half of the retail investor trades occurred on line; see http://www.nyse.com/marketinfo/summary.html.

85 <http://www.wizetrader.com/product/stats.html>.

86 <http://www.sec.gov/news/data.htm>.

controlling a block of shares pumps up the share price by releasing information about the company over the Internet. The person then dumps their shares at the inflated price. Most cases involve so-called *penny* or *microcap* stock, ie low-priced stock issued by companies whose capitalisation or membership falls below the thresholds set for SEC registration.[87] While there is little or no creditable public information about such companies, false information can be easily circulated on the Internet through spam, electronic newsletters and message boards.[88] Interesting to note is that one of the key elements of the pump and dump scheme — raising share price through public pronouncements — is not regulated by anything in New Zealand securities legislation.[89]

5 Insider trading

The new technology also intersects with the law of insider trading at several points.[90] The release of information on Internet sites bears upon whether and when information qualifies as public. Confidential data on computers provides another source of inside information. Under the Securities Amendment Act 1988, the employee who hacks this information would qualify as an insider but the outside hacker would not. The presence of firm-wide networks in securities firms and banks raises new issues for the implementation of Chinese walls. Finally, enforcement of insider trading law and, for that matter, securities law in general is significantly frustrated by the increasing use of on-line banking and trading accounts. The different elements of a transaction can be implemented in three or four different jurisdictions, each having its own rules respecting privacy, banking and securities transactions.

---

87 15 USC s 77l(g)(1) [$1m in assets and at least 750 shareholders]; Richard H Walker and David M Levine "'You've Got Jail': Current Trends in Civil and Criminal Enforcement of Internet Securities Fraud" (2001) 38 Am Crim L Rev 405. For two litigation releases involving pump and dump schemes, see *Broadband Stock Lit Rel No 16651* (2000) 2000 SEC LEXIS 1669 and *Fred Moldofsky Lit Rel No 16493* (2000) 2000 SEC LEXIS 593>. The SEC has an ongoing enforcement programme aimed at internet securities fraud, see <http://www.sec.gov/news/headlines/internet5.htm>.

88 <http://www.otcbb.com> (since 2000 companies listed on the otcbb must be registered under the Securities Act l934 and comply with the reporting obligations under that statute).

89 There is no equivalent to 15 USC s 78j(b) implemented through rule 10b-5 [17 CFR 240.10b-5] the general anti-fraud provision of the federal United States securities legislation. Rule 10b-5 can be found at <http://www.law.uc.edu/CCL/34ActRls/rule10b-5.html>.

90 Nineteen Charged with using Chat Rooms in Insider Trading Scheme Yielding $ 8.4 Million, "<http://www.uslaw.com/library/article/usl314instrad.html?area_id=9>"<http://www.uslaw.com/library/article/usl314instrad.html?area_id=9>; Robert Prentice "The Internet and Its Challenge for the Future of Insider Trading Regulation" (1999) 12 Harv J Law & Tech 263.

6 Disintermediation and gatekeepers

Contemporary securities regulation relies heavily on intermediaries. Brokers, dealers, exchanges and underwriters are subject to liability rules which force them to serve as gatekeepers.[91] However, direct trading and continuous issues over the Internet will reduce the need for these intermediaries. To maintain the current level of protection, the slack must be taken up by other existing intermediaries such as lawyers or accountants or by new intermediaries such as on-line chat rooms and investment sites.[92]

G Taxation

The rapidly increasing volume of electronic commerce has pushed two tax issues high up the agenda for regulatory reform. The one concerns the characterisation of digital products for tax purposes. The other relates to the cross-border feature of electronic commerce transactions.

1 Characterisation of digital products

Electronic commerce increasingly comprises traffic in digital commodities, particularly entertainment products, software and advice. Consider for example the commercial application distributed under a shrink-wrap or click-wrap contract. The issue arises whether the transaction should be treated as a sale of goods, a sale of services or as a licence arrangement. The characterisations attract different treatment for both GST and income tax. Traditionally, the characterisation has turned on the concept of tangibility. However, this makes little sense in the digital world where it is largely a matter of accident whether the product is delivered on a CD Rom or over the Internet. The United States Treasury has promulgated a regulation that distinguishes between the sale of the copyright and the sale of a copy, without regard to whether the transaction involves a tangible medium.[93] The sale of a single copy under a ten-copy licence would be treated like a sale of ten copies. The rule drives a wedge between the tax treatment and copyright treatment of the transaction and poses the risk of double taxation or non-taxation unless all jurisdictions adopt similar rules. The characterisation of the transaction also controls the operation of GST. If the imported software qualifies as a service, the transaction is not

---

91 See, for example, Securities Act l978 s 57(2)(c); Australian Corporations Act 2001 ss 729, 731 (due diligence defence available to experts).

92 Andrew R Thompson "Taming the Frontier?: Evaluation of the SEC's Regulation of Internet Securities Trading Systems" (1999) Colum Bus L Rev 165.

93 See Treas Reg 1.861-18 (1999) (1996). See also IRD draft ruling IG 0007 — Non-resident Software Suppliers" payments derived from New Zealand—income tax treatment (1997).

subject to GST. If it qualifies as goods, GST is payable and collected by the Customs Department.[94]

2 Trans-border transactions

A large percentage of e-commerce sales involve trans-border transactions. Both GST and income taxation have well established rules for dealing with trans-border transactions. For instance, income taxation relies on special deductions and credits, transfer pricing rules, the controlled company regime and tax treaties. However, the Internet undermines the efficacy of many of these institutions. Consider the impact of the Internet on the operation of tax treaties which usually turns on the concept of permanent establishment. Where an American company sells an item to a New Zealand purchaser, the profits will be taxed here or there according to whether the company has a permanent establishment here.[95] However, the concept of permanent establishment reflects the pre-Internet trade in tangible goods which involved physical presence in the form of factories, warehouses, sales and marketing agencies. In the on-line environment, many of these functions can be performed without a physical presence. Marketing, contracting and consumer support can be provided on-line and warehouses are not necessary where the product can be delivered in digital form. The American company can reduce if not eliminate its physical presence in favour of a web site. The site server, which substitutes for the warehouse and marketing agency, can be located as easily in the Cayman Islands as in either New Zealand or the United States. Its location no longer serves as a proxy for the source of income.

3 Residence-based taxation

The obvious solution is to use a residence-based regime for Internet transactions.[96] However, this is inconsistent with the neutrality principle. Also, in the on-line environment, residence is as ephemeral as source. Where is the residence of a retail distribution business that is incorporated in the Cayman Islands, has its principal server in Mexico City with mirrors in Frankfurt and Sydney, uses a help-desk in India and server support in California, and takes its products from on-line suppliers in various Southeast Asian countries? Reliance on residency encourages migration to tax havens, thus placing an increased regulatory burden on the regime for controlled companies. Residence-based taxation also benefits digital exporting countries such as the United States.

---

94 See *Case T28* (1997) 18 NZTC 8,197 (TC) (whether know-how package including software qualifies as goods or services for purpose of GST).

95 See Double Taxation Relief (United States) Order 1983 (1983/196) arts 5 and 7.

96 John Sweet "Formulating International Tax Laws in the Age of Electronic Commerce " (1998) 146 U Pa L Rev 1949.

4 Increased reliance on GST

Another alternative is increased reliance on GST. The source-based feature of income tax plays only a subsidiary role in the GST regime which is consumption-based. However, in relation to cross-border traffic in digital products, the taxing potential of GST in New Zealand is undermined so long as the characterisation of such products as imported services pushes them outside the GST net. This could, of course, be altered either by recharacterising the products or the place of supply. However, there still would remain the problem of tax collection. In the prototype domestic transaction, the tax is levied on and collected from the seller even though it is paid by the purchaser. In the case of imported goods, the tax is levied on and collected from the purchaser by the Customs Department. However, in the absence of treaty arrangements, neither alternative can be easily extended to the internet import transaction, particularly where the purchaser is a consumer. A recent modification of the EU Rules defines place of supply in cross-border Internet transactions as the customer's location.[97] Non-EU suppliers must register as VAT taxpayers in the jurisdiction where their EC customers are located. This proposal has a number of ramifications. First, it must be integrated with the income tax provision for payment of foreign taxes. There is also the problem of identifying and verifying the place of consumption. A sale of tangibles will require the purchaser to supply a mailing address. In the case of business-to-business (B2B) transactions, the purchaser of digital products has an incentive to provide verification in order to claim the input credit. However, the same incentive does not exist in relation to business to consumer (B2C) transactions. Identity can be further concealed by use of encryption software and/or anonymous payment devices. The approach also requires Internet vendors to keep track of the tax rules in the multiple jurisdictions into which they sell over the Internet. Whilst the EU regime will likely employ thresholds to protect small entities, this conflicts with the neutrality principle and gives them a competitive advantage.[98] One thing is certain. The need to tax Internet transactions will further complicate an already exceedingly complex area of the law. This calls for serious consideration of digitally-related and digitally-enforceable forms of taxation such as the bit tax.[99]

---

97 See EU press release 5/02 dated 13 Feb 2002 at <http://www.eurunion.org/news/press/2002/2002005.htm>.

98 Reimar Pinkernell "Application of the EU Value Added Tax to E-commerce Transactions" <http://www.pinkernell.de/euvat.htm>.

99 Clayton Chan "Taxation of Global E-Commerce on the Internet: The Underlying Issues and Proposed Plans" (2000) 9 Minn J Global Trade 233.

H Competition

1 Black hole

Digital technology presents competition law with a black hole. Markets involving digital technology have characteristics not anticipated by the neo-liberal economics which underlie current regulation. On the supply side, we encounter extreme economies of scale, which reflect the large investment required for development, coupled with the virtually zero marginal cost of production. On the demand-side, there are network effects that obtain when the utility of a product increases with the number of persons consuming the same product or a related product.[100] The utility of an operating system or office suite increases with the number of users of that product or an inter-operable product. Such markets are characterised by tipping and path dependency. Once a firm reaches a certain market share, the effects quickly push its share towards 100%. Once a market has tipped, switching costs can lock an entire industry into use of an inferior technology. The speed of innovation significantly increases the distortionary risks associated with the time lag for enforcement proceedings, particularly those involving litigation. Economists and courts are just beginning to explore how, if at all, these peculiarities should bear upon the design and enforcement of competition law. The issue has sharply divided the Chicago School which is the ideological source for much of New Zealand's competition regime. At one extreme, there is Judge Easterbrook who argues that the presence of rapid innovation will, without any change to the law, ensure achievement of allocative efficiency even in the medium term. At the other extreme are those like Elhauge who argue for structural and doctrinal changes.[101]

2 The Microsoft case

Many of these issues are involved in the Microsoft litigation. The government and 19 states sued Microsoft for illegal monopolisation, tying and exclusive dealing. The case revolves around Microsoft's response to Sun's Java middleware that enables developers to write one version of an application for multiple operating systems. Sun's distribution problem was to get its environment application onto the Windows platform, then and now the most common operating system. Sun contracted with Netscape to include a run time environment with its Internet client, which at the time commanded around 85% of the browser market. Fearing that the Java/Netscape combination would develop into a

---

100 Mark Lemley and David McGowan "Legal Implications of Network Economic Effects" (1998) 86 Calif L Rev 479.

101 Compare Frank H Easterbrook "Information and antitrust" (2000) U Chi Legal For 1 with Einer Elhauge "Tunney Act comments on proposed settlement between JUS and Microsoft" http://www.usdog.gov/cases/ms_tuncom/major/mtc-00027209.htm.

competing platform, Microsoft took a number of actions which eventually led to litigation. By delaying release of technical information, it prevented Netscape from having a compatible version of Navigator available for Windows95. At the same time, Microsoft devoted substantial resources to the development of its own Internet browser which was first released in mid-1995. It then gave that application away by bundling it with Windows and providing free copies to software developers and ISP's. Microsoft also entered into contracts with OEMs and ISP's requiring them to distribute or promote Explorer exclusively. From 1996 to 1998 Explorer's market share rose from 5% to 45% accompanied by a corresponding fall in Netscape's share. The trial Court held in favour of the plaintiffs on the monopolisation and tying counts.[102] It ordered Microsoft to divest either its operating systems or its applications business. On appeal, the Court upheld the monopolisation finding but overturned the tie-in decision, finding that the Explorer and operating system were not distinct products.[103] The Court also ordered a hearing on the appropriate remedy. After extended negotiations, the government and a number of the states agreed upon a remedy which was put to the Court. The proposed remedy is strongly opposed by most of the states as well as market participants including AOL and Sun.[104] Sun recently filed a $1 billion claim against Microsoft for similar anti-competitive conduct in the development and marketing of its XP operating system.[105]

3 Light-handed approach

These peculiar economic effects have special significance for light-handed competition regimes such as that in New Zealand. Leveraged monopoly and lock-in occurs very quickly. It was alleged that Microsoft would, over the course of a year, be able to lock up or at least to tip the additional markets to insulate its monopoly in the operating system. Its .NET initiative is widely viewed as an attempt to extend the Windows monopoly to Internet servers and other applications particularly those involving entertainment products.[106] Once a market has tipped it is difficult, and perhaps even undesirable, to undo any anti-competitive effects. Because of the network effects, the market is one that is prone to standardisation. In such circumstances, it is not clear that the optimal number of

---

102 *United States v Microsoft Corp*(2000) 87 F Supp 2d 30 (D DC), 97 F Supp 2d 59 (D DC).

103 *United States v Microsoft Corp* (2001) 253 F 3d 34 (DC Cir).

104 See submissions concerning proposed remedy at <http://www.usdoj.gov/atr/cases/ms_index.htm> (last accessed 01 April 2002).

105 *Sun Microsystems Inc v Microsoft Corp*, (ND Cal No C02-01150PVT, complaint filed 3/8/02); see report in BNA "Electronic Commerce and Law" (13 March 2002) at <http://subscript.bna.com/SAMPLES/>.

106 See Associated Press "Sun Exec Critcizes Microsoft.Net" (9 April 2002) at <http://stacks.msnbc.com/news/736248.asp?cp1=1>.

operating systems would be greater than one. Indeed, given the strong network effects, there is some question whether there is anything that the law can do to open the market to long-term competition.

4 Troublesome interfaces

In the information market, competition law interfaces the law of intellectual property on the one hand and the freedom of expression on the other. The latter interface is revealed by decisions like that discussed earlier in which the federal district court held unconstitutional on First Amendment grounds a state statute which required open access to cable modems.[107] The tension between competition law and the law of intellectual property most clearly emerges in connection with standards and protocols. On one view, the Internet comprises nothing more than a multi-layered set of standards for communication between computers. Until relatively recently, most of these standards have been open ones which are accessible and usable by any person without application or other formality. Over the last two years, there has been mounting pressure from certain industry groups to make network standards the subject matter of intellectual property rights. Other groups have argued, just as strenuously, that the essential facilities doctrine or compulsory licensing should be applied to ensure open access to protocols and application interfaces.[108]

5 Wider impact

As revealed by the recent OECD studies of broad-band access, the competition law issues have a wider social impact. New Zealand ranks near the bottom, a fact attributed in large part to its regulatory framework. Availability of affordable broad-band access is, according to the studies, a key driver for economic growth.[109]

III CONCLUSION

A Internet as a Big Event

For the legal community, the Internet is a big event. Nothing on this scale has occurred since advent of the law-and-economics phenomenon in the l960's. Like law-and-economics, the Internet is transforming every area of the law. Yet, the transformations are

---

107 *Advanced Cable v Broward County* (2000) 124 F Supp 2d 685 (SD Fla).

108 See W3C Patent Policy Framework (Working Draft 16 August 2001) at < http://www.w3.org/TR/2001/WD-patent-policy-20010816/>; J M Muiller "Patent Misuse through Capture of Industry Standards" (2002) 17 Berkeley Tech L J 623.

109 Working party on telecommunication and information services policies "The development of broadband access in OECD countries" (OECD doc JT00115500, 20 October 2001) (New Zealand ranked 20th, following Spain and Portugal) which can be accessed at www.oecd.org.

fundamentally different. Law and economics resulted in a top-down transformation. The neo-liberal ideology altered the law, which in turn lead to a change in our lives. The Internet transformation is a bottom-up one. The Internet and related technologies are, from one day to the next, changing our lives. The issue for the legal community is whether the changed reality warrants reform of the law. Internet-and-law discussions are often chaired by lawyer/engineers rather than lawyer/economists.

B Why change?

The reform or not issue is easily answered as a matter of principle. The Internet and related technologies make possible new forms of conduct, for example importing goods and services outside scrutiny of Customs, autonomous contracting, selling and publishing from websites with international reach, paperless public issues of company shares, and so on. Some of these are cost effective, others are not. Under existing law, some are allowed generally, others allowed for certain purposes and some are prohibited. For instance, a data message can be used for personal correspondence but not as the vehicle for a bill of exchange or effective notice to shareholders. Law reform should allow new forms of socially beneficial conduct that are made possible by the Internet but that are prescribed by existing law. On the other hand, the Internet and related technologies make possible a wide range of new conduct whose social benefit is less obvious. Examples include concealment by cryptography, aggregation and dissemination of personal data, surreptitious invasion and surveillance. The law should change to prohibit those new forms of socially nonbeneficially conduct that are allowed or at least not prohibited by existing law.

C Difficult agenda

Whilst easily formulated as a matter of principle, the law reform agenda is difficult to implement. At the threshold are cost/benefit questions. Given law enforcement issues, is it cost effective to allow individuals to encrypt emails or banks to issue digital cash? Given the potential for foreclosure of public information, is it cost effective to allow copyright holders the use of digital envelopes? Such questions raise all the indeterminacies that lead to the demise of welfare economics as a discipline. But even where the cost/benefit calculus leads to an obvious or mandated answer, effective law reform is subject to serious resource, technological and political constraints.

D Resource constraints

The opportunities for reform in New Zealand are, at the threshold, limited by lack of resources. This country's per capita GDP is less than half that of the United States, about the same as that of Greece and Portugal and closer to that of Hungary and the Czech

Republic than to that of Norway and Denmark.[110] This constrains our capability for law reform no less than for infrastructure development. Even jurisdictions at the top of the resource stack have been unable to legislate for some of the many law reform issues raised by the internet and related technology. Lesser resourced countries must be even more selective. Not surprisingly, this country identified electronic transactions and computer crime as the initial targets for reform with intellectual property waiting in the wings. But the drafting and delays encountered with those two proposals suggest that this country cannot even resource law reform in a single area, no more than it can resource modern land transport between Auckland and Wellington. It is likely that by the time of enactment, the Electronic Transaction Bill and Crimes Amendment Bill will, like the PPSA, have been overtaken by events.

E Technological and political constraints

Effective law reform is also constrained in New Zealand, as elsewhere, by the ubiquity and plasticity of the Internet. As illustrated by the attempt to regulate pornography, national legislation alone cannot, due to reach of the Internet, significantly curtail the abuse. As illustrated by the controversy over distributed file sharing, the Internet easily morphs around changes in the law. On a political level, local reform is constrained by the increasing use of treaties and conventions to deal with the ubiquity of the Internet. The most recent include the WIPO, TRIPS, and the Budapest Crime Convention. These limit New Zealand's legislative autonomy either because the country is a party, as in the case of TRIPS, or because of political and commercial pressure as in the case of WIPO and the Crime Convention.

F Hands off

Given the constraints on law reform in New Zealand, the obvious and easiest legislative option is continued inaction. Indeed, in view of the severe resource constraint, there may be no realistic alternative. However, legislative inaction will not result in regulatory stasis. Other non-legislative regulatory structures, including legal ones, will emerge for the new reality. The common law will continue to evolve as it has in the past to accommodate technological change. A prime example are the recent developments in tort law in the United States. As illustrated by the *Garrett* decision, it is also happening in this country. Even in the absence of electronic transactions legislation, courts would, sooner or later, approve electronic compliance with writing requirements. The institution of contact will also serve as the vehicle for other regulatory structures. For instance, ISPs can contract with customers to filter out objectionable content. In New Zealand markets, ones often dominated by one or a few suppliers, standard terms will emerge as private legislation. In

---

110 CIA Factbook 2001 <http://www.cia.gov/cia/publications/factbook/>.

both the mass business-to-consumer and more individualised business-to-business contracts used in electronic commerce, the inevitable choice of law clauses will subject New Zealand parties to overseas law. Another important source of regulation will be code itself. The obvious example is copyright protection. Today, in cyber-related reality, a given regulatory result can, as discussed by Lessig, be achieved either by code or by law.[111] Filters are the code solution to objectionable content, encryption the solution to security problems. As illustrated by digital rights management and the new on-line credit card protocols,[112] code solutions easily combine with contract regimes to provide highly effective regulatory structures.

G Sovereignty and the Commons

Reliance on these alternative regulatory structures have a couple of noteworthy implications. At the local level, they portend a governance shift. All three mechanisms operate outside of the democratic process associated with legislative regulation. At the international level, there will be loss of sovereignty. Contracts will be dictated by overseas suppliers. The regimes imported through their choice of law clauses will emanate from overseas lawmakers and courts. Code tends to be manufactured in Richmond and Palo Alto. Recent treaties have been driven by United States interests intent on using them to bootstrap legislation at home and overseas. There is, however, a possible offsetting benefit. The hands-off approach will leave the Internet a legislation-free zone in New Zealand. This may confer on local users and developers an intellectual and commercial advantage over their overseas counterparts particularly those in jurisdictions where legislation is fast closing the Internet commons.

---

111 Lawrence Lessig *Code and Other Laws of Cyberspace* (Basic Books, New York, 1999) l22-123.

112 For recent developments in credit card security, see <http://www.epaynews.com/index.cgi?survey=&ref=browse&f=view&id=10307047576222152l2&block= >. On digital rights management, see Benedict Dugan and Robert Dugan "Reform of Copyright Law" [2002] NZLJ 120.