Legal and Technical Issues Management Framework for Peer-to-Peer Networks

Elaine Lawrence[1], John Lawrence[2] and Gordana Culjak[3]

[1] University of Technology Sydney, Sydney, Australia, elaine@it.uts.edu.au
[2] King Street Chambers, Sydney, Australia, Johnlaw@bigpond.net.au
[3] University of Technology Sydney, Sydney, Australia, gordana@it.uts.edu.au

Abstract

In the area of electronic and mobile commerce there are unique legal risks as well as concerns that also apply to traditional businesses. This paper reviews the impact of peer-to-peer e-business models in a legal and technical context with a view to formulating technical and legal policy suggestions for technologists, scientists, managers and government policy makers. To assist in addressing the intractable nature of the problems the researchers have developed a preliminary Legal Issues Management Framework. Issues such as forensic auditing, technical diligence, lawful intercept and sovereign risk are canvassed as well as the threats to current e-business models. Various traditional laws have been successfully applied to electronic transactions and new laws (cyberlaws) have been devised to deal with the latest technologies. Practitioners of P2P businesses must be aware of legal requirements and the risks involved in doing business in cyberspace. The digital economy develops at e-speed but the law does not. This paper outlines the enormous technological advances that impact on P2P business models and illustrates, with international examples, the reactions from international and national legal communities.

Key words: e-commerce, intellectual property, sovereignty, forensic accounting,

1 Introduction

The arrival of Napster's implementation of Peer-to-Peer networking attracted enormous attention both from individuals who wished to share files and entities which did not want the wholesale, free sharing of music files. The major legal battle which led to the fall of Napster meant that peer-to-peer technology became *either glamorous or notorious, depending on which side of the copyright controversy you stand* [43]. Technology once again leapfrogged the issue with the advent of such software as Gnutella and Freenet. Napster imitators are now swapping music, movies, software, and any other content that can be condensed down to 1s and 0s. By November 2005 more than 140 million users had downloaded Morpheus [41] from StreamCast Networks, peer-to-peer file-sharing software, distributed at no cost to the user. In July 2005, Michael Weiss the CEO of Streamcast Morpheus stated: *We will continue our David vs. Goliath fight to prove that we operate 100% on the right side of the law* [41].

Such peer-to-peer systems, particularly Kazaa and Grokster, have been the subject of international law suits which have attracted a lot of media attention. A court in the Netherlands (March 2002) ruled that Kazaa as a file sharing network was not responsible for its users' piracy [8]. However in Australia in 2005 the court ruled that the downloading of Kazaa Media Desktop by users in Australia is not permitted, effectively ending its business in Australia. The court found that although the company, Sharman Networks, was not itself guilty of copyright infringement, it had "authorized" Kazaa users to illegally swap copyrighted songs. Sharman plans to appeal the decision. [42]

In April 2003, a United States federal judge ruled that companies providing peer-to-peer (P2P) file sharing esoftware could not be held liable for copyright infringement by users of the software [12], [34] (*MGM_v_Grokster*). Howver in June 2005, the Supreme Court unanimously moved to remand the MGM et. al. v. Grokster and StreamCast Networks, Inc. case back to the lower Federal Court, which previously had ruled in favor of file-sharing software. The ruling means that the trial Court has to look at the facts to see if StreamCast intended and encouraged Morpheus to be used to infringe on copyrights. Streamcast strongly denies this charge [41].

These P2P systems allow users worldwide access to a huge variety of information but with a level of privacy and security not possible in the present client-server architecture of the web [1]. Research has indicated that such P2P systems could lead to:

- degradation of system performance
- system vulnerability
- enormous pressure on copyright containment
- disputes about sovereign risk for countries and companies
- greater need for forensic auditing
- increased focus on legal risks and conflicts of interest
- threats to current e-business models.

Governments are seeking to control activities by using Lawful Intercept legislation and preparing e-business-appropriate regulations and laws to cover Internet based payment methods and new communication technologies, as is the case in the real world. The situation remains that, as fast as legal remedies appear, new technologies overtake the statutes.

This paper investigates, by examining cases, the interaction between e-technology and e-law. It firstly provides an overview of what is happening in the world of P2P networking and the law. Section 3 outlines the research methodology and the proposed legal Issues Management Framework, while the following sections deal with the legal and technical issues of P2P networking, intellectual property issues and jurisdiction. Finally the paper concludes by pointing the way to future research.

2 Overview

Traditional commercial transactions [23] are subject to a comprehensive system of controls consisting of the common law, legislation at state, national and international levels, and industry codes of practice. These controls have been established over time in an ad-hoc fashion in response to the need to provide a high degree of certainty in contractual relationships and to give the consumer confidence that he/she will obtain *a fair deal* in any spending decision. Both of these are necessary ingredients in the promotion of trade and commerce upon which modern economies depend. The controls have evolved and have been adapted to new technologies as they arise, although there is always a lag time before the controls "catch up" with the latest technology. Although international agreements do exist for the regulation of international trade, they are not keeping pace with commercial realities. The principal problem is that existing

agreements and even those proposed only deal with business or trade transactions. They do not deal with consumer purchases which are responsible for the growth in transactions over the Internet [11]. The European Community Convention on Law applicable to Contractual Obligations (the Rome Convention) provides for uniform rules about choice of law in contract in each of the member countries of the European Union [11] The cross border dimensions of many Internet transactions require not only that national regulations and practices be adapted to this new environment but also that international cooperation is necessary if fiscal sanctuaries are to be minimized [38]. In many P2P environments music and video file swapping does not involve the exchange of money even though the material is protected by copyright.

A recent court ruling has indicated that international publishers are no longer safe from potential litigation based on Australia's strong defamation laws. It ruled that material is published where *it is downloaded from the web, not where it is posted to the web* [3]. (See Table 1) In a P2P environment the proliferation of defamatory items would be impossible to contain and could entail a high number of legal actions in global jurisdictions.

Table 1 outlines recent examples of legal actions concerning the Internet, with particular reference to P2P cases.

Table 1: Legal Actions

Legal actions	**Outcomes**
Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242 (5 September 2005)	Kazaa to be shut down in Australia as it "authorized" users to illegally swap copyrighted songs (subject to appeal).
MGM v Grokster USA Supreme Court No 04-0480, 545 US (2005)	The Court said that Grokster had encouraged copyright infringement and could be sued, returning the matter to the lower court for judgement.
Taiwan office of IFPI v Taipei's largest P2P operator, Taipei District Court 9 September 2005	Company found guilty of copyright infringement and 3 executives given jail terms and a subscriber was sentenced to four months in jail for downloading 970 songs [9]
Sony, EMI, Universal v Sydney Melbourne Tasmania Universities, July 2003	The Music Industry was successful in gaining access to the Universities' computer systems for evidence relating to four students suspected of pirating music [29].
Recording Industry Association of America (RIAA) v four students for alleged copyright breaches (2003) and followed up with a further 261 cases	RIAA extracted fines of several thousand dollars from each as a warning to others [31].
Prosecution of Waddon in UK under Obscene Publications Act - 1999	Although pornography site set up on servers in USA, Waddon found guilty and sentenced to 18 months (suspended) as the court found that he had posted material on the web from his home in England [17].
Dow Jones & Company Inc v Gutnick [2002] HCA 56 (10 December 2002)	Australian defamation case – Ruling that material is published *where it is downloaded from the web, not where it is posted to the web. [*10]
Charges pending in Australia as a result of 228 arrests and summonses in Operation Auxin, the Australian arm of a world-wide investigation into the trafficking of online sex images	228 arrests and summonses in Operation Auxin [21]

3 Methodology

This paper follows on from previous studies on e-law and the technology of the digital economy undertaken by the researchers from 1997 –2003. These studies have been reported in a series of commercial publications [23], [24], [25], [26], [27]. The legal methodology is classical jurisprudence analysis which is the study of rules and regulations and case law to clarify these provisions which are recorded for the communication of generalizations. The resulting synthesis is then provided as a summary of the situation [7]. Table 1 sets out some of the major cases that have been studied by the authors. The identification of major global approaches to identifying and dealing with major legal and technical risks in P2P is considered to be essential in the ensuring that the development of the issues management framework will take the best of breed ideals into account.

The research domain for peer-to-peer e-business is particularly challenging, because of the lack of established definitions, and the high volatility of the phenomena [26]. Due to the present state of knowledge, a qualitative and exploratory research approach was used, especially in this area, when

theoretical propositions are few and field experience is limited. Exploratory research is useful for obtaining ideas for potential new strategies and opportunities. Because the purpose of focus discussions is to surface aspects, impacts and implications that are of concern, discussions were held with an international cross section of researchers, other lawyers, business persons, policy advisers and academics.

This research represents an exploratory study of the interaction between E-Technology and E-Law which is very much a new field. The legal and technical risks associated with P2P ebusiness models are considered to be of an intractable nature, along with other problems such as world health, universal education globalisation and overpopulation. The researchers contend that Globalisation, accelerated by the exponential expansion of the Internet is exposing serious flaws in the world's legal and risk management systems. Case research, literature reviews and the above mentioned discussions with legal and Internet experts led to the development of the following Legal Issues Management Framework to assist in addressing the intractable nature of the problems (see Figure 1). The authors' contention is that it is a dynamic framework that may be adapted to analyse similar intractable problems relating to new technologies and the law.

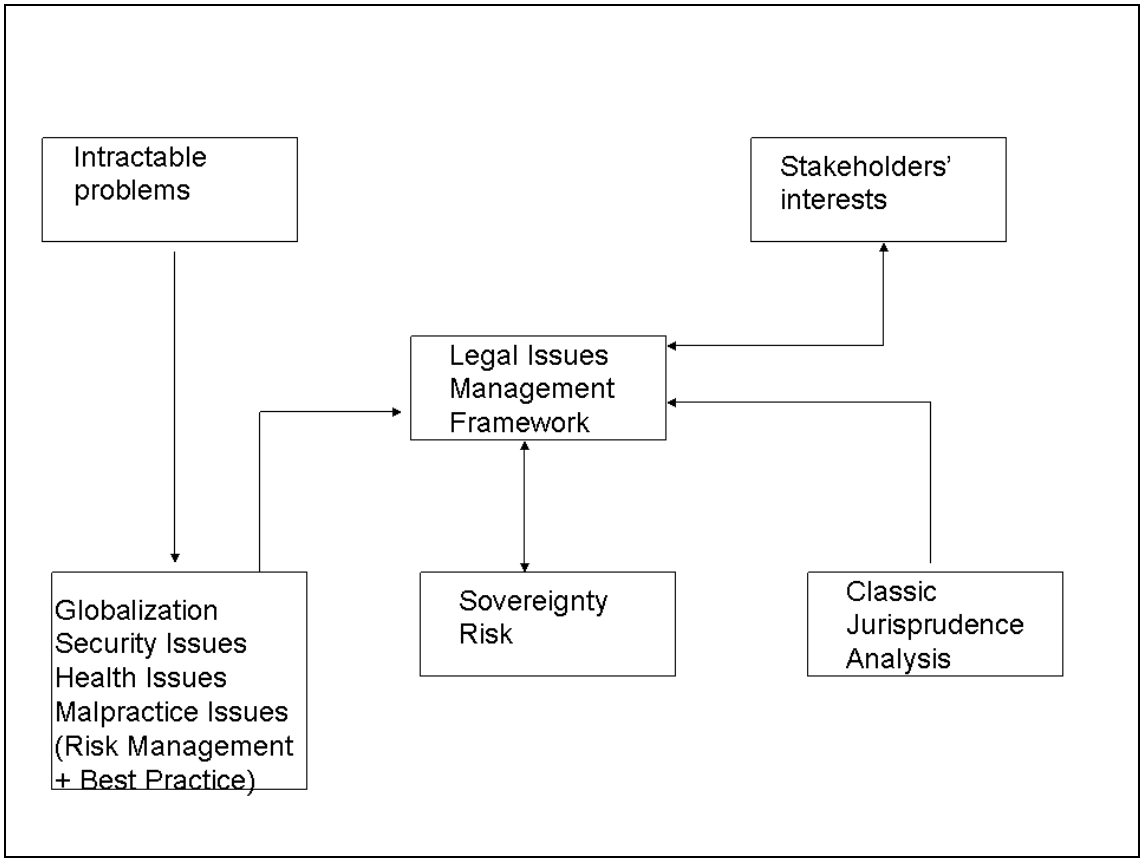

Figure 1: Legal Issues Management Framework

Risk Analysis has a successful track record in field such as engineering, yet has not been as useful in the area of computer security as it is difficult to calculate the risk that an attacker will be able to obtain system administrator privileges for example [13]. The use of Best Practice and Due Care is advocated by security practitioners. This involves a *series of recommendations, procedures and policies that are generally accepted within the community of security practitioners to give organisations a reasonable level of overall security and risk mitigation at a reasonable cost* [13]. Trying to assess risks or apply best practice in P2P networks, given the lack of central control, would introduce further difficulties. Universities, in particular, are warning students and staff of the dire consequences of having copyright material on University machines and ensuring that students and staff are aware of the university policy and the legal consequences. One Sydney University has made it very clear:

> *The university's Acceptable Use of IT Policy was finalised in 2001 and there has been extensive communication including broadcast emails, posters and brochures in student computing facilities, notices and web links on student login pages and information in new staff induction kits. It is not acceptable nor an excuse not to have read the policy* [39].

Exploratory studies are useful when researchers do not know much about the situation at hand [35]. This research was approached in two phases. First, a literature review was undertaken to understand and draw out the critical issues associated with e-technology for peer-to-peer e-business models. Secondly the researchers carried out research on legal cases directly connected with the digital economy. The literature and case law review and subsequent analysis of the issues and synergies drawn from these studies led to the development of the Legal issues Management Framework as well as the following research questions:

- *What are the forensic auditing requirements and sovereign risks for peer-to-peer e-business?*
- *What is the role of the law in these issues and requirements?*

The basic tenets underpinning the research approach may be summarized as follows:

1. need to define an issues management framework that reflects all stakeholders' interests;
2. P2P cannot be addressed independently of the Electronic Business Model (EBM) in use, planned and in prospect;
3. global P2P issues presume knowledge of adequate network externalities, where jurisdictional issues are involved;
4. knowledge management processes currently being implemented by transnational corporations offer possible models for legal entities;
5. unless harmonization solution is adequately addressed at the conceptual level, new technologies will pose an ongoing threat to business revenues (real world, eCommerce, P2P and mCommerce) [24].

4 P2P Business Models

Peer-to-peer (P2P) concerns applications in which users use the Internet to exchange files with each other directly or through a mediating server. IBM's Advanced Peer-to-Peer Networking (APPN) is a product that supports the peer-to-peer communication model. On the Internet, peer-to-peer is a type of transient Internet network that allows a group of computer users with the same networking program (e.g. Kazaa, Gnutella) to connect with each other and directly access files from one another's hard drives. Corporations are investigating using P2P as a way

- for employees to share files without the expense involved in maintaining a centralized server
- for businesses to exchange information with each other directly .

Another Peer-to-Peer e-business model that uses a distributed computing technology is called the **Publish-Subscribe** system (commonly referred to as pub-sub [40]. This is a communication infrastructure that enables data access and sharing over disparate systems and among inconsistent data models [40].

One widespread application of Peer-to-Peer business that is occupying the attention of lawmakers is the distribution of child pornography. Investigations by the Government Accounting Office of the United States (Feb, 2003) have revealed a large increase in the distribution of child pornography over P2P networks. Law enforcement agencies are putting more resources into investigating and charging people involved (Government Accounts Committee, 2003). In the following section the issues that are raised in this context are discussed below. Table 2 provides figures obtained from the United States General Accounting Office, sourced from the Customs CyberSmuggling Center in 2003.

Table 2:– Classification of Images downloaded through P2P File Sharing. [15]

Image Classification	Percentage downloaded through P2P Sharing Programs
Child erotica	13%
Nonpornographic images	14%
Adult pornography	29%
Child pornography	44%

Further investigation by the US General Accounting Office in 2004 provided the figures shown in Table 3 below. This analysis of 1,286 titles and file names identified through Kazaa searches on 12 keywords showed that 543 (about 42 percent) of the images had titles and file names associated with child pornography images. Of the remaining files, 34 percent were classified as adult pornography, and 24 percent as nonpornographic [15].

Table 3: Classification of Titles and File Names of Images Identified in KaZaa Search. [16]

Classification of 1286 Titles and Image Filenames identified in KaZaa	Percentages

Nonpornographic	24%
Adult pornography	34%
Child pornography	42%

4.1 Issues

In assessing risks, the following issues should be canvassed. In fact designers of P2P computer systems need to evaluate risks and trade-offs and pick reasonable solutions for a particular configuration and management [13].

- Completely distributed operation of P2P means that there is no centre to attack – physically, electronically or legally.
- High availability makes it attractive to businesses as content and services are distributed and replicated.
- Companies could have suppliers to quote for goods and services that are needed and these could be linked directly to an ERP system.
- Tighter physical security will be required if mission critical data is stored around the organisation rather than on a central server.
- Hackers could exploit P2P networks for denial of service attacks.
- New ways of looking at Risk Assessment and Best Practice Models are required.
- Companies must investigate how these new Risk Assessment and Best Practice Models could apply to P2P networks.
- Ways to police child pornography in P2P networks must be investigated.
- Sovereignty risks and stakeholders' interests must be assessed.

4.2 Mobile Business and P2P

According to [33] P2P could gain importance with the development of mobile business and ubiquitous computing. In a mobile environment it is necessary to establish communication among mobile, spontaneously networked peers such as PDAs. mobile phones and laptops without any centralised coordinating authority.

5 Copyright Overview

Copyright protects a wide array of material including writings, artwork, music, films, and computer programs and extends to broadcast material, quite separate to the copyright in the material which is transmitted [2]. The copyright automatically belongs to the creator, or the owner, from the time of creation of the material. International treaties such as the Berne Convention provide for protection of Australian copyright owners overseas and vice versa although the rights vary from country to country according to different subject matter. The United States cannot enforce its copyright laws on a citizen of Japan who is doing business in Japan and who owns no assets in the United States. Japanese citizens who bring goods into the United States to sell would be subject to applicable US copyright laws [30], [32]. The copyright owner has the right to use the material in a variety of ways and the rights may be assigned or leased with or without limitations or conditions. Use of copyright material, usually by copying without the permission of the owner, will ordinarily be an infringement of copyright, except in certain circumstances, for example copying of a limited portion of a book by a student (the "reasonable portion" test) [23, 24].

The Federal Government of Australia passed amendments to the Copyright Act that came into effect in March 2001. The right of communication applies to 'active communication, such as broadcast or cable transmission and to 'passive communication, such as making material available to be viewed or downloaded (e.g. a website). There are criminal penalties and civil remedies for making, importing or commercially dealing in devices and services that circumvent technological copyright protection measures such as decryption software (there are however permitted purpose exceptions - such as for governments and decompilers of software). Liability of carriers and Internet Service providers for infringing copyright is also dealt with as they are persons who provide the broadcast or determine the content of the communication. There are factors to be taken into account to determine whether a person is liable for authorizing or infringing and these factors are based on existing case law [23].

5.1 Copyright in P2P networks

One of the first steps in trying to establish a legal framework for any new technology is to classify it in order to establish how existing legislation may be made to fit the new technology. However such development takes a long time. Although the Internet Service Provider has become the major focus for attempts at legislative controls there is a wide variation between each country's approach [14]. Singapore, for

example, has classified the Internet Service Providers as broadcasting media, requiring them to be registered. It thereby exercises control by allowing access only to authorised Web sites. In the United States, the *Telecommunications Act (1996)* considers the Internet Service Provider to be a telecommunications carrier. The United States Supreme Court struck down the *Communications Decency Act*, which would have restricted indecent material on the Internet, as unconstitutional and an attack on free speech. An International Working Group, The Internet Content Rating Association (ICRA), supported by such computer industry leaders such as Microsoft, has been formed to establish world-wide standards for content rating [18].

In 2001 eight US film studios took a hacker to court for facilitating film piracy on his website 2600.com [11]. The hacker was accused of publishing software called DeCSS which enables the encryption codes on DVDs to be cracked so users may then download films to their computer. He has been accused of *Napsterising* film. This is a test case for the 1998 US law designed to protect digital copyright. In the United States, the courts are being used to remove competition coming from the users themselves and technology is being used via the use of code to protect against copying. This equation is called **Law plus Code (L + C).** The Digital Millennium Copyright Act's anti-circumvention clause makes it a crime to try to crack digital rights management software. Now the equation is **Law plus Code plus Law (L + C+ L)** [22].

Industry rules therefore are

- Persons may not trade music among themselves. (as per Napster)
- Persons may download music from industry with the restrictions we set in place.
- Industry will enforce those restrictions with code.
- It is a crime to break that code.

This is a massive expansion of copyright protection, a change that shifts the entire purpose of copyright from supporting creativity to granting total and absolute property rights not to artists but to middlemen [11]. P2P networks have been the reason for the entertainment industry reliance on code to stifle file swapping but the P2P networks have fought back with their own technology breaking techniques and software (as discussed in a Section 5.3). Studies into the effects of file swapping over the Internet have provided different results. Jupiter Research reported that about 34 percent of veteran file swappers (in a study of 3319 people) reported that they were spending more on music than they did before they started downloading files. About 14 percent of heavy file traders stated they spent less on music [5]. The music industry has figures that indicate file swapping has led to a loss of revenue for their industry and believe they must stop the piracy if their industry is to survive.

5.3 Legal cases

As seen in Table 1 many of the legal cases have concerned the copying of music and video files over Peer to Peer networks. In the ongoing Peer-to-Peer legal saga, the Recording Industry Association of America (RIAA) in April 2003 used the messaging systems built into Kazaa and Grokster peer-to-peer file swapping systems to emphasize to people that it is illegal to distribute music protected by copyright without permission [4]. However, yet again technology is being used to attempt to thwart the copyright police and music agencies. Peer-to-peer news sites, such as Zeropaid, publish lists of net addresses known to be used by the music industry and its proxies so that Net users with a personal firewall can tell their software to block these addresses so investigators cannot download their files. This makes it much harder for the music industry to find out if a particular track, which is being offered, is pirated [4].

Four university students in the United States who were accused of running an online music swapping service similar to the now defunct Napster have agreed to pay damages to the Recording Industry Association of America (RIAA). The defendants were charged with storing more than one million songs on central servers at their colleges so that people could access them from the universities' high-speed internet networks. The students did not admit any wrongdoing [4].

5.4 Australian cases

The first criminal prosecution for online music piracy occurred in 2003 when three Australian students were charged with copyright offences by the Australian Federal Police (AFP), following an investigation assisted by Music Industry Piracy Investigations (MIPI), the enforcement arm of the Australian record industry. The charges referred to an Australian-based Web site, MP3 WMA land, which allegedly offered illegal downloads of copyright-protected music and received seven million visitors. According to the AFP, the site contained links to digital recordings of several hundred commercially available music albums and individual recordings belonging to major music companies. Two of the students received 18 month suspended prison terms, the other was sentenced to 200 hours of community service and all were fined over $3000. The court imposed lenient sentences because the students had made no profit from the operation. The MIPI

lamented the court's leniency claiming that the students had cost the industry $60 million in lost income. [20].

The Kazaa protocol for PSP file sharing appeared in 2001 as Napster was shut down. Kazaa was sold to Sharman Networks of Australia following an order from a Dutch court (later reversed on appeal) that the Dutch owners were to take steps to prevent its users from violating copyrights or otherwise pay a hefty fine. In February 2004 the Australian Record Industry Association (ARIA) commenced legal action against Sharman and on 5 September 2005 the Federal Court ruled that although Sharman itself was not guilty of copyright infringement it had "authorized" Kazaa users to illegally swap copyrighted songs. Although Sharman had posted warnings about possible infringement of copyright the Court held that this was insufficient without filtering to prevent or restrict user's access to copyrighted material. The Court did not order the Kazaa system to be shut down but the technology was to be modified by suitable filters. Sharman managed to block Australian users from downloading Kazaa by identifying their ISP (See Table 1) . Sharman is planning an appeal [41].

6 Technologies to Track Internet Activities

Other technologies and the use of computer forensic methods are becoming increasingly important as tools to investigate suspected crimes. Forensic Computing involves a number of disciplines: namely, computer science, information systems, law, and social science. Table 4 provides an overview of some of the technologies that can be used to track activities on the Internet

Table 4 Overview of Internet Tracking Technologies

TECHNOLOGY	What it does	How it could be used
Id cards	These allow information to be sent to your computer from a web site - the site needs the numerical address of the consumer's PC on the Internet, the browser and operating system to send information.	To track potential copyright breakers
Web bugs or clear gifs	Embedded in an image on the screen. Web sites hide these information collecting programs on various parts of the sites - they are used by affiliates to gather consumer information. These tags help web sites and advertisers to track users' whereabouts online [36]	as above
Web Bug (WebBug FAQ) [36]	can reveal the following types of information to its related server: URL of the Web bug IP address Host name Browser version Operating system and version Web browser cookie (optional).	as above
Cookies	When a web-browser requests a page from a web-server, the web-server sends back to the web-browser not just the requested page, but also an instruction to the browser to write a cookie (i.e. a record) into the client-computer's storage. Once written into the storage, the user can be identified each time he visits the same site thus allowing a profile of the user to be established based on the usage patterns. To overcome such objections user could be informed if and when the cookies were to be placed, told of the uses to which the cookies would be put, given the choice as to whether the user wished to proceed or not. [[6], 24]	European Parliament has voted in favour of an amendment to a data privacy bill that will restrict the use of cookies or hidden identifiers by web sites such as Yahoo [28].
Watermarks	Digital watermarking, sometimes called "fingerprinting," allows copyright owners to incorporate into their work identifying information invisible to the human eye [19]	When combined with new tracking services offered by some of the same companies that provide the watermarking technology, copyright owners can, in theory, find all illegal copies of their photos and music on the Internet and take appropriate legal action. For webmasters, digital watermarking can help ensure that only lawful image and audio files are used, protecting webmasters against the dangers of copyright infringement [19].
Monitoring /auditing	Xerox used 'reactive monitoring' - in which a comprehensive log of Internet sites visited	

employees and students and their computers	every month is scanned for 'red flags' - i.e. sites deemed inappropriate for workplace access - and fired 40 of its workers for 'inappropriate use of the Internet [28].	

As well as the increase in the number of technologies that are being used to monitor activities on the Internet there is now growing evidence that governments are adapting their laws and companies are adopting and devising new business models to try to adjust to the new technologies. The Australian Copyright Council is recommending amending the Copyright Act to allow for private copying to follow the United States which allows people to make one copy of their legally purchased CDs or DVDs under a Fair Use Provision of their copyright law [37].

The Australian government is currently considering adding a copyright levy for all digital music and video player hardware. Companies such as iTunes and Sanity have introduced legal online purchases and studies reveal that there has been a slowing of illegal downloads. Evidence from consumer research however points to the fact that consumers do not take the laws against copying seriously as there is a low probability of getting caught and risk-taking is part of human nature [37].

7 Conclusion

The law is struggling to cope with the global phenomenon of P2P networks and the global implications of the digital economy. The widespread popularity of P2P networks which could be extremely useful in business environments is causing the entertainment industry to try to use the full force of the law to protect their copyright. However there is growing evidence that they are now attempting to use new business models for selling their tunes and videos. Lawmakers and governments are worried about the proliferation of child pornography over P2P networks and are trying to find and convict the people involved. As soon as the lawmakers try to solve an issue, the technologists come up with a new and more wide reaching technology. The researchers have put forward a Legal Issues Management Framework as an attempt to tackle the many intractable issues that confront the lawmakers. The legal efforts involved in bringing Napster under control led to the arrival of imitators such as Gnutella and Kazaa. There are at present very few legislative controls on the Internet although efforts are being made in various countries and internationally to draw up suitable model laws and guidelines. Countries are adopting different approaches to this issue depending upon their societal and cultural values but questions remain for future research. How can technology assist the law to help it operate quickly enough if laws are being broken?

References

[1] E. Adar. and B.A. Huberman. Free Riding on Gnutella, First Monday,2000. [Online] Available at: http://gunther.smeal.psu.edu/context/126721/0
[2] Australian Copyright Council. Online Information Centre, 2003 [Online] Available at: www.copyright.org.au
[3] C. Bannhan. Net Ruling smashes legal borders. The Sydney Morning Herald, December 11, p. 2 2002
[4] BBC News UK Edition File Swappers Fight Back, 2003[Online] Available at: http://news.bbc.co.uk/1/hi/technology/3013065stm
[5] J. Borland, J. Study: File Sharing Boosts Music Sales. C|NET News.Com, *2002* [Online] Available at: http://news.com.com/2100-1023-898813.html
[6] P. Ching, Cookie Monster? Communique, November, page 28. 2000.
[7] B.M. de Vuyst. Dispute Resolution of gTLD conflicts (CD-ROM) Proceedings of the 35th Hawaii International Conference on System Sciences, 0-7695-1435-9/02 IEEE, 2002Electronic Frontier
[8] J. Evers. Court gives Kazaa a Win on Piracy. PC World, 2002 [Online] Available at: http://www.pcworld.com/resource.printable.article/0,aid, 91744,00.asp).
[9] Rita Fang, Taiwan Journal, 27 September 2005. [Online} Available at http://www.gio.gov.tw/taiwan-website/4-oa/20050927/2005092701.html
[10] B. Fitzgerald and A. Fitzgerald, A. Cyberlaw: Cases and Materials on the Internet, Digital Intellectual Property and Electronic Commerce. Sydney: Lexisnexis Butterworths, p.172, 2002.
[11] J. Forder and P. Quirk. Electronic Commerce and the Law. Brisbane: John Wiley and Sons**.** 2001
[12] Foundation 2003 Win for Makers of Morpheus Peer-to-Peer Software! Court Rejects Entertainment Industry Copyright Claims, 2003 [Online] Available at: http://www.eff.org/IP/P2P/MGM_v_Grokster/030425_morpheus_win_pr.php
[13] S. Garfinkel and G. Spafford. Web Security, Privacy and Commerce, Cambridge, MA: OReilly. pp.10 – 11, 2002.
[14] Global Internet Liberty Campaign 2003, [Online] Available at: www.gilc.org

[15] Government Accounts Committee. File Sharing Programs: Peer to Peer Networks provide ready access to Child Pornography, Report to Committee on Government Reform – House of Representatives, 2003 [Online] Available at: http://www.gao.gov/new.items/d03351.pdf
[16] Government Accounts Committee. File Sharing Programs Users of Peer-to-Peer Networks Can Readily Access Child Pornography Statement of Linda D. Koontz May 6, 2004, Director, Information Management Issues GAO-04-757T
[17] Linda Harrison. Sick porn baron escapes jail. 1999
[Online} Available at : http://theregister.co.uk/1999/09/07)
[18] Internet Content Rating Association, www.icra.org
[19] D. Isenberg. Digital Watermarks: New Tools for Copyright Owners and Webmasters, 2003
[Online] Available at: http://www.webreference.com/content/watermarks/
[20] Matt Jacobs. Australia convicts music pirates, Jurist – Paper Chase 2003. [Online] Available at: http://jurist,law.pitt.edu/paperchase/2003_11_19_indexarch.php
[21] Mick Keelty. The Dark Side of technology, Austrlaian Institute of Criminology. Crime in Australia: International Connections Conference, 29 November, 2004 [Online] Available at: http://www.afp.gov.au/afp/page/Publications/Speeches/29November04_DatkSideTechnology.htm.
[22] R.Koman. Lessig: The Future of Ideas, 21 December 2001,
[Online] Available at: http://www.openp2p.com/pub/a/p2p/2001/12/21/lessig.html?page=1
[23] E. Lawrence., Newton, S., Lawrence, J., Dann, S., Corbitt, B. and Thanasankit, T Internet Commerce: Digital Models for Business, (3rd edition), Brisbane: John Wiley and Sons 2003.
[24]. E.Lawrence, Newton, S., Corbitt, B., Braithwaite, R. and Parker, C. Technology of Internet Business, Brisbane: John Wiley and Sons 2003a
[25] E. Lawrence and J. Lawrence. Threats to the Mobile Enterprise: Jurisprudence Analysis of Wardriving and Warchalking, International Conference on Information Technology: Computers and Coding (ITCC04) Volume 2, page 269- 273
[26] E. Lawrence and B. Garner. Global Paradigms For Taxing Internet Commerce, Eleventh International Bled Electronic Commerce Conference Proceedings, Bled, Slovenia, June 8-10, p.552.1998
[27] E. Lawrence and B. Garner. Harmonizing Global Internet Tax: A Collaborative Extranet Model, South African Computer Journal, (24), November, pp. 119-127.1999
[28] K. Needham. Yahoo says yoohoo, its time to cough up, Sydney Morning Herald, November 15, p.6.2001
[29] J. Pearce. AU students face court over piracy charges,. ZDNet. May 13, 2003 [Online] Available at: http://www.zdnet.com.au/newstech/ebusiness/story/0,2000048590,20274447,00.htm
[30] A. Perry. E-commerce in 2001. Conducting and Enforcing Electronic Transactions Seminar Notes (LAAMS) Sydney: Legal and Accounting Management Seminars Pty Ltd. 2001
[31] Anita Ramasastry. Privacy, Piracy and due process in peer-to-peer file swapping suits: A Federal District Court Strikes a Good Balance, November 10, 2004. [Online} available at: http:///writ.news.findlaw.com/ramsastry/20041110.html.
2004)
[32] G. Schneider and J. Perry. Electronic Commerce (2nd Edition) Cambridge, MA: Course Technology, p.399.2001
[33] D Schoder and K. Fischbach. Viewpoint: Peer to Peer prospects, Communications of the ACM, [February 46(2), pp.27–29.2003.
[34] E. Schonfeld. Goodbye Napster, Hello Morpheus (and Audiogalaxy and Kazaa and Grokster.) Future Boy2002 [Online] Available at: http://www.business2.com/futureboy/
[35] U. Sekaran. Research methods for Business: A Skill-Building Approach, 2nd Edition, John Wiley & Sons, New York, USA.1992
[36] R.Smith. The Web Bug FAQ (Version 1.0) 1999 [Online] Available at: http://www.tiac.net/users/smiths/privacy/wbfaq.htm
[37] L.Timson, Tempting isn't it? Icon, Sydney Morning Herald, pages – 6-7 April 1- 2, 2006)
[38] D. Townsend. Briefing report on Telecommunications Regulatory Issues for Electronic Commerce. 1999 [Online] Available at:
http://www.infodev.org/projects/ecommerce/341itu8/341.pdf
[39] UTS. University of Technology Acceptable Use of Information Technology Facilities, UTS Rules, Policies and Procedures 2003 [Online] Available at:
http://www.uts.edu.au/div/publications/policies/select/itfacilities.html
[40] C. Wang, Carzaniga, A., Evans, D., and Wolf, A. Security Issues and Requirements for Internet Scale Publish-Subscribe Systems, (CD ROM) Proceedings of the 35th Hawaii International Conference on System Sciences 2002, 0-77695-1435-9/02/2002 IEEE. 2002
[41] Michael Weiss. StreamCast Networks. 2005 [Online] Available at http://www.streamcastnetworks.com/
[42] Wikipedia 2005 [Online] Available at http://en.wikipedia.org.wiki.Kazaa
[43] S. Wither Peer, there, and everywhere Australian Personal Computer, May, p.91 2001