The Impact of Internet Intermediary Liability

19,503 Words

Author: Craig S Wright

University registration number: 05028244

Objectives

To consider look at the effects of legal liability as it pertains to Internet Intermediaries. Such examples would include defamation and copyright violations on ISP's where a subscriber has breached their legal obligations as well as the hosting of illicit materials (such as child porn).

In carrying out my project my aim is to:

1. Analyse English law as it relates to Internet Intermediary liability
2. Review the current cases
3. Consider the opinions of practitioners, academics, the Law Commission and the press/public
4. Analyse reforms/proposals for reform in other jurisdictions and the changes to the EU and the consequential effects that this will have on Internet Intermediaries.
5. Suggest how, if reform is needed, this should be effected
6. Detail the Impact of Internet Intermediary Liability across different groups and the economy

i Table of Contents

ii List of Cases

- 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council, Official Journal L 215 , 25/08/2000 P. 0007 - 0047
- *A & M Records, Inc. v Napster,* Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000).
- *A&M Records Inc v Napster*, Inc 239 F 3d 1004 (9th Cir 2001)
- *Anns v. Merton London Borough Council*, [1978] A.C. 728
- *Armagas Limited v Mundogas S.A.* [1986] 1 AC 717
- *Attorney General v Observer Ltd. and Others* [1990] 1 AC 109,
- *Australasian Performing Right Association v Jain* (1990) 18 IPR 663
- *Broom v Morgan* [1953] 1 QB 597.
- *Bugge v Brown* (1919) 26 CLR 110
- *Byrne v Deane* [1937] 2 All ER 204.
- *Campbell v MGN Ltd* [2004] A.C.457
- *Caparo Industries Plc. v. Dickman*, [1990] 2 A.C. 605
- *Carpenter v United States*, 484 U.S. 19(1987)
- Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* (Opinion of Advocate General Kokott), July 18, 2007.
- Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU (Opinion of Advocate General Kokott), July 18, 2007.
- *Century Insurance Co Limited v Northern Ireland Road Transport Board* [1942] 1 All ER 491;
- *Coco v AN Clark (Engineers) Ltd*. [1969] RPC 41
- *Cons. P. v. Monsieur G.,* TGI Paris, Gaz. Pal. 2000, no. 21
- *Cubby v CompuServe*, 776 F.Supp.135 (S.D.N.Y. 1991)
- *Deatons Pty Ltd v Flew* (1949) 79 CLR 370

- *DiMeo v Max* , WL 2717865 (3rd Cir. Sept. 19, 2007)
- *Doe v. GTE Corp*. 347 F.3d 655 (7th Cir. 2003)
- *Douglas v Hello! Ltd* [2001] QB 967, per Keene LJ.
- *Faccenda Chicken Ltd v Fowler* [1987] Ch. 117
- *Fair Housing Council of San Fernando Valley v. Roommates.com*, LLC , CV-03-09386-PA (9th Cir. May 15, 2007)
- *Fonovisa, Inc. v Cherry Auction, Inc*., 76 F.3d 259, 264 (9th Cir. 1996).
- *Gentry v eBay, Inc*., 121 Cal. Rptr. 2d 703 (Ct. App. 2002)
- *Gibbons v Brown* (1998) 1998 716 So. 2d 868
- *Godfrey v Demon Internet Ltd*, QBD, [1999] 4 All ER 342, [2000] 3 WLR 1020; [2001] QB 201
- *Goldman v The Queen* (1979), 108 D.L.R. (3d) 17 (S.C.C.)
- *Hern v Nichols* (1701) 1 Salk 289
- *Hospital Products Ltd v United States Surgical Corp* (1984) 156 CLR 41 at 96
- *Kenneth Zeran v America On-line Incorporated* 4th Circuit (No. 97-1523 1997)
- *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470 (1974)
- *Lloyd v Grace, Smith & Co*. [1912] AC 716
- *Malone v Metropolitan Police Commissioner* [1979] 2 WLR 700
- *Mark Williams and another vs. AMERICA ONLINE*, Inc. 2001 WL 135825 (Mass. Super., February 8, 2001)
- *Mercedes Benz (NSW) v ANZ and National Mutual Royal Savings Bank Ltd*, No. 50549 of 1990 (Unreported)
- *Meridian Global Funds Management Asia Limited v Securities Commission*, [1995] 2 AC 500

- *Metro-Goldwyn-Mayer Studios Inc v Grokster Ltd* No.s CV-01-08541-SVW, CV-01-09923-SVW (CD Cal, 25 April 2003)
- Metro-Goldwyn-Mayer Studios, Inc. v Grokster, Ltd., 380 F.3d 1154 (9th Cir.)
- *Microsoft Corporation v Marks* (1995) 33 IPR 15.
- *Modbury Triangle Shopping Centre Pty Ltd v Anzil* [2000] HCA 61.
- *Moorhouse v University of New South Wales* [1976] R.P.C. 151
- *Mousell Bros Limited v London and North-Western Railway Company* [1917] 2 KB 836,
- Murray v Yorkshire Fund Managers Ltd [1968] 1 WLR 951
- *Oxford v Moss*, (1978) 68 Cr. App. R. 183
- *Panorama Developments (Guildford) Limited v Fidelis Furnishing Fabrics Limited* [1971] 2 QB 711
- *Pearks, Gunston & Tee Limited v Ward* [1902] 2 KB 1
- *Perathoner v Pomier*, TGI Paris, May 23, 2001
- *Playboy Enterprises Inc v Calvin Designer Label* (1997) 44 USPQ 2d (BNA) 1156 (ND Cal).
- *Playboy Enters., Inc. v Frena*, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993)
- *R v Crozier* [1991] Crim LR 138, CA
- *R v ROSEMARY PAULINE WEST* 1996 LTL C0004000
- *R v Smith and R v Jayson* 2002 EWCA Crim 683 (No. 2001/00251/YI)
- *R v Stevens* [1999] NSWCCA 69 (15 April 1999).
- *RCA Corp. v John Fairfax & Sons Ltd* [1982] R.P.C. 91
- *RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC., (RIAA) v Verizon Internet Services*, 351 F.3d 1229 (DC Cir. 2003)
- *Religious Tech. Ctr. v Netcom*, Inc., 907 F. Supp. 1361, 1372 (N.D. Cal. 1995)

- *Reno v American Civil Liberties Union* 521 U.S. 844 (1997).
- *Rindos v Hardwicke* No. 940164, March 25, 1994 (Supreme Ct. of West Australia) (Unreported);
- *Roadtech Computer Systems Ltd v Mandata (Management and Data Services) Ltd* (25 May 2000) unreported, High Court, Chancery Division HC 1999 04573 per Master Bowman.
- *Smith v Leurs* (1945) 70 CLR 256; (1945) 51 ALR 392; (1945) 19 ALJR 230
- *Soc'y of Composers, Authors and Music Publishers of Can. v. Canadian Assoc. of Internet Providers*, [2004] S.C.C. 45, 240 D.L.R. (4th) 193, 92.
- *Stevenson Jordan Harrison v McDonnell Evans* [1952] 1 TLR 101 (CA)
- *Stratton Oakmont, Inc. v. Prodigy Services*, 23 Media L. Rep. (BNA) 1794 (N.Y. Sup. Ct. 1995), 1995 WL 323710
- *Sutherland Shire Council v Heyman* (1985) 157 CLR 424.
- *System Corp. v Peak Computer Co.*, F.2d 511 (9th Cir. 1993)
- *Telstra Corporation Limited v Australasian Performing Rights Association Limited* (1997) 38 IPR 294.
- *Tesco Supermarkets Limited v Nattrass* [1972] AC 153
- *Thompson v Australian Capital Television*, (1996) 71 ALJR 131
- *Tiger Nominees Pty Limited v State Pollution Control Commission* (1992) 25 NSWLR 715.
- *Trintec Indus. v Pedre Promotional Products*, 04-1293 (Fed. Cir. Jan. 19, 2005)
- *United State v Riggs and Neidorf*, 741 F.Supp.556 (N.D II 1990)
- *United States v Cherif*, 943 F.2d.692 (7th Circuit 1991)
- *United States v Girard*, (2nd Circuit 1979)
- *United States v Morrison*, 859 F.2d.151 (4th Circuit 1988))

- *Universal Communication Systems, Inc. v Lycos, Inc.* , 2007 WL 549111 (1st Cir. Feb. 23, 2007)
- *University of New South Wales v Moorhouse* (1975) 133 CLR 1
- *W v Edgell* [1990] Ch. 389
- *Warne and Others v Genex Corporation Pty Ltd and Others* [NSW, Australia] BC9603040 4 July 1996 (unreported decision).
- *WEA International Inc v Hanimex Corp Limited* (1987) 10 IPR 349 at 362
- *Western Provident v. Norwich Union* (The Times Law Report, 1997).

iii List of Statutes and Delegated Legislation

United Kingdom

- *Anti-Terrorism, Crime & Security Act* 2001 (UK).
- *Communications Decency Act* 1996 (UK).
- *Computer Misuse Act* 1990 (UK).
- *Consumer Credit Act* 1974, UK
- *Consumer Protection Act* 1987 (Product Liability) (Modification) (UK)
- *Criminal Justice (Terrorism and Conspiracy) Act* 1998 (UK).
- *Criminal Justice Act* 1988 (UK).
- *Criminal Justice and Public Order Act* 1994 (UK).
- *Data Protection Act* 1998 (UK).
- *Electronic Commerce (EC Directive) Regulations* 2002 (UK).
- *Electronic Communications Act* 2000 (UK); Statutory Instrument 2000 No. 1798 (C. 46) ELECTRONIC COMMUNICATIONS Electronic Communications Act 2000 (Commencement No. 1) Order 2000;
- *Electronic Signatures Regulations 2002* (UK) (Statutory Instrument 2002 No. 318)
- Enterprise Act 2002 (UK)
- *Human Rights Act* 1998 (UK)
- *Indecent Displays (Control) Act* 1981 (UK).
- *Interception of Communications (Lawful Business Practice) Regulations* 2000 (UK).
- *Obscene Publications Act* 1959 (UK).
- *Obscene Publications Act* 1964 (UK).

- *Privacy & Electronic Communications (EC Directive) Regulations* 2003 (UK).
- *Protection of Children Act* 1978 (UK).
- *Public Order Act* 1986 (UK).
- *Regulation of Investigatory Powers Act* 2000 (UK).
- *Sale of Goods Act* 1979, UK
- *Sale of Goods (United Nations Convention) Act* 1994 (UK)
- *Sexual Offences (Conspiracy and Incitement) Act* 1996 (UK).
- *Sex Offenders Act* 1997 (UK)
- *Sexual Offences Act* 1956 (UK).
- *Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations* 2000 (UK).
- *Telecommunications Act* 1984 (UK).

Australia

- *Broadcasting Services Act* 1992 (Cth, Australia)
- *Copyright Act* 1968 (Cth, Australia)
- *Copyright Amendment Act* 1984 (Cth, Australia)
- *Copyright Amendment (Digital Agenda) Act* 2000 (Cth, Australia)
- *Copyright Amendment (Moral Rights) Act* 2000 (Cth, Australia)
- *Copyright Amendment (Parallel Importation) Bill* 2001 (Cth, Australia)
- *Circuit Layouts Act* 1989 (Cth, Australia)
- *Corporations Act* 2001 (Cth, Australia)
- *Designs Act* 1906 (Cth, Australia)
- *Employees Liability Act (NSW)* 1991 (Australia).

- *Patents Act* 1990 (Cth, Australia)
- *Patents Amendment (Innovation Patents) Act* 2000 (Cth, Australia)
- *Privacy Act* 1988 (Cth, Australia)
- *Telecommunications Act* 1997 (Cth, Australia)
- *Trade Marks Act* 1995 (Cth, Australia)
- *Trade Practices Act* 1974 (Cth, Australia)

United States of America

- *Alien Tort Claims Act* (ATCA) 1789 (United States of America)
- *Communications Decency Act* 1996 (CDA) (United States of America)
- *Computer Fraud and Abuse Act* (CFAA), (18 U.S.C. 1030) 1986 (United States of America)
- *Computer Misuse Act* 1990 (United States of America)
- *Digital Millennium Copyright Act* (known as DMCA 512 or the DMCA 1998) (United States of America) (Public Law No. 105-304, 112 Stat. 2860, 2877).
- *Foreign Intelligence Surveillance Act* (FISA) (as codified in 50 U.S.C. §§1801–1811, 1821–29, 1841–46, and 1861–62) 1978 (United States of America)
- *Online Copyright Infringement Liability Limitation Act* (OCILLA) 1998 (United States of America)
- *Patent Act* 1790 (United States of America)
- *Private Securities Litigation Reform Act* 1995 (United States of America)
- *Restatement and Uniform Trade Secrets Act* 1985 (United States of America)
- *Telecommunications Act* 1996 (United States of America)

- *Trademark Act* 1946 (United States of America)
- *Uniform Electronic Transactions Act* 1999 (United States of America)
- *Restatement (Second) of Contracts*, S 56 & The United States Framework for Global Electronic Commerce (United States of America)

Other Legislation, Statues and Directives

- *Copyright Act* 1985 (Canada) (R.S., c. C-30, s. 1)
- *Data Protection (Amendment) Act* (2003) Ireland
- *Data Protection Act* (1998) Ireland
- *Laki tietoyhteiskunnan palvelujen tarjoamisesta* (458/2002) Finland.
- *Loi relative à l'économie numérique (*2002) France
- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996), with additional article 5 bis as adopted (United Nations Model Law on Electronic Commerce (1996))

EU Directives

- *European Union Directive* 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- *European Union Directive* 2000/31/EC on Electronic Commerce OJ 2000 L 178/1 and Council Directive 94/44/EC on Certain Aspects of the Sale of Consumer Goods and Associated Guarantees OJ I 171 7.7.99
- *European Union Directive 2000/31/EC* (on Electronic Commerce OJ L 178 p1, 17 July 2000)
- *European Union Directive 2002/58/EC* (The E-Privacy Directive);
- *European Union Directive 85/374/EEC* (The Product Liability Directive)

- *European Union Directive 95/46/EC* (Data Protection Directive);

iv Acknowledgements

This dissertation is dedicated to the persons listed below who have all , in their way , made this possible. To the many people who have encouraged me during my Masters learning I offer my sincere thanks.

I would also like to take this opportunity to sincerely thank the people at BDO where I work for their time, patience and understanding. I would especially thank Allan Granger for his reading and his advice.

A special mention and thanks to my supervisor and to all my lecturers in the LLM in International Commercial Law (2005/2007) at Northumbria, UK for their invaluable guidance.

Micheal Shehadie (BA LLB Solicitor) has contributed digests of reported and unreported judgments of federal courts, supreme courts and selected specialist courts and tribunals throughout Australia.

Last, but most importantly, I would like to thank my wife, Lynn Wright for her time and her willingness to be used as my sounding board throughout the process of writing this paper (and for remaining sane).

This masterwork has been much improved by their contributions of all these people and more through their patience, understanding and comments. Despite their best efforts, it still has faults and areas that could be improved – all of those are my own.

I. Introduction

The Internet is fundamentally a means of communication. Issues with law that have arisen because of the Internet are thus a result of the differences between communication in the physical world and communication using the Internet. Contractual negotiations are the result of a series of communications that create a legally binding agreement[1].

This paper will demonstrate that inaction from ISPs and other intermediaries is risky and that the most effective enforcement framework involves enforcement from the least cost provider as proposed by Mann & Belzley[2]. There are various kinds of services connected with the Internet, and the liability of the service provider may depend on what is being provided. At one extreme there are the long distance telecommunications providers, at the other there are Internet publishers and other providers of material. In between there are a range of providers such as operators of node computers, Internet access providers, providers of bulletin boards, Usenet group organizers and providers of host computers for web pages.

In many cases, liability will depend upon how a court faced with a case of first impression analogises a particular Internet service provider to more conventional categories of information providers. For example, should the service provider be viewed as the equivalent of the telephone company, purely a conduit for information? This might be the right analogy for the telecommunications link provider, but clearly does not fit the publisher. On the other hand, if the provider is viewed as analogous to a publisher of a printed publication, there is a much greater exposure to liability[3]. The provider of a host computer for third party web pages could be compared to a printer or perhaps a distributor of printed publications. It could also be argued that a Usenet

[1] An electronic contract has a twofold structure. Thought of electronically, the contract is a sequence of numbers and code saved to some electronic or magnetic medium. Alternatively, the contract becomes perceptible through a transformation of the numeric code when broadcast to a computer output device such as a printer or screen . Prior to the passing of the ECA, this dichotomy exasperated the uncertainty contiguous with whether an electronic contract can be regarded as being a contract in writing.

[2] Mann, R. & Belzley, S (2005) "The Promise of the Internet Intermediary Liability" 47 William and Mary Law Review 1 <http://ssrn.com/abstract=696601> at 27 July 2007]

[3] The distributed nature of the Internet means that a publisher can reach far more people. A company with a web site in the UK for instance has direct access to the US, Canada, Australia and many other countries with the primary limitations being language.

group or bulletin board is analogous to a library, so that the provider should be treated as the librarian.

The foremost dilemma with the study of electronic law is the complexity and difficulty in confining its study within simple parameters. Internet and e-commerce do not define a distinct area of law as with contract[4] and tort law. Electronic law crosses many legal disciplines, each of which can be studied individually. Examples of a range of areas of law that electronic, e-commerce, and Internet law touch upon can be seen in the following pages.

In fact, existing laws already address the majority of situations that may impact an Internet intermediary. In most cases (for instance), cybercrimes are just age-old crimes committed using a new technology. Identity theft, for instance, has existed for hundreds of years, only now the speed and volume, and hence the consequence of the offence is increased. What is important to the intermediary is the increased scope of responsibility that many of them now face.

New challenges do arise through the nature of widely distributed networks such as the Internet. Some legal jurisdictions have addressed this issue through the enhancement of existing laws. Most however, have adopted an approach where they define solutions to a uniquely perceived legal difficulty through the creation of separate digital laws. In particular, these are manifest in the numerous additions to computer crime statutes that have recently populated the various criminal codes.

Of particular confusion to the internet intermediary is the distinction between what is illegal and what is criminal. This, however, is not a distinction solely confined to electronic law. It is important to note that although many actions are illegal, they may not be criminal in nature. This is important as the evidentiary requirements in criminal cases are far stricter than in civil litigation. This is also reflected in the actions that the intermediary will be required to take, both to stop another party[5] who

[4] It has been argued that the digital contract may appear on the computer screen to consist of words in a written form but merely consist of a virtual representation . The **Electronic Communications Act 2000** [ECA] has removed the uncertainty and doubt surrounding the question as to the nature of electronic form used in the construction of a contract. In this, the ECA specifies that the electronic form of a contract is to be accepted as equivalent to a contract in writing

[5] Such as with regards to taking action on notice of hosting child pornography.

is involved in a criminal activity, and also counter to minimise the tortuous actions that they may be exposed to.

II. The Changing Nature of the Internet and Opportunities for Transgressions

In the physical world, intermediaries are generally conscious players that are actively involved with a transaction. They will generally have some type of legal relationship with the other party that has been negotiated and agreed in advance. An Internet intermediary may not be consciously involved in the transaction and further may not have any pre-existing relationship[6].

A. The composition of the Internet

The Internet is formed from the interconnection of a succession of linked hosts. Originally envisaged by the United States government, The Internet was developed to offer a network solution to the military in time of war. It has been adapted to use by the general public opening up access to private companies hence creating an international commercial network.

The Internet has become a network of privately controlled networks and hosts that communicate using a TCP/IP (Transfer Control Protocol/Internet Protocol). A request from a host for data over the Internet involves the routing of data to the system that holds the requested content and then back from that system to the original user. The structure of the Internet and the common use of TCP/IP for transfer between networks create a common backbone that allows disparate systems to communicate seamlessly.

An Internet intermediary can in effect provide either of two services to either a single party or multiple parties. These services include the provision of access to communication channels or the provision of an additional service over these channels. In the first instance we are looking at a traditional Internet service provider or ISP. An ISP can provide general backbone routing services and connectivity. This is the

---

[6] The inclusion of electronic agents makes the traditional requirement for a "meeting of minds" more difficult to prove. With many smaller vendors, hosting and creating their own e-commerce enabled web site requires the interaction of a third party. Often, this involves the use of an external service provider, which offloads the Internet shopping trolley function. In this way, smaller vendors can create an e-commerce enabled site quickly and simply.

The issue, which arises in this instance, is in determining the contracting parties. Many small vendors provide little more than billboards style advertising through their web site. The complex task of maintaining the databases, transaction processing, and the shopping cart function becomes simplified when outsourced to another provider. In some instances, a redirection takes the customer to a completely new site or domain.

most fundamental of the services as without a connection to the Internet no other Internet-based services may be accessed. Additionally, an ISP can also provide access to systems and storage space.

The second instance involves an Internet content provider or ICP. An ICP can cover a far wider range of activities than an ISP. In its most basic form this is the provision of transaction services between parties, identification and authorisation of parties, the provision of search capabilities or a combination of any of the above. In effect, the addition of web portals to traditional banking systems has turned the banking industry into an Internet content provider. The bank provides authorisation, identification and transaction processing capabilities. These capabilities extend beyond simple transaction processing and the accessing of one's own account. Services such as PayPal[7] have emerged to offer intermediary payment facilities over the Internet allowing users to transact without developing these capabilities themselves and offering a service in such a manner that the end client may not even be aware of the existence of the payment intermediary.

B. Actors who define the Internet

Dr Russell Smith of the Australian Institute of Criminology[8] stated in 2000 that:

> *"The perpetrators of many on-line scams … are often not large corporations. They are able to close-down their operations quickly and easily, move assets to secure locations and use digital technologies to conceal their identities and disguise evidence. In such cases there is little likelihood of success whether civil or criminal proceedings are taken."*

Dr Smith noted that fraud may be committed both electronically and in paper based payment systems by individuals opening accounts with false identification details. These individuals may then exceed credit balances or alter instruments or

7 PayPal is an online financial transaction broker, PayPal lets people send money to each other's e-mail addresses. At no time will either party see the other's credit card or bank information. Currently, 95% of eBay's purchases go through PayPal. Similar to an escrow service, PayPal acts as the middleman holder of money. Through its policies, practices, and business integrity, PayPal has earned the trust of both parties. See https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/bizui/WhatIsPayPal-outside

8 Smith, 2000 "Confronting Fraud in the Digital Age"

messages used to authorise transactions. On the Internet, traditional methods of fraud and criminal activity have been updated such that they use this new technology capably. However, there are dilemmas other then fraud on the Internet. It is necessary to understand the relationship between the various parties on the Internet and how they interact if we are to gain an understanding of the issues facing Internet intermediaries.

1. Primary Malfeasors

The primary malfeasors that impact Internet content or service providers are those who proffer or obtain illicit material across the Internet. This material ranges from breaches of copyright, objectionable content, child pornography, unlicensed gambling, and trademark dilution or infringement as well as a number of less common offences including money laundering and terrorism. Most countries have strict licensing requirements for gambling sites if they allow this activity at all. A website can offer its services to any nation if it so chooses. As such, an online casino could be setup to solicit clients from other jurisdictions that do not allow online gambling (such as the USA).

In other cases, the provision may be legal in its own jurisdiction (such as the offering of "hard-core" pornography in Denmark) but breach the laws where it is being accessed. An individual that introduces malware into the Internet is also placing content onto the systems that comprise the Internet. This is an action that could threaten many other people and organisations. As many SCADA[9] systems are connected to networks, an Internet worm could have the impact of affecting the physical world.

2. Internet Intermediaries

It was originally argued that widespread disintermediation[10] would occur over the Internet. It was originally believed that the Internet would provide a means to allow transacting parties to deal directly with each other. In reality the opposite has

[9] Supervisory Control and Data Acquisition. These are systems that are used by many critical services, including power and emergency services.

10.See, Shapiro, Andrew L., Digital Middlemen and the Architecture of Electronic Commerce, 24 OHIO N.U. L. REV. 795 (1998).

occurred with additional layers being formed rather than removed. There are two primary reasons for this growth of intermediaries, the first is related to the need to connect to the Internet and the second derives from both trust and the availability of payment. In either case any transaction conducted over the Internet will not be in person. The consequence being that cash exchanges cannot occur and the third-party will need to provide the trusted source of funds. The simple need to connect also derives from the distance that may be involved. When communicating across vast distances in small amounts of time and intermediary is always needed. In the past telecommunications carriers provided fax and phone services to satisfy this transaction. In effect what the Internet has done is to supplant fax, telephony, telex and electronic data interchange (EDI) with new and more universally accepted protocols. It would be rare to find any two parties with sufficient resources to construct and connect a global internetwork themselves.

The issue of trust surrounds payments creating opportunities for both payment and auction intermediaries. In a contemporary transaction for the sale of a product any one individual would not be able to assemble the essential resources necessary to reach a global market. The growth of auction intermediaries such as eBay[11] has created the ability to offer products and services internationally creating global markets. The consequence is that intermediaries have created market segments that were not thought possible and did not previously exist curtailing the expected disintermediation of the Internet.

Internet service providers

An Internet service provider or ISP provides the communication backbone supporting the Internet.[12] To end-users, the ISP is the entity responsible for opening access to the content on the Internet. Generally speaking, an end-user is unlikely to care about the true path traversed in receiving their data. Most users will not care

[11] Ebay.com states its purpose to be "the world's online marketplace; a place for buyers and sellers to come together and trade almost anything!" (for a detailed description, see http://pages.ebay.com/help/newtoebay/questions/about-ebay.html).

12. Bick (1998) states that "*Even the simplest internet transaction usually involves a user's computer, an internet service provider's access computer, a regional router, a governmental backbone computer, another regional router, another internet service provider's computer, and a content provider's computer. So, even in the simplest transactions, there are many more intermediaries than users or content providers*".

about the nature of Internet protocols, how routing systems function, what type of physical infrastructure is in place as long as they receive their transmission. In becoming acquainted with the significance of a suitable regulatory design of sensitivity to context, it is imperative to differentiate distinct roles that an ISP can play in the provision of standard Internet services.

There are in effect three primary classifications and ways of distinguishing ISPs. It is likely that any Internet-based transaction will follow through a path of *Source ISP*, *Backbone Providers*, and arrive at a *Destination ISP* where both the source and destination ISPs are effectively *endpoints*. Backbone providers include the class of telecommunication carriers who deal solely with the transmission and routing of packets across provider networks. For purposes of liability, backbone providers offer little more than a conduit for contractual loss from other providers that they deal with. Backbone providers are unlikely to have the capabilities or capacity that will allow them to distinguish between data, traffic or protocol content making the ability to filter illicit activity next to impossible at this level.[13] Source and destination ISPs are in effect similar in many ways. In particular, any endpoint ISP will at some stage act as either and both source or destination ISP.

Any end-user request over the Internet is served by a destination ISP. A *Source ISP* is the organisation that supplies access to the servers and systems where the unlawful content (both lawful and illicit) is presented or hosted.[14] There are two significant differences involving the Source ISP and the Destination ISP when viewed under a regulatory framework. Firstly the Destination ISP serving ordinary end-users is most unlikely to have any direct association with or precise information concerning the primary malfeasor. Any logs or materials that may be maintained are unlikely to hold the level of detail necessary to prove malfeasance. A Source ISP conversely is likely to maintain logs and track access to the content that it maintains. It is necessary to weigh any process of assessing how "*fair*" it would be to "*hold responsible*" the

13.Many commenters on the Internet hold the view that the difficulty of understanding the data that travels over ISP networks is an artefact of the internet's basic transmission protocol, under which the data that travels over those networks is in the forms of disintegrated packets of any particular file. It seems that regulation at the backbone level is likely in most cases to involve costs to *all* traffic that would outweigh the benefits reasonably attributed to the regulation.

14.This point is best made by Zittrain, (2003). *Internet Points of Control*, 44 B.C. L. REV. 653

Source ISP for the misconduct of its clients or other parties and also in determining how successfully the Source ISP could serve as a regulator in controlling misconduct against a variety of factors. In many cases, the Source ISP may be located in a jurisdiction without reciprocal regulations thus preventing prosecution. Next, the Source ISP may itself be a victim of illicit activity.

In the instance that a Source ISP supplies both the host that contains content and also the access to that material, it is likely to be able to more effectively monitor and control the activity of its users than would an ISP that provides only access to the material. A Destination ISP can not readily remove itself from the authority of the regulatory regime in whose jurisdiction the users are situated. To do so would result it in also removing its ability to serve those end-users. A Source ISP and the content it hosts, if desiring to make possible prohibited conduct, can move itself to an alternate jurisdiction that does not disallow the illicit conduct. For instance, a Source ISP that wishes to implement access to Internet gambling can locate itself in a jurisdiction where these activities[15] are legal and thus legitimised. This in effect places these organisations beyond the jurisdiction and capability of the majority international legal edicts and the related enforcement capabilities.[16] The Destination ISP however is not beyond this reach. An ISP in London with local clients that allows its clients to connect to a child pornography site in Nigeria needs a local presence in London. At this least this would include a local sales office, local servers, cabling, power and equipment such as switches and routers.

A Destination ISP supplies an end-user with the data that they have requested from Internet. Many ISPs are merely resellers of Internet connectivity maintaining only simple connection, billing and routing systems. As such, Destination ISPs may

15. In such a structure, there is and has been an international race to the bottom to attract business to certain countries by decreasing the legal obstacles to their establishment. In the context of internet gambling, the winner of this race has arguably been the small island of Antigua in the British West Indies. *See* Don Yaeger, *Bucking the Odds*, SPORTS ILLUSTRATED, Jan. 8, 2001, at 26 ("Some 850 Web gambling sites are based [in Antigua] and an estimated 80% of all gaming URLs on the Web can be traced back to servers on the 108-square-mile island."); UNITED STATES GENERAL ACCOUNTING OFFICE, REPORT GAO-03-89, INTERNET GAMBLING: AN OVERVIEW OF THE ISSUES 52 (2002), *available at* http://www.gao.gov/new.items/d0389.pdf [hereinafter GAO REPORT] (listing 35 of 88 internet gambling websites as registered in either Antigua or Barbuda, but failing to report the percent of internet gambling taking place at these sites).

16. Indeed the United States even brought a case against the country of Antigua and Barbuda before the WTO in an effort to curtail the proliferation of internet gambling operations on that tiny island nation. The United States lost that suit. *See* Naomi Rovnick, *Herbies Helps Antigua in WTO Outsourcing Victory*, LAWYER, April 5, 2004, at 10.

be further subdivided into the additional subcategories of *Retail ISPs* and *Link ISPs*. A *Retail ISP* is the one that maintains and operates an end-user billing system. A *Link ISP* provides not just access but also hosts systems needed to access internet applications including SMTP, POP3 and World Wide Web systems (for e-mail and web access respectively). These organisations also act as the gateways allowing end-users to access the various internet protocols. As the administrators of systems that link disparate networks and the Internet backbone, as well as encapsulating application data into an arrangement that may be broadcast along the backbone, Destination ISPs are capable of averting selected attacks through the blocking of access to certain sites, hosts or even selected data available on the Internet. They may also aide in mitigating or at least slowing the transfer of certain other malicious classes of data such as worms or other malware.

Link ISPs and Retail ISPs need to integrate to present the end-user with access to the Internet and the related services[17]. It is possible to consider their functions to be either integrated or disintegrated based on the circumstances.

Where legislation is focussed on stopping selected Internet access it is fitting to concentrate on those Retail ISPs dealing directly with those affected by the legislation. Legislation mandating IP address filtering (such as to block access to pornographic sites) is better directed to Link ISPs as they can process Internet traffic more effectively than Retail ISPs[18]. Ideally, it is beneficial to consider a single entity *Destination ISP* formulated from a collaborating Retail ISP and Link ISP group.

Payment intermediaries

The difficulties in transferring cash payments over large distances and between people who may have never met and may never meet created the need for payment intermediaries in Internet transactions. Payment intermediaries provide both trust and some realistic means for a purchaser to transfer consideration to the seller reliably. For instance, if a buyer on an online auction site comes up with the highest

[17] Many ISPs were set up by the same kind of people who tend the carry out computer hacking, phone phreaking or similar activities. This group of people tends to believe that any kind of property rights in information are basically wrong, particularly if that information is owned by the Government or big business, and take great pride in discovering and making available such confidential information. It is, therefore, not surprising that there have been a number of cases in the United States, which involve the publication of stolen proprietary information.

[18] Many Retail ISPs maintain little or no technological capability to filter internet traffic.

bid incurring a debt, a payment intermediary would be involved in order to arrange a transfer of funds either from the purchases banking account or via some payment card system cons making the transaction.

As an example, if party A located in Singapore was to sign up for an account with a licensed online casino such as Lasseter's online in Australia, party A would require some means of transferring funds from their banking account to a trust account managed and maintained by Lasseter's. When party A has subsequently been successful at their gambling pursuit playing online poker, the party would require some means of ensuring the return of their winnings. If on the other hand party A had accumulated gambling debts, Lasseter's would require some means of ensuring that funds in the trust account we used to pay those debts.

In the case of less significant amounts, this may be as simple as holding party A's credit card details in a database. In situations where the transactions a large, Lasseter's may wish to use party A's bank to transfer money in advance or otherwise to secure some assurance that A's potential gambling losses will be covered. The payment card company or bank in practice is an essential actor for the conduct in which "party A" desires to enact.

It was originally believed[19] that digital cash or electronic money would be created or minted allowing for some type of universal credit and would facilitate Internet transactions. Although a number of schemes did emerge, the vast majority of transactions that occur across the Internet are made by means of traditional means such as credit cards.[20] Rather than digital cash being minted, a new type of payment intermediary developed. Peer to peer (P2P) payment systems,[21] such as PayPal, emerged allowing individuals to receive transactions directly[22], bypassing merchants and also act as a means of consolidating payment methods by providing a mechanism to interact with various banks and payment card institutions directly.

---

[19] Anderson et al. in their Dec 1997 presentation "*Exploring Digital Cash*" argued that digital cash would "*likely continue to evolve remarkably quickly*".

20 In 2002, roughly ninety percent of internet transactions used credit cards. Ronald J. Mann, *Regulating Internet Payment Intermediaries*, 82 TEXAS L. REV. 681, 681 (2004).

21 In this context, P2P stands for "person-to-person." The term is to be distinguished from the more common use of the same acronym to describe the peer-to-peer file sharing discussed in the context of piracy.

22 *See* Mann, at 683.

Peer-to-peer processing networks have aided the growth of auction intermediaries such as eBay.[23] Payment card providers, P2P systems, and other entities that act as a mechanism to facilitate commercial transactions[24] also have the capability to stop illicit transactions and act as revelatory enforcement points. A commercial site distributing child pornography from Nigeria cannot be run profitably without an economical method of receiving consideration. If the site operators cannot reliably receive payment, they will quickly shut down. As the financial gatekeepers, payment intermediaries can be used to prevent illicit activity over the Internet. Either through proactive actions or upon the receipt of court orders and Internet payment intermediary could be used as an aid to curtail undesirable activities occurring across the Internet.

Auction intermediaries

The auction intermediary has become the predominant means of matching buyers and sellers. These range from the classic option structure as defined by the industry leader, eBay, through to a more dynamic market structure more reminiscent of a stock exchange futures exchange trading floor. At the simplest, these parties provide client to client matching services allowing individuals and small corporations across the globe to deal (seemingly) directly.

These organisations are the target of most complaints concerning breaches of contract, illicit or illegal goods and even failure to act. One of the difficulties is the direct result of legislative differences between jurisdictions. In many cases, goods or services that may be legal in one jurisdiction could be controlled or proscribed in another. Liability for internet auction intermediaries mirrors those principles that have been created and applied in disputes concerning traditional or real-world auction intermediaries as may be seen in *Fonavisa*.[25]

23 Id.

24 Because of the fluidity of payment mechanisms on the internet, there are a wide variety of service providers of various kinds (such as organisations like Checkfree, Cybernet & Authorize.net) that might or might not be regarded as intermediaries, depending on the circumstances. For purposes of this Essay, however, we focus on the dominant intermediaries like Visa, MasterCard, and PayPal.

25.Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

3. Government and Regulators

Many people believe that the Internet is a legislative nowhere land. The truth however is quite different with the majority of governments acting quickly correcting legal deficiencies and holes in recognition of the importance and value of information technology and the Internet. In many ways, law reform has moved faster around the Internet than many other technologies. The US in particular, has been quick to act introducing various specific immunities for Internet intermediaries. Many other jurisdictions including the EU have implemented substantial programs aimed at curtailing any legislative flaws.

The US has introduced a detailed set of immunities is a part of the online copyright infringement liability limitation act[26] (contained within the Digital millennium Copyright act) in order to ratify the provisions of the WIPO Copyright Treaty[27]. These provisions provide immunity from prosecution to Internet intermediaries involved in the *mere transmission* of packets[28], who maintain automated cache Systems, who host third-party resources and those who provide search tools. There are conditions associated with these immunities. It is required that the Internet intermediary has a lack of knowledge of the transgression, but they do not receive direct financial benefit from it, and that they respect and do not try to bypass copyright protection technologies.

General immunity provisions have also been introduced within the US through the Communications Decency Act (1996)[29]. This act introduced new criminal offences of knowingly creating, sending, transmitting or displaying of obscene or indecent materials to minors. This act introduced a number of "*Good Samaritan*" provisions permitting ISPs to introduce blocking or filtering technology while not

[26] The Online Copyright Infringement Liability Limitation Act (OCILLA) is a portion of the Digital Millennium Copyright Act known as DMCA 512 or the DMCA takedown provisions. It is a 1998 United States federal law that provided a safe harbour to online service providers (OSPs, including ISPs, internet service providers) that promptly take down content if someone alleges it infringes their copyrights. Section 512 was added to the Copyright law in Title 17 of the United States Code (Public Law No. 105-304, 112 Stat. 2860, 2877).

[27] The European Union's Electronic Commerce directive contains similar notice and takedown provisions in its Article 14. In France, the Digital Economy Law ("Loi relative à l'économie numérique") implements this directive. In Finland "Laki tietoyhteiskunnan palvelujen tarjoamisesta" implements the directive.

[28] The UK legislation, Statutory Instrument 2002 No. 2013, The Electronic Commerce (EC Directive) Regulations 2002 states in section, "Mere conduit" is functionally equivalent to this provision..

[29] Communications Decency Act (1996)

becoming classified by the courts to be a publisher or editor. This allows an ISP to filter this material without assuming any responsibility for third-party content.

The EU E-Commerce Directive[30] provides a similar provisions offering protection for both packet transmitters and cache operators[31]. It is still possible however that an ISP could be required to either actively monitor content or at the least to take down prescribed content following a notification or advice as to its existence. If, following being advised, the ISP had not removed the offending content, liability would still apply.

The US Senate has approved S.B. 2248, a measure that grants immunity from prosecution to telecommunications companies such as ISPs that cooperate with intelligence gathering requests from the government[32]. This amendment to the Foreign Intelligence Surveillance Act (FISA)[33] would if passed increases government powers to eavesdrop on communications in certain cases without a warrant. Though there is an increase to selected protections for Internet intermediaries, there are still issues. If for instance an ISP sees an action to violate the constitutional rights of their

---

[30] Directive 2000/31/EC on Electronic Commerce OJ L 178 p1, 17 July 2000

[31] Statutory Instrument 2002 No. 2013, The Electronic Commerce (EC Directive) Regulations 2002 states in section, "Caching": "Where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that transmission where -

(a) the information is the subject of automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request, and

(b) the service provider -

(i) does not modify the information;

(ii) complies with conditions on access to the information;

(iii) complies with any rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(iv) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(v) acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement."

[32] See, http://www.washingtonpost.com/wp-dyn/content/article/2008/02/12/AR2008021201202_pf.html

[33] The Foreign Intelligence Surveillance Act (FISA) of 1978 is a U.S. federal law prescribing procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between or among "foreign powers" on territory under United States control. FISA is codified in 50 U.S.C. §§1801–1811, 1821–29, 1841–46, and 1861–62.[1] The subchapters of FISA provide for Electronic Surveillance, Physical Searches, Pen Registers and Trap & Trace Devices for Foreign Intelligence Purposes, and Access to certain Business Records for Foreign Intelligence Purposes.

clients and does not immediately respond, they do not receive immunity if eventually forced to respond. Further, the immunity only applies selectively to government agencies and no other actions.

The UK at the moment is in a state of flux. The release of the "*Creative Britain; new talents for the new economy*"[34] proposal carries with it the potential to create additional liabilities for Internet intermediaries. It is proposed that either Internet service providers engage in a voluntary code of conduct that provides security controls and monitoring, or else it is likely that the government will implement these controls. Ideally, intermediaries will work together formulate an industry code of practice thus negating the need for government intervention and also reducing their exposure to both contractual breaches[35] and tortuous liability.

C. Present Liability Schemes and Sanctions

The actor with the best capability to thwart most forms of internet-related misconduct is the primary malfeasor. The release of malware such as a "worm" is without doubt best prevented from causing harm by the person that created and released it against the Internet. For pornography sites to succeed there is a requirement for both a viewer and commercial website. If either party is absent, the commercial viewing of pornography and obscenity will not take place. This is even truer in the case of an interactive service such as gambling and online casinos. As such, direct control of either of these actors will thwart much of the social harm caused by this type of activity. This straightforward approach is the one most commonly utilised by the law.

Regulations attempting to avert misconduct through a process of protecting the primary malfeasors from their own actions are becoming less effective in the distributed world of the Internat. Both when the actors are judgment proof and in cases where prosecution is unproductive due to a high degree of dealings or due to the low worth of each transaction, this legislative approach has proved ineffective.

[34] Department for Culture, Media and Sport, 22 Feb 2008

[35] The major uncertainty with electronic contracts stems from the facts of the individual dispute. This can lead to breaches as parties who do not understand the issues surrounding the contract seek to get around them. Fundamentally; offer, acceptance and consideration to fill the requirements of creation of the contract. Being that the offeror may stipulate the method of acceptance, it would be prudent for the contracting parties to agree to the form of acceptance prior to the conclusion of the contractual negotiations.

Consequently the direct regulation of individuals (such as in cases involving an infringement of copyrighted material) who use the Internet remains ineffective in diminishing undesired conduct.[36] The result is that Internet Intermediaries are commonly seen as both the target of opportunity and also the answer to judgement proof actors.

1. Remedy in Tort and Civil Suits

The availability of the Internet Intermediary as co-targets for actions makes them susceptible to the actions of both their clients and also uninterested third parties for passing off and misleading and deceptive conduct. An action for intentional interference with business by unlawful means may also be possible. The tort of intentional interference with business by unlawful means may be available where the use of the trade mark is unlawful.

The courts generally seem willing to apply conventional fault-based tort principles to weigh up the behaviour of intermediaries. The instances in which comparatively egregious conduct has ended in the liability of the intermediary are few,[37] and the majority of cases conclude with the absolution of the intermediaries from blame.[38] Those circumstances that have resulted in a decision by the court that in effect declare that the intermediaries hold considerable accountability for the behaviour of any primary malfeasors have mutually in the EU and the US Congress resulted in the respective parliaments acting to overrule the decision through the legislative conceding of expansive exemptions from liability to the intermediaries.[39] "*The paths share not only the reflexive and unreflective fear that recognition of liability for intermediaries might be catastrophic to internet commerce; they also share a myopic focus on the idea that the inherent passivity of internet intermediaries makes it normatively inappropriate to impose responsibility on them for conduct of primary*

36. A number of innovative approaches to solving the issue are provided by Lemley & Reese; WILLIAM W. FISHER III, PROMISES TO KEEP (2004).

37.*See* A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000).

38.For criticism of this perspective, see Landes & Lichtman.

39.The most obvious example of this action can be found in the history of the Communications Decency Act. Congress directly responded to the ISP liability found in *Stratton Oakmont, Inc. v. Prodigy Services*, 23 Media L. Rep. (BNA) 1794 (N.Y. Sup. Ct. 1995), 1995 WL 323710, by including immunity for ISPs in the CDA, 47 U.S.C. § 230(c)(1) (2004) (exempting ISPs for liability as the "publisher or speaker of any information provided by another information content provider"), which was pending at the time of the case. Similarly, Title II of the Digital Millennium Copyright Act, codified at 17 U.S.C. § 512, settled tension over ISP liability for copyright infringement committed by their subscribers that had been created by the opposite approaches to the issue by courts. *Compare* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993) (finding liability), *with* Religious Tech. Ctr. v. Netcom, Inc., 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) (refusing to find liability).

malfeasors. That idea is flawed both in its generalization about the passivity of intermediaries and in its failure to consider the possibility that the intermediaries might be the most effective sources of regulatory enforcement, without regard to their blameworthiness"[40].

In the US, Congress has endorsed legislative protections for intermediaries from liability through defamation with the introduction of the Communications Decency Act[41]. In 47 U.S.C. §230, it is unambiguously positioned as regarding internet regulation[42] that the act introduced a series of "Good Samaritan provisions" as a part of the *Telecommunications Act of 1996.* This was tested in *DiMeo v Max* (2007),[43] in which the court found the defendant not liable for comments left by third parties on a blog. The plaintiff alleged that the defendant was a publisher of the comments hosted on the website but did not allege that the defendant authored the comments on the website or that the defendant was an information content provider. Under 47 U.S.C. § 230 (f)(3), the court determined "*the website posts alleged in the complaint must constitute information furnished by third party information content providers*" and as a consequence immunity applied to the forum board operator. The Court upheld the dismissal of the suit.

The act, first passed in 1996[44] and subsequently amended in 1998,[45] has the apparent rationale of minimising Internet regulations in order to promote the

---

[40] Mann, R. & Belzley, S (2005) "The Promise of the Internet Intermediary Liability" 47 William and Mary Law Review 1 <http://ssrn.com/abstract=696601> at 27 July 2007]

41 The Communications Decency Act of 1996 (CDA)

42.47 U.S.C. § 230(b) (2004) (emphasis added)

"*It is the policy of the United States—*
(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer".

[43] WL 2717865 (3rd Cir. Sept. 19, 2007); See also *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* , CV-03-09386-PA (9th Cir. May 15, 2007); and *Universal Communication Systems, Inc. v. Lycos, Inc.* , 2007 WL 549111 (1st Cir. Feb. 23, 2007)

44.1996, Pub. L. 104-104, Title I, § 509.

45.1998, Pub. L. 105-277, Div. C, Title XIV, § 1404(a).

development of the Internet and safeguard the market for Internet service. The internet has consequently become so essential to daily life that it is improbable that the addition of extra legislation would intimidate service providers away from the provision of services at a competitive rate.[46]

In the US, 47 U.S.C. § 230(c)(1) provides a defence for ISPs stating that, "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*." This statute would seem[47] to afford absolute immunity from any responsibility. Contrasting the DMCA, the ISP or ICP could chose not to do away with material in the event that the ISP or ICP has tangible awareness of the defamatory nature of material it is in fact hosting.[48] Notwithstanding the focal point of this legislation having been towards liability for defamation, it has pertained to seemingly unrelated auction intermediaries, including eBay.[49]

Inside the European Union, judgments obtained in the courts of one state are enforceable in any other state included within the Brussels Convention. If not, a judgment in one state will be enforceable in another only where there is a bilateral treaty creating the provision for such reciprocal enforcement between them. Frequently, these treaties add formalities surrounding the enforcement process that offer the courts of the jurisdiction in which the defendant is situated prudence both as to a decision to enforce, or to what degree. It is consequently vital when deciding on a jurisdiction to bring suit to decide if any judgment obtained is enforceable against a defendant who may in effect be judgement proof.

2. Cyber Negligence

Not acting to correct a vulnerability in a computer system may give rise to an action in negligence if another party suffers loss or damage as the result of a cyber-

46.There remains, however, the fear that additional regulation will stifle innovation in the industry. Would, for instance, eBay enter the market as a new company today if it were liable for trademark infringement it facilitated? Such liability adds new start-up and ongoing costs that may make some new ventures unprofitable (or even more unprofitable). For an article addressing regulation in this way, see Lemley & Reese.

47.There is at least the possibility that the statute would permit a State to require intermediaries to act. *See* Doe v. GTE Corp. 347 F.3d 655 (7th Cir. 2003) (per Easterbrook, J.) (suggesting that Section 230(e)(3) "would not pre-empt state laws or common-law doctrines that induce or require ISPs to protect the interests of third parties").

48.Thus minimising the likelihood of a decision such as *Godfrey* in the United States. *See supra* note 102.

49.Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703 (Ct. App. 2002)

attack or employee fraud. Given proximity[50], a conception first established in *Caparo Industries Plc. v. Dickman*, [1990][51] and reasonable foreseeability as established in *Anns v. Merton London Borough Council*, [1978][52] A.C. 728, the question of whether there exists a positive duty on a party to act so as to prevent criminals causing harm or economic loss to others will be likely found to exist in the cyber world. The test of reasonable foreseeability has however been rendered to a preliminary factual enquiry not to be incorporated into the legal test.

The Australian High Court regarded a parallel scenario, whether a party has a duty to take reasonable steps to prevent criminals causing injury to others in *Triangle Shopping Centre Pty Ltd v Anzil*[53]. The judgment restated the principle established by Brennan CJ in *Sutherland Shire Council v Heyman*[54]. The capacity of a plaintiff to recover hinges on the plaintiff's ability to demonstrate a satisfactory nexus (e.g. a dependence or assumption of responsibility) between the plaintiff and the defendant such that it gives rise to a duty on the defendant to take reasonable steps to prevent third parties causing loss to the plaintiff[55]. Consequently, if a plaintiff in a case involving a breach of computer security could both demonstrate that the defendant did not in fact take reasonable measures to ensure the security of their computer systems (as against both internal and external assault), and they show the act of the third person (e.g. an attacker/hacker or even a fraudulent employee) occurred as a direct consequence of the defendant's own fault or breach of duty, then an action in negligence is likely to succeed[56].

Many organisations state that current standards of corporate governance for IT systems pose a problem due to the large number of competing standards. However, it

---

[50] Proximity, a notion first established in *Caparo Industries Plc. v. Dickman*, [1990] 2 A.C. 605, is the initial phase of the assessment. The subsequent phase enquires as to whether there are policy considerations which would reduce or counteract the duty created under the initial stage. Mutually, the phases are to be met with reference to the facts of cases previously determined. The dearth of such cases would not however avert the courts from finding a duty of care.

[51] [1990] 2 A.C. 605

[52] [1978] A.C. 728

[53] Modbury Triangle Shopping Centre Pty Ltd v Anzil *[2000] HCA 61.*

[54] (1985) 157 CLR 424.

[55] Dixon J elucidated how a "special relationship" of this variety may occur in Smith v Leurs (1945) 70 CLR 256. This case was derived from an indication of occurrences that entail a special danger and the control or of actions or conduct of the third person; See also [2000] HCA 61, para 140.

[56] See: Clerk and Lindsell on Torts, 19th Edition (2006), Chapter 28, paragraph 28-05

needs to be taken into account that all of these standards maintain a minimum set of analogous requirements that few companies presently meet. Most of these standards, such as the PCI-DSS[57] and COBIT[58], set a requirement to monitor systems. COBIT control ME2 (Monitor and Evaluate Internal Controls) is measured through recording the "*number of major internal control breaches*". PCI-DSS at 10.5.5 states a minimum requirement to "*use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)".* As a general minimum, it may be seen that an organisation needs to maintain a sufficiently rigorous monitoring regime to meet these standards.

Installation guidelines provided by the Centre for Internet Security (CIS)[59] openly provide system benchmarks and scoring tools that contain the "*consensus minimum due care security configuration recommendations*" for the most widely deployed operating systems and applications in use. The baseline templates will not themselves stop a determined attacker, but could be used to demonstrate minimum due care and diligence.

It is interesting to contrast this general proposition with a peculiar case where the plaintiff went to great lengths in an attempt to recover loss caused by its own negligence, namely loss suffered due to computer fraud perpetrated by its own employee in its own system.

In *Mercedes Benz (NSW) v ANZ and National Mutual Royal Savings Bank Ltd*[60] (unreported), the Supreme Court of New South Wales considered if a duty to avert fraud would occur in cases where there is an anticipated prospect of loss. The Mercedes Benz employee responsible for the payroll system fraudulently misappropriated nearly $1.5 million by circumventing controls in the payroll software. Mercedes Benz alleged that the defendants, ANZ and NMRB, were

---

[57] PCI-DSS (version 1.1) is the Payment Card Industry Data Security Standard and is contractually required to be adhered to by all merchants that process VISA, Mastercard and other payment card products. This requirement and standard is maintained by the PCI Standards Council at https://www.pcisecuritystandards.org/

[58] COBIT v 4.1 is the computer control objectives and standard maintained by ISACA at http://www.cobitonline.info

[59] CIS benchmark and scoring tools are available from http://www.cisecurity.org/

[60] No. 50549 of 1990.

negligent in paying on cheques that where fraudulently procured by the employee and in following her direction. The plaintiff's claim was dismissed by the court. It was held that employers who are careless in their controls to prevent fraud using only very simple systems for the analysis of employee activities will be responsible for the losses that result as a consequence of deceitful acts committed by the organisations' employees. It takes little deliberation to extend this finding to payment intermediaries.

The decision was founded on the judgment of Holt CJ in *Hern v Nichols* (1701)[61] that stated in "*seeing somebody must be a loser by this deceit, it is more reason that he that employs and puts a trust and confidence in the deceiver should be a loser than a stranger*"[62]. The question remains open as to the position that may result from unsound practices operated not by the plaintiff but by an organisation in supplying services under an outsourcing agreement. In either event, the requirement for an organisation to provide controls to ensure a minimum level of system security is clear.

The situation is further compounded in instances of cyber-attack that lead to a loss. An innocent third party that suffers an attack that originates from an inadequately secured system would be able to easily demonstrate a lack of reasonable care if the minimum consensus standards mentioned above are not achieved. Coupled with facts demonstrating that the attack originated from the defendant's insecure system, the evidence would provide the requisite substantiation of both proximity and reasonable foreseeability.

3. Vicarious Liability

Liability against an Intermediary, whether in the traditional view of ISP and ICP as well as that of employers and other parties remains a risk.

Civil Liability

The conduct of both agents and employees can result in situations where liability is imposed vicariously on an organisation through both the common law[63]

[61] (1701) 1 Salk 289

[62] Id., at 358.

[63] Broom v Morgan [1953] 1 QB 597.

and by statute.[64] The benchmark used to test for vicarious liability for an employee requires that the deed of the employee must have been committed during the course and capacity of their employment under the doctrine *respondeat superior*. Principals' liability will transpire when a `principal-agent' relationship exists. Dal Pont[65] recognises three possible categories of agents:

(a) those that can create legal relations on behalf of a principal with a third party;

(b) those that can affect legal relations on behalf of a principal with a third party; and

(c) *a person who has authority to act on behalf of a principal*.

Despite the fact that a party is in an agency[66] relationship, the principal is liable directly as principal as contrasting to vicariously, "*this distinction has been treated as of little practical significance by the case law, being evident from judges' reference to principals as vicariously liable for their agents' acts*"[67]. The consequence being that an agency arrangement will leave the principle directly liable rather then vicariously liable.

The requirement for employees to have acted "*within the scope of employment*" is a broad term without a definitive definition in the law, but whose principles have been set through case law and include:

- where an employer authorises an act but it is performed using an inappropriate or unauthorised approach, the employer shall remain liable[68];

---

[64] Employees Liability Act 1991 (NSW).

[65] G E Dal Pont, Law of Agency (Butterworths, 2001) [1.2].

[66] The inclusion of electronic agents makes the traditional requirement for a "meeting of minds" more difficult to prove. With many smaller vendors, hosting and creating their own e-commerce enabled web site requires the interaction of a third party. Often, this involves the use of an external service provider, which offloads the Internet shopping trolley function. In this way, smaller vendors can create an e-commerce enabled site quickly and simply.

The issue, which arises in this instance, is in determining the contracting parties. Many small vendors provide little more than billboards style advertising through their web site. The complex task of maintaining the databases, transaction processing, and the shopping cart function becomes simplified when outsourced to another provider. In some instances, a redirection takes the customer to a completely new site or domain.

[67] Ibid [22.4].

[68] Singapore Broadcasting Association, SBA's Approach to the Internet, See Century Insurance Co Limited v Northern Ireland Road Transport Board [1942] 1 All ER 491; and Tiger Nominees Pty Limited v State Pollution Control Commission (1992) 25 NSWLR 715, at 721 per Gleeson CJ.

- the fact that an employee is not permitted to execute an action is not applicable or a defence[69]; and
- the mere reality that a deed is illegal does not exclude it from the scope of employment[70].

Unauthorised access violations or computer fraud by an employee or agent would be deemed remote from the employee's scope of employment or the agent's duty[71]. This alone does not respectively absolve the employer or agent from the effects of vicarious liability[72]. Similarly, it remains unnecessary to respond to a claim against an employer through asserting that the wrong committed by the employee was for their own benefit. This matter was authoritatively settled in the *Lloyd v Grace, Smith and Co.*[73], in which a solicitor was held liable for the fraud of his clerk, albeit the fraud was exclusively for the clerk's individual advantage. It was declared that "*the loss occasioned by the fault of a third person in such circumstances ought to fall upon the one of the two parties who clothed that third person as agent with the authority by which he was enabled to commit the fraud*"[74]. It would be interesting to see how the courts decide on the instance of a "security consultant" or penetration tester who had used the tools and access provided by the firm to conduct activities that where not authorised (such as breaching client networks in excess of authority).

Lloyd v Grace, Smith and Co.[75] was also referred to by Dixon J in the leading Australian High Court case, *Deatons Pty Ltd v Flew*[76]. The case concerned an assault by the appellant's barmaid who hurled a beer glass at a patron. Dixon J stated that a servant's deliberate unlawful act may invite liability for their master in situations where "*they are acts to which the ostensible performance of his master's work gives occasion or which are committed under cover of the authority the servant is held out*

---

[69] Tiger Nominees Pty Limited v State Pollution Control Commission (1992) 25 NSWLR 715.

[70] Bugge v Brown (1919) 26 CLR 110, at 117 per Isaacs J.

[71] Even in cases where the employee is engaged to break into systems legally, as in the case of a penetration tester or auditor, the employee will have received authorisation – even where the people do not know of the deed, some level of management will have knowledge and have passed authority.

[72] unreported decision in Warne and Others v Genex Corporation Pty Ltd and Others -- BC9603040 -- 4 July 1996.

[73] [1912] AC 716

[74] [1912] AC 716, Lord Shaw of Dunfermline at 739

[75] [1912] AC 716

[76] (1949) 79 CLR 370 at 381

as possessing or of the position in which he is placed as a representative of his master"[77].

Through this authority, it is generally accepted that if an employee commits fraud or misuses a computer system to conduct an illicit action that results in damage being caused to a third party, the employer may be supposed liable for their conduct. In the case of the principles agent, the principle is deemed to be directly liable.

In the context of the Internet, the scope in which a party may be liable is wide indeed. A staff member or even a consultant (as an agent) who publishes prohibited or proscribed material on websites and blogs, changes systems or even data and attacks the site of another party and many other actions could leave an organisation liable. Ste*venson Jordan Harrison v McDonnell Evans* (1952)[78] provides an example of this category of action. This case hinged on whether the defendant (the employer) was able to be held liable under the principles of vicarious liability for the publication of assorted "*trade secrets*" by one of its employees which was an infringement of copyright. The employee did not work solely for the employer. Consequently, the question arose as to sufficiency of the "*master-servant*" affiliation between the parties for the conditions of be vicarious liability to be met. The issue in the conventional "*control test*" as to whether the employee was engaged under a "*contract for services*", against a "*contract of service*" was substituted in these circumstances with a test of whether the tort-feasor was executing functions that were an "*integral part of the business*" or "*merely ancillary to the business*". In the former circumstances, vicarious liability would extend to the employer. Similarly, a contract worker acting as web master for an organisation who loads trade protected material onto their own blog without authority is likely to leave the organisation they work for liable for their actions.

In *Meridian Global Funds Management Asia Limited v Securities Commission*[79], a pair of employees of *MGFMA* acted without the knowledge of the company directors but within the extent of their authority and purchased shares with

[77] Ibid.

[78] [1952] 1 TLR 101 (CA).

[79] [1995] 2 AC 500

company funds. The issue lay on the qualification of whether the company knew, or should have known that it had purchased the shares. The Privy Council held that whether by virtue of the employees' tangible or professed authority as an agent performing within their authority[80] or alternatively as employees performing in the course of their employment[81], both the actions, oversight and knowledge of the employees may well be ascribed to the company. Consequently, this can introduce the possibility of liability as joint tort-feasors in the instance where directors have, on their own behalf, also accepted a level of responsibility[82] meaning that if a director or officer is explicitly authorised to issue particular classes of representations for their company, and deceptively issues a representation of that class to another resulting in a loss, the company will be liable even if the particular representation was done in an inappropriate manner to achieve what was in effect authorised.

The degree of authority is an issue of fact and relies appreciably on more than the fact of employment providing the occasion for the employee to accomplish the fraud. P*anorama Developments (Guildford) Limited v Fidelis Furnishing Fabrics Limited*[83] involved a company secretary deceitfully hiring vehicles for personal use without the managing director's knowledge. As the company secretary will customarily authorise contracts for the company and would seem to have the perceptible authority to hire a vehicle, the company was held to be liable for the employee's actions. Similarly, the unauthorised use of Internet bandwidth assigned to a client of an ISP by an employee of the ISP would seem to be covered under perceptible authority.

Criminal Liability

As employers, Internet intermediaries can be held to be either directly or vicariously liable for the criminal behaviour of their employees.

Direct liability for organisations or companies refers to the class of liability that occurs when it permits the employee's action. Lord Reid in *Tesco Supermarkets*

[80] see Lloyd v Grace, Smith & Co. [1912] AC 716

[81] see Armagas Limited v Mundogas S.A. [1986] 1 AC 717

[82] Demott, Deborah A. (2003) "*When is a Principal Charged with an Agent's Knowledge*?" 13 Duke Journal of Comparative & International Law. 291

[83] [1971] 2 QB 711

Limited v Nattrass[84] formulated that this transpires when someone is "*not acting as a servant, representative, agent or delegate*" of the company, but as "*an embodiment of the company*"[85]. When a company is involved in an action, this principle usually relates to the conduct of directors and company officers when those individuals are acting for or "*as the company*". Being that directors can assign their responsibilities, direct liability may encompass those employees who act under that delegated authority. The employer may be directly liable for the crime in cases where it may be demonstrated that a direct act or oversight of the company caused or accepted the employee's perpetration of the crime.

Where the prosecution of the crime involves substantiation of *mens rea*[86], the company cannot be found to be vicariously liable for the act of an employee. The company may still be found vicariously liable for an offence committed by an employee if the offence does not need *mens rea*[87] for its prosecution, or where either express or implied vicarious liability is produced as a consequence of statute. Strict liability offences are such actions. In strict liability offences and those that are established through statute to apply to companies, the conduct or mental state of an employee is ascribed to the company while it remains that the employee is performing within their authority.

The readiness on the part of courts to attribute criminal liability to a company for the actions of its employees seems to be escalating. This is demonstrated by the Privy Council decision of Meridian Global Funds Management Asia Ltd v Securities Commission[88] mentioned above. This type of fraudulent activity is only expected to become simpler through the implementation of new technologies by companies. Further, the attribution of criminal liability to an organisation in this manner may broaden to include those actions of employees concerning the abuse of new technologies.

---

[84] [1972] AC 153

[85] ibid, at 170 per Lord Reid

[86] See Pearks, Gunston & Tee Limited v Ward [1902] 2 KB 1, at 11 per Channell J, and Mousell Bros Limited v London and North-Western Railway Company [1917] 2 KB 836, at 843 per Viscount Reading CJ.

[87] See Mousell Bros Limited v London and North-Western Railway Company [1917] 2 KB 836, at 845 per Atkin J.

[88] [1995] 2 AC 500.

It is worth noting that both the *Data Protection Act 1998*[89] and the *Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000*[90] make it illegal to use equipment connected to a telecommunications network for the commission of an offence. The *Protection of Children Act 1978*[91] and *Criminal Justice Act 1988*[92] make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent. Further, the *Obscene Publications Act 1959*[93] envelops all computer material making it a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it. While these Acts do not of themselves create liability, they increase the penalties that a company can be exposed to if liable for the acts of an employee committing offences using the Internet.

Chapter Summary

Although the Internet has changed the backdrop of the economy and society, it has not radically changed the nature of either civil or criminal transgressions. Rather it has added a layer of complexity through the speed and volumes of transactions that it has enabled. The issue for the law and society is not an introduction of new crimes or new transgressions, but an enhanced capability both to engage in these activities and also the increased capacity to find them. Here again another issue develops with the juxtaposition of security and privacy. The increased ability of the intermediaries to monitor and control our actions is directed by the need to protect personal liberty. The incorrect balance of these forces leading to either too little security and a possible finding of negligence (or worse) or the breach of controls designed to protect society and the possible criminal effects of these actions.

[89] Data Protection Act 1998 [UK]

[90] Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 [UK]

[91] Protection of Children Act 1978 [UK]

[92] Protection of Children Act 1978 and Criminal Justice Act 1988 [UK]

[93] Obscene Publications Act 1959 [UK]

III. Applications to Specific Types of Conduct

Six principal situations could generate civil liability for Internet Intermediaries. These are:

1. defamation, libel and harm to reputation;
2. invasion of privacy, misuse or failure to protect personal information;
3. distributing restricted materials;
4. communication of erroneous information;
5. violation of secrecy; and
6. unfair competition.

Differing provisions cover each of these avenues for liability and based on both the jurisdiction and nature of the intermediary, any or all of these may apply. This section details the acts that are of primary concert to internet intermediaries.

A. Dissemination of Content

The Internet has offered a place that has allowed for the rebirth of many old crimes and torts. Obscene and ethically abusive acts (including child pornography) have developed to be both easier and may be more widespread in effect as a consequence of the Internet. This has resulted from the ubiquitous nature of both e-mail and the World Wide Web in modern society. Countless conventional crimes including intimidation and harassment, blackmail, fraud and criminal defamation have remained for all purposes, essentially the same. The simplicity and relative anonymity of the Internet have acted to increase their prevalence. Trafficking in contraband and counterfeit products, unlicensed and illegal gambling by use of the Internet and defamatory material sent to cause damage to another individual's reputation are just the start of the many issues that the Internet has offered increased opportunities.

The Internet Intermediary has to ensure that they are able to meet a minimum level of practice and governance if they do not wish to become liable for these actions. At the least, inaction could result in action based on negligence.

In the US case of *Williams v America Online Inc*[94], some of the difficulties that that may occur where demonstrated. In this case, Mr Williams started proceedings in Massachusetts stemming from a class action over the installation of AOL software. AOL asserted that the proceedings must commence in Virginia as the terms state Virginia was the exclusive jurisdiction or any claim. Mr Williams however argued that alterations to his computer came about before he agreed to the conditions. Mr Williams described the complicated process by which he had to "agree" to the conditions after the configuration of his computer had already occurred.

Further, Mr Williams demonstrated he was able to click, "I agree" without seeing the terms of service. This meant that the actual language of AOL's terms of service failed to display on the computer screen unless the customer specifically requested it, overriding the default settings. The court rejected AOL's assertions[95]. Although this was a contract case, the difficulties posed through the media add additional burdens to an already burdened system. So in this case, the license associated with the disseminated content was subverted by the ineffectiveness of the means of distributing it.

In Europe, the potential for a wide divide has opened due to the perceived disparity between personal privacy and intellectual property protection. The recent Spanish case C-275/06 (Productores de Música de España Promusicae vs. Telefónica de España SAU) highlights this disparity[96]. A Spanish Court of Madrid asked the ECJ for the interpretation of the EU law on this matter. Advocate General Kokott came to the determination that EU law does not oblige Internet intermediaries to hand over private information in civil litigation. The Spanish music Association Promusicae had requested that the ISP Telefonica provide the identities and addresses of its clients who had connected and allegedly disseminated multimedia files that were protected through copyright provisions using the Kazaa P2P network. Telefonica objected to

---

[94] **MARK WILLIAMS and another(1) vs. AMERICA ONLINE**, INC. 2001 WL 135825 (Mass. Super., February 8, 2001)

[95] "the fact the plaintiff may have agreed to an earlier terms of service for the fact that every AOL member enters into a form of terms of service agreement does not persuade me that plaintiff's ... have notice of the forum selection cause in the new terms of service before reconfiguration of their computers."

[96] Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU (Opinion of Advocate General Kokott), July 18, 2007.

this request stating that it would only do so in the course of a criminal investigation or in matters of public security and national defence.

Such a determination could be seen as contrary to the French "three strikes" model[97] that is being considered in the recent "Creative Britain; new talents for the new economy"[98] framework. Although this proposed legislation could do much to curtail intellectual property losses by requiring ISPs to monitor the illicit activities of their subscribers, it is yet to be seen how the court will interpret this. Taken in view of the determination handed down from C-275/06[99], it is likely that any legislative requirements could be construed as being problematic and have a high potential to be struck down by the European Court of Justice, hence rendering them an effective. The best outcome then would be a voluntary agreement that was implemented and affected through the ISPs themselves. The difficulty in reaching such an agreement however is likely to cause to be this doubtful.

1. Internet Piracy, Contraband and Counterfeit Products

Copyright

It may often occur that works offered over on the Internet, either by a service provider or its subscribers, is included within the copyright owned by a third party who has not sanctioned the works distribution. In some instances, a service provider may be liable for a copyright infringement using its service and systems.

In the UK, copyright law is governed through the "Copyright, Designs and Patents Act 1988 (the "*1998 Act*") and the ensuing decisions of courts. The Australian

---

[97] The French President announced a plan on the 23rd Nov 2007 to curb Intellectual property theft and other Internet related crimes. He stated that: "Today an accord is signed and I see a decisive moment for the civilised internet. Everywhere, in the US, UK and others, industry and government have tried... to find a permanent resolution to the problem of piracy. We are the first, in France to try to build a national grand alliance around clear and viable proposals." Geoff Taylor of the British record institute stated that: "We will continue to pursue voluntary arrangements, but unless these are achieved very soon we believe that the UK Government must act, as the French government has, to ensure that the urgent problem of internet piracy is tackled effectively."

Further details are available inline from: http://www.zeropaid.com/news/9114/France+to+Ban+Illegal+File-Sharers+From+the+Internet

[98] The "Creative Britain; new talents for the new economy" strategy was issued on the 22nd Feb 2008 and is available online at <http://www.culture.gov.uk/NR/rdonlyres/096CB847-5E32-4435-9C52-C4D293CDECFD/0/CEPFeb2008.pdf>

[99] Ibid.

position[100] mirrors that of the UK where protection of a work is free and automatic upon its creation and differs from the position in the US, where work has to be registered to be actionable. While some divergences may be found, Australian copyright law largely replicates the frameworks in place within the US and UK. The copyright term is shorter than these jurisdictions in Australia being the creator's life plus 50 years whereas the UK has a term of 70 years from the end of the calendar year in which the last remaining author of the work dies for literary works. As co-signatories to the Berne Convention, most foreign copyright holders are also sheltered in both the UK and Australia.

The 1988 Act catalogues the copyright holder's exclusive rights as the rights to copy, issue copies of the work to the public, perform, show or play in public and to make adaptations. An ephemeral reproduction that is created within a host or router is a reproduction for the intention of copyright law. Though, there appears to be no special right to broadcast a work over a network, a right is granted in Section 16(1)(d) to broadcast the work or include it in a cable program service. The notion of "*broadcast*" is restricted to wireless telegraphy receivable by the general public. Interactive services are explicitly excluded from the designation of "*cable program service*" (S.7 (2)(a)). A proviso making an individual an infringer of the act in the event of remote copying has been defined to encompass occasions where a person who transmits the work over a telecommunications system[101] knowing or reasonably believing that reception of the transmission will result in infringing copies to be created.

The law contains provisions imposing criminal penalties and civil remedies for making importing or commercially trading in items or services designed to thwart technological copyright protection instruments, and sanctions against tampering with electronic rights management information and against distributing or commercially dealing with material whose rights management information has been tampered with.[102]

---

100 The Australian Act is modelled on the 1956 UK Act.

101 This does not include broadcasting or cable

102 See also, UK Intellectual Property Office (http://www.ipo.gov.uk/), Australian Copyright Council Online Information Centre (http://www.copyright.org.au) and the US Copyright Office (http://www.copyright.gov/)

There are several legislative limitations on the scope of exclusive rights under UK law[103]. Liability is also possible for secondary infringement including importing and distributing infringing copy prepared by a third party. The scope of the exclusive rights of the copyright owner is extensive enough to include an ISP or ICH that utilises or consciously allows another to its system in order to store and disseminate unauthorized copies of copyright works. This situation would create the risk of civil action. A contravention could constitute a criminal offence if a commercial motivation for copyright infringement could be demonstrated.

The Australian High Court decision in *Telstra Corporation Ltd v Australasian Performing Rights Association Limited*[104] imposed primary liability for copyright infringement on Telstra in respect of music broadcast over a telephone "hold" system. A large part of the decision concentrated on the definition of the diffusion right in Australia.[105] It follows from this decision that if an ISP broadcasts copyright works to in the general course of disseminating other materials through the Internet, that diffusion is a "*transmission to subscribers to a diffusion service*" as defined by the Australian Copyright Act[106]. It consequently emerges that an ISP may be directly liable for an infringement of copyright caused by that transmission under Australian common law for the infringements of its customers.[107]

A determination as to whether a message using telecommunications is "*to the public*"[108] will likely hinge on whether the message is made "*openly, without*

---

[103] See ***Queen's Bench in Godfrey v. Demon Internet Ltd, QBD, [2001] QB 201***. The United Kingdom Parliament took no action to exempt Internet Intermediaries from liability after the court held that an internet service provider liable as the publisher at common law of defamatory remarks posted by a user to a bulletin board.

104 Telstra Corporation Limited v Australasian Performing Rights Association Limited (1997) 38 IPR 294. The Majority of the High Court (with Justices Toohey and McHugh dissenting) upheld the Full Court that music on hold transmitted to users of wired telephones represents a transmission to subscribers over a diffusion service. The Court further unanimously held that music on hold transmitted to users of mobile telephones involves a broadcast of the music.

105 Section 26 of the Australian Copyright Act 1968.

[106] Copyright Act 1968 (Cth, Australia)

107 This decision has created apprehension amongst authors. E.g. Simon Gilchrist "Telstra v Apra –Implications for the Internet" [1998] CTLR 16 & MacMillian, Blakeney "The Internet and Communications Carriers' Copyright Liability" [1998] EIPR 52.

108 Ibid; See also Goldman v The Queen (1979), 108 D.L.R. (3d) 17 (S.C.C.), at p. 30. It would therefore appear that it 70 is the intention of the sender of the message which is determinative of the private or public nature of the message

concealment"[109] to a sufficiently large number of recipients. No case has attempted to quantify a specific cut-off point.

In *Moorhouse v. University of New South Wales,*[110] a writer initiated a "*test case*" asserting copyright infringement against the University of New South Wales. The University had provided a photocopier for the function of allowing photocopying works held by the university's library. A chapter of the plaintiff's manuscript was copied by means of the photocopier. The library had taken rudimentary provisions to control the unauthorised copying. No monitoring of the use of the photocopier was made. Further, he sign located on the photocopier was unclear and was determined by the Court to not be "*adequate*"[111]. The Australian High Court held that, whilst the University had not directly infringed the plaintiff's copyright, the University had sanctioned infringements of copyright in that the library had provided a boundless incitement for its patrons to duplicate material in the library.[112]

In July 1997, the Attorney-General published a discussion paper[113] that proposed a new broad-based technology-neutral diffusion right as well as a right of making available to the public[114]. This provides the position where direct infringement by users of a peer-to-peer (P2P) file-sharing network would be covered in Australian law in a manner comparable to the US position in both Napster and Grokster[115].

---

109 Spar, D. (2001) at 11-12

110 [1976] R.P.C. 151.

111 This is similar to the findings in RCA Corp. v. John Fairfax & Sons Ltd [1982] R.P.C. 91 at 100 in which the court stated that "[A] person may be said to authorize another to commit an infringement if he or she has some form of control over the other at the time of infringement or, if there is no such control, if a person is responsible for placing in the hands of another materials which by their nature are almost inevitably to be used for the purpose of infringement."

112 [1976] R.P.C. 151 "[A] person who has under his control the means by which an infringement of copyright may be committed - such as a photocopying machine - and who makes it available to other persons knowing, or having reason to suspect, that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit use to legitimate purposes, would authorize any infringement that resulted from its use".

113 See Attorney-General's Discussion Paper, "Copyright and the Digital Agenda", July 1997 at 71. The goal of this paper was to indicate the method by which Australia could implement the international copyright standards agreed at the December 1996 WIPO meeting.

114 See Attorney-General's Discussion Paper, note 11.

115 A&M Records Inc v Napster, Inc 114 F Supp 2d 896 (ND Cal 2000) & A&M Records Inc v Napster, Inc 239 F 3d 1004 (9th Cir 2001); Metro-Goldwyn-Mayer Studios Inc v Grokster Ltd No.s CV-01-08541-SVW, CV-01-09923-SVW (CD Cal, 25 April 2003) ('Grokster') (available at www.cacd.uscourts.gov) & Grokster Nos CV-01-08541-SVW, CV-01-09923-SVW (CD Cal, 25 April 2003), 21-2.

Mann and Belzley's[116] position holds the least cost intermediary liable is likely to be upheld under existing UK, US and Australian law. The positions held by the court in Telstra v Apra[117] and Moorhouse v UNSW[118] Define the necessary conditions to detail public dissemination and infringement through a sanctioned arrangement. The public dissemination of music clips on a website could be seen as being analogous to the copying of a manuscript with the ISP's disclaimer being held as an inadequate control. It is clear that the provision of technical controls, monitoring and issuing of take down notices by the ISP would be far more effective at controlling copyright infringement than enforcing infringements against individuals.

Several cases have occurred in the US involving ISPs or other service providers that hosted copyright material made available to those accessing the site. A significant decision was made in *Religious Technology Center v Netcom On–line Communication Services, Inc*[119]. The case involved the posting of information online which was disseminated across the Internet. The postings were cached by the hosting provider for several days, and robotically stored by Netcom's system for 11 days. The court held that Netcom was not a direct infringer in summary judgment[120]. It was held that the mere fact that Netcom's system automatically made transitory copies of the works did not constitute copying by Netcom. The court furthermore discarded arguments that Netcom was vicariously liable. The Electronic Commerce (EC Directive) Regulations 2002[121] warrants that the equivalent outcome would be expected in the UK[122].

116 Mann, R. & Belzley, S (2005) "The Promise of the Internet Intermediary Liability" 47 William and Mary Law Review 1 <http://ssrn.com/abstract=696601> at 27 July 2007]

117 Spar, D. (2001) at 11-12

118 47 U.S.C. § 230(c)(1) (2004) (This sections details the requirements of the CDA that do not apply to ISPs).

119 907 F. Supp. 1361 (N.D. Cal. 1995)

120 See also, System Corp. v Peak Computer Co., F.2d 511 (9th Cir. 1993), in which it was held that the creation of ephemeral copies in RAM by a third party service provider which did not have a license to use the plaintiff's software was copyright infringement.

121 Statutory Instrument 2002 No. 2013

122 The act states that an ISP must act "expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network". The lack of response from Netcom would abolish the protections granted under this act leaving an ISP liable to the same finding.

The US Congress has acted in response with a number of statutes by and large that are intended to protect the intermediary from the threat of liability.[123] The Digital Millennium Copyright Act (DMCA)[124] envelops the possibility of liability from copyright liability. The DMCA is prepared such that it exempts intermediaries from liability for copyright infringement whilst they adhere to the measures delineated in the statute. These in the main compel them to eliminate infringing material on the receipt of an appropriate notification from the copyright holder.

In the UK, "*fair dealing*" exceptions are a great deal more restricted than the US "*fair use*" exceptions. Netcom[125] if tried in the UK would have to deal with the explicit requirements of Section 17 of the 1988 Act that entails copying to include storage by electronic means and also covers the creation of transient or incidental copies. These provisions make it probable that the result in the UK would have varies from that in the US at least in the first instance. The inclusion of storage differentiates ISPs and ICPs from telephone providers aligning them closer to publishers.

AN ISP or ICP could attempt to argue a similarity to a librarian over that of a publisher. The statutory provisions providing certain exemptions from liability for libraries under the 1988 Act and accompanying regulations are unlikely to apply to an

---

123. With some minor exceptions, other countries have also seen broad liability exemptions for internet intermediaries as the appropriate response to judicial findings of liability. The United Kingdom Parliament took no action after the Queen's Bench in **Godfrey v. Demon Internet Ltd, QBD, [2001] QB 201**, held an Internet service provider liable as the publisher at common law of defamatory remarks posted by a user to a bulletin board. In the U.S., §230 of the CDA would prevent such a finding of liability. Similarly, courts in France have held ISPs liable for copyright infringement committed by their subscribers. *See* Cons. P. v. Monsieur G., TGI Paris, Gaz. Pal. 2000, no. 21, at 42–43 (holding an ISP liable for copyright infringement for hosting what was clearly an infringing website).

In 2000, however, the European Parliament passed Directive 2000/31/EC, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf, which in many ways mimics the DMCA in providing immunity to ISPs when they are acting merely as conduits for the transfer of copyrighted materials and when copyright infringement is due to transient storage. *Id.* Art. 12, 13. Further, the Directive forbids member states from imposing general duties to monitor on ISPs. *Id.* Art. 15. This Directive is thus in opposition to the British and French approaches and requires those countries to respond statutorily in much the same fashion as Congress responded to *Stratton Oakmont* and *Religious Technology Centers*. Of course courts are always free to interpret the Directive or national legislation under the Directive as not applying to the case at hand. *See, e.g.*, Perathoner v. Pomier, TGI Paris, May 23, 2001 (interpreting away the directive and national legislation in an ISP liability case).

Canada has passed legislation giving ISPs immunity similar to the DMCA. *See* Copyright Act, R.S.C., ch. C-42, §2.4(1)(b) (stating "a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public"). The Canadian Supreme Court interpreted this provision of the Copyright Act to exempt an ISP from liability when it acted merely as a "conduit." Soc'y of Composers, Authors and Music Publishers of Can. v. Canadian Assoc. of Internet Providers, [2004] S.C.C. 45, 240 D.L.R. (4th) 193, ¶92. The court in that case also interpreted the statute to require something akin to the takedown provision of the DMCA. *See id.* at ¶110.

124. Pub. L. No. 105- 304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

125 907 F. Supp. 1361 (N.D. Cal. 1995)

ISP as the ability for a librarian to make copies is controlled under strict conditions. It is doubtful that these conditions could be met by either an ISP or ICP.

Modern peer-to-peer networks have separated the network from software with a decentralised indexing process[126] in an attempt to defend themselves from an exposure to vicarious liability as in *Napster*.[127] The methods suggested by Kraakman's analysis of asset insufficiency,[128] have led ICPs and ISPs to become judgment proof, thus restraining the effectiveness of sanctions even against the intermediaries. It seems natural to expect as the technology develops that it in practice will be so decentralized as to obviate the existence of any intermediary gatekeeper that could be used to shut down the networks.[129]

The success of modern peer to peer networks has resulted in the content industry targeting those individual copyright infringers who use peer-to-peer networks to disseminate or download copyrighted material.[130] Existing peer-to-peer networks and software permits the capture of sufficient information concerning individuals who attach to the network to identify the degree of infringement and possibly who is responsible[131]. Recent advances to the P2P networking protocols have allowed users to screen their identity removing the ability for copyright holders to bring their claims to court[132]. As copyright infringement evolves, it will become more improbable to expect a solution through prosecuting individual users[133].

---

126. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir.) (Refusing to find liability for Grokster even though it aided end-users in copyright infringement because the service. This case is fundamentally different than Napster), cert. granted, 125 S. Ct. 686 (2004).

127. Id.

128. Kraakman, Corporate Liability Strategies, at 869.

129. See generally Tim Wu, When Code Isn't Law, 89 Va. L. Rev. 679 (2003) (explaining that peer to peer networks have removed the intermediary on which copyright enforcement requires).

130. See Amy Harmon, Subpoenas Sent to File Sharers Prompt Anger and Remorse, N.Y. Times, July 28, 2003, at C1. See also Brian Hindo & Ira Sager, Music Pirates: Still on Board, Bus. Wk., Jan. 26, 2004, at 13. See J. Cam Barker, Grossly Excessive Penalties in the Battle Against Illegal File-Sharing: The Troubling Effects of Aggregating Minimum Statutory Damages for Copyright Infringement, 83 Texas L. Rev. 525 (2004).

131. See Alice Kao, Note, RIAA v. Verizon: Applying the Subpoena Provision of the DMCA, 19 Berkeley Tech. L.J. 405, 408.

132. Scott Banerjee, P2P Users Get More Elusive, Billboard, July 31, 2004, at 5.

133. Perversely, what probably has in fact reduced the frequency of copyright infringement is more crime: using P2P systems subjects a computer to the threat of viruses that are spread inside the files obtained. Wendy M. Grossman, Speed Traps, Inquirer (U.K.), Jan. 14, 2005, at ___ , available at http://www.theinquirer.net/?article=20718 (last visited Jan. 15, 2005). Another dissuasion has been the systematic effort by the recording industry to saturate P2P systems with dummy files that make getting the music a user actually wants quite difficult. See Malaika Costello-Dougherty, Tech Wars: P-to-P Friends, Foes Struggle, PC

This type of action is currently being fought in the EU with Danish ISP, Tele2, planning to fight a court order requiring it to block access to the Bit-Torrent website known as Pirate Bay. The ISP has cut off access to the site for its customers but other ISPs in Denmark are yet to receive letters requesting that they also prevent their users from accessing the website. The International Federation of the Phonographic Industry (IFPI) has stated that it plans to dispatch the letters this week (Feb, 2008)[134].

Trademark Infringement

A trademark infringement refers to the unauthorized use of a protected trademark or service mark, or use of something very similar to a protected mark. The success of any legal action to stop (or injunct) the infringement is directly related to whether the defendant's use of the mark causes a likelihood of confusion in the average consumer. If a court determines that a reasonable average consumer would be confused then the owner of the original mark can prevent the other party from making use of the infringing mark and even possibly collect damages. A party that holds the legal rights to a particular trademark can sue other parties for trademark infringement based on the standard "*likelihood of confusion*"[135].

Road Tech Computer Systems Limited v Mandata (Management and Data Services) Limited[136] involved Mandata, a rival of Roadtech, deploying metatags[137] in their WebPages that used several of Roadtech's trade marks. These included the name of the company and the name of a registered product, "*ROADRUNNER*". Roadtech initiated action against Mandata for passing off and trade mark infringement in an action for summary judgement. Mandata admitted using the trademarked material.

World, Mar. 13, 2003, at __ , available at http://www.pcworld.com/news/article/0,aid,109816,00.asp (last visited Jan. 15, 2005) (documenting the practice and attributing it to a company called Overpeer, which is apparently an industry anti-piracy company).

[134] See, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9062482&source=rss_topic17 and http://www.heise-online.co.uk/security/Code-injection-vulnerability-in-Adobe-s-Flash-Media-Server--/news/110115

[135] In the US, the Trademark Act of 1946, statutes § 1114 and § 1125 are specific to trademark infringement.

[136] Roadtech Computer Systems Ltd v Mandata (Management and Data Services) Ltd (25 May 2000) unreported, High Court, Chancery Division HC 1999 04573 per Master Bowman.

[137] When a website is designed, it may include a number of key words in its code which reflect the content of the website. These are known as metatags and they enable a company's site to be catalogued according to such matters as the title of the web page, the company's name, its trademarks, history, type of business and location. Metatags are used in particular by certain search engines to match key search words against the metatags available — inevitably the validity of the search will very much depend on the original use of the metatags on a website

The court held that Mandata had infringed Roadtech's trademarks. It was further asserted that Mandata's use of these metatags was effectively an act of misrepresentation as those individuals seeking Roadtech or its merchandise using a search engine would be directed to Mandata's web site[138]. The misrepresentation comes from allowing the individuals searching for these products to believe that Mandata was one way or another associated with Roadtech. The misappropriation of Roadtech's goodwill and the meagre quality of Mandata's website resulted in damage to Roadtech's brand. It was concluded that Roadtech was also permitted to receive summary judgment in respect of passing off.

There are a number of ways that trademark infringements could occur on the Internet. An ICP could add metatags to increase traffic (either with or without the client's explicit permission) and equally, a client of an ISP could embed violating material into its WebPages. An ISP caching this information may inadvertently cache this material even after a take down order had been applied to the original offender.

Patents and Patent Infringement

A patent is a right granted for any device, substance, method or process which is new, inventive and useful. It is essentially a monopoly right over a registered invention or discovery that is legally enforceable and provides the holder the exclusive right to commercially exploit the invention for the life of the patent. A patent is not automatic and it must be applied for and registered in each country to which it is to apply (there is no such thing as an international patent). Patents give effective protection if you have invented new technology that will lead to a product, composition or process with significant long-term commercial gain.

The sale of goods using an intermediary can create personal jurisdiction for patent infringement over the Internet. In *Trintec v. Pedre Promotional Products*[139], Trintec initiated action against Pedre for an infringement of their patent in the District of Columbia. Trintec accused Pedre of contravening Trintec's patents for the

[138] The original metatag case was based on similar facts. *Playboy Enterprises Inc v Calvin Designer Label* (1997) 44 USPQ 2d (BNA) 1156 (ND Cal). Was based on the use of registered trade marks of Playboy Enterprises Inc ("PEI"), PLAYMATE and PLAYBOY, as terms in the meta tags of their web sites as well as in the domain names used for their sites.

[139] Trintec Indus. v. Pedre Promotional Products, 04-1293 (Fed. Cir. Jan. 19, 2005)

automation of printed faces used in watches. Pedre moved for dismissal due to a lack of personal jurisdiction and improper venue. Pedre attested it operated exclusively in a single office in NY and was without facilities or representatives in Washington D.C. The district court granted Pedre's motion and discharged the action for a lack of personal jurisdiction.

The case was appealed. The Federal Circuit reconsidered the issues surrounding general and specific jurisdiction:

> "*Specific jurisdiction 'arises out of' or 'relates to' the cause of action even if those contacts are 'isolated and sporadic.' . . . General jurisdiction arises when a defendant maintains 'continuous and systematic' contacts with the forum state even when the cause of action has no relation to those contacts*.

The court noted that they were "*left totally in the dark about the reasons for the district court's action.*" The dismissal was vacated. As a consequence, jurisdiction may be found under D.C.'s long-arm statute[140] in the event that Pedre's merchandise was offered for sale in DC. The court considered the extent that an interactive website would create jurisdiction but expressly determined not to decide that issue, leaving this matter open. In matters of Patient law, the process of selling over the Internet from a site not covered by Patient protections to one that the patient is protected could lead to legal action.

2 Child Pornography and Obscenity

Any work that depicts the sexual behaviour of children is classified as child pornography. The anonymity and ease of transfer provided through the Internet has created an international problem with child pornography[141]. The increasing

[140] Gibbons v Brown (1998) 1998 716 So. 2d 868; A car accident resulted following bad directions; the plaintiff sought to assert jurisdiction over non-resident on the grounds that the defendant had filed a lawsuit in the forum two years earlier stemming from the same incident (the plaintiff was not a party to that suit). The FL long arm-statute permitted jurisdiction over those "*engaged in substantial and not isolated activity*" within the state. It was held, bringing an action in the state two years earlier does not qualify as substantial activity, no personal jurisdiction. In the case of Dealing with a website (as was expressly not decided in Trintec Indus. v. Pedre Promotional Products) it is likely that a website would have to be shown to operate extensively or particularly target the location for jurisdiction to be applied. As an example, a site in the UK that operates a US page and sells product stating that they deliver to the US could be covered by the US long-arm statutes.

[141] The exploitation from child pornography can result in far reaching negative effects and suffering. Those concerned with the child pornography trade often entice problem or disabled children with pledges of pecuniary or other payments. Children who are sufferers of sexual exploitation may undergo lifelong depression, emotional dysfunction fear and anxiety.

pervasiveness of chat rooms, instant messaging (IM) and Web forums[142] has increased the potential for sexual abuse to occur against children. This use of chat rooms by paedophiles for the purposes of sexually abusing children by starting relationships with them online is widespread. This normally involves making friends with the child, beginning a stable rapport and then steadily exposing the children to pornography through means of images or videos that include sexually overt matter.

Additionally, the Internet has increased how readily available pornography is to children. The ability of children to view pornographic magazines, adult films and movies can be guarded making it difficult for children to obtain illicit materials. As many parents are less computer literate than their children, it is often difficult for them to stop pornography from being downloaded using the Internet by their children. Further, freely available pornographic publications in open areas such as newsagents are controlled through legislation and are only allowed to contain "s*oft*" pornography.

There are few restraints to publishing pornography on the Internet. In fact, "*hard-core*" pornography is legal within many countries. For example, Denmark[143] has legalised any category of pornography (except child pornography) allowing it to be produced, sold, displayed in cinemas to persons who are 16 years or older and published on the Internet. This includes extreme violence and bestiality. The availability of pornography from these jurisdictions aids in its distribution between school children. An immense amount of obscene matter concerning children is also available. *R v Smith* and *R v Jayson*[144] were heard jointly in the Court of Appeal. The Court addressed the matter as to what constitutes "*making a photograph or pseudo photograph*" for the purposes of s.1(1)(a) of the Protection of Children Act 1978. *Jayson* avowed that the act of willingly downloading an indecent image from the Internet to a computer screen represents "*making*." Similarly in *Smith* it was held that opening an e-mail attachment enclosing an indecent picture could comprise "*making*." The necessary *mens rea* in each case is that the performance of "*making*" need be a

[142] such as Facebook and chat rooms.

[143] Quimbo, Rodolfo Noel S (2003) "Legal Regulatory Issues in the Information Economy", e-ASEAN Task Force, UNDP-APDIP (MAY 2003); See also, JT03220432 (2007) "*Mobile Commerce*" DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY COMMITTEE ON CONSUMER POLICY DSTI/CP(2006)7/FINAL, 16-Jan-2007

[144] 2002 EWCA Crim 683 (No. 2001/00251/YI)

conscious operation with the awareness that the picture was, or was likely to be, "*an indecent photograph or pseudo-photograph of a child*". It was demonstrated that it is not necessary to prove an intention to store the image in order to fulfil the prerequisite of *mens rea*.

The Obscene Publications Act 1959[145] [the "1959 Act"] relates to media with the potential "*to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it*"[146]. The volumes of case law[147] that have defined obscenity have created a range of classifiers that when taken as a whole would be seen to have a propensity to deprave and corrupt the kind of individuals that have witnessed it. Due to their capability to be influenced, children face a greater peril. Print media based "*hard-core*" pornography can be limited whereas digital pornographic images on the Internet are readily available and require additional measures to restrict access. The Criminal Justice and Public Order Act 1994[148] [the "*1994 Act*"] was enacted to include the obscene images stored or broadcast as electronic data.

The 1959 Act defines the publication[149] or possession with the intention of publication for gain of an obscene item to be a criminal act. The additions to the law introduced by the 1994 Act connote that an ISP or ICP could face prosecution for the publication of obscene material introduced through an intermediary without consent as the 1959 Act does not require that the defendant had the intent to deprave or corrupt. If the ISP can argue that no examination of the offending media and no reasonable cause to suspect an obscenity existed, they have a defence to the charge. However, a notification and subsequent failure to act within a reasonable time would remove this protection. The wide-held knowledge of the types of materials being disseminated across the Internet would make the introduction of monitoring software prudent.

---

[145] Obscene Publications Act 1959, UK; see also Obscene Publications Act 1964, UK

[146] Ibid, S 1.1.

[147] Case law on obscenity predates the Internet and may be extrapolated from the large amount of case law concerning mail order pornographic material, video tapes and printed media.

[148] Criminal Justice and Public Order Act (UK) 1994 CHAPTER 33

[149] Publication includes of any variety of sale, distribution or performance.

More crucially, the Protection of Children Act 1978[150] (as revised by the 1994 Act) makes it a crime "*to take, or permit to be taken or to make, any indecent photograph or pseudo-photograph of a child*", "*to distribute or show such indecent photographs or pseudo-photographs*" or to hold "*possession such indecent photographs or pseudo-photographs*". The revisions of the 1994 Act extended the definitions to include any "*data stored on computer disk or by other electronic means which is capable of conversion into a photograph*" with the introduction of the expression "*pseudo-photograph*". The act also extends the definition of child to include any image where the principal sense derived from the image would lead one to believe that the picture is of a child, whether or not the person (or representation[151]) in the image was actually a child. The nature of the images must be "*indecent*"[152] to be included within the provisions of the 1978 Act. The danger for an ISP or ICP is that mere possession is all that is required to be prosecuted under this Act leaving it possible for both the content owner and the service provider to be jointly charged. Child pornography is also covered by the Criminal Justice Act 1988[153]. The possession of an indecent photo of a child is an offence under the act which is also amended by the 1994 Act.

Under the Telecommunications Act 1984[154] it is an offence to transmit any communication of a grossly offensive, indecent, obscene or menacing character through means of a telephone from the UK. As the definition of communication includes data transmissions sent by modem Internet transmissions are also included. An Internet service provider would not be expected to be effected by this Act as it is aimed at the instigator of the message containing the illicit material. However, the increasing use of VoIP[155] and the associated capability to record and replay communications could place a service provider at risk it they came to know about an illicit transmission and did not act to mitigate it.

---

[150] The Protection of Children Act 1978 (UK).

[151] The Act includes computer-generated and manipulated images and if these are significantly similar to the image of a child such that they are likely to be taken to be a child shall be treated as such.

[152] Indecent is different from obscene. Indecency occurs at a reduced level of offensiveness than obscenity. In particular where children are involved a lower standard of offensiveness will be required.

[153] The Criminal Justice Act 1988 (UK).

[154] The Telecommunications Act 1984 (UK).

[155] Voice over IP.

The Indecent Displays Act[156] added the offence of publicly displaying indecent material. The individual who creates an indecent display as well as somebody who causes or permits such a display can be held guilty of an offence. Display is defined under the act to be visible from any public place including free Internet transmission. Section 1(3) states that the requirement of a payment to access the material means that such a site is not on public display. Thus a pay for view pornographic website is not covered by the Act. The Act applies to both individuals and organisations.

The Sexual Offence (Conspiracy and Incitement) Act[157] made it an offence to conspire or incite others in the UK to perform sexual offences outside of the UK. Under this Act, the foreign poster of an Internet communication comprising an incitement under the act could be prosecuted in the UK. A service provider or other organisation with knowledge of such a transmission who subsequently fails to act could face both criminal and civil action.

The US Congress tried to address the problem of the ease of access to this type of material by children through the Telecommunications Act of 1996. Title V of the act (commonly known as the Communications Decency Act, CDA) included provisions with the intent to regulate the dissemination on the Internet of material deemed to be inappropriate to minors. Shortly afterwards however, the Supreme Court struck down sections 223 (a) and (d) in *Reno v. American Civil Liberties Union*[158] result of these and subsequent cases is that there is no clear "*community standard*" which defines obscenity. In cases such as child pornography, this is being clearly held not to be expression protected by the First Amendment. The Internet has provided offenders with greater access to obscene materials and even aids in the solicitation of children by paedophiles.

---

[156] The Indecent Displays (Control) Act 1981. The aim of the Act is to make fresh provision with respect to the public display of indecent matter and to this end a number of existing statutes dealing with indecent public display. These are replaced by a new offence in section 1 of the Act of publicly displaying indecent matter.

[157] Sexual Offences (Conspiracy and Incitement) Act 1996 (UK). See also Sexual Offences (Conspiracy and Incitement) Act 1996, Sex Offenders Act 1997, Criminal Justice (Terrorism and Conspiracy) Act 1998, Sexual Offences Act 1956.

[158] 521 U.S. 844 (1997).

The issue of free speech protections in the US does not preclude being prosecuted in a jurisdiction with extremely stringent standards (such as China) for matter that would not be deemed offensive in its homeland. This would be of greatest concern to the most significant service providers that have multinational operations and thus may face International actions[159].

An alternative option to limit child pornography over the Internet is to target payment intermediaries. These organizations allow it to remain profitable to sell child pornography across the internet. Even though a great quantity of pornography is distributed through non-commercial transactions[160], commercial sites are a key supplier of child pornography over the internet. The commercial sources of a great deal of child pornography could be curtailed by targeting payment intermediaries. As commercial pornographic distributors commonly oblige credit card processing and necessitate this information to be held in a database for processing before granting access the service, the credit card both ensures payment for the service and authenticates the client's age. This approach thwarts many of the issues a site could be exposed to if it permitted minors to access pornographic material.[161] Thus access to credit card processing is vital to the operation of a commercial website offering pornography[162].

159 Yahoo in 2000 lost a case brought by the French Government seeking a ruling to prevent people in France gaining access to websites offering Nazi memorabilia. Yahoo France does not carry the auctions but French internet users can access the company's US site at the click of a mouse. Judge Jean-Jacques Gomez confirmed a ruling that he first issued on May 22 ordering Yahoo to prevent people in France from accessing English-language sites that auction Nazi books, daggers, SS badges and uniforms.

160. Williams, Katherine S. (2003; File-Sharing Programs: Child Pornography is Readily Accessible over Peer-to-Peer Networks, Testimony Before the Comm. on Gov. Reform, House of Reps. (Statement of Linda D. Koontz, Mar. 13, 2003), available at http://www.gao.gov/new.items/d03537t.pdf at 5 (Stating that Usenet groups and peer-to-peer networks are the principal channels of distribution of child pornography).

161.Pornography websites were channelled into the use of credit cards to verify age in part by the affirmative defence offered by §231 of the Communications Decency Act. 47 U.S.C. §231(c)(1)(A) ("It is an affirmative defence to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors by requiring use of a credit card, debit account . . . .").

162.See id. at 5–6 (Concerning a child pornography ring that included websites operating from Russia and Indonesia (content malfeasors located out of US jurisdiction) and a Texas-based firm that supplied the credit card billing and access service for the sites.

3. Electronic Espionage

The UK differs from the United States with its efforts at codification through the Restatement and Uniform Trade Secrets Act[163] to introduce a legislative set of controls preventing electronic espionage. The English law as it relates to a breach of confidential information is exclusively derived from the common law as it has evolved through the cases. A duty of confidence arises when confidential information comes to the knowledge of a n individual in circumstances where it would be unfair were that information to be divulged to another. This could be a result of the receiver of the information being on notice, or having an agreement, that the information was to be so handled. A breach of confidence is the contravention of a duty which can result in a civil action[164]. Breach of confidence will regularly occur in association with the disclosure of data with a commercial value. It can also comprise of personal information regarding individuals.

Breach of confidence is complex. It enlarges to "*reflect changes in society, technology and business practice*"[165]. Furthermore, Art. 8 of the European Convention on Human Rights (concerning the right to privacy) have expanded the available actions connected with a breach of confidence to include safeguarding against the misuse of private information[166]. Under English law, it is required that the plaintiff proves three things in order to succeed in an action for a breach of confidence:

1. the information must be confidential, but does not apply to information which is trivial[167];

163 The Restatement and Uniform Trade Secrets Act (1985) USA. "In view of the substantial number of patents that are invalidated by the courts, many businesses now elect to protect commercially valuable information through reliance upon the state law of trade secret protection. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974), which establishes that neither the Patent Clause of the United States Constitution nor the federal patent laws pre-empt state trade secret protection for patentable or unpatentable information, may well have increased the extent of this reliance".

164 Lord Nicholls in Campbell v MGN Ltd [2004] A.C.457 at 464-5 summarised the law of confidence as "[the imposition] of a duty of confidence whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential"

165 Douglas v Hello! Ltd [2001] QB 967, per Keene LJ.

166 Campbell v MGN Ltd [2004] A.C.457

167 Faccenda Chicken Ltd v Fowler [1987] Ch. 117

2. the information was provided in circumstances importing an obligation of confidence;

3. there must be an unauthorised use or disclosure of the information, and, at least, the risk of damage[168].

The jurisdictional basis in English law of the action for breach of confidence is unclear. The foundation most regularly relied upon is contract[169]. Frequently the parties will have incorporated express terms relating to confidentiality, but the courts have also commonly acted on the basis of an implied confidentiality provision in an existing contractual relationship. The courts have also created an equitable obligation of confidentiality autonomous of any contractual relationship. This obligation applies to the initial beneficiary of the information, and to third parties who receive unauthorised disclosures of confidential information. This has also been used in addition to a contractual obligation, and at times in substitution for a contractual obligation.

The duty that confidence should be preserved may be outweighed by a variety of other civic causes. These call for disclosure in the public interest. Either the world at large or the appropriate authorities should be informed. It is generally necessary for a court to seek equilibrium for the protection of the public interest. This balance is judged in placing confidentiality against a use or disclosure that favours society and creates quantifiable gains[170]. Disclosure of confidential information will not be reserved where there is a '*just cause or excuse for disclosing it*'[171].

An ISP or ICP needs to consider both the need to protect data against the needs of data protection and that of the public interest. A failure to safeguard the

---

[168] Coco –v- AN Clark (Engineers) Ltd. [1969] RPC 41; Murray –v- Yorkshire Fund Managers Ltd [1968] 1 WLR 951. See generally Clerk & Lindsell on Torts, 19th edition (2006), Chapter 28, paragraphs 28-01 and 28-02

[169] The formation of electronic contracts subsists as a subset of all contractual formation. By their very nature and as it is expressed in a large number of contractual disputes which occur every year without dispute as to the content of the contract, contracts are uncertain. Thus it must logically follow that there will always remain a level of uncertainty in electronic contract formation. At best, if all uncertainty associated with the electronic nature of a contract was removed leaving no dispute between the natures of formation whether written, verbal or electronic; there remains room for uncertainty.

[170] Attorney General v Observer Ltd. and Others (on appeal from Attorney General v Guardian Newspapers (No.2)) [1990] 1 AC 109, see especially pages 281 B-H and 282 A-F, per Lord Goff of Chieveley. See: Clerk and Lindsell on Torts, 19th Edition (2006), Chapter 28, paragraph 28-05

[171] Malone v Metropolitan Police Commissioner [1979] 2 WLR 700 at 716, per Sir Robert Megarry V-C and see also W v Edgell [1990] Ch. 389; and R v Crozier [1991] Crim LR 138, CA.

interests of their clients places the intermediary in damage of civil actions. This issue is a particular concern for ICPs (who have some obligation unless explicitly excluded in contract) and particularly service providers specialising in the provision of security services. These providers are contracted to ensure that the security of their clients is maintained and are open to actions in both contract and negligence if they fail in their duties.

One of the greatest difficulties arises as an ISP or content hosting operator will clearly not be in a contractual relationship with the owner of the confidential information. The equitable doctrine, imposing an obligation of confidentiality in respect of information which the recipient knows or ought to have known to be confidential, and further which was proffered under circumstances implying confidentiality may be appropriate in selected circumstances. Nevertheless, it is clear that there remains a substantial dilemma for the plaintiff in proving that such an obligation exists. This would be predominantly true where an ISP or ICP declares unawareness of what content was on the site.

Data Protection

In December 2000, the *Privacy Amendment (Private Sector) Act 2000*[172] modified the *Privacy Act*[173] in Australia making it apply to various private sector organisations. The Australian legislation was updated to reflect the EU[174] and is based on the Organisation for Economic Cooperation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). The National Privacy Principles[175] (the NPPs) in the *Privacy Act* detail the methods that the private sector should use to "*collect, use, keep secure and disclose personal information*".[176]

---

[172] This Act came into effect from 21 December 2001.

[173] Australia has an informational privacy regime at the federal level based on the Privacy Act 1988 which initially applied mainly to Commonwealth and ACT Government public sector agencies.

[174] European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[175] The National Privacy Principles are extracted from the compilation of Act No. 155 of 2000 Act No. 119 of 1988 that was prepared on 10 January 2001

[176] The Australian Office of the Privacy Commissioner has released "INFORMATION SHEET 2 -2001 Preparing for 21 December 2001" which is available from http://www.privacy.gov.au/publications/IS2_01.doc

These principles provide individuals with a statutory right to discern the extent of information held concerning them by an organisation. It further introduces a right to correct information that is incorrect. An ISP or ICH in Australia would be covered by the amended Privacy Act. The State and Territory privacy legislation also needs to be considered.[177] Likewise, an ISP or ICP in the UK would be covered under the principles laid out in European Union Directive 95/46/EC.

An ISP or ICH that hosts sites for other parties could be held liable if they fail to maintain a reasonable level of system security and a breach of this leads to a compromise of an individuals private data.

Criminally, the UK has no legislation specifically focussed to dishonest acquisition of pure information[178]. The law holds that information is not property capable of being stolen such as was decided in *Oxford v Moss*[179], where a university student broke into the Examination Committee's premises, studied and made a copy of the exam paper and departed, leaving the original exam paper behind. The student's actions were held not to be theft[180].

In the event that improperly obtained credit card numbers are published on a website facilitating the enacting of fraudulent purchases using those card numbers, if the intermediary operator knows or ought to known of this action, liability may exist. It is possible that the ISP or ICP could also be a secondary participant in the crime[181]. There is also the possibility of a charge of conspiracy, if the necessary agreement

---

[177] See further, The Office of the Federal Privacy Commissioner, Privacy in Australia <http://www.privacy.gov.au/publications/pia1.html>

[178] There have been a number of cases in the United States, which involve the publication of stolen proprietary information. For example, United State v Riggs and Neidorf, 741 F.Supp.556 (N.D II 1990), the defendants had between them hacked into a Bell Telephone Company computer, obtained highly confidential information about that computer company's emergency telephone number system, and had published it in a magazine. They were prosecuted under the 1986 Computer Fraud and Abuse Act, and also under federal statutes dealing with wire fraud and interstate transfer of stolen property.

[179] (1978) 68 Cr. App. R. 183

[180] In the UK, placing stolen Government confidential information on a bulletin board is likely to fall foul of the Official Secrets Act. However, catching the culprit is the main problem; the UK Government has been unable to prevent Sinn Fein putting information about police and army facilities and security on its Web page based in Texas.

[181] US Cases involve Defense Department information (United States-v-Morrison, 859 F.2d.151 (4th Circuit 1988)), law enforcement record (United States-v-Girard, (2nd Circuit 1979)), banking information (United States-v-Cherif, 943 F.2d.692 (7th Circuit 1991)) and stock market information (Carpenter-v-United States, 484 U.S. 19(1987). Besides these federal statutes, which only apply where there has been a transfer across State lines, a number of States have laws, which make criminal the theft of confidential information.

between the intermediary and subscriber could be demonstrated (such as through a contract to not conduct standard checks).

Criminal liability may occur in instances where the subscriber of an ICP publishes passwords allowing unauthorised entry into a computer system. The intermediary may be liable for an offence under the Computer Misuse Act[182] that is committed using those passwords. The precise nature of any liability will be dependant on the facts of the case. In the event that the intermediary had advertised to a category of persons who are expected to execute an attack against a computer system using those passwords made available on the web server, this could amount to incitement to commit an offence under the Computer Misuse Act[183]. To establish incitement, it must be demonstrated that the defendant knew or believed that the individual so incited had the required *mens rea* to commit the offence. As the *mens rea* for an offence under Section 1 of the Computer Misuse Act is simply that the defendant intends to gain access to a computer system and knows that such access is not authorised it should be a simple fact to establish.

Alternatively the intermediary could be charged with aiding, abetting, counselling or procuring commission of an offence. In all cases, the defendant must have the intention to do the acts which he knows to be capable of assisting or encouraging the commission of a crime, but does not actually need to have the intent that such crime be committed. There must be a causal link for procurement, aiding requires support but not consensus nor causation, while abetting and counselling necessitate consensus but not causation.

4. Hate Crimes, Defamation and the things we say

Contempt of Court

The global character of the Internet poses hurdles protecting judicial proceedings. A foreign national may publish substance with a prejudicial nature, or may be present at a hearing subject to reporting limitations and subsequent to

[182] Computer Misuse Act (1990) UK

[183] In a case involving police radar detectors, it was held that advertising an article for sale, representing its virtue to be that it may be used to do an act which is an offence, is an incitement to commit that offence-even if the advertisement is accompanied by a warning that the act is an offence.

returning to a foreign country, publish a report on the case[184]. In this event, the authorities may proceed against a UK based Internet service provider through whose service the contempt is published.

Inciting Racial Hatred

The Public Order Act[185] created explicit offences in respect of racial hatred. The provisions detailed in sections 19 and 21 of the Act relate to actions that may be completed using the Internet. It has been made an offence under Section 19 for an individual to publish or distribute intimidating, abusive or insulting printed material in order to either to inflame racial hatred or where the conditions make it likely that the material is expected to provoke racial hatred. Section 21 of the Act makes the distributing, showing or playing to the public or a section of the public a recording of visual images or sounds to the same effect an offence. There may be an offence under section 18 of the Act for displaying written material fulfilling the stipulations of the Act. In the event that material detailed by section 19 is merely displayed and not downloaded, there is no offence when the material is viewed inside a private dwelling and people in that or another home only view it. An offence under section 23 encompasses the mere possession of racially inflammatory material if there is an intention to display it in public.

These offences may apply to Internet intermediaries in a variety of possible ways. An e-mail message sent between two individuals containing racially inflammatory material could be stored (possession), forwarded or otherwise published by the ISP/ICP. Without further publication, there would be no offence under sections 19 and 21 as these sections both require public display or distribution. If either party is not in a private home then there could be an offence under section 18, and if the sender intends the receiver to then publish the material both parties have committed an offence under section 23. The Intermediary could also be attributed to this offence

[184] R v ROSEMARY PAULINE WEST 1996 LTL C0004000; where reporting restrictions were not lifted, but a transcript of the committal hearing was put on the Internet in the US.

[185] Public Order Act 1986 UK

if a number of scenarios occur. If the e-mail is published by the ISP/ICP as a part of an e-mail list service[186], then the e-mail would be published under the Act.

A communication published to a Usenet site containing racially inflammatory content or a Website containing racially inflammatory material is each a public publication. The individual who distributed or published the communication or Web page will have committed an offence. The liability of an intermediary is dependant based on its operation. A defence is provided by sections 19 and 21 (3). These allow an intermediary that did not intend to inflame racial hatred to provide evidence that the organisation was not conscious of the nature of the material or recording. It is also required that the ISP/ICP had neither suspicions nor any grounds to infer any material it hosted was intimidating, abusive or insulting. A web page or a Usenet group formed explicitly for the function of propagating racially inflammatory content will not be covered in these defences. For instance, the marketing of a monitoring service may constitute foreknowledge mitigating this statutory defence. The Act has provisos extending liability to corporate bodies or companies. Following a conviction, a court can order the forfeiture of any written material or recording associated with the offence. This provision could in effect shutdown an internet intermediary as the outcome of having systems seized could be an inability to service its other clients.

If the offending content is hosted in a different jurisdiction, legislation is not treated to have an extra-territorial consequence except when it has purposely declared this to be so. Legislation of this nature will be generally limited to specific aspects of international law. These areas will include hijacking or piracy. An action for common law incitement may be possible, but this is improbable due to the requirement to first start extradition proceedings. The difficulty of which reserves them for the most sombre criminal actions.

Defamation

The first claims in the UK of defamation using e-mail as a means of distribution occurred in the mid 1990's. In one, the Plaintiff alleged that the

[186] Many ISPs and ICPs offer list servers. These systems provide a shared e-mail service. In some instances, an ISP/ICP may also publish these e-mails to a web server for public display. This event would be seen as similar to publishing to a Usenet server as is defined below.

Defendant published a message using a computer system asserting that the Plaintiff had been sacked for incompetence. The case did not include the service provider as a defendant. In another case and more widely publicised case[187], a police officer on complaining to his local branch of a national supermarket chain about an allegedly bad joint of meat was dismayed to discover that the store had distributed an e-mail communication to other branches of the chain. The subject of the e-mail stated; "*Refund fraud -- urgent, urgent urgent*". He settled with the chain for a substantial sum as damages and an apology in open court from the supermarket management.

This issue has also occurred in the US. Litigation was started against CompuServe[188], an intermediary, as a result of assertions made in an electronic newsletter[189]. CompuServe successfully argued that its responsibility was comparable to that of a library or a book seller. In *Stratton-Oakmont, Inc. v Prodigy Service Co.*[190], the plaintiff asserted that a communication distributed by an unidentified third party on Prodigy's "*Money Talk*" anonymous feedback site damaged the plaintiff's IPO due to the libellous nature of the message. It was asserted that this resulted in a substantial loss.

Prodigy filed a motion for summary judgment. It asserted that the decision in CompuServe[191] applied making them the simple distributor of the communication and hence not liable for the substance of the message. The court determined that Prodigy was a publisher as they implemented editorial control over the contents of the "*Money Talk*" site. As the editors used screening software to eliminate offensive and obscene postings and used a moderator to manage the site, they could be held accountable for the posting of a defamatory statement. Prodigy settled but subsequently unsuccessfully attempted to vacate the judgment. The Communications Decency Act

---

[187] As reported in the UK Telegraph by Kathy Marks on the 20th Apr 95. The policeman is quoted: *"...If this had got out unchecked it could have done me serious professional harm. I am in a position of extreme trust and there has got to be no doubt...that I am 100 percent trustworthy*".

[188] Cubby v CompuServe, 776 F.Supp.135 (S.D.N.Y. 1991). Another case, this time involving AOL was that of Kenneth Zeran v America On-line Incorporated heard by the United States Court of Appeals for the 4th Circuit (No. 97-1523 which was decided in November 1997). This was a case against AOL for unreasonably delaying in removing defamatory messages. The Court in 1st Instance and the Court of Appeal found for AOL.

[189] Compuserve offered an electronic news service named "Rumorville". This was prepared and published by a third party and distributed over the CompuServe network.

[190] (NY Sup Ct May 24,1995)

[191] Ibid

(CDA)[192] was subsequently enacted in the US to present a defence to intermediaries that that screen or block offensive matter instigated by another. The CDA presents, *inter alia*, that the intermediary may not be determined to be the publisher of any matter presented by another. Further, an intermediary shall be liable for any deed engaged in "*good faith"* to limit the spread of "*obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable*" materials[193].

Users view the Internet as if it was a telephone service with no enduring record. E-mails frequently contain imprudent declarations and japes. These communications offer an evidential confirmation absent in a telephone exchange. Deleted e-mail can persist in a variety of locations and forms, including back-up tape or disk, on the ISP and may have been forwarded to any number of other people. Any of these are subject to disclosure in litigation[194].

Western Provident v Norwich Union[195] concerned a libel by e-mail. Communications exchanged within Norwich Union by its staff libellously concerned Western Provident's financial strength. The case settled at a cost of £450,000 in damages and costs. For electronic distributions, the moderators of bulletin boards and Internet service providers are implicated only if they exercise editorial control or otherwise know directly of a libellous communication. In G*odfrey v. Demon Internet*[196], Godfrey informed the ISP of the existence of a libellous communication on a site managed by Demon. Demon did not act to remove the communication for the period of two weeks that such communications were made available on the site. The court asserted that as soon as Demon was alerted to the communication they ought to have acted. It was held that:

---

[192] Communications Decency Act

[193] The was first made to include those postings even when that material is protected under the US Constitution. This has been subsequently amended.

[194] The EU Electronic Commerce Directive (No. 2000/31/EC) has now specifically limited the liability of an ISP to where it has been informed of a defamatory posting and has failed to remove it promptly as was the situation in Demon Internet. Lawrence Godfrey v Demon Internet Limited (unreported Queens Bench Division - 26th March, 1999)

[195] Western Provident v. Norwich Union (The Times Law Report, 1997).

[196] Godfrey v Demon Internet Ltd, QBD, [1999] 4 All ER 342, [2000] 3 WLR 1020; [2001] QB 201; Byrne v Deane [1937] 2 All ER 204 was stated to apply.

> "*The transmission of a defamatory posting from the storage of a news server constituted a publication of that posting to any subscriber who accessed the newsgroup containing that posting. Such a situation was analogous to that of a bookseller who sold a book defamatory of a plaintiff, to that of a circulating library which provided books to subscribers and to that of distributors. Thus in the instant case D Ltd was not merely the owner of an electronic device through which postings had been transmitted, but rather had published the posting whenever one of its subscribers accessed the newsgroup and saw that posting*".[197]

Shevill v Presse Alliance[198] established that in the European Union where an international libel is committed, an action for libel may be initiated against the publisher. This may be commenced either in the country that the publisher is based or in any other country where the publication was disseminated and where the Plaintiff had experienced damaged reputation. There is little reason to doubt that principles applicable to libel through the press will apply equally to computer libel.

Australian defamation laws are complicated by a state based nature in that they differ across each jurisdiction in content and available defences. Various Australian state laws include offence provisions for both civil defamation and criminal defamation. Civil liability transpires as a consequence of publications that are expected to harm a person's reputation and the penalties are monetary. Criminal liability transpires as a consequence of publications that concern society, including those with a propensity to imperil the public peace, and penalties in the majority of jurisdictions incorporate incarceration. Significant distinctions exist between civil and criminal defamation law in relation to both liability and defences.

The Western Australian Supreme Court decided in *Rindos* v. *Hardwick*[199] that statements distributed in a discussion list can be defamatory and lead to an action. The court thought that it was inappropriate to apply the rules differently to the Internet

---

[197] Godfrey v Demon Internet Limited [1999] 4 All.E.R.342

[198] C.68/93

[199] Rindos v. Hardwicke No. 940164, March 25, 1994 (Supreme Ct. of West Australia) (Unreported); See also Gareth Sansom, Illegal and Offensive Content on the Information Highway (Ottawa: Industry Canada, 1995) <http://www.ic.gc.ca/info-highway/offensive/offens_e.rtf>.

from other means of communications. The court acknowledged the instigator's accountability for defamatory proclamations broadcast across a discussion group[200]. The matter of the liability of other participants on the list was not considered during the trial.

It is considered unlikely that an ISP would scrutinize all material presented across its network[201] and this may not be economically feasible[202]. Mann & Belzley address this through "*targeting specific types of misconduct with tailored legal regimes*"[203]. These regimes would leave the ISP responsible for the defamatory publications of its users where they have failed to take reasonable action to mitigate these infringements. The existing law in Australia leaves all parties considered to be a "publisher" liable[204]. Cases do exist[205] where ISPs have removed content proactively.

The common law defence of innocent dissemination exists in Australia. *Thompson v Australian Capital Television*[206] demonstrated this when Channel 7 asserted that transmission of a "*live*" show to the ACT retransmitted from Channel 9 NSW in effect placed it as a subordinate publisher that disseminated the material of the real publisher devoid of any material awareness or influence over the content of the show. They argued that this was analogous to a printer or newspaper vendor.

---

[200] Ibid, it was the decision of the court that no difference in the context of the Internet News groups and bulletin boards should be held to exist when compared to conventional media. Thus, any action against a publisher is valid in the context of the Internet to the same extent as it would be should the defamatory remark been published in say a newspaper.

[201] RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC., (RIAA) v. Verizon Internet Services, 351 F.3d 1229 (DC Cir. 2003); See also Godfrey v Demon Internet

[202] ; Further, in the US, the Digital Millennium Copyright Act's (DMCA's) "good faith" requirement may not require "due diligence" or affirmative considerations of whether the activity is protected under the fair-use doctrine. In contrast, FRCP 11 requires "best of the signer's knowledge, information and belief formed after reasonable inquiry, it is well grounded in fact and is warranted by existing law…". Additionally, with the DMCA, penalties attach only if the copyright owner "knowingly, materially" misrepresents an infringement, so the copyright owner is motivated to not carefully investigate a claim before seeking to enforce a DMCA right.

[203] Brown & Lehman (1995) (The paper considers the arguments to creating an exception to the general rule of vicarious liability in copyright infringement for ISPs and those that reject this approach), available at http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf.

[204] Thompson v Australian Capital Television, (1996) 71 ALJR 131

[205] See also "Google pulls anti-scientology links", March 21, 2002, Matt Loney & Evan Hansen , www.News.com, Cnet, http://news.com.com/2100-1023-865936.html; "Google Yanks Anti-Church Site", March 21, 2002, Declan McCullagh, Wired News, http://wired.com/news/politics/0,1283,51233,00.html; "Church v. Google How the Church of Scientology is forcing Google to censor its critics", John Hiler, Microcontent News, March 21, 2002, http://www.microcontentnews.com/articles/googlechurch.htm; Lawyers Keep Barney Pure, July 4, 2001, Declan McCullagh, Wired News, http://www.wired.com/news/digiwood/0,1412,44998,00.html.

[206] See Reidenberg, J (2004) "*States and Internet Enforcement"*, 1 UNIV. OTTAWA L. & TECH. J. 1

The High Court held that the defence of innocent dissemination is available to television broadcasts as well as printed works. In this instance it was held that the facts demonstrated Channel 7 maintained the capacity to direct and oversee the material it simulcasts. The show was broadcast as a live program through Channel 7's choice. They chose this format in full knowledge that a diffusion of the show would be next to instantaneous. The where further conscious of the nature of the show, a "*live-to-air current affairs programme*"[207] and understood that this program conceded an elevated risk of transmitting defamatory material. It was decided by the facts that Channel 7 was not a subordinate publisher on this occasion.

The Federal Broadcasting Services Act 1992[208] affords a legislative defence to an ISP or Internet Content Host (ICH) that transmits or hosts Internet based content in Australia if they can demonstrate that they were reasonably unaware of the defamatory publication. s.91(1) of Schedule 5 to the Broadcasting Services Act[209] grants that a law of a State or Territory, or a rule of common law or equity, has no effect to the extent to which the ISP "*was not aware of the nature of the internet content"*.

The BSA[210] defines "*internet content*" to exclude "*ordinary electronic mail*". This is a communication conveyed using a broadcasting service where the communication is not "*kept on a data storage device*". Consequently, the s.91 defence will not be offered in cases concerning such material. In such cases, an ISP or ICH may be still attempt to rely on the defence of innocent dissemination. The applicability of the common law defence of innocent dissemination remains to be

---

[207] Ibid.

[208] <http://scaleplus.law.gov.au/html/pasteact/0/136/top.htm>

[209] s.91(1) of Schedule 5 to the Broadcasting Services Act states:

(i) subjects, or would have the effect (whether direct or indirect) of subjecting, an internet content host/internet service provider to liability (whether criminal or civil) in respect of hosting/carrying particular internet content in a case where the host/provider was not aware of the nature of the internet content; or

(ii) requires, or would have the effect (whether direct or indirect) of requiring, an internet content host/internet service provider to monitor, make inquiries about, or keep records of, internet content hosted/carried by the host/provider.

[210] The Broadcasting Services Act specifically excludes e-mail, certain video and radio streaming, voice telephony and discourages ISP's and ICH's from monitoring content by the nature of the defense. See also, Eisenberg J, 'Safely out of site: the impact of the new online content legislation on defamation law' (2000) 23 UNSW Law Journal; Collins M, 'Liability of internet intermediaries in Australian defamation law' (2000) Media & Arts Law Review 209.

determined by the Australian courts.[211] As a consequence, any reliance on these provisions by an ISP or ICHs carries a measure of risk.

Harassment

Harassment may occur through all forms of media, the Internet is no exception. Junk mail, sexually offensive e-mails and threats delivered through online means (including both e-mail and instant messaging) are all forms of harassment. The inappropriate accessing of sexually explicit, racist or otherwise offensive material at the workplace is another form of harassment. This includes the sending of unwelcome messages that may contain offensive material to another co-worker.

E-mail Crimes and Violations

In reality, e-mail crime is not new. Instead, the Internet has enabled many old crimes to be reborn. Many morally violating acts such as child pornography have become far more widespread and simpler due to the ease and reach of e-mail. Many traditional crimes such as threats and harassment, blackmail, fraud and criminal defamation have not changed in essence, but the ease of e-mail has made them more prevalent.

Chain letter

Chain letters are another form of abuse that are seamlessly migrated from the physical world to cyberspace. A chain letter is an e-mail that was sent progressively from e-mail user to e-mail user. It will generally instruct the recipient to circulate further copies of the e-mail and usually to multiple recipients. These chain letters often promise rewards or spiritual gain if the e-mail was sent and may also threaten loss or harm if the recipient does not forward it. Often the authenticity of a chain letter cannot be verified as the header information from the original sender has been lost in retransmission.

[211] See also EFA, Defamation Laws & the Internet <http://www.efa.org.au/Issues/Censor/defamation.html>

Spamming

Spamming can be defined as sending unsolicited commercial e-mails (UCE). The more common term for spam is junk mail. Spammers obtain e-mail addresses by harvesting them from Usenet, bots, postings, DNS listings, and/or Web pages.

Spammers are smart, determined criminals, with a broad understanding of technology. They are willing to do anything to get access to mailing lists, vulnerable servers, and insecure routers. Spammers use their brains and well-crafted tools to make money and remain anonymous.

Spam is generally sent to a large number of e-mail addresses simultaneously. The sending address in the e-mail is generally forged allowing spammers to hide their identity. The From and Reply To fields in an Internet e-mail header allow the spammer to provide false or otherwise misleading information designed to entice the recipient into opening the e-mail. An ISP that fails to take adequate care in securing their systems and consequently is used as a spam relay site would in risk of an action for negligence.

Mail bombing

Mail bombing is a simple attack that has been around for a long time. It involves the intentional sending of multiple copies of an e-mail to a recipient. The objective is simply to overload the e-mail server. This is achieved by either filling the user's inbox so that they cannot access any more mail or flooding the server connections. Flooding server connection would be aimed at the general infrastructure whereas flooding an inbox is aimed at an individual. Mail bombing is malicious and abusive. Even when aimed at an individual to prevent other users from accessing the mail server.

Mail storm

A mail storm is a condition that occurs when computers start communicating autonomously. This process results in a large volume of junk mail. This may happen innocently through the auto forwarding of e-mails when configured to a large number of mailing lists, through automated responses and by using multiple e-mail addresses. Additionally, malicious software including the Melissa and IloveYou viruses can

result in mail storms. Mail storms interfere with the usual communication of e-mail systems.

Identity Fraud

Identity theft is becoming more widespread due to the ease and profitability. This action involves the stealing of someone's identity for fraudulent financial gain. It is in effect a larceny. The sending of offers e-mails that are too good to be true, fake websites and other forms of phishing are all used to capture an identity. Many groups specialize in the capture of information and make financial games by selling this information to groups who will make illegitimate purchases or financial transactions.

5. Distributing a Virus or other Malware

The Internet allows an individual to either inadvertently or purposely disseminate malware (such as a virus) to other systems globally. The potential impact could encompass the "infection" or compromise of millions of hosts. This has occurred. A "*harmless experiment*" by Cornell University student Robert Morris involved the release onto the Internet of a type of malware called a "*worm*" that compromised over 6,000 computers and required millions of dollars worth of time to eradicate. As several "*non-public computers*" run by the US Government were damaged[212] , Morris was prosecuted under the US Computer Fraud and Abuse Act (CFAA). He was convicted notwithstanding his declaration that he had no malicious objective to cause damage.

It is probable that a service provider or content hosting entity will face a degree of liability dependant on intention. If malware is intentionally posted such as in the Morris' case, no uncertainty as to whether the conception and insertion of the malware was deliberate exists. Morris stated that he did not intend harm, but the fact remained that he intentionally created and released the worm. In the United States both Federal and State legislation has been introduced to deal with the intentional formation and release of malware.

[212] Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030; There is an obligation for prosecution under the CFAA that a non-public computer is damaged where the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information.

In the UK, the introduction of malware is covered by section 3 of the Computer Misuse Act[213]. The Act states that a crime is committed if a person "*does any act which causes an unauthorised modification of the contents of any computer"* and the perpetrator intends to "*cause a modification of the contents of any computer*" which may "*impair the operation of any computer*", "*prevent or hinder access to any program or data held in any computer*" or "*impair the operation of any such program or the reliability of any such data*". The deliberate introduction of any malware will meet any of these requirements by taking memory and processing from the system and feasibly damaging the system. It is also necessary for a successful prosecution to demonstrate a "*requisite knowledge".* This "*is knowledge that any modification he intends to cause is unauthorised*". With the volume of press coverage concerning the damage that can be caused by malware and the requirements for authorisation, it is highly unlikely that an accused party would be able to successfully argue ignorance as to authorisation.

Malware is generally distributed unintentionally subsequent to its initial creation. Thus an ICP or an ISP would not be found criminally liable under either the Computer Fraud and Abuse Act or the Computer Misuse Act for most cases of dissemination. For the majority of content providers on the Internet, there exists no contractual agreement with users browsing the majority of sites without any prospect of consideration. The consequence being that the only civil action that could succeed for the majority of Internet users would be a claim brought on negligence. Such a claim would have to overcome a number of difficulties even against the primary party who posted the malware let alone going after the ISP.

It would be necessary to demonstrate that the ISP is under a duty of care. The level of care that the provider would be expected to adhere to would be dependant on a number of factors and a matter for the courts to decide and could vary on the commerciality of the provider and the services provided. The standard of due care could lie between a superficial inspection through to a requirement that all software is validated using up-to-date anti-virus software on regular intervals with the court deciding dependant on the facts of the initial case that comes before the courts. The

[213] Computer Misuse Act 1990 (c. 18), 1990 CHAPTER 18

duty of care is likely to be most stringently held in cases where there is a requirement for the site to maintain a minimum standard of care, such as in the case of a payment provider that processes credit cards. Such a provider is contractually required to adhere to the PCI-DSS as maintained by the major credit card companies[214] and would consequently have a greater hurdle in demonstrating that they where not negligent in not maintaining an active anti-virus programme.

Loss of an entirely economic nature cannot be recovered through an action for negligence under UK law. There is a requirement that some kind of "*physical*" damage has occurred. The CIH or Chernobyl virus was known to overwrite hard-drive sectors or BIOS. This could in some cases render the motherboard of the host corrupt and unusable. In this instance the resultant damage is clearly physical; however, as in the majority of Internet worms[215], most impact is economic in effect. Further, it remains undecided as to whether damage to software or records and even the subsequent recovery would be deemed as a purely economic loss by the courts.

It may be possible to initiate a claim using the Consumer Protection Act[216] in the UK and the directives that are enforced within the EU[217]. The advantage to this approach is that the act does not base liability on fault. It relies on causation instead of negligence in determining the principal measure of liability. The act rather imposes liability on the "*producer*" of a "*product*". A "*producer*" under the act includes the classification of importer, but this definition would only be likely to extend to the person responsible for the contaminated software such as the producer or programmer. It also remains arguable as to whether software transmitted electronically forms a "*product*" as defined under the act.

---

[214] The PCI-DSS at section 5 requires that "Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software."

[215] Scandariato, R.; Knight, J.C. (2004) "*The design and evaluation of a defense system for Internet worms*" Proceedings of the 23rd IEEE International Symposium on Reliable Distributed Systems, 2004. Volume, Issue, 18-20 Oct. 2004 Page(s): 164 - 173

[216] The Consumer Protection Act 1987 (Product Liability) (Modification) Order 2000 (Statutory Instrument 2000 No. 2771)

[217] See also, Electronic Commerce (EC Directive) Regulations 2002, SI 2000/2013 and the provisions of the Product Liability Directive (85/374/EEC)

B. Breaches to Security and Privacy

"*If a security breach is attributable to a failure by a company to take reasonable steps to implement a robust e-security architecture, shareholders may ask questions. They may want to know what steps (if any) the directors took to prevent the breach of network security. After all, directors have a duty to exercise fiduciary care*[218] *and due diligence*[219] *in the protection of corporate assets and minimisation of loss*". For that reason, to comply with their obligations, directors must ensure that suitable measures are taken to protect the company's information systems and the data on those systems. This is only incensed when the company also maintains data belonging to another party such as in the case of an ICP.

Privacy

Privacy is a critical component of the EU data protection regime[220] with non-compliance being likely to lead to a variety of breaches both locally in the UK and Internationally. [221] The security principle of the Data protection Act[222] "*requires that appropriate measures (technical and organisational) must be taken by data controllers against unauthorised or unlawful access to personal data and against accidental loss or destruction of personal data. It has significant application in an FE or HE e-learning environment. Since an e-learning system may include data such as student details, a student's submitted work and academic results; this principle makes it vital that such data are securely maintained*".

---

[218] Hospital Products Ltd v United States Surgical Corp (1984) 156 CLR 41 at 96

[219] UK; Section 180 of the Corporations Act 2001 (Australia, Commonwealth): "A director or other officer of a corporation must exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise"

[220] See: Walden "Data Protection" in Reed and Angel (Eds.), Computer Law (5th Ed. 2003, Chapter 11); Oxford University Press; London, UK;

[221] The Privacy Amendment (Private Sector) Act 2000 ("Privacy Amendment Act") contains the provisions for ensuring privacy in Australia. Also see the Directive 95/46/EC (Data Protection Directive); The Irish Data Protection Acts 1998 and 2003; Article 8 of the European Convention on Human Rights; The UK Regulation of Investigatory Powers Act 2000; US 'Safe Harbor' Rules; Employers' Data Protection Code of Practice; Model Contracts for Data Exports; The UK Interception of Communications (Lawful Business Practice) Regulations 2000; Electronic Communications Directive; The UK Anti-Terrorism, Crime & Security Act 2001; Directive 2002/58/EC (the E-Privacy Directive); and The UK Privacy & Electronic Communications (EC Directive) Regulations 2003.

[222] 1998, UK

Consequently, an organisation must take reasonable measures to protect the personal information it holds from misuse and loss, from unauthorised access, modification or disclosure. Protecting the security of personal information involves implementing reasonable steps to maintain: physical security, computer and network security, the security of communications and the appropriate training of staff. Information ought either be destroyed or de-identified when it is no longer needed for the purpose of collection, any permissible secondary purposes or for the purpose of meeting a legal requirement to retain the information. A security policy that deals with privacy issues is essential for an organisation that wants to avoid breaching the National Privacy Principles as it establishes strict systems to ensure that personal information held or processed by the organisation is not subject to unauthorised access or use. For instance, in an online environment, a policy would dictate that personal data would never be stored in the clear on a transaction server.

Organisations need to become aware of the massive reputation risks related to a breach of security associated with the disclosure of personal information. In 1995 Skeeve Stevens was convicted for breaking into AUSNet's network using the user account and password associated with one of AUSNet's technical directors[223]. He proceeded to alter home page of the company's and displayed a message that customer credit card information had been distributed over the internet. He subsequently published a number of credit card details belonging to selected individuals. Stevens was sentenced to three years imprisonment, with eighteen months non-parole. The intrusion resulted in only a minor direct financial loss. The reputation of AUSNet was materially damaged and the incident is alleged to have resulted in widespread loss of consumer and business confidence costing AUSnet more than $2 million in clients and contracts after the incident.

Any ICP needs to ensure that the data it maintains on its clients is secure, but additionally, in cases where it maintains some responsibility for the security and protection of client data; it also needs to ensure that this is adequately secured.

[223] *R v Stevens* [1999] NSWCCA 69 (15 April 1999).

Contract

Entities that have contractual relationships[224] with a company who suffers a breach of computer security may sue for breach of contract or under an indemnity clause if they incur loss or damage as a result. This is more likely to happen if a party has an express obligation in relation to electronic security and the breach of security could have been prevented if reasonable steps had been taken to secure the relevant systems. Any case involving an allegation of breach of contract will largely turn on interpretation and the incorporation of terms in the contract.

C. Prevention is the key

The vast majority of illicit activity and fraud committed across the Internet could be averted or lease curtailed if destination ISP and payment intermediaries implemented effective processes for monitoring and controlling access to, and use of, their networks. Denning (1999) expresses that, "*even if an offensive operation is not prevented, monitoring might detect it while it is in progress, allowing the possibility of aborting it before any serious damage is done and enabling a timely response*"[225].

As is being noted above, there are a wide variety of commonly accepted practices, standards and means of ensuring that systems are secured. Many of the current economic arguments used by Internet intermediaries are short-sighted to say the best. The growing awareness of remedies that may be attained through litigation coupled with greater calls for corporate responsibility[226] have placed an ever growing burden on organisations that fail to implement a culture of strong corporate governance. In the short term the economic effects of implementing sound monitoring and security controls may seem high, but when compared to the increasing volume of litigation that is starting to incorporate Internet intermediaries, the option of not securing a system and implement in monitoring begins to pale.

---

[224] A number of offer and acceptance issues that had not been completely resolved remain. The question of online software downloads generates its own difficulties. For instance, does the downloading of software constitute acceptance, installing the software, etc? Many software vendor licenses for instance state that the "loading of the software onto a computer indicates your acceptance of the following terms... " The terms of the agreement are likely to be enforceable if the software company is able to demonstrate that the user had an opportunity to view the terms prior to installing the software.

[225] Dorothy E. Denning, Information Warfare and Security, ACM Press, New York, 1999

226 See for instance Hazen (1977); Gagnon, Macklin & Simons (2003) and Slawotsky (2005)

The introduction of contractual fines through the PCI-DSS[227] will certainly curb the economic argument against enforcing controls at an Internet intermediary. With Visa and MasterCard set to issue fines of $25,000 (US) per day for noncompliant organisations, the cost of implementing monitoring controls starts to become insignificant, at least where payment systems are concerned. The added benefit of meeting corporate governance requirements and being able to argue that the organisation has provided at least a minimum due care implementation for its systems will also provide an added defence when facing certain tortuous claims. When the potential stipulations being sought through the "Creative Britain" strategy are added to this equation, the need for organisations, particularly Internet intermediaries, to implement secure systems and monitoring becomes essential.

227 Details of the PCI-DSS are available online at http://www.pcicouncil.org.

Conclusion

The Internet remains the wild, wild, web not because of a lack of laws, but rather the difficulty surrounding enforcement. The Internet's role is growing on a daily basis and has reached a point where it has become ubiquitous and an essential feature of daily life both from a personal perspective and due to its role in the international economy. The recently released "Creative Britain; new talents for the new economy"[228] framework paper has demonstrated a reversal of many of the positions formerly held by the British government. This new position is likely to require internet service providers to take action on illegal file sharing, as a consequence leaving intermediaries liable if they fail to take action.

If an ISP is to be held liable for authorisation as an intermediary, it must have knowledge, or otherwise deduce that infringements are proceeding.[229] Although, intermediaries commonly monitor their systems and have the means to suspect when infringements are occurring, Internet intermediaries also require the authority to prevent infringement if they are to be held liable for authorisation, a condition that entails an aspect of control.[230] The government's proposal[231] requires monitoring from the destination ISP places the responsibility firmly on the local provider of Internet services. Though this may seem unfair to many, as source ISPs may be located in any location in the world and can easily move when facing restrictions, holding the destination ISP responsible for monitoring content would appear as the only feasible solution as it is infeasible for the destination ISP to provide services within the UK from other locations.

It is clear that a framework similar to that proposed by Mann and Belzley[232] or by Lichtman & Posner[233] is needed to effectively control infringements over the

---

[228] Department for Culture, Media and Sport, 22 Feb 2008

[229] Ibid, Gibbs J at 12-13; cf Jacobs J at 21-2. See also Microsoft Corporation v Marks (1995) 33 IPR 15.

[230] Ibid, University of New South Wales v Moorhouse, supra, per Gibbs J at 12; WEA International Inc v Hanimex Corp Limited (1987) 10 IPR 349 at 362; Australasian Performing Right Association v Jain (1990) 18 IPR 663. See also Lim YF, 199-201; S Loughnan, See also BF Fitzgerald, "Internet Service Provider Liability" in Fitzgerald, A., Fitzgerald, B., Cook, P. & Cifuentes, C. (Eds.), Going Digital: Legal Issues for Electronic Commerce, Multimedia and the Internet, Prospect (1998) 153.

[231] Supra Note 97

[232] Mann, R. & Belzley, S (2005) "The Promise of the Internet Intermediary Liability" 47 William and Mary Law Review 1 <http://ssrn.com/abstract=696601> at 27 July 2007]

Internet and that such a solution is economically the most effective solution. The proposed strategy of the British government[234] is unlikely to be popular at first. Recommendations for a French style system of three strikes[235] would require additional monitoring from the ISP and also introduce a possibility of infringing the customer's privacy rights[236]. The concurrence of privacy legislation and the need for additional controls will make the introduction of these initiatives interesting to say the least. The pirates are starting to replace the Cowboys changing the wild, wild, web to that of the proverbial high seas. The need for sensible legislation that will limit the increasing criminal activity while also considering the impacts on the law-abiding users of the internet is clear. The proposed strategy of the British government[237] offers great potentials, but will come down to the implementation as to whether these are successful. The Internet is entering its final stage of development, legislative control.

Anonymity and leaky international boundaries impede the prosecution of the primary malfeasors. Internet intermediaries, especially those that service end users are both easily identifiable and have many of their assets within the UK. The malfeasors require payment intermediaries to process their transactions. The "Creative Britain" strategy[238] has provided little in either incentive or regulation concerning these actors. Payment intermediaries have the technological competence to avert detrimental transactions at the lowest cost of any intermediary with the largest potential payback. Further, in many cases the largest effect on the Internet pirates is provided through economic means. As such, the legislation should be adapted to mandate internet intermediaries control illicit transactions and consequently protect the public interest. To do this effectively will require more than just a mandate that

---

[233] Lichtman & Posner (2004) "Holding Internet Service Providers Accountable"

[234] Supra Note 97.

[235] One of the current recommendations is based on the three-strikes policy began in France late last year. The violation of digital rights management or other similar infringements including provisions for Internet users that are caught distributing copyrighted files would require the ISP to send an e-mailed warning to the infringing user. The second offence would then have file-sharers face a temporary account suspension. On a third offence, they would be entirely cut off from the Internet. (See also http://arstechnica.com/news.ars/post/20080218-three-strikes-infringement-policy-may-be-headed-down-under.html).

[236] The UK Privacy & Electronic Communications (EC Directive) Regulations 2003 and Directive 2002/58/EC (the E-Privacy Directive) may create problems. The juxtaposition of privacy versus control creates a fine line that is easily crossed.

[237] Supra Note 97.

[238] Supra Note 97.

Internet intermediaries monitor illicit activity. It will be also necessary to regulate liability in order to protect Internet intermediaries from the actions that they are required to take in order to protect the Internet. The constant seesawing between policy positions that has occurred in respect of the Internet demonstrates that we have not achieved this yet.

The position of the British Government[239] with its recent moves to call Intermediaries to action in the formation of a voluntary body to stop Intellectual Property violations is a start to the reforms that are needed. The problem is well defined in this call for reform, however, the call for voluntary changes are unlikely to bring about the required changes. Intermediaries have the capability to stop many of the transgressions on the Internet now, but the previous lack of a clear direction and potential liability associated with action rather than inaction[240] remains insufficient to modify their behaviour. Even in the face of tortuous liability, the economic impact of inaction is unlikely to lead to change without a clear framework and the parallel legislation that will provide a defence for intermediaries who act to protect their clients and society.

[239] Supra Note 97.

[240] Supra 39; The fear of being seen as a publisher rather than mere conduit has resulted in many ISPs and ICPs to a state of inaction.

Bibliography

Books

Anderson, Carol; Butler, Carol; Kirch, Arti; McMahon, Daniel; Murtha, Rick & Parks, Lisa, (1997) "*Exploring Digital Cash*" Information Systems 204 – Fall 1997 UC Berkley

Bainbridge, D (2000) "*Introduction to Computer Law*" Longman/Pearson Education: Harlow

Dal Pont, G E, (2001) "*Law of Agency*" Butterworths.

Denning, Dorothy E. (1999) "*Information Warfare and Security*", ACM Press, New York

Fisher III, William W. (2004) "*Promises to Keep: Technology, Law, and the Future of Entertainment*" Stanford University Press'

Fischer, S & Hurley, A. (1995) "*Trade and Commerce - International Trade*", in Halsbury's Laws of Australia, Vol 27 Title 420.

Hallberg, Bruce A. (2005) "*Networking: a Beginner's Guide, 4/e*" McGraw-Hill Professional USA

Lim, Yee Fen (2002) "*Cyberspace Law, Commentaries and Materials*", Oxford University Press UK

Power, R., (2000) "*Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace",* Que Corporation, Indianapolis,, at p283-284

Reed, Chris (2004) "*Internet Law Text and Materials*", 2nd Edition, Cambridge University Press, UK

Schneier, B., (2000) "Secrets & Lies: Digital Security in a Networked World", John Wiley & Sons Inc, New York, 301-302.

Spar, D. (2001) "*Ruling the Waves: From the Compass to the Internet, a History of Business and Politics along the Technological Frontier*", Harvest Books (January 7, 2003)

Treitel, G.H. (2003) "*The Law of Contract*". 11th Edition, London: Sweet & Maxwell

University of London (2006) "Recent developments in Laws" Published by: University of London Press

Vaughan, Jane; Sewards, Tanya & Kelso, Ross (1997) "*The Law of Internet Commercial Transactions*", Centre for International Research on Communication and Information Technologies, Australia.

Walden (2003) "Data Protection" in Reed & Angel (Eds.), Computer Law (5th Ed. 2003, Chapter 11); Oxford University Press; London, UK

Articles, Discussion Papers and News Reports

Attorney-General's Discussion Paper, Australia (1997) "*Copyright and the Digital Agenda*", July 1997

Banerjee, Scott (2004) "*P2P Users Get More Elusive*", Billboard, July 31, 2004

Brown, RH & Lehman, BA (1995) "*INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS*", INFORMATION INFRASTRUCTURE TASK FORCE, "Intellectual Property and the NII", U.S. Patent and Trademark Office

Campbell, Roderick (2001), "*Consultant Motivated by Greed, Court Told*", Canberra Times, 24/04/2001

Dept. for Innovation Universities and Skills (2008) "*Creative Britain; new talents for the new economy*" (22nd Feb 2008) <http://www.culture.gov.uk/NR/rdonlyres/096CB847-5E32-4435-9C52-C4D293CDECFD/0/CEPFeb2008.pdf>

Gagnon, Georgette; Macklin, Audrey & Simons, Penelope (2003) "*Deconstructing Engagement, Corporate Self-Regulation in Conflict Zones – Implications for Human Rights and Canadian Public Policy*" A Strategic Joint Initiative of the Social Sciences and Humanities Research Council and the Law Commission of Canada

Grossman, Wendy M. (2005) "*Speed Traps"*, Inquirer (U.K.), Jan. 14, 2005

Hindo, B. & Sager, I., (2004) "*Music Pirates: Still on Board*", Business Week, Jan. 26, 2004, at 13.

JT03220432 (2007) "*Mobile Commerce*" DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY COMMITTEE ON CONSUMER POLICY DSTI/CP(2006)7/FINAL, 16-Jan-2007

Kane, Paul (2008) "*Senate Authorizes Broad Expansion of Surveillance Act*" Washington Post, Wednesday, February 13, 2008; A01

Quimbo, Rodolfo Noel S (2003) "*Legal Regulatory Issues in the Information Economy*", e-ASEAN Task Force, UNDP-APDIP (MAY 2003)

Rovnick, Naomi (2004) "*Herbies Helps Antigua in WTO Outsourcing Victory"*, Lawyer, April 5, 2004

Yaeger, Don, (2001), "*Bucking the Odds"*, Sports Illustrated, Jan. 8, 2001, at 26

Academic and Legal Journals

Barker, J. Cam, (2004) "*Grossly Excessive Penalties in the Battle Against Illegal File-Sharing: The Troubling Effects of Aggregating Minimum Statutory Damages for Copyright Infringement*", 83 Texas L. Rev. 525

Bick, Jonathan D., (1998) "*Why Should the Internet Be Any Different?*" 19 Pace L. Rev. 41, 63

Bowne, A (1997) "*Trade Marks and Copyright on the Internet*" 2 Media and Arts Law Review 135

Collins M, (2000) "*Liability of internet intermediaries in Australian defamation law*" Media & Arts Law Review 209

Cooney, K (1997) "*Liability for On-line Images: How an Ancient Right Protects the Latest in Net Functions*" 16 Communications Law Bulletin 5

Demott, Deborah A. (2003) "*When is a Principal Charged with an Agent's Knowledge*?" 13 Duke Journal of Comparative & International Law. 291

Eisenberg J, (2000) "*Safely out of site: the impact of the new online content legislation on defamation law*" UNSW Law Journal

Gilchrist, Simon (1998) "*Telstra v Apra –Implications for the Internet*" [1998] CTLR 16.

Hare, Christopher (2004) "*Identity Mistakes: A Missed Opportunity*?" The Modern Law Review, Volume 67 Page 993 - November 2004 Volume 67 Issue 6

Harmon, Amy (2003) "*Subpoenas Sent to File Sharers Prompt Anger and Remorse"*, N.Y. Times, July 28, 2003, at C1.

Hazen, Thomas L. (1977) "*Transfers of Corporate Control and Duties of Controlling Shareholders. Common Law, Tender Offers, Investment Companies. And a Proposal for Reform*" University of Pennsylvania Law Review, Vol. 125, No. 5 (May, 1977), pp. 1023-1067

Kao, A. (2005) "*RIAA v. Verizon: Applying the Subpoena Provision of the DMCA"*, 19 Berkeley Tech. L.J. 405, 408.

Kraakman, Reinier H. (1984) "***857** CORPORATE LIABILITY STRATEGIES AND THE COSTS OF LEGAL CONTROLS*", Yale Law Journal April, 1984 (93 Yale L.J. 857)

Landes, William & Lichtman, Douglas, (2003) "*Indirect Liability for Copyright Infringement: An Economic Perspective*", 16 HARV. J.L. & TECH. 395.

Lemley Mark A. & Reese, R. A., (2004) "*Reducing Digital Copyright Infringement without Restricting Innovation*", 56 STAN. L. REV. 1345.

Leroux, Olivier (2004) "*Legal admissibility of electronic evidence 1*", International Review of Law, Computers & Technology; Volume 18, Number 2 / July 2004; Pp 193-220

Lichtman, Douglas Gary & Posner, Eric A., (July 2004). "*Holding Internet Service Providers Accountable*". U Chicago Law & Economics, Olin Working Paper No. 217. Available at SSRN: http://ssrn.com/abstract=573502 or DOI: 10.2139/ssrn.573502 (viewed 15 Jan 2008)

Lim, YF, (1997) "*Internet Service Providers and Liability for Copyright Infringement through Authorisation*" 8 Australian Intellectual Property Law Journal 192.

Loughnan, S., (1997) "*Service Provider Liability for User Copyright Infringement on the Internet*" 8 Australian Intellectual Property Law Journal 18

MacMillian, Blakeney "*The Internet and Communications Carriers'* Copyright Liability" [1998] EIPR 52

Mann, Ronald J., (2004) "*Regulating Internet Payment Intermediaries"*, 82 Texas L. Rev. 681, 681

Mann, R. & Belzley, S (2005) "*The Promise of the Internet Intermediary Liability*" 47 William and Mary Law Review 1 <http://ssrn.com/abstract=696601> at 27 July 2007]

Olovsson, Tomas, (1992) "*A Structured Approach to Computer Security*", Department of Computer Engineering Chalmers University of Technology, Gothenburg SWEDEN, Technical Report No 122, 1992

Paynter, H & Foreman, R (1998) "*Liability of Internet Service Providers for Copyright Infringement*", University of NSW Law Journal, [1998] UNSWLJ 61

Quimbo, Rodolfo Noel S (2003) "Legal Regulatory Issues in the Information Economy", e-ASEAN Task Force, UNDP-APDIP (MAY 2003)

Reidenberg, J (2004) "States and Internet Enforcement", 1 UNIV. OTTAWA L. & TECH. J. 1

Scandariato, R.; Knight, J.C. (2004) "*The design and evaluation of a defense system for Internet worms*" Proceedings of the 23rd IEEE International Symposium on Reliable Distributed Systems, 2004. Volume, Issue, 18-20 Oct. 2004 Pp 164 - 173

Shapiro, Andrew L., (1998) "*Digital Middlemen and the Architecture of Electronic Commerce*", 24 OHIO N.U. L. REV. 795

Slawotsky, Joel (2005) "Doing Business around the World: Corporate Liability under the Alien Tort Claims Act" 2005 MICH. ST. L. REV. 1065

Smith, Russell. (2000) "*Confronting fraud in the digital age*", Presented at Fraud prevention and control conference, Gold Coast Australia 24-25 August 2000

Tickle, K. (1995) "*The Vicarious Liability of Electronic Bulletin Board Operators for the Copyright Infringement Occurring on Their Bulletin Boards*", 80 Iowa Law Review 391 at 397

Williams, K. S. (2003) "*Child Pornography and Regulation on the Internet in the United Kingdom: The Impact on Fundamental Rights and International Relations*", Child Abuse Review, Volume 14, Issue 6 , Pages 415 – 429 (Special Issue: New Technologies . Issue Edited by Bernard Gallagher). Published Online: 20 Dec 2005, John Wiley & Sons, Ltd.

Wu, Tim, (2003) "*When Code Isn't Law*", 89 Va. L. Rev. 679

Zittrain, Jonathan (2003) "*Internet Points of Control"*, 44 B.C. L. REV. 653

Websites

The Center for Internet Security < http://www.cisecurity.org/>, last viewed 26 Feb 2008

Costello-Dougherty, Malaika (2003) "*Tech Wars: P-to-P Friends, Foes Struggle*", PC World, Mar. 13, 2003, available at http://www.pcworld.com/news/article/0,aid,109816,00.asp (last visited Feb. 19, 2008)

Heise Security (2008) "*Code injection vulnerability in Adobe's Flash Media Server*" 13 February 2008, IT security news and services at heise Security UK, viewed online at http://www.heise-online.co.uk/security/Code-injection-vulnerability-in-Adobe-s-Flash-Media-Server--/news/110115 (last viewed on 19 Feb 2008)

Kirk, Jeremy (2008) "*Danish ISP prepares to fight Pirate Bay injunction Battle with music industry expected to draw considerable attention*" Computerworld, February 13, 2008; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9062482&source=rss_topic17 (last viewed on 19 Feb 2008)

PCI Council <https://www.pcisecuritystandards.org/> Last viewed 25 Feb 2008. Contains links to the PCI-DSS (V1.1)

SANS Institute < http://www.sans.org/> Last viewed 25 Feb 2008. "*SANS is the most trusted & by far the largest source for information security training, certification & research in the world.*"

United States General Accounting Office, (2002) "*Report GAO-03-89, Internet Gambling: An Overview of the Issues 52 (2002)*", *available at* http://www.gao.gov/new.items/d0389.pdf