The Problems of Jurisdiction on the Internet

Róisín Lautman, University of Ulster, UK

Kevin Curran, University of Ulster, UK

ABSTRACT

The relationship between jurisdiction and the internet has been the subject of wide ranging discussion ever since the boom in domestic internet usage. Without clear legislation, laws have been created on an ad hoc basis, often in response to specific cases. It is difficult to predict whether any one law will ever be sufficient to cope with the great variety of alleged crimes which take place on the internet. This paper discusses the problems associated with jurisdiction on the internet, presenting sample cases which have influenced the current laws and have fuelled a long term debate that continues to get more heated especially in recent times with UK celebrities being exposed on sites such as Twitter.

Keywords: Internet Jurisdiction, Internet Legislation, Internet Usage, Twitter, UK Celebrities

1. INTRODUCTION

What if information on the website of a company in country A, is considered defamatory, an infringement of copyright, or an interference with a business relationship, by a company in country B? What if the allegedly wronged party sues for one of the foregoing causes of action in country A? Would the company in country B have to undergo the trauma, expense, and inconvenience of defending itself in country A? Cases such as this highlight the importance of jurisdiction, the authority of the defendant over the subject matter that has led to the prosecution, the authority of the prosecuting court over the defendant, despite their geographical location and the locations in which the crimes were committed. Jurisdiction generally describes any authority over a certain area or certain persons. In the law, jurisdiction sometimes refers to a particular geographic area containing a defined legal authority. Determining jurisdiction in a case of internet crime has proved to be near impossible in many cases and in some cases it has appeared that the determining of jurisdiction has relied on opinion rather than fact (Whitehead & Spikes, 2006).

With the recent passing of the Digital Economy Act (passed in UK parliament on 7th of April 2010) the debate over internet jurisdiction has become highly public, with many people, including those the act claims to benefit, fiercely opposing its law, protesting that it is too severe and close minded. It has also in recent times exploded as a topic of conversation where a married footballer was named on Twitter as

DOI: 10.4018/jaci.2011070105

having an injunction over an alleged affair with a reality TV star. This particular footballer was eventually identified in Parliament as Ryan Giggs by Liberal Democrat MP John Hemming during a Commons question on privacy orders. The MP using parliamentary privilege to break the court order, said it would not be practical to imprison the 75,000 Twitter users who had named the player (Letts, 2011). This again was a problem of jurisdiction in that UK authorities simply knew that they could not ultimately defend against the 'chatter' on the Internet. This paper discusses the problems associated with jurisdiction on the internet, presenting well known cases which have influenced the current laws and have fuelled a long term debate that continues to get more heated.

2. COUNTRY SPECIFIC LAWS GOVERNING INTERNET JURISDICTION

Since the boom of domestic internet usage in the mid to late 1990's, new laws have been created to help dictate what should be considered as correct and legal use of the internet. This section of the paper will document and explain some of the most significant laws to have been passed in an attempt to govern the internet. The first real act governing the use of data in the UK in response to the introduction of computerised systems and networks in an industrial capacity was the Data Protection Act (DPA), first introduced in 1983 and amended in both 1987 and 1998. The DPA does not have much jurisdiction over internet usage as it mainly governs the holding of data on computerised systems and can only be applied if data has been transferred over the internet in a way that does not comply with the DPA, for example if it has been sent from a company's system that has the right to hold the data to a company's system that has no right to hold the data. The majority of laws that have come into force governing the use of the internet have been aimed at child protection, a major issue on the internet. In the UK it is illegal both online and offline to:

- Entice or coerce a child under 16 to engage in sexually explicit conduct
- Import or transport obscenity using telecommunications public networks
- Knowingly receive child pornography or advertise child pornography
- Depict minors (or appear to be minor) engaged in sexually explicit conduct (even in pseudo-form)
- Advertise sexually explicit conduct by giving the impression that minors are engaged in sexually explicit conduct

However the law does not govern explicit material that is transported into the UK, a problem of geographical jurisdiction. In cases like this, courts will rely on the country which has jurisdiction over the material to prosecute using their laws. In a child protection case this is rarely a major problem as, although there are not many laws governing the internet, many countries have laws governing child protection on the internet as this is publicly acknowledged to be one of the largest risks posed by the internet.

The US Congress has passed 3 major laws to govern child protection online. The Communications Decency Act, or CDA (1996), was Congress's first law to govern child protection. It made it illegal to place content that could be classified as 'indecent' on the internet where a child could access it. However, in 1997 it was ruled that the law was unconstitutional (did not comply with the US constitution) in that it suppressed the right to free speech by adults. In 1998 a more exclusive version of the CDA was passed, the Child Online Protection Act dictated that commercial websites most request users to verify their age before allowing them access to sexually explicit material. However the law again came up against the constitution, in 1999 a permanent injunction was ordered against its enforcement and in 2003 it was declared unconstitutional. Another law to be passed by the US Congress governing child protection was the Child's Internet Protection Act in 2000 which dictated that all schools and libraries that received federal government fund-

ing must install pornography blocking software on all their computers. This law encountered a constitutional argument from the Eastern District of Pennsylvania which ruled that the library portion of the law was unconstitutional; however after an appeal from the US government the Supreme Court overturned the Eastern District of Pennsylvania's ruling. As well as these child protection laws, the USA also has a number of laws in place to govern copyright, which can be argued has become a victim of the digital revolution (Sander, 1999).

The Digital Millennium Copyright Act (DMCA), which was made law in the USA in October 1998, made it illegal to facilitate unauthorized access to copyrighted works. Unlike the UKs Digital Economy Act, it did not hold Internet Service Providers responsible for users accessing file sharing sites but rather targeted those who created and maintained the sites (Lee, 2006). The DMCA only governs works that are complete and therefore are fully copyrighted and so in 2005, in response to the rise of the early release of products such as films and software before the company who is responsible for the product has made it publicly available and filming in movie theatres, the Family Entertainment and Copyright Act was introduced (Dean, 2004). In 2000, Ireland introduced the Copyright and Related Rights Act in an attempt to give artists and copyright holders the right to claim ownership over intellectual property such as sound recordings and writing, and the right to prosecute if the copyright has been deemed to have been broken (ISB, 2000). The most recent (and perhaps most controversial) legislation that has been passed in the UK regarding internet jurisdiction is the UK's Digital Economy Act (DEA). The act claims to protect the economy of the music and film industry by dissuading users by forcing Internet Service Providers to contact suspected offending users and restrict the broadband connection to an address if it has been proven that file sharing has taken place at that address and also block sites that are suspected of facilitating file sharing. Due to mass opposition to this penalty, it has been decided that fines shall be tested for one year and then it shall be decided by government whether or not to introduce restrictions to broadband service. The act comes after a massive rise in file sharing which many record companies and film studios have argued have broken copyright.

3. INTERNET JURISDICTION STANDARDISATION

The laws discussed in the previous section are all subject to geographical jurisdiction, meaning they are only enforceable if the person who is held responsible for the crime committed the crime within the borders of the country. There have been a number of attempts by international organizations to standardize copyright laws in order to remove the problem of geographical jurisdiction in copyright cases. In 2004 the European Union introduced the Intellectual Property Rights Enforcement Directive, which covers all civil courts in the member states of the EU. The directive addresses the intentional infringement of copyright on a commercial scale and aiding infringement of copyright (Nilsson, 2009).

The most recent international move to standardize laws governing the internet, and therefore removing a majority of jurisdiction problems, is the controversial Anti-Counterfeiting Trade Agreement (ACTA). The agreement is the result of negotiations between the USA, the EU and countries such as Japan, South Korea, Mexico and Australia on the international practice of file sharing. ACTA, which has not yet been introduced, dictates that ISPs all over the world would be held responsible for instances of file sharing if they did not impose a penalty on customers suspected of file sharing, such as restricting or removing their broadband connection. The area which many countries readily agree on in regard to the internet is the area of child protection and its jurisdictions. In order to combat international child abuse rings, the international authority Interpol works with 188 countries to help catch and prosecute child offenders. The introduction of the DEA comes after many campaigns by large record

companies and film studios that have sought to force ISPs to monitor their users to prevent file sharing. A landmark case in this long running campaign was the case of the Irish subsidiaries of EMI, Sony BMG, Universal and Warner against Eircom, Irelands largest ISP which began in March 2007. The record companies argued that Eircom was aware that the file sharing was taking place on their servers and yet had failed to implement measures to prevent this, such as software that filters internet traffic and can block specified recordings. In October of 2007, Eircom stated that it would not be feasible for them to run the specialised software on their servers and that they were not legally obliged to monitor the traffic on their servers (RTE, 2008).

Another case which has publicised file sharing and has fuelled the arguments of record companies and film studios is the case of the well known torrent search site piratebay.org. Torrents are quite simply the most common file type used for downloading. The pirate bay is based in Sweden and was initially launched in 2003 by the Swedish anti copyright organization *The Piracy Bureau*. In 2008 a criminal and civil prosecution case was brought against them and a Swedish businessman called Carl Lundström, who was accused of selling services to the site, by the Swedish Court supported by the International Federation of the Photographic Industry. The prosecutors claimed that in maintaining and hosting the site they had facilitated users in breaking copyright law. The defendants were found guilty on 17th April 2009 and sentenced to one year imprisonment and a fine of 2.7 million euro. This case was a landmark in the battle between file sharers and the companies that to claim to be adversely affected by this practice. In this case, personal jurisdiction was placed upon these website operators, despite that fact that none of the operators had directly contacted any users of the site and encouraged them to break copyright (Murphy, 2009).

In the case of copyright infringement on the internet, many people argue that it is hard to find the victim in many of the cases; however there are darker sides to internet crime which have very clear victims. With the rise of 'home-shopping', more and more people are transferring debit and credit card details over the internet which, on an unsecured network, can be extremely risky. Skilled hackers have been known to hack into many types of networks, such as online shopping and banking networks and view customers entire bank account details. Some criminal organizations have made an international business out of trading thousands of these stolen account details. In 2006, six men were convicted in Moscow of manufacturing 5000 false credit cards using stolen account details and selling them both in Russia and abroad (Rianovosti, 2006). The men were sentenced by Russian courts however it can be argued that as they sold the false credit cards to other countries apart from Russia, they facilitated credit card fraud in other countries and so they could also be liable to face trial in those countries. The most heavily legislated area of the internet is the area of child protection. Although internet crimes involving children can take place across a global network, many countries have been quick to act in these cases, despite geographical jurisdiction, for example in 2006 the U.S and international authorities charged 27 people in nine U.S states and three countries in connection to an international child pornography ring. However, in less developed countries which do not have a strong legal and justice system, cases of child pornography are rarely discovered and prosecuted and therefore result in child pornography from theses less developed countries being distributed internationally.

4. OPPOSITION TO INTERNET JURISDICTION

The majority of protests against acts such as the Digital Economy Act and the proposed Anti-Counterfeiting Trade Agreement have been based on issues regarding human rights. Groups such as the UK's House of Lord's Joint Committee on Human Rights has stated that "at the moment the Bill defines a process of appeals with no presumption of innocence" and that "[this] process will be applied irrespective of the sanction or evidence" (Arthur, 2010).

The DEA has been described as indiscriminate as, in an age where most UK households have internet access on multiple machines such as laptops and PCs and an increasing amount of cafes and hotels offering internet access to their customers, it could affect members of the public who have not violated the act.

Another argument on the topic of human rights is the right to privacy. To prosecute in a copyright infringement case, a user's internet activity must be tracked and logged and then this information must be passed from the ISP to the company lodging the infringement complaint. Human rights groups argue that this is too intrusive by removing users' right to privacy while they are browsing. The DEA has also received criticism from key ISPs. UK ISP TalkTalk is the first UK ISP to take a stand against the measures proposed by the DEA. They have stated that they will refuse to hand over customer details to any rights holder unless a court order can be obtained ordering them to do so and neither will they comply with the technical measures imposed by the bill, such as disconnecting or restricting a customer's broadband connection (Arthur, 2010). It has been debated that the current laws for imposing jurisdiction in internet cases, particularly in copyright cases, that the laws will not apply jurisdiction fairly, especially personal jurisdiction. It has been said that under the new DEA, personal jurisdiction will be exercised over innocent parties as the act targets the owner of the connection, not particular users.

The major argument in internet jurisdiction has been how to determine who should jurisdiction be applied to? And once that has been decided, how can they be held accountable? All connections to the internet have an Internet Protocol address (or IP address) and it is this address that prosecutors use to locate file sharing offenders. However, due to the rise in copyright infringement prosecution, experienced internet users have developed methods which can prevent companies from connecting an offending IP address to a user. The most common and long established method is the proxy server. A proxy server will navigate the internet on your computers behalf, acting as a relay between the internet and your machine, therefore any activity that could be punishable is tracked back to a server and not a user. This causes problems in determining jurisdiction, meaning that a rights holder who wishes to prosecute for an infringement of copyright must find a way to prove the service provider responsible, something which this paper has shown has been very difficult to do in past cases. Businesses have also risen out of the need to 'cover your browsing tracks' by hiding an IP address for a subscription fee. This is effect makes it impossible for a copyright holder to locate copyright infringements and therefore impossible to apply personal jurisdiction to a specific user. The only chance a copyright holder will have for prosecution is if they can prove that the subscription site is operating primarily for the use of illegal file sharing and therefore personal jurisdiction can be applied to the site. However this is very difficult to prove as a majority of these sites are advertised as merely aiding internet privacy and therefore can be argued as protecting user's human rights to privacy. The rise in wireless technology has also posed a problem in determining jurisdiction over file sharing cases. Any computer with the facility to connect to a wireless network can use a household's wireless connection without being inside the house, if the signal is strong enough to reach outside. It can be very easy to hack a household wireless connection, with step by step guides being made available online. This can result in wrongful accusations as it is the household router's IP address that is tracked, not an individual machine, therefore the household can be prosecuted for breaching copyright by illegal file sharing. It has been argued, even by intellectual property solicitors, that IP addresses alone are not enough to establish a firm case of file sharing. In 2008 Michael Coyle, an intellectual property solicitor with the firm Lawdit, stated that "The IP address alone doesn't tell you anything. Piracy is only established beyond doubt if the hard-drive is examined." It was revealed in 2008 that the file sharing site PirateBay had been inserting

random IP addresses; even of people who may not even know what file sharing is, into their list of downloaders, to mislead investigators (BBC, 2008).

5. CONCLUSION

The problems of internet jurisdiction are constantly evolving, as each new law is passed it creates loopholes, which in turn fuels the technology designed to take advantage of these loopholes. The main problem which seems to affect every law that is made is what exactly qualifies as a crime? Not all cases of internet jurisdiction are black and white and therefore it is impossible to create a blanket law that can be applied to all cases. It can only be said that when it comes to jurisdiction and the internet, it is an ongoing fight with no clear winners or losers on either side.

REFERENCES

Arthur, C. (2010, February). *Opposition to digital economy bill grows.* Retrieved from http://www.guardian.co.uk/technology/2010/feb/05/digital-economy-bill

BBC. (2008, February). *Games firms 'catching' non-gamers.* Retrieved from http://news.bbc.co.uk/1/hi/technology/7697898.stm

Dean, K. (2004, November). *A kinder, gentler copyright bill?* Retrieved from http://www.wired.com/politics/law/news/2004/11/65796

ISB. (2000). *Copyright and related rights act.* Retrieved from http://www.irishstatutebook.ie/2000/en/act/pub/0028/index.html

Lee, T. (2006). *Circumventing competition: The perverse consequences of the digital millennium copyright act: Policy analysis, no. 564*. Washington, DC: Cato Institute.

Letts, Q. (2011, May 24). *Good man John Hemming brought an end to the farce.* Retrieved from http://www.dailymail.co.uk/debate/article-1390215/Ryan-Giggs-super-injunction-John-Hemming-brought-end-farce.html#ixzz1O24eCqmw

Murphy, D. (2009, April 17). *The Pirate Bay founders sentenced to prison, website soldiers on.* Retrieved from http://www.engadget.com/2009/04/17/the-pirate-bay-founders-head-to-prison-website-soldiers-on/

Nilsson, H. (2009, October). *Sweden implements IP rights enforcement directive for copyright.* Retrieved from http://www.twobirds.com/English/News/Articles/Pages/Sweden_implements_IP_Rights_Enforcement_Directive_for_Copyright.Aspx

Rianovosti. (2006, June 16). *Moscow court gives lengthy jail terms to credit card fraud gang.* Retrieved from http://rianovosti.com/russia/20060616/49635773.html

RTE. (2008, April 21). *Eircom rejects record firms' claims*. Retrieved from http://www.rte.ie/business/2008/0421/eircom.html

Sanders, J. (1999). The regulation of indecent material accessible to children on the Internet. *Catholic Law*, 125-129.

Whitehead, R., & Spikes, P. (2003, July). *Determining Internet jurisdiction.* Retrieved from http://www.nysscpa.org/cpajournal/2003/0703/features/f072403.htm

Róisín Lautman is currently working in the Irish computing industry. Her research interests include internet law and network security.

Kevin Curran BSc (Hons), PhD, SMIEEE, FBCS CITP, SMACM, FHEA is a Reader in Computer Science at the University of Ulster and group leader for the Ambient Intelligence Research Group. His achievements include winning and managing UK & European Framework projects and Technology Transfer Schemes. Dr. Curran has made significant contributions to advancing the knowledge and understanding of computer networking and systems, evidenced by over 650 published works. He is perhaps most well-known for his work on location positioning within indoor environments, pervasive computing and internet security. His expertise has been acknowledged by invitations to present his work at international conferences, overseas universities and research laboratories. He is a regular contributor to BBC radio & TV news in the UK and is currently the recipient of an Engineering and Technology Board Visiting Lectureship for Exceptional Engineers and is an IEEE Technical Expert for Internet/Security matters. He is listed in the Dictionary of International Biography, Marquis Who's Who in Science *and* Engineering and by Who's Who in the World*. Dr. Curran was awarded the Certificate of Excellence for Research in 2004 by Science Publications and was named Irish Digital Media Newcomer of the Year Award in 2006. Dr. Curran has performed external panel duties for various Irish Higher Education Institutions. He is a fellow of the British Computer Society (FBCS), a senior member of the Association for Computing Machinery (SMACM), a senior member of the Institute of Electrical and Electronics Engineers (SMIEEE) and a fellow of the higher education academy (FHEA). Dr.. Curran's stature and authority in the international community is demonstrated by his influence, particularly in relation to the direction of research in computer science. He has chaired sessions and participated in the organising committees for many highly-respected international conferences and workshops. He is the Editor-in-Chief of the* International Journal of Ambient Computing and Intelligence *and is also a member of 15 Journal Editorial Committees and numerous international conference organising committees. He has served as an advisor to the British Computer Society in regard to the computer industry standards and is a member of BCS and IEEE Technology Specialist Groups and various other professional bodies.*