

Internet Safety: Young People And The Law In An On-Line World

Judge David J. Harvey
District Court Judge

Introduction

In this paper I intend to consider some of the wider issues that surround Internet safety and young people. Much of the focus upon access to the Internet by young people, and the concerns that arise from that access, are related to the ease by which objectionable material may be obtained and the associated concerns involving trading in that material and the inevitable contact with the twilight zone of pornography traders and paedophiles. Alongside the enormous promise of information availability, enhanced communication, educational opportunities and commercial activity, that lies within the Internet are, as in the real world, enhanced and increased opportunities for unlawful and criminal activity to which young people may be exposed.

It is not possible within the scope of this paper to examine all or some of these problems in great depth. Rather, I shall take this opportunity to sketch out some of the areas where young people may be exposed to risk of unlawful criminal activity. Such activity is dangerous for both the victim and the perpetrator.

Background

Perhaps a starting point for this broad examination may be to consider the way in which the very nature of the Internet itself may bring a young person much closer to criminal activity than may be the case in the real world.

Criminal activity in the real world involves issues of physical location. To become involved in criminal or unlawful activity, such as theft, car conversion, assault or the like, a young person must be in the vicinity of the property to be stolen, the motor vehicle to be converted or the victim of the assault. In many cases, these offences arise within the context of the *gestalt* of the peer group which necessarily involves presence within the group. In virtually all cases this offending takes place away from the home and away from the potential for parental or adult supervision.

On the other hand, the potential for criminal or unlawful activity on the Internet may take place within the home environment, away from the influences of the peer group (absent chat room activity) and in an environment where there is clearly the potential for parental supervision and parental control. However, the internet enables unlawful activity to take place within the privacy of the home. It is with good reason that it is suggested that the family computer be located in an area of the home to which all members of the family have ready access or through which they pass frequently.

A further difficulty with the Internet involves the theory that the Internet is a world without borders. Recent case law would tend to suggest otherwise as domestic jurisdictions apply their own rules to Internet activity within their own territory¹. One of the difficulties, as I shall point out later in this paper, arises from the fact that although access to the Internet may take place in New Zealand, consequences of that access may be felt in other jurisdictions which could have considerable implications if the young person should choose to travel or pursue a course of study overseas.

Another problem is that actions which may be clearly reprehensible, wrong or unlawful in the real world and which take place in the presence of a victim (be it of an assault or of a fraud) and which necessarily they have an inhibitory effect upon culminating the unlawful activity, become actions involving a seemingly anonymous actor and anonymous victims, thus having the effect of reducing inhibition as a result of depersonalisation.

I am not for one moment advocating that, because of these opportunities for unlawful behaviour, young people should not have access to the Internet, or that the Internet should be banned or disconnected or that access should be curtailed or restricted. Life in society is full of risk and the issue really is one of identifying risk, being aware of it and managing it.

The Law and The Internet

Prior to its commercialisation in the early 1990's the Internet was a shared system between universities, research and defence organisations. It was international, operating in countries outside of the United States primarily through universities and educational institutions. Even before its commercialisation the vulnerability of networked systems had been demonstrated.

In 1982 a group of students used terminals, modems and long-distance telephone lines to break into computers in Los Alamos and the Columbia Medical Centre. Unauthorised access to university computers by students had taken place, but universities were not in the business of maintaining security over information; rather they shared, spread and disseminated it. There were no vast data banks of vulnerable proprietary information stored in computers which could be accessed or copied without permission and in the early days of the Internet the stakes were low. Indeed, in the 1970's and 1980's the focus was more upon those who attempted to access telephone systems without paying².

By the 1990's when the Internet went commercial and the widespread use of computers and their vulnerability when attached to networks became apparent, society was forced to tackle issues of property in cyberspace. The stakes became high as the information society began to develop.

Not only did issues develop regarding unauthorised access to network systems (commonly known as "hacking") but, with the development of commercial activity on the Internet, questions began to be asked about the application of the law to the Internet. In the early and mid-1990's legal theorists began to consider this issue. Some considered that the Internet was no different from other communication systems and subject to domestic or territorially based regulation³. Others considered that cyberspace was essentially a new area which required a new approach as far as regulatory activity was concerned⁴. When the United States Congress passed the Computer Decency Act in 1995 (aspects of which were ruled to be unconstitutional by the United States Supreme Court in the case of **Reno v ACLU**⁵) John Perry Barlow, an Internet enthusiast and former lyricist for the grateful dead, published his "Declaration of Independence for Cyberspace" suggesting that Government's had no place on the Internet⁶.

The fact of the matter is that Governments and State have the right to regulate activities within their own borders. In confronting new technology the enquiry must be whether or not the law as it stands may apply to the new technology or, if it does not what changes need to be made to make behaviour within cyberspace consistent with behaviour in the real world.

Crime and the Internet

It is well known premise of law that the definition of prohibited or criminal activity must be clear and unequivocal. Some concerns were expressed by the Law Commission regarding unauthorised access to computer systems in its 1999 report "Computer Misuse"⁷. As a result of this the Crimes Amendment Bill (No.6) is presently before Parliament proposing specific offences for unauthorised access to the computer systems.

However, it has been established that current legislation *does* encompass computer or Internet based activities. For example, in certain circumstances a password may be a document for the purposes of an offence against s.229A of the Crimes Act 1961 which covers offences of taking or dealing with certain documents with intention to defraud. Offences under s.229A cover activities regarding documents which are capable of being used to obtain a privilege, benefit, pecuniary advantage or valuable consideration. The essence of the offence involves using a document to obtain something that does not necessarily have to be money but which may be provide an advantage. Thus the offence is very wide. A password may be used or there may be an attempt to use a password to obtain a benefit or an advantage.

The only requirement that is necessary for a password to become a document is for it to be stored in some way, shape or form. Thus, the storage of a password on a computer hard drive or in a computer text file or word processing "document" will make it a "document" for the purposes of the offence. If the password is written down on a piece of paper, naturally it is a document in such a case. However, if I am standing behind a computer user and observe the keystrokes that he or she executes in inputting a password and then commit those keystrokes to my memory, the password is not a document. If I use the password that I recall from my memory to access a computer, the documentary requirement for an offence under s.229A does not exist.

How does this pose a danger for young people? The first thing that must be remembered is that ignorance of the law is no excuse. The second thing is that if a young person is given a password by which he or she may access the Internet or somebody's account or somebody's private web page or any other information on the Internet, and if the use of that password is not authorised by its owner, there is a serious risk that a criminal offence has been committed. It matters not that there has been no financial benefit. It matters not that money may not have been transferred from one bank account to another. It matters not that the information obtained by the activity may not have been reproduced by hard copy from the printer. What has happened is that by the unauthorised use of the password the young person has obtained an advantage or a benefit to which he or she is not entitled.

It is well known that password swapping takes place in school playgrounds. It is not so well known that the utilisation of these passwords could constitute a criminal offence.

Let me give you another example. Although the mere fact of unauthorised access to a computer system is not specifically prohibited by the law, certain activities associated with hacking fall within the ambit of s.298 of the Crimes Act 1961 which criminalises wilful damage and renders the offender liable to imprisonment for a term not exceeding five years⁸). The reason for this is that the definition of damage extends to a computer hard drive and covers access to a computer (by way of hacking or unauthorised access) where changes may be made to the victim's hard drive. For example, the installation of a "back door" program which allows subsequent access, changes the functionality of the victim computer in such a

way as to comprise damage. The deletion of files involves a rearrangement of the magnetic particles on the hard drive which constitutes damage. It is debatable whether or not the simply copying of a file from the victim computer to the hacker's computer would comprise damage because no material changes have taken place on the victim computer's hard drive. However, as a result of recent cases, it has become clear that the law is not as deficient as was suggested by the Law Commission in 1999. Some existing offences encompass and criminalise access and changes to computer systems.

How does this impact upon young people? It is easy to obtain on the Internet programs or tools which enable access to other computers on the network. These may be described as hacking tools. In addition, many commercially available computer security programs contain within them tools which may be turned to enable unauthorised access to network systems. These programs may be easily used by young people who, sitting in the privacy of their own home, and using the apparent anonymity of the Internet, may access other people's computers and may consider themselves invulnerable. This is simply not the case. Anyone who has followed an Internal Affairs investigation into trading of pornography on the Internet will realise how easy it is to track an Internet user by use of the Internet Protocol (IP number) followed by an enquiry to the Internet Service Provider to whom that IP is assigned. In addition, firewall programs⁹ are now readily available which will warn a victim user of a potential intruder and disclose the ubiquitous IP number thus making identification of the "hacker" so much easier. Anonymity on the Internet is a myth. In fact, a user of the Internet leaves a trail that is much easier to follow than a person's activities in the real world.

Other Unlawful and Dangerous Activities

What then of non-criminal activities? The issue of copyright immediately springs to mind.

A well-publicised case in the United States involving the peer-to-peer file sharing application known as Napster¹⁰ and another less well known case in the United States involving the distribution of a program that enables the copying of files from a DVD disk, highlight the risks that are involved associated with the laws relating to copyright.¹¹ Digital technology such as computers, rely upon copying to operate. Running a program involves the copying of all or some of the operating parts of the program into the memory of the computer. Copyright infringement takes place when a work is copied and is described as a restricted act. Unauthorised issuing of copies of a work is also a restricted act. Thus to get around this every program contains within it an express or implied licence authorising such copying.

Digital technology also allows the copying of files. Unlike copying the contents of a CD onto an audio-tape or a television program onto a video-tape where quality degrades with each subsequent copying, there is no degradation of quality with copied digital files. Compression formats, such as MP3, for music files or DivX for video-files, mean that the transmission of these files over the Internet can take place quickly and easily. The problem is that there are substantial penalties associated with copyright breach. Some of these penalties may arise as a result of specific offences provided by the Copyright Act but copyright owners also have the right to commence proceedings against those who breach their copyrights and seek damages and compensation which can run into tens and hundreds of thousands of dollars.

The technology for making copies of compact disks has been known for some time. However, compact disk manufacturers have not made this technology available in compact disk players – at least until recently. The advent of the computer with CD burners, incorporating the copying aspects for compact disks, has changed that. Concern has been

expressed by music companies at what is viewed as widespread copying of CDs using CD burners and the distribution of these unauthorised copies around schools. Much of this unlawful activity, constituting an infringement of the copyright holder's rights, takes place because it is easy and because those engage in such activity wish to enhance their prestige or reputation in the school yard.

Simple copying is called primary infringement. Secondary infringement is considered more seriously. These include activities such as:

1. importing infringing copies otherwise than for a person's private or domestic use, associated with knowledge of the infringing nature of the copy;
2. possessing or dealing with infringing copies knowing that the copy is an infringing copy and the aspect of dealing carries with it the taint of commercial activity.
3. if a person possesses in the course of business an object which is designed or adapted for making infringing copies of a work, such an action can constitute secondary infringement.

Interestingly, copyright in a work is infringed by a person who other than pursuant to a copyright licence transmits the work by means of a telecommunications system, knowing or having to reason to believe that infringing copies of the work will be made by means of the reception of the transmission in New Zealand or elsewhere. Clearly, this form of secondary infringement contemplates transmission of infringing copy by means of the Internet.

The Copyright Act 1994 provides various steps that may be taken by copyright owners for remedies by way of damages, injunctions or accounts. In considering the measure of damages the Court must have regard to all the circumstances and in particular to:

- (a) The flagrancy of the infringement; and
- (b) Any benefit accruing to the defendant by reason of the infringement and may award such additional damages as the justice of the case may require.

In addition, injunctions may be obtained, along with orders for delivering infringing copies up.

The Copyright Act 1994 also provides for criminal liability for making or dealing with infringing objects and primarily covers aspects of secondary infringement. Criminal liability normally attracts to those infringements of copyright that have a commercial taint. The penalties are substantial and include fines of \$10,000.00 for every infringing copy up to a maximum of \$150,000.00 together with power to the Courts to order reparation and orders for delivery of infringing copies.

In addition, there are provisions in the Copyright Act covering devices that are designed to circumvent copy protection¹². In the digital environment copyright owners frequently embed into the digital files some form of code that will prevent copying of the file. The Content Scrambling System (CSS) contained on DVD's is an example. The Act gives to copyright owners rights against those

1. who make, import, sell, let for hire, offer or expose for sale or hire, advertise for sale or hire, any device or means specifically designed or adapted to circumvent a form of copy protection or,

2. publish information intended to enable persons to circumvent copy protection when those people know or have reason to believe that the devices, means or information will be used to make infringing copies.

Thus, if a young person is asked for a circumvention device knowing that the person asking for it is going to infringe copyright or, alternatively, makes such a program or attempts to sell such a program or even publishes information which assists people circumventing copyright protection, then the copyright owner has rights against such a person.

I raise the issue of copyright as an example only. It is an issue that concerns young people particularly, as I have already mentioned, as there has been some publicity about the copying of compact disks and their distribution in the school yard. Although Napster may have been closed down there are a number of other peer-to-peer file sharing programs all of which involve potential issues of copyright infringement¹³. The consequences can be considerable.

Copyright owners are pursuing Internet-based copyright infringement vigorously and aggressively. The steps that were taken by the Recording Industry Association of America regarding the Napster case provide an example. The Motion Picture Association of America's steps against those who attempted to distribute a program that circumvented the content scrambling system of DVDs is another.

It has been suggested that copyright owners pursued Napster and 2600.com¹⁴ (the DeCSS distributor) because they were large, visible and identifiable contributors to copyright infringement. What is not so well known is that a number of programs have been developed that enable copyright owners to identify those who are using file sharing programs on the Internet by name or "handle", identify the type of file sharing program, the names of the files that are being transferred or transmitted, the IP number and the Internet Service Provider for the potentially infringing customer. Armed with this information it becomes an easy matter to identify the individual who is infringing copyright.

Once this person is identified there are a number of draconian steps that a copyright owner might take against an infringer. One involves what is called an Anton Piller Order which enables the copyright owner, authorised by the Court, to enter upon premises and seize computers and hard drives containing potentially infringing material for the purposes of preservation of evidence. Although there have been no incidents of court-based infringement enforcement against individuals in New Zealand for "Napster-type" activities, a large scale copyright infringer could be identified using the tools that I have described and steps could be taken against that person. Young people should be aware that their expectation of privacy within their home whilst using a computer on the Internet is non-existent and any expectation that they may have anonymity whilst on the Internet is a myth. Copyright infringement may be facilitated by network systems, but its detection is also enhanced.

The International Nature of the Internet – Multi-Jurisdictional Dangers

The final caution that I shall offer about unlawful activities on the Internet involves the international character of the Internet itself and the fact that one's actions in one jurisdiction may have an impact upon another. An early example demonstrating the multi-jurisdictional nature of the Internet is that of **US v Thomas**¹⁵. The Thomas's were Californian residents who operated a bulletin board on a server situated in California. They traded in material which, although not classified as objectionable within the State of California, was so classified in the State of Tennessee. Files were so transmitted by the Thomas's from their

server in California to a recipient in Tennessee who turned out to be a law enforcement official. The Thomas's were prosecuted in Tennessee for transmitting objectionable material. The Court held that the prosecution was properly brought, notwithstanding that the material was lawful in California.

Another example of the difficulties that may be experienced with the international nature of the Internet is demonstrated by the case of **LICRA and UJEF v Yahoo**¹⁶. In addition, to its search engine, Yahoo, based in San Jose, California, operates an auction site. It also has subsidiaries in many countries around the world including France. One of the auctions that was advertised on Yahoo involved the sale of Nazi memorabilia. The commercial distribution of Nazi memorabilia in France is prohibited by law. Yahoo, aware of this prohibition, made sure that the auction was not advertised by means of its French servers. However, French residents could still access the Yahoo site in the United States.

LICRA and UJEF are two organisations who took exception to the advertisement of the auction anywhere and brought proceedings in the French Court seeking a direction that Yahoo cease the auction. There was a considerable amount of concern expressed. Effectively, a Court in France was being asked to rule upon activities which originated in the United States and which were lawful in that jurisdiction but unlawful within the French jurisdiction. The French Court indeed held that it had jurisdiction to entertain the case and make the orders sought because, under French law, jurisdiction could be assumed if the effect of Yahoo's actions were felt in France. Because French citizens could access the Yahoo site in the United States the effect was therefore felt in France.

The most recent example of cross-border jurisdiction involves the arrest and prosecution of Dmitri Sklyarov. Sklyarov was a Russian citizen employed by a company known as Alcom Soft, a Russian company. A software company named Adobe published e-books (books in electronic format) which were subject to copy protection. Sklyarov, in accordance with the provisions of Russian law, circumvented copy protection algorithms that were embedded in the e-books so that copies could be made. Russian law requires that the owner of a software program must be able to make one copy of the program. Thus the circumvention of the algorithm was therefore lawful in Russia.

In July 2001, Sklyarov attended the DefCon Convention in Las Vegas, Nevada and was arrested for breaches of the Digital Millennium Copyright Act which prohibits the utilisation of circumvention devices. He faced five charges and up to 25 years imprisonment and fines of up to \$2.25 million. This was the first criminal prosecution under the Digital Millennium Copyright Act. However, since his arrest he has entered into an arrangement with prosecuting authorities and the proceedings will no longer continue against him.

The case demonstrates that actions that may be lawful in one country may not be lawful in another. Although no steps were taken to extradite Sklyarov from Russia (even if that could have been done) the case demonstrates that, if one enters a jurisdiction where one's Internet based activities are unlawful, one may be facing sanction in that other jurisdiction. Thus, if a young person has been involved in activities which may be lawful under New Zealand law but which breached the Digital Millennium Copyright Act, and then travels with his family for holiday in the United States, he or she could find him\herself liable to arrest and prosecution.

Conclusion

The examples that I have given in this brief and broad discussion demonstrate some of the dangers that are inherent for young people on the Internet. Many of these potential dangers and the risks associated with them are unknown to parents, family members, guardians or teachers. Part of the problem has arisen from misinformation about the application of the law to the Internet and confusion as to the application of provisions of current law to the Internet.

The potential multi-jurisdictional features of the Internet are not widely known. As I have suggested, many young people are unaware of the risks that their behaviour may pose for them, falsely believing that privacy and supposed anonymity may protect them from detection. That attitude was demonstrated by Andrew Garrett who publicly suggested, after he had used the Internet to unlawfully copy and reproduce passwords obtained from other people by use of a hacking program, that the law could not touch him. He was convicted in 2001 for offences arising out of those activities

Ensuring the safety of our young people in their use of the Internet is complex. As I have suggested, many parents and those charged with the supervision of young people are themselves unaware of the extent of the problem which involves the wider aspects of criminal and unlawful activities which may take place. Considerable effort will need to be directed towards identification of the risk areas and the development of a program to educate the educators and supervisors of young people and the young people themselves of the risk areas.

Pornography, objectionable content and the activities in the twilight zone occupied by paedophiles and pornography traders is a small but very visible aspect of the dangers of the Internet and an area where, of course, we must be concerned for the safety of our young people. However, it is my suggestion that Internet safety embraces a much wider spectrum of activities as I hope this paper has demonstrated. It is up to us to develop the methods and the tools by which our young people may be educated in the wider aspects of Internet safety.

¹ See LICRA & UEJEF v Yahoo Inc; Gutnik v Dow Jones; US v Thomas

² Referred to as "phreakers". One well-known "phreaker" was Steve Wozniak who, with Steve Jobs, developed the Apple Computer.

³ "Cyberspace and the Law of the Horse" Frank H. Easterbrook (1996) Univ Chicago Legal Forum 207;

"Against Cyberanarchy" Jack Goldsmith, 65 University of Chicago Law Review 1199 (1998)

⁴ . See David R. Johnson and David Post, Law And Borders--The Rise of Law in Cyberspace, 48 Stan L Rev 1367, 1367 (1996). See also David Post and David R. Johnson, Borders, Spillovers, and Complexity: Rule-making Processes in Cyberspace (and Elsewhere), draft presented at the Olin Law & Economics Symposium on "International Economic Regulation" at Georgetown University Law Center (Apr 5, 1997); David Post and David R. Johnson, The New 'Civic Virtue' of the Internet (also published in The Emerging Internet, Feb 1998, the Annual Review of the Institute for Information Studies), available online at [http:// www.cli.org.paper4.htm](http://www.cli.org.paper4.htm) ; David G. Post, Governing Cyberspace, 43 Wayne L Rev 155 (1996); David G. Post, Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace, 1995 J Online L, Article 3, available online at www.wm.edu/law/publications/jol/post.html . Commentators who have made similar arguments include John T. Delacourt, The International Impact of Internet Regulation, 38 Harv Intl L J 207 (1997) ; Dan L. Burk, Federalism in Cyberspace, 28 Conn L Rev 1095 (1996); Joel R. Reidenberg, Governing Networks and Rule-making in Cyberspace, 45 Emory L J 911 (1996)

⁵ 521 US 874 (1977)

⁶ John Parry Barlow, A Cyberspace Independence Declaration, available online at www.eff.org/barlow

⁷ Law Commission, Wellington; Report 54

⁸ s.298(4) Crimes Act 1961

⁹ Such as Zone Alarm

¹⁰ A & M Records et al v Napster 114 F Supp 2d 896 (District Court); 239 F 3d 1004 (9th Circuit)

¹¹ Universal City Studios v Corley 111 F. Supp 2d 246 (SDNY 2000); 237 F. 3d 429 (2nd Circuit)

¹² Section 226

¹³ For example WinMX – www.winmx.com ; AudioGalaxy <http://www.audiogalaxy.com/> and filesharing programs based on Gnutella <http://gnutella.wego.com/>

¹⁴ www.2600.com

¹⁵ 74 F.3d 701 (6th Cir, 1996)

¹⁶ Superior Court of Paris, First Deputy Chief Justice Gomez; 22 May 2000
<http://www.lapres.net/html/yahen.html>