Shooting the Messenger? Recent Developments in the Area of Internet Service Provider Liability

Mark Wing

The struggle for the control of the internet and control of its content continues apace. Governments and rights holders seek new strategies and methods to bring a semblance of the control they have in the real world to the digital environment. How does one regulate what, supposedly, cannot be regulated?

It is clear that an individual is responsible for content they post on the internet, whether it is material infringing intellectual property rights on a peer-to-peer file-sharing system or on a website, or it is other illegal material such as child pornography and defamatory material. In some states with a less tolerant approach to individual freedoms this approach can extend to material critical of a government or its policies.

This article intends to focus, in particular, on the current debate concerning control over intellectual property infringement using peer-to-peer technologies *via* controlling internet service providers (ISPs).

There is a single fundamental problem with a strategy of pursuit of the individual user. However, there are so many of them that, especially, in areas such as intellectual property, enforcement prosecutions in the civil courts can only ever act as a deterrent and warning to other users. There is some evidence[1] that prosecutions have some effect, but not nearly as much as the rights holders would like, and this evidence is by no means unchallenged – for example, the Gowers Report notes (at paragraph 5.93) that peer-to-peer usage has still *doubled* in size since litigation commenced against users of it

[1] http://news.bbc.co.uk/1/hi/entertainment/4627368.stm.

in 2003.[2] The problems continue to be the difficulty of detection of wrongdoers, the confirmation of the identity of the person actually at the keyboard where, eg a PC is shared physically, or a single internet address is used by several PC's connected to the internet *via* a router using Network Address Translation (NAT), and jurisdictional problems related to legal proceedings outside the rights holder's own countries.

The explosion in the use of broadband internet has exacerbated the problem.[3] In the past downloading, for example, a DivX illegal copy of a film would have taken many hours or even days over a dial up internet connection. With a broadband connection this is reduced to just hours. With a broadband connection a single illegal mp3 digital music file takes just seconds, and an entire music album just minutes.

A new strategy has, therefore, been forming over the past few years. If it is difficult or impossible to regulate millions of internet users, it should be theoretically easier to regulate a smaller group, upon which the millions depend – their internet service providers (ISP).

There is no one clear definition of what an ISP actually is, but Tiberi and Zamboni[4] adopt a most worthwhile categorisation of the essence of what an ISP does and the legal liabilities that can arise thereunder. ISP activities typically revolve around at least one but usually a combination of:

- network operations, the hardware facilities that are needed for the transmission of data;
- provision of access, providing users with access to the internet and email accounts;
- provision of hosting services, rental of, eg web space;

[2] Gowers Review of Intellectual Property 2006, p103, accessed at http://www.hm-treasury.gov.uk/media/6/E/pbr06_gowers_report_755.pdf.

[3] http://www.statistics.gov.uk/cci/nugget.asp?id=8.

[4] L Tiberi and M Zamboni, 'Liability of Service Providers', 2003 *CTLR* 49.

- operation of bulletin boards, newsgroups and chatrooms being typical examples;
- information location tool provider, provision of tools assisting in locating information on the internet;
- content provider, providing actual online content, whether it be news, images music files software or any other digital content.

In the UK and other member states of the EU, governments have been pressing ISPs to prevent peer-to-peer file-sharing and other potentially illegal activities. In the UK's 2006 Gowers Report recommendation 39 stated:

> Observe the industry agreement of protocols for sharing data between ISPs and rights holders to remove and disbar users engaged in 'piracy'. If this has not proved operationally successful by the end of 2007, Government should consider whether to legislate.[5]

UK government officials have made it clear they will legislate on the matter if voluntary measures are not implemented.[6] It is the purpose of this work to examine the current legal and technical situation to see if these threats are either justified or workable from the perspective of a European Union ISP.

Internet Service Provider Liability

Overview

This is a complex topic involving potential liability of several fronts, including, perhaps most commonly, defamation and liability for intellectual property infringements – chiefly copyright. Overarching all the potential liabilities is European Union Law, specifically, the Electronic Commerce Directive.[7] The parts of this Directive of

[5] *Ibid*, note 2 above.

[6] http://news.bbc.co.uk/1/hi/technology/7059881.stm.

[7] Directive 2001/31.

particular relevance in this context are Articles 12-14.[8] To summarise these provisions – an ISP is not liable where they are a 'mere conduit' of information[9] or where they are merely caching information[10] or where they are hosting information and have no knowledge of anything illegal, and when they have such knowledge but act quickly and expeditiously to remove it.[11] This has led many in the ISP industry to simply disavow responsibility for infringements taking place, using their systems, as they are 'mere conduits'.[12] However, the matter is complicated by Articles 12(3), 13(2) and 14(3) of the Directive, which provide traditional remedies to prevent or stop infringements of rights.[13]

Article 14(3) also provides: 'This Article shall not ... affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.'

Where there is material which is deemed to be 'cached' or 'hosted' by an ISP, liability may also arise on receipt of actual knowledge of an infringement, followed by inactivity on the part of the ISP.

[8] These Articles are implemented in UK law by the Electronic Commerce (EC Directive) Regulations 2002/2013; Regulations 17-19 correspond to Articles 12-14.

[9] See discussion directly below on Article 12.

[10] See discussion below on Article 13.

[11] See discussion below on Article 14.

[12] See note 4 above.

[13] typically in an English court injunctive relief.

Recent Developments

A Duty for ISP's to Control their Networks?

SABAM v Tiscali (Scarlet)[14]

The Belgian authors collecting society initiated legal proceedings against Tiscali internet (who later became known as Scarlet) for failure to control their internet traffic – specifically, in this instance, for failing to control peer-to-peer downloading and uploading. Traditionally, ISPs have argued that, as they are 'mere conduits' of internet traffic, they are not liable for their user's activities. This is based on the provision in Article 12 of Directive 2000/31. The Brussels Court of First Instance considered the relationship between various provisions of the E-Commerce Directive and its implementation in Belgian law. As these are for the most part national implementations of pan-EU measures, the case is of considerable interest to those from any EU member state.

> Article 12
>
> 'Mere conduit'
>
> 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
>
> (a) does not initiate the transmission;
>
> (b) does not select the receiver of the transmission; and

[14] June 29, 2007 (so far unreported).

> (c) does not select or modify the information contained in the transmission.
>
> 2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Note in this context paragraph 3 of Article 12 - the mere conduit defence does not confer absolute protection. This paragraph would appear to suggest that ISPs remain under some form of duty of care, as suggested, *inter alia*, by Tiberi and Zamboni,[15] possibly under individual national laws. This matter is further explained by the various recitals to the Directive, in particular, recitals 42 – 48:

> (42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, *which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.* (author's emphasis)

[15] Above, note 4 (at page 51).

What is interesting, and potentially worrying, from an ISP's perspective about this recital's explanation is the following: If, through technological processes, it *becomes possible* or *it is already possible* to have both knowledge and control over the information transmitted across its systems, do the mere conduit and caching exemptions still apply? Is this why the expert's report on possible controls to peer-to-peer file-sharing in the *SABAM case* seemed quite crucial to the decision?

Article 15 of the Directive provides -

> Article 15
>
> No general obligation to monitor
>
> 1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
>
> 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

This is further explained by recital 47 and 48:

> (47) Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in

> particular, *does not affect orders by national authorities in accordance with national legislation.* (authors emphasis)
>
> (48) This Directive does *not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.* (author's emphasis)

Article 15, supported by recitals 47 and 48, states that there is no *general* duty to monitor internet traffic; indeed, member states are prevented from imposing such a duty. Could it be argued, however, that something such as peer-to-peer traffic represents a specific case in the terms of recital 47 or a certain type of illegal activity, as mentioned in the recital? It does seem clear these are specifically matters for national law.

Taking all these provisions together, it seems that the Court of First Instance of Brussels felt that Tiscali/Scarlet were under a duty to control the traffic on their network in a more forthright manner than had previously been the case. Reading Recital 42 of the Directive, it would appear the 'mere conduit' defence may not apply where an ISP is able to control the traffic on their system, or a general duty of care in national law was involved. It is trite to say, however, that a court can only order an ISP to do what is technically possible. A key factor in this case appears to have been the production for the court of a report by an expert setting out what control options were possible for the defendant.[16] A number of technical solutions to peer-to-peer traffic have become available in recent years, produced by companies such as Audiblemagic[17] Sandvine[18] and Safemedia,[19] among others.

[16] The SABAM press release, http://www.sabam.be/website/data/Communiques_de_presse/SABAM_vs_TISCALI_engl.pdf.

[17] http://www.audiblemagic.com/products-services/copysense/.

[18] http://www.sandvine.com/solutions/p2p_policy_mngmt.asp.

These solutions, installed in an ISP's premises, typically examine packets of data for characteristics which have characteristics of illegal traffic, incoming or outgoing to their networks, and block access to them or severely restrict the bandwidth allocated to the traffic. They are more or less completely automated and so require little direct action from an ISP's staff. This, at least, is the theory.

It is submitted that, while these solutions *may* be effective with the current standard peer-to-peer clients out there, if blocking becomes standard practice among ISP's, owing to threatened or actual litigation, it will not be long before new peer-to-peer clients come out, which can circumvent these systems. These systems may, then, adapt to the new clients and block them; then the clients adapt and become unblockable and a potentially endless circle develops of threat, followed by counter-threat, followed by new threat, similar to that which has been ongoing in the anti-virus market for several years. Such peer-to-peer clients, able to bypass common monitoring and preventative measures, are already out there.[20] Is it wise to legally oblige an ISP to become involved in this technical/legal merry-go-round, where one day's certain solution can be the following day's legacy software/hardware? Are courts and the legal process in fact equipped to deal with this extremely rapid-moving and complex technical area?

This matter is further complicated by several factors, for which no easy solutions have been put forward.

Firstly, increasingly, legitimate commercial concerns are using peer-to-peer variants to distribute data. Blizzard Software, for example, producers of the tremendously popular online role-playing game, *World of Warcraft*, use a BitTorrent (a common peer-to-peer client) derivative to download updates to this extremely popular game. Both Sky and the BBC also use peer-to-peer systems for their 'Sky Anytime' and 'iPlayer' systems. The reasons for this are quite

[19] http://www.safemediacorp.com/.

[20] See, for example, RODI a next generation peer-to-peer system at http://rodi.sourceforge.net/aboutRodi.html.

straightforward. Rather than have thousands of single users download from, eg, Sky's content provider server, which would place tremendous strain on the system with multiple requests, and occupy significant bandwidth, it is easier to spread the load around a distributed network of the companies' own servers and also from other downloaders who have already, at least, partially downloaded the content *via* peer-to-peer systems. By spreading the load across several or several hundred different systems, it places significantly less stress on the primary download server and the companies' bandwidth. Kontiki, the peer-to-peer technology used by Sky, is such an integral part of their system that removal of the software from a PC will cause the Sky Anytime systems to cease to function on that PC.

Thus, the line between illegal and legal uses and users of certain technologies is blurring, and this makes inspection and detection of genuine infringements significantly more difficult.

Secondly, Deep Packet Inspection (DPI) is an increasing concern to the internet community. Many of the next generation methods of detecting illegal material on an ISP's network use these technologies. Traditional packet inspection only 'scrapes the surface' of data packets, crossing a network by looking at their 'headers', and is easily bypassed or circumvented. DPI, by contrast, looks much further down into the data layers of a packet of data on a network and can be used to detect many forms of illegal activities. It can also be used to prioritise certain forms of internet traffic over others, such as favouring, for example, internet video which requires high bandwidth over something like peer-to-peer, which is seen to be undesirable, most traffic being illegal, and a high bandwidth consumer to boot. Being a relatively new technology, the legality of DPI has yet to be tested, and a full examination of the implications is outside the scope of this work. However, potential future sources of conflict may arise in relation to an individual's right to privacy under Article 8 of the European Convention of Human Rights, as well as legislation concerning data protection[21] and interception of communications. For

[21] Directive 2002/58 Article 5 Confidentiality of the communications.
1. Member States shall ... prohibit listening, tapping, storage or other kinds of interception or

example, it would not seem legal for ISPs to intercept and examine packets of data beyond a superficial level unless ordered to do so by the correct authorities, as required by, for example, the Regulation of Investigatory Powers Act 2000.

Anonymity of Users

Another key issue for ISPs is the anonymity of their users. When an individual uses the internet, their PC has an Internet Protocol (IP) address, unique to that machine. This address is a series of numbers such as 192.64.21.1, which identifies the computer. Every computer connected to the Internet has such an address. ISPs typically allocate their customers such addresses by one of two different methods – either *via* a static IP address – that is, a single user or network keeps a single address for use, or much more commonly, *via* dynamic IP addressing – that is, the user is allocated an IP address from a pool of available addresses each time they log in. Whichever method is used, it is a user's IP address that is the identifier of the user and their activities. Unfortunately, for rights holders a simple numeric address tells them little of illegal activities or potential targets for litigation. This address needs to be traced back to a specific internet service provider, and then the provider needs to supply the actual details of the user to the rights holders by matching the time and use of the internet address with its database of customers and their personal details. A number of companies specialise in this tracing process, perhaps the most high-profile being SafeNet MediaSentry Inc.[22] Perhaps, understandably, the ISPs have been reluctant to divulge the details of their paying customers, thereby exposing them to threatened or actual litigation. There are also issues concerning human rights, in particular, the right to privacy, and data protection rights, bound up in this question.

---

surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).

[22] http://www.mediasentry.com/index3.html.

A typical scenario would be – a user makes publicly available an mp3 music file *via* a peer-to-peer client, such as Kazaa or BitTorrent, for other users to upload from their PC. This act of making available constitutes an infringement of copyright throughout all EU member states, owing to national implementations of Article 3 of Directive 2001/29 which states:

> Article 3
>
> Right of communication to the public of works and right of making available to the public other subject-matter
>
> 1. Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.
>
> 2. Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:
>
> (a) for performers, of fixations of their performances;
>
> (b) for phonogram producers, of their phonograms;
>
> (c) for the producers of the first fixations of films, of the original and copies of their films;
>
> (d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.

> 3. The rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article.

The rights holders, therefore, need to obtain the personal details of the alleged infringer from the ISP before they can pursue legal action against the individual. This is actually a much used deterrent tactic by rights holders, and some high-profile examples have been made of users providing many files for upload off their system.

In the ECJ case, *Productores de Música de España Promusicae v Telefónica de España SAU*[23] the Advocate-General, Juliane Kokott, the advisor to the European Court of Justice, who produces a usually highly influential preliminary opinion on the legal issues involved in a case, concluded that ISPs were not obliged to reveal personal data of their clients in cases concerning civil litigation. This opinion, if followed by an ECJ ruling, could severely restrict the ability of intellectual property rights holders, in particular, to track down individuals who allow large-scale uploads off their systems.

This case concerned a typical dispute between an ISP and a rights holder. The Spanish collecting society for music, Promusicae, requested client details from the ISP Telefonica so that they may enforce their members' rights against alleged infringers on Telefonica's network. This request concerned users of the Kazaa peer-to-peer client. Telefonica retained such data for a set period, and Promusicae wanted it.

The Advocate-General's opinion looked at the relationship between a number of different directives, but her primary focus was on Directive 2002/58.[24] The Advocate-General stated this Directive derived from

[23] C-275/06 ECJ.

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201 , 31/07/2002 P. 0037 – 0047.*

fundamental human rights, including, especially, the right to Privacy and Family Life, enshrined in Art 8, ECHR.[25]

A fundament of Directive 2002/58 is Article 5(1):

> Confidentiality of the Communications
>
> 1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

This general principle is subject to exceptions, however, just as the basic human right to privacy is subject to exceptions where they are necessary in a democratic society and proportionate.[26]

Promusicae tried to argue that some of the exceptions, found in either Article 6 or Article 15 of Directive 2002/58, might have applied. In particular Article 15 (1) is relevant here:

> Article 15
>
> Application of certain provisions of Directive 95/46/EC

[25] Paras 51-54.

[26] Art 8(2).

> 1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes *a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system*, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union. (authors emphasis)

The Advocate-General, however, rejected that any of the exceptions in Article 6 or 15 applied to the general duty of confidentiality, expressed in Article 5 (1) in the case of disclosure of customer or traffic data by an ISP to a litigant or potential litigant.

This view, if followed by the ECJ, has widespread implications for intellectual property enforcement in the EU by rights holders against peer-to-peer and other potential intellectual property infringers. In future, enforced disclosure of such details might only be possible for one of the purposes set out in Article 15 – which would typically be to government agencies, or by order of the court. Matters relating to national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system relate to essentially criminal matters, and not the civil lawsuit of copyright infringement.

Practical realities being what they are, most rights holders will not be using a potentially expensive and complex procedure against individuals where there is little realistic chance of getting the financial outlay for such an action back from the defendant.

The Final decision of the European Court in *Promusicae* is much anticipated and needed by the member states. There is much confusion, evident in the decisions of national courts in several member states attempting to reconcile several related directives on areas such as intellectual property rights, their enforcement, and the relationship between those directives and those on Data Protection.[27] This may be a double-edged sword, however, for ISPs. If rights holders find it increasingly difficult to pursue more obvious infringers using peer-to-peer or other web technologies, the focus may turn even more towards the ISPs, and this may result in more, not less, litigation.

To conclude, the focus of both government and intellectual property rights holders are very firmly placed upon ISPs at this time. This is an unenviable position for the ISPs to be in. The bodies representing the rights holders and governments seem to regard asking ISPs to get more involved in helping to prevent and punish intellectual property theft as a key strategy in their plan – to quote Gower. There is a logic to this, but any measures, eventually adopted, need to take account of the considerable technical and legal complexity involved in any solutions. Recent suggestions by the music industry to extend the liability of ISPs[28] are probably unworkable, not least because of the UK's obligations under the various directives already discussed. The Gower Report's suggestion to create a 'Best Common Practice' (BCP) document, agreed between the ISP's and rights holders, remains a good solution, and is being discussed at length at the time

[27] See, for example, E Prosperetti, 'The Peppermint "Jam": peer-to-peer goes to court in Italy', (2007) 18(8) *Ent LR*, 280-283; D. Stols, '*Brein v KPN Telecom* and the Dutch Civil Code – ISPs under pressure', (2007) 18(4) *Ent LR* 147-149.

[28] Association of Independent Music (AIM), the MCPS-PRS alliance and the Musicians' Union, joint release, issued on July12, 2006 for a 'Value Recognition Right'.

of writing (Autumn 2007). However, securing agreement for this is not going to be easy with the current legal framework.

Rights holders want speedy discovery of the details of individual infringers of their rights. However, an ISP that conforms with this may well be risking alienating other customers of theirs, which in a very competitive industry is most unwise. It may also leave itself open to claims that it has breached privacy rights and rights associated with data protection law of the user, whose details are given to rights holders.

Rights holders may want infringing users to be cut off from the Internet or have their accounts suspended. Again, this raises a minefield of potential problems for the ISP. If an ISP suspends an internet connection, increasingly, these days the ISP will not only be suspending access to the internet but could be also suspending access to voice over IP telephone services such as Skype, and also television and many others. This could be illegal under Telecoms legislation and may result in the involvement of OFCOM.

Rights holders may wish for illegal peer-to-peer traffic to be blocked over an ISP's network. But, how do you distinguish the illegal uses from increasing legal uses of the method? Even detecting the type of traffic that is illegal may itself be of questionable legality if DPI is used. Is an ISP legally permitted to look so deeply into traffic data of users, which may reveal all sorts of things about that user (not just that they are conducting an illegal peer-to-peer file-sharing, but perhaps, also, their political interests, their sexual orientation, their relationships or any one of a number of other possibilities, which are properly private, and considered sensitive data under data protection legislation? To use an analogy, it is like expecting the post office to open every piece of mail to check for correspondence relating to illegal activities. DPI is an intentionally intrusive technology which might be effective at controlling peer-to-peer technologies of today, but for which encryption of the packets of data sent by any internet application, including peer-to-peer clients, can effectively defeat it. If DPI is in fact legal, expect the next big internet peer-to-peer client to

find a way around it. Just as, when Napster was shut down, the internet community looked to much more distributed models to bypass the Napster ruling, and systems such as Kazaa and Edonkey came about, so, the same is likely to happen with any effective technical form of detection or control today. That control is only likely to be temporary.

What is needed today is for the rights holders to continue to provide low cost affordable and value-added services, related to music and other copyright content. Considerable new profits are being made in this area. They need to work together to come up with a common standard for digital rights management solutions which allow them to protect what they distribute and which do not inconvenience the users of their products any more than a bare minimum, and they need to continue to build a constructive relationship with internet service providers. But, that solution needs to recognise the extremely difficult position ISPs are in, given the current legal framework[29].

[29] The author would like to thank Peter Milford, the Regulatory Affairs Manager of Newnet plc for his generous input and advice on the technical aspects of this article.