

Internet access controls: Three Strikes 'graduated response' initiatives¹

Johnny Ryan, Senior Researcher, IIEA and Caitriona Heintz, Researcher, IIEA

May 2010

Note for comment

Project Introduction

The Institute of International and European Affairs (the "IIEA") has been commissioned by the European Commission to prepare a study of non-legislative measures to prevent the distribution of violent radical content on the Internet.

More detail on this research project can be found at <http://www.iiea.com/staff?workingGroupUrlKey=violent-radicalisation> and in the project's Terms of Reference.²

¹ The views presented in this draft note are not necessarily the view of the Institute of International & European Affairs.

² http://ec.europa.eu/justice_home/funding/tenders/2009_S041_058796/annex_1_en.pdf

Table of Contents

Introduction	3
EU Member States.....	4
The EU Telecommunications Reform Package	4
France - a legislative approach	5
Ireland – a non-legislative approach	6
Technical issues	8
1. Deep packet inspection: Audible Magic.....	8
2. IP hunting: DtecNET.....	10
Italy	11
United Kingdom.....	12
Other countries	14
The Anti-Counterfeiting Trade Agreement (ACTA)	14
New Zealand.....	14
South Korea	15
Taiwan.....	15
Conclusion.....	17

DRAFT

Introduction

This document presents an overview of “three strikes” measures, what they seek to achieve, the mechanisms by which they operate, and the difficulties currently experienced within the EU and beyond in their introduction. The purpose of this document is to establish whether a three strikes mechanism is applicable to illegal violent radical content online, and whether it is transferrable across the EU.

Though three strikes measures are in prospect in a number of EU Member States, no functioning system has yet been implemented as a matter of government policy. Ireland, where the dominant ISP has recently agreed to implement a three strikes system, offers an insight into the technical measures proposed for this system. Since the three strikes approach is at so early a stage this study also includes a number of related initiatives in countries beyond the EU to provide sufficient information.³

Note: Three strikes measures, also referred to as “graduated response”, are not explicitly mentioned in the Terms of Reference for the NLM Study. However they represent a developing mechanism by which authorities in many Member States and Third Countries are presently seeking to prevent the dissemination of illegal, in this case copyright infringing content. As an experimental and highly visible instance of measures, in some cases non-legislative measures, the three strikes system is within the study team’s remit.

This document is a necessary product of the NLM study for the simple reason that, to our knowledge, no other overview of three strikes initiatives is presently available.

³ Note re Singapore: It was incorrectly reported by various media outlets that Singapore was considering implementing a three-strikes option in August 2009. The Intellectual Property Office of Singapore (IPOS) clarified the matter on its website. No further statements on the matter have been issued by IPOS, indicating that Singapore has not taken a decision to pursue a three-strikes system. See “Graduated Response Systems or “Three Strikes” Law”, IPOS website, 24 August 2009 (URL: www.ipos.gov.sg/ipos/template/Index.aspx, last accessed 11 April 2010).

EU Member States

The EU Telecommunications Reform Package

The EU Telecommunications Reform Package was agreed on 5 November 2009, following two years of negotiations. The European Parliament formally endorsed the Package on 24 November 2009.

This Reform Package includes a new Internet freedom provision, which allows for the protection of citizens' rights relating to Internet access. It provides that

Measures taken by Member States regarding end-users' access to or use of services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law.⁴

In addition the new provision states that measures taken by Member States must have "due respect for the principle of presumption of innocence and the right to privacy".⁵ Furthermore, "the right to an effective and timely judicial review shall be guaranteed".⁶ This is due to be transposed into national legislation in the Member States by June 2011.

The Internet freedom provision refers to measures taken by Member States and does not expressly refer to the actions of private sector parties such as Internet Service Providers (ISPs). However, Viviane Reding, then Commissioner for the Information Society and Media, declared that, "any measures taken regarding access to and use of services and applications must always respect the fundamental rights and freedoms of citizens".⁷ It might be construed that this will also prevent ISPs from disconnecting users' Internet access without some form of judicial procedure.⁸

Furthermore, it is unclear whether the provision will also apply to a non-legislative three strikes mechanisms such as that due to be implemented in Ireland by private agreement between the Irish ISP, Eircom, and the representative body of the music industry in Ireland, IRMA. However, the Internet freedom provision refers to the protection of citizens' fundamental rights by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. It is uncertain whether the legal standing of such agreements could be called into question. There exists the possibility of further action by the Commission, or a decision to this effect by the courts of a Member State or the Courts of Justice of the European Union.

⁴ Article 1(3)a, amendments to Directive 2002/21/EC, amended in Directive 2009/140/ec of the European Parliament and of the Council, 25 November 2009.

⁵ *ibid.*

⁶ *ibid.*

⁷ Speech by Commissioner Viviane Reding, Barcelona, 23 November 2009 (URL: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/551>, last accessed 21 April 2010).

⁸ "European Commission: No 3 Strikes without Judicial oversight", 24 November 2009 (URL: <http://torrentfreak.com/european-commission-no-3-strikes-without-judicial-oversight-091124/>, last accessed 16 April 2010).

France - a legislative approach

The Creation et Internet Bill, more commonly known as HADOPI, was initially introduced in May 2009. It provided for the creation of a new authority, the Higher Authority for the Distribution of Works and the Protection of Copyright on the Internet (HADOPI), to oversee a graduated response system to online copyright infringement. The new authority would receive complaints about copyright infringers from rights-holders, and would issue warning notices to Internet users by way of their ISPs. After two such warnings an Internet user's access could be disconnected for up to one year.⁹ A user disconnected in this way would also be placed on a national blacklist that would prevent their reconnecting to the Internet with a different service provider. The legislation did not provide for the prior intervention of judicial authorities.

The HADOPI Bill was struck out by the French Constitutional Court in June 2009. The Court deemed the Bill was unconstitutional because it gave the new HADOPI agency judicial functions, such the power to sanction Internet users without the oversight of a court. These powers were deemed inappropriate for an administrative authority.¹⁰ The Constitutional Court also referred to Amendment 138 (now known as Amendment 46) of the EU Telecommunications Reform Package, which states that it is a violation of fundamental rights to disconnect an alleged copyright infringer without receiving a prior ruling from judicial authorities, in accordance with Article 11 of the Charter of Fundamental Rights of the European Union.¹¹

Following the Constitutional Court's decision the HADOPI Bill was redrafted to allow for the new agency to report alleged copyright infringers to the courts following receipt of three warnings. Under the redrafted legislation cases are to be reviewed by the judiciary, which can impose sanctions including the disconnection of Internet access, a fine of €300,000, and a two-year prison sentence. This legislation was approved by the Senate in October 2009, and was due to come into force in January 2010.

However, its entry into force has been delayed by the Commission Nationale de l'Informatique et des Libertes (CNIL), the government agency dealing with personal data and online privacy, which must first approve the legislation before its entry into force. The CNIL has not yet given its approval since it must ensure that data collection by HADOPI will not affect data privacy.¹² Its entry into force may be further delayed if issues arise in its

⁹ "France to cut illegal download connections", 13 May 2009, David Hamilton (URL: www.laquadrature.net/en/the-whir-france-to-cut-illegal-download-connections, last accessed 19 April 2010)

¹⁰ "French court savages "three-strikes" law, tosses it out", Nate Anderson, 10 June 2009 (URL: <http://arstechnica.com/tech-policy/news/2009/06/french-court-savages-3-strikes-law-tosses-it-out.ars>, last accessed 19 April 2010)

¹¹ "Eircom/IRMA three-strikes deal rocked by French court ruling, 11 June 2009, SiliconRepublic.com (URL: www.siliconrepublic.com/news/article/13175/comms/eircom-irma-three-strikes-deal-rocked-by-french-court-ruling, last accessed 19 April 2010); see also "Commission position on Amendment 138 adopted by the European Parliament in plenary vote on 24 September 2008" (URL: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/681>, last accessed 21 April 2010).

¹² "France three strikes law by govt's own data watchdog", 5 January 2010, Ars Technica (URL: <http://arstechnica.com/tech-policy/news/2010/01/france-three-strikes-law-delayed-by-govts-own-data-watchdog.ars>, last accessed 19 April 2010).

harmonisation with the EU Telecommunications Reform Package of November 2009.¹³

In January 2010 Trident Media Guard (TMG), a private investigative company, was appointed by an industry association, the Société Civile des Producteurs Phonographiques (SCPP), to track down and report copyright infringers to the authorities. TMG will pass data on alleged infringements to the SCPP who will manually review and then transmit to HADOPI.¹⁴ Should copyright infringers move from P2P to other methods of distribution, as may have occurred in the aftermath of the initial HADOPI debate, the legislation and the systems used by TMG would not cover their activities.¹⁵ However, TMG has announced that after one year of P2P investigating the company will proceed to examine other platforms for sharing to allow for new patterns in infringement.¹⁶ Details of how the TMG system operates are unclear, but it appears to be similar to the DtecNET system, which is discussed in the next section.

Ireland – a non-legislative approach

Unlike France, Italy, and the United Kingdom, where three-strikes measures have been mooted as national policy, the discussion in Ireland on three-strikes has revolved around a legal battle between the representative body of the recording industry in Ireland and the largest ISP in the country, Eircom.

A case in the Irish High Court between Eircom and the Irish Recorded Music Association (IRMA) resulted in a settlement in January 2009. Under the agreement Eircom has committed to:

1. inform its broadband subscriber that the subscriber's IP address has been detected infringing copyright and
2. warn the subscriber that unless the infringement ceases the subscriber will be disconnected and
3. in default of compliance by the subscriber with the warning it will disconnect the subscriber.¹⁷

Since this constitutes a private agreement by way of court settlement, and since there is no court ruling on the matter, it does not constitute legal precedent.

¹³ "As in UK, French Three Strikes May Be Delayed To After Elections", *The Guardian*, 4 January 2010, last accessed 19 April 2010.

¹⁴ "Hadopi : TMG désigné pour traquer les pirates", 01net, 25 January 2010 (URL: www.01net.com/editorial/511544/hadopi-tmg-designe-pour-traquer-les-pirates/), last accessed 2 May 2010).

¹⁵ Based on new study published by the University of Rennes, last accessed 19 April 2010. See "Piracy rises in France despite three strikes law", *TorrentFreak*, 9 March 2010 (URL: <http://torrentfreak.com/piracy-rises-in-france-despite-three-strikes-law-100609/>), last accessed 2 May 2010).

¹⁶ "Hadopi : TMG désigné pour traquer les pirates", 01net, 25 January 2010 (URL: www.01net.com/editorial/511544/hadopi-tmg-designe-pour-traquer-les-pirates/), last accessed 2 May 2010).

¹⁷ "Ireland - P2P infringement case settled", Press Release, IRMA, 29 January 2009 (URL: http://www.ifpi.org/content/section_news/20090129a.html, last accessed 2 May 2010); for more detail on the particulars of the settlement see paras 9-13 of the judgement in the case of *EMI Records & Ors -v- Eircom Ltd*, [2010] IEHC 108, 16 April 2010 (URL: www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d8840802577070035082f?OpenDocument, last accessed 1 May 2010).

Yet the settlement is significant not only because Eircom is the largest broadband wholesaler in Ireland with 40% of the market, but also because its settlement with IRMA was predicated on IRMA's concluding similar agreements with other ISPs in Ireland under which they would also be required to implement a three-strikes system that would negate any competitive disadvantage that Eircom might have suffered had it been the only ISP to do so.¹⁸ To this end IRMA took BT Ireland and UPC Ireland to court in June 2009. The proceedings were stalled when the Data Protection Commissioner raised a number of data protection concerns that put the original IRMA-Eircom settlement into question.

In a letter of 4 December 2009 Data Commissioner asked whether "data comprising IP addresses... constitute "personal data" for the purposes of the Data Protection Acts", and whether Eircom's processing of this data "represent[s] 'unwarranted [processing] by reasons of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject?'. Finally, the Data Protection Commissioner asked:

is it open to EMI and/or Eircom to implement the graduated response process ... where:

(a) In doing so they would be engaged in the processing of personal data and/or sensitive personal data (in so far as the data can be considered to relate to the commission of a criminal offence), including the provision of such data from one private entity to another private entity; and

(b) The termination of an internet user's subscription by Eircom would be predicated on the internet user in question having committed an offence ... but without any such offence having been the subject of investigation by an authorised body; and, further, without any determination having been made by a court of competent jurisdiction, following the conduct of a fair and impartial hearing...¹⁹

Yet according to a FAQ document on the IRMA website, "ISPs will be reacting to information legally obtained by copyright holders who have accessed P2P networks where it is publically available".²⁰ In April 2010 the High Court rejected the Data Protection Commissioner's concerns. In his judgement Mr Justice Peter Charleton was influenced by the fact that

Neither DtecNet ... nor any of the plaintiffs whose copyright material is being infringed would ever know through this process that the infringer is a particular person living in a particular place in Ireland. What they do know is that a particular IP address has been involved in the downloading.²¹

Eircom alone would know the identity of the alleged infringer, and how that person is treated. The only data IRMA is to receive are aggregated data

¹⁸ "Major music labels in court move to force internet providers to act on downloads", *Irish Times*, 20 June 2009.

¹⁹ Data Protection Commissioner's letter 4 December 2009, language rephrased in letter of Philip Lee of 15 January 2010, quoted in Judgement in the case of EMI Records & Ors -v- Eircom Ltd, [2010] IEHC 108, 16 April 2010 (URL: www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d8840802577070035082f?OpenDocument, last accessed 1 May 2010).

²⁰ IRMA website FAQ (URL: www.irma.ie/piracy_faq.htm#grc, last accessed 6 April 2010).

²¹ Judgement in the case of EMI Records & Ors -v- Eircom Ltd, [2010] IEHC 108, 16 April 2010 (URL: www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d8840802577070035082f?OpenDocument, last accessed 1 May 2010).

prepared by Eircom showing annual figures for number of 1st, 2nd, and final notices issued. Moreover, the judgement observed that there was no requirement for investigation by a court since “to determine that an offence has in fact been committed. That is because ... no one is accusing anyone of an offence. There is no issue as to anything beyond civil copyright infringement”.²²

Mr Justice Charleton concluded that “these are adequate procedural safeguards in the protocol [established under the settlement between IRMA and Eircom] and there is conformity, in addition, in my view, with” the new EU Telecommunications Reform Package.²³ However, he also noted that “the right to an effective and timely judicial review can be enabled by the State”.²⁴ However, it remains to be seen whether the decision of the High Court in April 2010 will be appealed for further consideration. IRMA is now resuming its court case against UPC, another major ISP in Ireland, on June 2010. Other negotiations with ISPs that were paused pending the Court’s decision are being resumed. IRMA expects that most of the market will agree in the near future - though this is not by any means guaranteed.²⁵

Technical issues

IRMA’s case against UPC is technically significant because UPC’s network differs from Eircom’s and would require a different technical approach. These two approaches are examples of the primary methods currently favoured by ISPs and, or, rights-holders pursuing three strikes mechanisms in Ireland and elsewhere.

1. Deep packet inspection: Audible Magic

IRMA adopted a technology neutral approach, inviting the ISPs to propose technologies suited to their respective networks.²⁶ However, an FAQ on the IRMA site cites an expert’s report produced during the Sabam v Scarlet (previously Tiscali) case in Belgium in 2007, which indicates one possible technical approach.²⁷ The SABAM v Scarlet case was taken by rights holders represented by the Société d’Auteurs Belge (SABAM), who sought to force an ISP (Scarlet) to act against users transferring music that infringed copyright via peer-to-peer connections (P2P) across its network. The expert consulted in the case referred to a system called “Audible Magic”,²⁸ which IRMA initially thought applicable to the Eircom network. However, Eircom’s network does not support “deep packet inspection” (DPI), which is required to operate Audible Magic. UPC’s network on the other hand does.

²² *ibid.*

²³ *ibid.*

²⁴ *ibid.*

²⁵ Interview with IRMA, April 2010.

²⁶ *ibid.*

²⁷ IRMA website FAQ (URL: www.irma.ie/piracy_faq.htm#grc, last accessed 6 April 2010).

²⁸ English Translation of Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels, 29 June 2007, translated by Fran Mady, Julien Bourrouilhou, and Justin Hughes

Cardozo Arts & Entertainment Journal (URL:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1027954, last accessed 6 April 2010), pp. 4-5.

DPI is a system of inspecting packets of data crossing a network for various purposes such as the gathering of statistics, targeted advertising, identification of spam and viruses, and of copyright infringing content in the case of Audible Magic.²⁹ It remains to be seen how the DPI reliant approach tallies with Article 15 of the E-Commerce Directive, which states that ISPs will not be under a general obligation of monitor traffic on their networks, nor should they be put under “a general obligation to seek facts or circumstances indicating illegal activity”.³⁰

In any event, the Audible Magic system faces significant technical difficulties. The Audible Magic system was initially developed to allow businesses duplicating large volumes of CDs to check that clients seeking to replicate media held the rights to do so. The audible magic system faces difficulties online that do not apply to the off line CD duplication system. As Scarlet noted in its 2007 case, the expert noted certain caveats about Audible Magic. Among these was “the growing use of encryption in this type of application ... over the middle term (2-3 years)”.³¹ In reality, by this time P2P applications had already begun to include encryption for a number of years.³² IRMA’s FAQ suggests that encryption is not a substantial problem for such a system on the grounds that:

[m]ost peer-to-peer traffic is currently not encrypted. While encrypted traffic may call for a different approach to filtering, it certainly does not prevent the use of technology to tackle infringements.³³

If most P2P traffic is not encrypted at present this could rapidly change because many freely available P2P programs have the facility to encrypt built in. Since P2P software can use industry standard encryption widely used in other programs, which is of a standard sufficient to provide assurance to online consumers that their transactions are secure, it is unlikely that this could be easily decrypted and examined.

The expert in the SABAM v Scarlet case also noted that Audible Magic was targeted at the education sector and might not scale up to suit a large network operated by an ISP. “A high acquisition and exploitation cost [might be required] to compensate for this under-design”.³⁴ This second point may have already been resolved.

In addition to these two reservations, Audible Magic had already been the subject of two notes from the Electronic Frontier Foundation (EFF) in 2004

²⁹ As a broader general observation, the question to what extent might DPI reintroduce the controls that had been built into the X.25 protocol in the 1970s, and from which TCP/IP liberated us, deserves immediate and earnest discussion.

³⁰ Article 15.1, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, the “E-Commerce Directive”.

³¹ English Translation of Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels, 29 June 2007, translated by Fran Mady, Julien Bourrouilhou, and Justin Hughes, *Cardozo Arts & Entertainment Journal* (URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1027954, last accessed 6 April 2010), pp. 4-5.

³² “Debunking Audible Magic — Again”, EFF, 20 July 2004 (URL: http://w2.eff.org/share/audible_magic.php?f=audible_magic2.html, last accessed 6 April 2010).

³³ IRMA website FAQ (URL: www.irma.ie/piracy_faq.htm#grc, last accessed 6 April 2010).

³⁴ English Translation of Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels, 29 June 2007, translated by Fran Mady, Julien Bourrouilhou, and Justin Hughes, *Cardozo Arts & Entertainment Journal* (URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1027954, last accessed 6 April 2010), pp. 4-5.

that indicated it was vulnerable to circumvention.³⁵ The EFF reported that “Audible Magic’s technology can easily be defeated ... by modifying the behaviour of the network stack to ignore RST packets”.³⁶ As one observer noted, this is the same method of circumvention used by the Computer Security Group at Cambridge University in 2006 to defeat the Chinese “Great Firewall”.³⁷

If UPC does implement a three strikes system using Audible Magic a range of challenges, technical and legal, may arise.

2. IP hunting: DtecNET

Though UPC and some other ISPs have networks that are equipped for DPI, Eircom does not. This means that Audible Magic can not function upon it, and an alternative system is required. According to IRMA this will be provided by a company called DtecNET.³⁸ A recent judgement from the Australian Federal Court, released in February 2010, reveals how the DtecNET system operates.

In late 2008 the Australian Federation Against Copyright Theft (AFACT) brought a case against an Australian ISP called iiNet, who it accused of facilitating infringement of copyright. AFACT acted on the basis of data provided by DtecNET. DtecNet is a private detective service that searches for instances of file sharing on P2P networks, and had been used by AFACT since August 2007 to gather the IP addresses of alleged copyright infringers using the BitTorrent P2P system.³⁹

While Audible Magic operates as a part of an ISPs own network, acting on data in transit, DtecNET operates independently from the ISP. DtecNET subscribed to iiNet and used BitTorrent to observe the addresses of other file sharers on the same P2P network. The company uses a customised BitTorrent client program called “DtecNET Agent” that opens .torrent files in the same manner that normal client programs do in order to commence a download. The judgement describes how the agent operated:

the DtecNet Agent downloaded one complete copy of the film sought to be investigated. ... The DtecNet Agent then reconnected to iiNet users who had a copy of the file or parts of the file of interest and downloaded a piece of that file from those users. It then matched the piece downloaded with the piece hash through [a] hash checking process. ... The DtecNet Agent then recorded information referable to the peer from which it had downloaded that piece of the file. ... Every aspect of the

³⁵ “Audible Magic - No Silver Bullet for P2P Infringement”, EFF 12 July 2004 (URL: w2.eff.org/share/audible_magic.php?f=audible_magic.html, last accessed 6 April 2010); Debunking Audible Magic — Again, EFF, 20 July 2004 (URL: http://w2.eff.org/share/audible_magic.php?f=audible_magic2.html, last accessed 6 April 2010).

³⁶ “Audible Magic - No Silber Bullet for P2P Infringement”, Electronic Frontier Foundation, 12 July 2004 (URL: http://w2.eff.org/share/audible_magic.php, last accessed 11 April 2010).

³⁷ “Evading Audible Magic's Copysense filtering”, Taint.org, 12 March 2008 (URL: <http://taint.org/2008/03/12/124926a.html>, last accessed 11 April 2010); “Ignoring the “Great Firewall of China”, 27 June 2006 (URL: www.lightbluetouchpaper.org/2006/06/27/, last accessed 11 April 2010).

³⁸ Interview with IRMA, April 2010.

³⁹ DtecNet’s initial investigation examined four different file sharing protocols before concentrating on BitTorrent. See Judgement in the case of Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24, 4 February 2010, p. 29.

connection and download was recorded and logged by the DtecNet Agent ... and stored securely on DtecNet's servers ... in Copenhagen.⁴⁰

AFACT presented iiNet with various data that DtecNET compiled on infringements, including IP addresses of alleged infringers.⁴¹ It should be noted that the citation of IP address, which is commonly used under the Digital Millennium Copyright Act (DMCA) in the United State to track illegal torrent downloads to a downloader's IP, has been vulnerable at least in some cases to "spoofing", circumvention which results in warnings being sent to the wrong IP address.⁴² In addition to IP address details DtecNET also provided alleged infringers' PeerIDs, a unique address generated by BitTorrent client programs, which the Court accepted as proof that the DtecNet Agent could show that multiple instances of infringement emanated from a single computer.⁴³ Though iiNet fought against AFACT in court, its CEO, Michael Malone, agreed that the DtecNET method of collecting evidence was "compelling".⁴⁴ He regarded DtecNET approach as far more credible than that of a different company that rights holders had previous employed (Media Sentry).⁴⁵ Moreover, because DtecNET acts as just another client in the BitTorrent swarm of connected computers, encryption that might baffle a DPI based system such as Audible Magic is rendered irrelevant.

Italy

Three strikes measures may be pursued by the Italian Government, subject to developments in France. On 20 January 2009, the Italian Ministry of Culture made an agreement with its French counterparts that both countries would cooperate against copyright infringement.⁴⁶ The Italian Minister for Culture, Sandro Bondi, announced that Italy would follow the "French model". The delays in the HADOPI proposals suggest a degree of uncertainty about the future of the Italian three strikes system.⁴⁷

⁴⁰ *ibid.* pp 34-5.

⁴¹ These were the date and time of incidents, relevant IP addresses of iiNet customers at the time of infringement, the title of the content that was allegedly infringed, and the name of the rights holder, 'PeerID', 'Peer client info', 'Target Port' and 'Fingerprint'. See Judgement in the case of Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24, 4 February 2010, pp 29-30, 45.

⁴² Michael Piatak, Tadayoshi Kohno, Arvind Krishnamurthy, "Challenges and Directions for Monitoring P2P File Sharing Networks – or – Why My Printer Received a DMCA Takedown Notice", USENIX Workshop on Hot Topics in Security 2008 (URL: http://dmca.cs.washington.edu/dmca_hotsec08.pdf, last accessed 11 April 2010).

⁴³ Judgement in the case of Roadshow Films Pty Ltd v iiNet Limited (No. 3) [2010] FCA 24, 4 February 2010, p. 79.

⁴⁴ *ibid.*, p. 51.

⁴⁵ *ibid.*, p. 51, see also p. 143.

⁴⁶ *The Hollywood Reporter* (URL: www.hollywoodreporter.com/hr/content_display/news/e3i40152e91c349224f967b46592f151b71, recited from "Italy to Follow French 3 Strikes Model for P2P", *TorrentFreak*, 21 January 2009 (URL: <http://torrentfreak.com/italy-to-follow-french-3-strikes-model-for-p2p-090121/>, last accessed 11 April 2010).

⁴⁷ "Cassinelli, l'Italia non adotti l'HADOPI francese", *Diritto Online*, 8 April 2009 (URL: www.webnews.it/news/leggi/10525/cassinelli-litalia-non-adotti-lhadopi-francese/, last accessed 11 April 2010).

United Kingdom

The Digital Economy Act, granted royal assent on 8 April 2010, establishes the basis through which a graduated response mechanism could be introduced in the UK. The Act imposes an obligation on ISPs to notify subscribers that IP addresses with which they are associated are alleged to have been used in the illegal downloading of copyrighted material.⁴⁸ ISPs are also under the obligation to maintain records of the number of notices issued to each subscriber.⁴⁹ The Act requires that ISPs, if requested by a copyright owner, compile an anonymous list of subscribers who have received a specified number of notices. ISPs will only disclose the personal identity of subscribers to rights holders after the rights holder has obtained a court order.⁵⁰ The Government's explanatory note on the Act illustrates how the provisions might work in practice:⁵¹

- Copyright owners identify cases of infringement and send details including IP addresses to ISPs;
- The ISPs verify that the evidence received meets the required standard, and link the infringement to subscriber accounts;
- The ISPs send letters to subscribers identified as apparently infringing copyright. They keep track of how often each subscriber is identified;
- If asked to do so by a relevant copyright owner, ISPs supply a copyright infringement list showing, for each relevant subscriber, which of the copyright owner's reports relate to that subscriber. The list does not reveal any subscriber's identity;
- Copyright owners use the list as the basis for a court order to obtain the names and addresses of some or all of those on the list. At no point are individuals' names or addresses passed from the ISP to a copyright owner without a court order;
- Copyright owners send "final warning" letters directly to infringers asking them to stop online copyright infringement and giving them a clear warning of likely court action if the warning is ignored; and
- Copyright owners take court action against those who ignore the final warning.

The notices issued to alleged copyright infringers must be issued no later than one month after the infringement has been detected, and show the evidence of the alleged infringement, information on the appeals process, alternative legal sources, and the means to protect against unauthorised use of ones IP addresses by other parties who may have been responsible.⁵²

These obligations will not have effect until a code specifying the process by which infringements are detected, standards of evidence, routes of appeals, and formats of notices has been endorsed or created by OFCOM, the UK communications regulator.⁵³ The Government envisages that this code will be created by industry, rights holders, and consumers, and will then be subject to the approval of OFCOM. If this is not possible, OFCOM will itself create a code.⁵⁴

⁴⁸ UK Digital Economy Act, sections 124A to 124N.

⁴⁹ *ibid.*, section 124B

⁵⁰ Explanatory Notes, Digital Economy Act 2010, Office of Public Sector Information, p. 8 (URL: www.opsi.gov.uk/acts/acts2010/en/ukpgaen_20100024_en_1, last accessed 22 April 2010).

⁵¹ *ibid.*, pp 6-7.

⁵² *ibid.*, p. 7.

⁵³ *ibid.*, p. 5.

⁵⁴ *ibid.*, pp 8-9.

Section 124G of the Act provides that after one year from the time this code enters into force the Secretary of State has the power to impose further “technical obligations” on ISPs, such as limiting Internet access to subscribers who have been linked to a specified number of infringements. According to the explanatory note, technical measures:

would be likely to include bandwidth capping or shaping that would make it difficult for subscribers to continue file-sharing. ... If appropriate, temporary suspension of broadband connections could be considered.⁵⁵

However this is only in the event that the codes in effect are proving insufficient to properly act against illegal downloading, and in the event that OFCOM has assessed that such measures are necessary. Moreover, in order to introduce technical obligations, the Secretary of State must first lay the proposal before Parliament, which will then be subject to a sixty-day period of scrutiny, and require the approval of both Houses.⁵⁶

If the approval of both Houses is received, OFCOM is then required under section 124J to establish a code by which these technical obligations should be operated, and appeals dealt with. A new body to deal with these appeals may be established by OFCOM.⁵⁷ Subscriber appeals, when successful, will result in compensation and “reasonable” costs to be paid to the subscriber.⁵⁸ Alleged infringers have the right to appeal decisions of ISPs to use technical measures against them and no such measure can be imposed if an appeal is under consideration. The appeal is to a “person independent of OFCOM, with a further right of appeal to the First-tier Tribunal”.⁵⁹

This means that if a full three strikes system were to be introduced in the UK it could not be initiated until at least 14 months after OFCOM has first approved or created the initial code, and would be further delayed by OFCOM’s preparation of the additional code to cover the “technical obligations” introduced by the Secretary of State.

⁵⁵ *ibid.*, p. 5.

⁵⁶ *ibid.*, p. 11.

⁵⁷ Digital Economy Act, section 124D(5)(e) and 124I(3)

⁵⁸ Explanatory Notes, Digital Economy Act 2010, Office of Public Sector Information, p. 12.

⁵⁹ *ibid.*, p. 6.

Other countries

The Anti-Counterfeiting Trade Agreement (ACTA)

The ACTA arises from talks launched in 2006 by Japan and the United States. Preliminary talks continued throughout 2006 and 2007, with Canada, the European Union, and Switzerland joining the talks. In June 2008, when negotiations on the agreement began, the initial set of parties involved had grown to include Australia, Canada, the EU and its Member States, Japan, Mexico, Morocco, New Zealand, the Republic of Korea, Singapore, Switzerland, and the United States.⁶⁰

Section 4 of chapter 2 of the publically released draft text of the Agreement related to intellectual property rights enforcement in the digital environment.⁶¹ An option within Article 2.18 allows protections for service providers that “do not have actual knowledge of the infringement and is not aware of factors or circumstances from which infringing activity is apparent”.⁶² Other options allow for similar factors including “technical processes [that keep the provider from taking measures to prevent the infringement]”.⁶³ Elsewhere language currently subject to negotiation says that ISPs should would not be expected to be “monitoring its services or affirmatively seeking facts indicating that infringing activity is occurring”.⁶⁴ ISPs that “remove or disable access to material” once given “legally sufficient notice of alleged infringement”, or in an alternative form of language that remains under discussion, “an order from a competent authority”, and in the absence of a “legally sufficient” response from an Internet user to the effect that the notice was “the result of mistake or misidentification”.⁶⁵

New Zealand

In 2008 new legislation was introduced to provide a three-strikes measure in New Zealand. On 11 April 2008 the Copyright Amendment Act was passed, introducing several new sections to the Copyright Act of 1994.⁶⁶ The sections most relevant to three-strikes measures are sections 92A-C.

Section 92A states that an “Internet service provider must have a policy for terminating accounts of repeat infringers”.⁶⁷ According to the then Associate Commerce Minister, Judith Tizard, the majority of the Act was scheduled to come into force on 31 October 2008, and Section 92A was

⁶⁰ "Summary of key elements under discussion in the on-going ACTA negotiations", produced by the ACTA negotiating partners, available via the European Commission DG Trade (URL: <http://trade.ec.europa.eu/doclib/html/145271.htm>, last accessed 23 April 2010), p. 1.

⁶¹ "Consolidated text prepared for public release: Anti-Counterfeiting Trade Agreement", April 2010, chapter 2, section 4, pp 18-24.

⁶² *ibid.*, pp 19-20.

⁶³ *ibid.*, p. 20.

⁶⁴ *ibid.*, p. 21.

⁶⁵ *ibid.*, p. 21.

⁶⁶ Copyright (New Technologies) Amendment Act 2008 No 27, Public Act.

⁶⁷ *ibid.*

initially due to come into force on 28 February 2009.⁶⁸ However the introduction of Section 92A has been delayed following stiff opposition, and a political decision to redraft the section.⁶⁹ It is not known whether an alternative, which would present some new formulation for three-strikes measures, will be presented.

South Korea

Unlike three-strikes mechanisms mooted in France or that proposed by IRMA in the Eircom case in Ireland, the South Korean approach toward the three-strikes mechanism appears to emphasise the hosters of content within the Korean jurisdiction rather than the downloaders of content that is hosted beyond the jurisdiction.

On 23 July 2009 a number of amendments to the Korean Copyright Act entered into force. Under the new law the Ministry of Culture, Sports, and Tourism (MCST) can issue an order to suspend a copyright infringer's "website account" for up to six months, but only with the ISP through whose service the infringement occurred.⁷⁰ This order does not suspend the infringer's Internet access as a whole, allowing him access to other ISPs, and to E-mail services associated with the suspended account.⁷¹ Before the MCST can issue a suspension order it is first examined by the internal committee of the Korea Copyright Commission and both ISP and account holder can submit their opinions beforehand. Once the order is issued the ISP has ten days to act before notifying the MCST.⁷² The new law also provides for the MCST issuing notices to suspend the service of web services for up to six months that have already received three notices to cease transmitting copyright infringing material.⁷³

According to one report there have been no user accounts suspended from the time that law entered into force until at least as late as February 2010.⁷⁴ This may be due to technical delays in establishing a system to detect individual users.

Taiwan

⁶⁸ Press Release, Judith Tizard, Associate Commerce Minister, 3 October 2008 (URL: www.beehive.govt.nz/release/copyright+new+technologies+amendment+comes+force, last accessed 6 April 2010).

⁶⁹ Press Release, Simon Power, Minister of Commerce, 23 March 2009 (URL: www.scoop.co.nz/stories/PA0903/S00330.htm, last accessed 6 April 2010).

⁷⁰ This is the language used in "Major Amendments to Korean Copyright Act – April, 2009", Asian Patent Attorneys' Association Annual Report 2009 (URL: www.apaaonline.org/pdf/APAA_56th_&_57th_council_meeting/copyright/2-Korea%20Copyright%20Cttee%20Country%20Report%202009.pdf, last accessed 6 April 2010).

⁷¹ *ibid.*

⁷² *ibid.*, p. 6.

⁷³ *ibid.*, p. 7.

⁷⁴ "Three Strikes Rule: Sleeping for Seven Months", Heesob's IP blog, 9 March 2010 (URL: <http://hurips.blogspot.com/2010/03/three-strikes-rule-sleeping-for-seven.html>, last accessed 6 April 2010).

On 21 April 2009, the ISP Liability Limitation Bill was passed, and entered into force on 13 May 2009.⁷⁵ The Taiwan Intellectual Property Office (TIPO) released the regulations governing the implementation of the new law on 7 September 2009.⁷⁶ Under the new law Internet users who have been found to be “uploading, posting, or using P2P to transmit unauthorized videos, music, or writings, as well as selling pirated goods over on-line auction site” can face “partial or complete termination of services would be carried out [by their ISP] if they have three repeated alleged infringements”.⁷⁷

The law allows copyright holders to “send a ‘warning’ to the IP address of that user ... via the service provider ... and remind him/her to refrain from infringement activities”.⁷⁸ However, as one analysis notes, the new law may simply be a way of satisfying those who have lobbied for three-strikes without necessarily impinging on the rights of Internet users.⁷⁹ It does not actually oblige ISPs to terminate service, nor do the regulations announced by TIPO in September 2009 give any detail on how the three-strikes measures should function in practise. Thus any suspensions of service or throttling back of access speeds that do result from the new law may be performed under the rubric of the contractual conditions between the ISP and the user.

Aside from the three-strikes measure, the new legislation also provides for the take down of offending material from hosts operating in the jurisdiction, and provides for a “counter notification” appeal by which a user can request that their material is restored following its take down from a hosting service.⁸⁰ Provided “counter notification” is not made by a user, the ISP will be prevented from disclosing the user’s personal information to the rights holder.

⁷⁵ *Tai E Quarterly*, Tai E International Patent & Law Office (URL: www.taie.com.tw/English/pdf/012922.pdf, last accessed 11 April 2010).

⁷⁶ “Implementing regulations for ISP safe harbor amendments announced”, Winkler Partners, November 2009 (URL: www.winklerpartners.com/a/2009/11/, last accessed 11 April 2010).

⁷⁷ “ISP Liability Bill Completed Third Reading at the Legislative Yuan on April 21”, Taiwan Intellectual Property Office, 24 April 2009 (URL: www.tipo.gov.tw/en/News_NewsContent.aspx?NewsID=3675, last accessed 11 April 2010).

⁷⁸ *ibid.*

⁷⁹ “Implementing regulations for ISP safe harbor amendments announced”, Winkler Partners, November 2009 (URL: www.winklerpartners.com/a/2009/11/, last accessed 11 April 2010).

⁸⁰ “ISP Liability Bill Completed Third Reading at the Legislative Yuan on April 21”, Taiwan Intellectual Property Office, 24 April 2009 (URL: www.tipo.gov.tw/en/News_NewsContent.aspx?NewsID=3675, last accessed 11 April 2010).

Conclusion

Three-strikes measures are immature at the present time, and much about the legal and technical basis on which they may (or may not) one day function is not yet known.

Though they are expected to be used in a number of Member States the introduction of three-strikes legislation in France, Italy, and the United Kingdom was pending or stalled at the time of writing. At least one Member State, Germany,⁸¹ has ruled out its introduction on the grounds that it is unconstitutional. Even where three strikes legislation has been passed the new EU Telecommunications Reform Package may have an impact. In a robust speech in Barcelona in November 2009, Viviane Reding (then Commissioner for Information Society and Media) expressed her concern that three strikes measures being considered by the Spanish government should comply with the EU Telecommunications Reform Package.⁸² The government opted against three strikes measures, and in January 2010 it proposed new legislation to shut down file-sharing websites offering illegal downloads.⁸³

The recent judgment of the Irish High Court in April 2010 on the IRMA versus Eircom case has only now allowed for the private agreement to introduce of a non-legislative three strikes measure, and this currently relates to a single ISP. Even so, this decision could yet be subject to appeal. Moreover, other Irish ISPs such as UPC continue to resist non-legislative three-strikes measures despite the Eircom settlement. In New Zealand, where three strikes legislation has been passed, the relevant provisions have not yet entered into force – and may be indefinitely stalled. In South Korea and Taiwan, where three-strikes legislation has actually come into force, it does not appear to be robustly applied. In Taiwan, for example, the emphasis

⁸¹ as suggested by Brigitte Zypries, then Minister for Justice, in January 2009. In March 2010 the current Minister for Justice, Sabine Leutheusser-Scharrenberger, confirmed that Germany will not implement three strikes legislation. In an agreement of the Government coalition (CSU/FDP) in October 2009 it was also agreed that the coalition would not implement measures to block Internet access for copyright infringement. See “Germany rejects three-strikes piracy plan”, *BillBoard*, 10 February 2009 (URL: www.billboard.biz/bbbiz/content_display/industry/e3i73b3660e2c6025e6507555e3cfec977d, last accessed 22 April 2010); “Justizministerin will Surf-Verbot fuer Raubkopierer verhindern”, *Der Spiegel*, 3 March 2010 (URL: www.spiegel.de/netzwelt/netzpolitik/0,1518,681142,00.html, last accessed 22 April 2010); see also “Germany speaks out against global internet ban for pirates”, *Der Spiegel*, 3 March 2010 (URL: www.spiegel.de/international/europe/0,1518,681498,00.html, last accessed 22 April 2010).

⁸² “Regulation in a convergent environment”, Commissioner Viviane Reding, 23 November 2009 (URL: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/551>, last accessed 22 April 2010).

⁸³ The Spanish approach envisages an Intellectual Property Commission (IPC) composed of independent legal and technology experts, situated within the Ministry of Culture. The IPC will consult a judge, who will have four days to hear arguments from all parties before issuing a judgment on whether a site should be shut down. Prior to this legislation it could take more than a year to shut down a website for breach of copyright law.⁸³ The new legislation has yet been approved by Parliament. See “Spain passes anti-piracy law – new law targets producers, not users of pirated content”, *The Hollywood Reporter*, 8 January 2010 (URL: www.hollywoodreporter.com/hr/content_display/film/news/e3if944e88734e00aa3358cfd1b6d614e92, last accessed 26 April 2010); and “Spain, France tackle Internet piracy”, *MSNBC*, 8 January 2010 (URL: www.msnbc.msn.com/id/34769344/ns/technology_and_science-tech_and_gadgets/, last accessed 22 April 2010).

appears to remain on ISPs' contracts with subscribers as a basis for discontinuing or altering service, since the new legislation has not been followed by regulations to dictate how the three-strikes mechanism should function.

Yet despite the relative immaturity of the three strikes approach and the dearth of information about how it might operate in practise against violent radical content, a number of observations can be made that mitigate against the adoption of three strikes solutions as part of a non-legislative measure to prevent the dissemination of violent radical content on the Internet.

The investigative system that companies such as DtecNET and Trident Media Guard employ could be used to investigate and track the dissemination of illegal video, audio, and text material across P2P networks. Indeed the IRMA/Eircom settlement illustrates how they could be employed on a non-legislative basis under some circumstances. However, an understanding of the technology that at the very least equals that available in the private sector would be required to adapt to new methods of illegal activity on P2P networks.⁸⁴ An exhaustive knowledge of the relevant illegal materials would also be required to identify the materials on the P2P networks.

This last challenge would be particularly acute in the case of a system based on Audible Magic, which requires a vast catalogue of the materials it is searching for. Such a dataset is easy for rights holders to collect, since they are merely required to catalogue their own content. Yet the same task would be a significant challenge for security service if they were required to gather and catalogue samples of the bulk of violent radical videos, images, texts, and audio files present on the Internet. Music and film distributors supply Audible Magic with updated records of their catalogues, and Audible Magic's "Replicheck" software uses so-called finger print samples of the media to verify media to be replicated. As Audible Magic's website notes, Replicheck scans for data including:

song title, performing artist, releasing label and copyright date for songs and the application name, version, publisher and date published for software. This information can then be cross-referenced against a customer's license documentation.⁸⁵

For the system to operate an extensive database of proscribed media must be available in a usable form. In the context of rapidly changing violent radical content, this might be a considerable challenge. While particularly popular videos, such as the Juba sniper series for example, might easily gathered, the administrating authority, however, would require an extensive array of information gathering and analysis capabilities to keep such a repository up to date.

⁸⁴ In one instance DtecNet came under criticism for fundamental technical mistakes in an important assessment. See "RIAA Anti-Piracy Partner Clueless About BitTorrent", TorrentFreak, 28 October 2009 (URL: <http://torrentfreak.com/riaa-anti-piracy-partner-clueless-about-bittorrent-091028/>, last accessed 1 May 2010); the issue of circumvention was raised by the same writer who criticized DtecNet's assessment. See "How File-Sharers Will Bypass UK's Anti-Piracy Act", TorrentFreak, 12 April 2010 (URL:<http://torrentfreak.com/how-file-sharers-will-bypass-uks-anti-piracy-act-100412/>, last accessed 1 May 2010).

⁸⁵ "Replicheck", Audible Magic (URL: www.audiblemagic.com/products-services/replicheck/, last accessed 11 April 2010).

In addition, the variety of technologies used on different ISPs networks means that a range of approaches would be required. The IRMA campaign in Ireland provides an example. Some networks, as with Eircom, would be unable to use Audible Magic. There would not be a one fit solution that could be applied across the EU. Indeed, as IRMA's case against UPC in June shows, a non-legislative solution based on copyright infringement also faces considerable challenges in securing the cooperation of the many ISPs that operate even within a single jurisdiction.

DRAFT