Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

22-Jun-2011

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP(2010)11/FINAL
Unclassified

THE ROLE OF INTERNET INTERMEDIARIES IN ADVANCING PUBLIC POLICY OBJECTIVES

Forging partnerships for advancing policy objectives for the Internet economy, Part II

JT03304378

English - Or. English

TABLE OF CONTENTS

FOREWORD

Internet intermediaries – Internet service providers (ISPs), hosting providers, search engines, e-commerce intermediaries, Internet payment systems and participative Web platforms – provide essential tools that enable the Internet to drive economic, social and political development, for example by facilitating aggregation of demand, new models of collaboration, citizen journalism and civic participation. Yet intermediary platforms can also be misused for harmful or illegal purposes, such as the dissemination of security threats, fraud, infringement of intellectual property rights, or the distribution of illegal content.

The Declaration on The Future of the Internet Economy, adopted at the OECD meeting at Ministerial level in Seoul in 2008, invited the OECD to: examine "the role of various actors, including intermediaries, in meeting policy goals for the Internet economy in areas such as combating threats to the security and stability of the internet, enabling cross-border exchange, and broadening access to information". In response, the OECD's Committee for Information, Computer and Communications Policy (ICCP) undertook a broad project to gain a more comprehensive view of Internet intermediaries, their economic and social functions, development and prospects, benefits and costs, and roles and responsibilities as part of its programme of work.

The first part of the project (*The Economic and Social Role of Internet Intermediaries*) developed a common definition and understanding of what Internet intermediaries are, of their economic function and economic models, and discussed market developments and the economic and social uses that these actors satisfy.

The present report (*The Role of Internet Intermediaries in Advancing Public Policy Objectives*) is the second part of the project. It examines the roles and responsibilities of Internet intermediaries in advancing public policy objectives, as well as the costs and benefits of their involvement. After introducing how intermediaries could take on a policy role through responses to legal requirements; through industry self-regulation; and through their business practices, this report takes an issue-based approach to evaluate possible involvement of Internet intermediaries in helping to advance specific policy objectives. Case studies look at the free flow of information, reinforcing cyber-security, combating illegal content and child inappropriate content, deterring illegal online gambling, ensuring respect of copyrights and trademarks, and protecting consumers in e-commerce transactions.

The third part provides a summary of the workshop on "The Role of Internet Intermediaries in Advancing Public Policy Objectives", held in Paris on 16 June 2010. Its goal was to identify best practices and lessons learned from Internet intermediaries' experience advancing public policy objectives.

The report was prepared by Ms. Karine Perset of the OECD's Directorate for Science Technology and Industry (DSTI) under the guidance of Mr. Dimitri Ypsilanti, also of the OECD's DSTI. The legal section draws extensively on work by Ms. Lilian Edwards, Professor of E-Governance at Strathclyde University. Mr. Mark MacCarthy, Professor at Georgetown University, researched and drafted several case studies." The research of Mr. Bruno Basalisco of Imperial College Business School is also acknowledged. This paper has greatly benefited from the expert input of delegations from the Business and Industry Advisory Committee (BIAC), the Civil Society Internet Society Advisory Council (CSISAC), and the

Internet Technical Advisory Committee (ITAC), in addition to OECD member countries and observers. The support of the Norwegian Ministry of Government Administration and Reform and the Norwegian Ministry of Transport and Communications for this project is gratefully acknowledged.

The report was declassified by written procedure of the Committee for Information, Computer and Communications Policy (ICCP) in February 2011.

MAIN POINTS

The role of Internet intermediaries

As the Internet has grown to permeate all aspects of the economy and society, so too has the role of the Internet intermediaries that enable economic, social and political interactions between third parties on the Internet. They provide access to host, transmit and index content originated by third parties on the Internet; facilitate interactions or transactions between third parties on the Internet; or provide other Internet-based services to third parties.[1]

This report discusses public policy issues associated with Internet intermediaries, in particular their roles, legal responsibilities and related liability limitations regarding the actions of third-party users of their platforms. Throughout, it is important to be mindful that the nature and role of intermediaries are evolving and likely to change considerably. The models of Internet intermediaries discussed are thus necessarily a snapshot of a dynamic system.

Information on the Internet is distributed, hosted and located by Internet intermediaries, whose role in the structure of the Internet economy is critical. They provide increasingly significant social and economic benefits through information, e-commerce, communication/social networks, participative networks, or web services. They contribute to economic growth; finance, operate and maintain most Internet infrastructure; stimulate employment and entrepreneurship; and enable creativity, collaboration and innovation as well as user empowerment and choice. By enabling individuality and self-expression, they also offer potential improvements in the quality of societies in terms of fundamental values such as freedom and democracy.

Legal issues may arise because of the distribution of content or the provision of services on the Internet. While the vast majority of activities on Internet intermediary platforms are lawful, illegal activities raise questions of liability. A text, image, song or user-generated video might be defamatory, contain illegal images of child pornography, infringe a copyright, incite racial hatred, infringe laws on truthful advertising, give misleading advice, or reveal facts embargoed by laws of confidence or contempt of court rules.

In such cases, questions arise. To what extent should Internet intermediaries, which own and operate Internet platforms, be responsible for content originated by third parties using their Internet network or services? How far should responsibility remain solely with the original author, provider or party distributing unauthorised content? What are the consequences, if any, of that responsibility for online innovation and free speech? If intermediaries are deemed even partially responsible for the dissemination of the content or its use, should they be required to remove it or even to prevent its being made available in the first place? Alternately, if only the third-party user is held responsible, what are the implications, if any, for control of the dissemination of undesirable content, or, as with copyright protection, the abuse of legitimate content, or the viability of legitimate innovative business models? If Internet intermediaries have liability, what will its impact be on their business models and economic viability, given the extra costs involved? Finally, how would liability affect online innovation and the free flow of information in the Internet economy?

Internet intermediaries' success in developing innovative technologies, policies and practices to deal with such issues should be underscored. Most have explicit policies that prohibit illegal activities by those

using their systems. These are often supplemented by specific policies and procedures to respond to particular policy concerns through voluntary individual actions or implementation of codes of conduct. Critical questions for the Internet economy include: When do Internet intermediaries have business incentives to respond voluntarily to policy concerns about undesirable or harmful content in the absence of legal responsibility? What positive or negative implications do such voluntary actions entail? What models of corporate decisions or implementation of industry codes have been successful?

Internet intermediaries' evolving legal responsibilities

Since about 2000, most OECD countries' approaches to limitation of liability for intermediaries for illegal or actionable content or activity by third parties have been converging through regulations defining specific liability regimes for Internet access providers, hosts and, less consistently, other types of intermediaries.

These regimes have generally been organised around two broad principles. In general, intermediaries are not responsible for third-party content distributed or conveyed on the Internet without modification by the intermediary, or for transactions taking place through their platform outside of their knowledge or control, nor do they have a general monitoring and surveillance obligation. This type of system was first implemented in the United States in Section 230 of the *Communications Act*. Nevertheless, specific obligations condition liability in other circumstances, such as identifying users, preserving traffic data in response to requests, removing ("taking down") content upon receipt of a valid notice, etc. Such "limited liability" or "safe harbour", providing limitation of remedies, was implemented in Europe in the E-Commerce Directive, and in the United States in the *Digital Millennium Copyright Act* (DMCA, for copyright-infringing material only). Such frameworks for limiting liability, which may include certain conditions and obligations, have been instrumental in the growth of Internet service providers, e-commerce and emerging user-generated content (UGC) platforms.

Legal and regulatory regimes for limitation of liability of Internet intermediaries were established in recent years and the scope and types of actors in the Internet landscape have continued to evolve. New issues have now arisen, creating regulatory challenges and a large quantity of case law. Several OECD countries are considering how best to reconcile current liability regimes with emerging issues or ongoing issues that have increased in scale, without adversely affecting the characteristics of the Internet on which the economy and society now depend. Among the issues that arise are:

- The notions of intermediary and content provider are increasingly blurred, especially on participative networking sites, raising the question of how legal frameworks should respond. Depending on the specific roles and services provided by intermediaries, when questions regarding liability limitations are assessed, attention may be paid not just to the intermediary's knowledge, but also to its neutrality and the financial gain derived from hosting or linking activities. These considerations can require a more subjective case-by-case assessment of whether they qualify for limitation of liability, and may increase uncertainty for intermediaries and other interested parties operating in an ever-changing environment.
- There are questions about whether new types of intermediaries or intermediaries whose role has increased (search engines, social networking sites), and perhaps others yet to emerge may need distinct safe harbours. In addition to different categories of intermediary activity (hosting, conduit, linking, etc.), there are questions about whether small and large intermediaries need different rules for their role in addressing illegal activity on their platforms.
- Rules limiting their liability can encourage co-operation by Internet intermediaries, thereby promoting the Internet as a trusted medium for commerce and speech.

- Pressures and priorities differ in the areas of responsibility for copyright, pornography, privacy, consumer protection or security, raising questions as to whether "one size fits all" and horizontal regimes are workable or desirable.
- *Ex ante* filtering rather than *ex post* take-down is increasingly provided voluntarily by some types of intermediaries for some types of content/activity or promoted by intellectual property right holders and law enforcement agencies. This raises the question of how far, if at all, the law should intervene. However, if intermediaries have to meet new obligations to retain limited liability, it will be necessary to assess the costs, to see if their duties can be automated to ensure that the obligations can be fulfilled reasonably and that consumers are not unnecessarily burdened with additional costs.
- The impacts of new proposals on public and user interests (freedom of expression, access to knowledge, privacy, preserving and protecting the rule of law on the Internet) need to be assessed. Their costs and benefits should be examined against the relative costs and benefits of the *status quo*. Respect for fundamental rights such as freedom of expression, protection of property, privacy and due process need to be addressed and safeguards should be provided.
- The role of multi-stakeholder bodies and other forums for communications has increased. Given the complex issues and the many actors, consultation with all interested stakeholders in developing policies can help form the necessary multi-stakeholder partnerships to address emerging Internet-related policy issues.
- Given the global distribution of and access to online content, as well as the delivery of online services across the globe by multinational operators, the global dimension of liability rules becomes a significant question.

Business practices and self- or co-regulatory codes

Market forces, with informal encouragement by governments, can often help resolve issues, improve standards of operation, or promote the desire to forward particular principled ideas, without the need for legislative intervention. Legal frameworks that have been the subject of public debate and multi-stakeholder input can help set the parameters for self- or co-regulatory initiatives, with government acting to facilitate public-private partnerships and encourage broad-based involvement. Overall, self-regulation is most likely to be effective when: *i)* industry has a collective interest in solving issues; *ii)* industry is able to establish clear objectives for a self-regulatory scheme; *iii)* the likely solution matches legitimate consumer and citizen needs; and; *iv)* the schemes yield rules that are enforceable through contracts and private legal actions or government enforcement, or both.

The report examines various market-based, self- and co-regulatory approaches taken by Internet intermediaries that help achieve public policy goals. These include satisfying customers' needs for more accurate and reliable information, offering better services or better security or meeting different national policy requirements in the case of trans-border access to content. It highlights the role of experimentation and learning from experience to develop innovative solutions and best practices.

Case studies: examples of Internet intermediaries' practices

Case studies on the free flow of information, privacy and security, illegal content and child-inappropriate content, illegal online gambling, copyright and counterfeiting, and consumer protection in e-commerce payments examine the role and legal responsibilities of Internet intermediaries for third-party use of their platforms. The practices of one or two categories of intermediaries are discussed in each area, highlighting policy and legal implications such as technical feasibility, costs of compliance, appropriateness and reasonableness, privacy, speech, and due process concerns and precedents.

Issues raised include whether enforcement by private-sector Internet intermediaries to advance certain public policy objectives could be easier, cheaper or more effective than traditional enforcement by government law enforcement or judicial authorities that require access to and full assessment of the evidence before they can be justified. Another is intermediaries' enforcement of their own terms of use as a way to prohibit illegal activity. At the same time, encouraging or requiring private parties to restrict access to content or impose burdens or penalties on citizens raise policy questions in terms of due process and oversight.

The **global free flow of information** case study looks into actions Internet intermediaries can take to minimise the human rights and privacy implications of operating in countries that use Internet intermediaries to help censor the Internet. The Global Network Initiative is a self-regulatory initiative requiring its members to conduct *ex ante* civil rights impact assessments and develop risk mitigation strategies, which many consider best practice. At the government level, whole-of-government approaches are needed to advance free flow of information objectives.

The **security** case study examines the role of Internet service providers in improving the security of those who may lack sufficient incentives or ability to improve it. Malware-compromised home computers and botnets (networks of compromised computers) raise very serious security threats and ISPs are therefore beginning to provide more security. Japan's and Korea's public-private partnerships involve voluntary industry codes of conduct and standard processes for notifying, communicating with and helping subscribers whose computers may be infected by malware. They are being emulated elsewhere. Advantages of voluntary initiatives and of government funded resource centres include that they can minimise potential negative impact on smaller firms and on competition.

The **child protection** case study investigates measures to help curtail material on sexual abuse of children and to verify age. Intermediaries' terms of service forbid the use of their systems for such content and often use age verification procedures to limit access to adult-only material. They have co-operated with law enforcement and private-sector organisations to deny payment and Internet access to sites with such content. Filtering has become widespread, with blacklists provided both by private organisations and by government agencies. In some OECD countries, such actions raise policy and constitutional concerns and efforts to expand blacklists to other content are controversial in terms of free expression. Mandatory filtering regimes should provide for due process, accountability and transparency. Increased international co-operation is needed to detect and close down sites with such content.

The **copyright** case study examines steps Internet intermediaries are taking to respond to online copyright infringement. It examines notice and take-down, notice and notice, and graduated response regimes. The problem is sizeable although quantitative information is limited. Some countermeasures appear somewhat effective. Private arrangements may be effective but may only affect the parties to the agreement and may not be the result of a transparent, multi-stakeholder process. It is necessary to assess the costs and effectiveness of different regimes, the efficiency and equity of cost-sharing arrangements, and the cost and feasibility of emerging proposals for graduated response, dynamic network-level filtering and ISP blocking of infringing websites. Expedited adjudication processes for allegations of copyright infringement to facilitate prompt and cost-effective enforcement while preserving due process should be considered. The impact of piracy on new legitimate and innovative business models and the impact of such business models on deterring copyright infringement by individual users call for attention.

The **counterfeiting** case study examines steps taken by search engines, online marketplaces and social networks regarding the use of their systems to sell counterfeit goods. Some Internet intermediaries respond voluntarily to complaints and take pro-active steps to control counterfeit sales. Some courts seem satisfied with the current notice and take-down practices, but many courts find that further measures are required. Some argue that additional international harmonisation would help to prevent overlapping and

conflicting requirements. Enforcement efforts should weigh the benefits from reducing counterfeiting against the costs of enforcement; voluntary negotiations among affected parties can help determine an equilibrium point.

The **Internet gambling** case study examines policy responses to the online availability of gambling services based in other jurisdictions. One focus is the US *Unlawful Internet Gambling Enforcement Act*, which requires payment intermediaries to control illegal Internet gambling. The study examines how payment intermediaries adapt their systems so as to block Internet gambling transactions in some jurisdictions but allow them in others. It finds that enforcement by payment intermediaries significantly reduced the US gambling market but excessively blocks legal gambling. While monitoring systems can detect gambling activity, they cannot determine whether it is illegal. Over-blocking arises from ambiguity in law, which gives payment intermediaries substantial unsupervised discretion.

The **consumer protection** case study examines the role of payment intermediaries in providing consumers with protection from online fraud resulting in unauthorised charges and with dispute resolution and redress mechanisms to address issues regarding the receipt, nature, or quality of online purchases. The policy objectives of policy makers and payment intermediaries are often aligned because both have strong incentives to develop a robust online marketplace. Consumer liability for unauthorised payments is limited by legal frameworks for traditional payment systems and by voluntary practices put in place by alternative payment systems. A question is whether and to what extent it would serve policy objectives to harmonise and extend consumer liability limitations to all e-commerce payment systems. Another is the extent to which consumer protection should be tailored to the different payment mechanisms and legal frameworks. Liability regimes can also be designed to encourage further development of fraud prevention and reduction mechanisms for all types of payment systems. Member countries could also explore with payment intermediaries how best to provide consumers with dispute resolution and redress mechanisms for cross-border e-commerce transactions.

THE LEGAL RESPONSIBILITIES OF INTERNET INTERMEDIARIES

Historical development

The liability of Internet intermediaries for content authored by or activities carried out by third parties – known at first as "ISP liability", but now much wider in scope – was one of the earliest issues facing the emerging Internet industry.[2] Early cases mainly originated in the United States and focused on the liability of early commercial Internet service providers (ISPs) such as AOL or CompuServe for hosting, transmitting or publishing material that was legally actionable, such as libellous, defamatory or containing pornographic content.[3]

Problematic content may originate from a party with whom the ISP had a contractual relationship, such as a subscriber, from a third party with no contractual relationship with the ISP, such as a newsgroup posting, or from the ISP itself. The policy issues raised by the different classifications of authorship, responsibility, control and types of content were generally not uniformly dealt with in early jurisprudence. The result was widely differing regimes both across legal systems and under the same legal system, depending on the type of content or the type of "publisher", "author" or "host".

By 1995 the emerging US online industry recognised the serious threat posed by the risk of intermediary liability for content posted by third parties. The early *Stratton Oakmont, Inc. v Prodigy Services Co.* case suggested that service providers who assumed an editorial role with regard to customer content were publishers and thus responsible for their customers' libel and other torts. It was feared that this responsibility might discourage providers from taking self-regulatory initiatives to monitor content. Partly in response, the US Congress enacted a provision now commonly known as "Section 230" (part of the *Telecommunications Act* of 1996), which provided online service providers broad protection from liability for content posted by others. It is often considered to have contributed to the significant growth over the past 15 years of innovative online sites and services (especially user-generated content sites).

In Europe, from the mid-1990s, the lack of harmonisation in emerging case law led to industry calls for special statutory regimes. In the late 1990s, the liability regime debate came to be seen, at least in Europe, not only as tied to different threats (libel, pornography, infringement of copyright, but also as a the more general problem of whether Internet intermediaries should be responsible for the content they made available to the public and whether they could take steps to manage this responsibility and limit their liability.

At the same time, the issue of liability for third-party content or activities became a major concern not just for the traditional ISP community, but also for Internet hosts such as universities, traditional media organisations online, such as the BBC or the Times, software providers, libraries, chat rooms and blog sites, individuals with their own websites and emerging social networking sites. Potential liability also affected communications intermediaries such as Internet backbone providers, cable companies and mobile phone operators. Providers of telecommunications services, such as mobile operators, began providing content and value-added services such as geolocational data. This showed the need for an online intermediary liability regime that was practical, uniform, acceptable to industry and also protective of consumers, citizens, institutions and businesses.

The development of the limited liability paradigm

Secondary liability exists in most legal systems. It applies liability to an individual or company based on the actions of another party.[4] Principles of secondary liability are established in various jurisdictions; common law jurisdictions have the concepts of vicarious liability and contributory liability, and, in the United States, of inducement liability. The concept of authorisation exists in common law countries such as Australia and the United Kingdom, as well as liability based on joint tort-feasorship or aiding and abetting. In civil law jurisdictions, national civil codes contain general provisions imposing a duty of care and tort liability, which can be incurred by both direct and indirect infringers.

Today, most intermediary liability issues involve: hosting and transmission of child pornography and other types of criminal content; material that infringes intellectual property rights, especially copyright but also trademarks, patents and publicity rights; and libellous or defamatory material. The growth of music, film and information content piracy and peer-to-peer networks in recent years has raised many issues. In addition to its adverse impact on authors and distributors of content, piracy has exposed ISPs and hosts to a volume and manner of potential risk different from that anticipated in early cases. As such, piracy concerns continue to reshape this area of law.

Given their role as enablers of Internet publication, ISPs and hosts quickly became aware of their potentially high risks in content liability cases. Therefore, in the early to mid-1990s, these intermediaries' plea for immunity from content liability around the world played a role in the development of immunity from liability provided by Section 230 as well as in the limitations on liability regimes in the United States' copyright statute, the *Digital Millennium Copyright Act* (DMCA) and the EC Electronic Commerce Directive (ECD), Articles 12-15.

The concerns of Internet intermediaries, ISPs in particular, were mainly of three sorts: *i)* the potential negative consequences of liability on growth and innovation; *ii)* their lack of effective legal or actual control; and *iii)* the inequity of imposing liability upon a mere intermediary (common carrier argument).

On the first point, although the rise in illegal activity challenged legitimate business models, there were concerns that imposing liability on ISPs and hosts for content authored by others would stifle growth and innovation. These concerns are still present today in the broader debate about maintaining respect for legal norms in the online environment. Since growth and innovation of e-commerce and the Internet economy depend on a reliable and expanding Internet infrastructure, an immunity or "limited liability" regime was, and is, in the public interest. A related desire was to preserve the open and decentralised architecture of the still growing Internet.

Second, Internet intermediaries argued that they could not manually check the legality of all the material that passed through their network routers or servers, and that it might not be feasible or possibly legal to do so without invading their subscribers' privacy and confidentiality.[5] Automation is one way to circumvent the problem of filtering large amounts of information, but in the late 1990s, content classification and filtering technologies remained very unsatisfactory and tended to under- and over-block significantly. In areas such as libel, false advertising and hate speech, where semantic meaning depends on human interpretation, filtering usually was, and still is in many cases, judged impractical.[6] There were, and still are, questions about the effectiveness and proportionality of filtering from the technical, cost and operational perspectives, and some argue that they are easy to circumvent.

The 2000 *LICRA v Yahoo!* case was a turning point. The defence presented to the French court argued that it was technically impossible for Yahoo! US, as host of online auctions, to block access to pages on its site selling Nazi memorabilia to "all persons from France". The Court passed the question of automated filtering of requests from a particular location to a technical sub-committee for investigation. They reported

that, in fact, Yahoo! had the ability – already used to put advertisements into the relevant language to users in a given country – to identify and block access to 90% of French citizens.[7] Accordingly, Yahoo! was instructed to block access. This decision related to content blocking for a particular location. In this case, third parties who posted items for sale on Yahoo! manually classified the types of items for sale. However, in cases of pure automated content classification, the view widely held was that Internet intermediaries could not yet successfully automate the filtering of unwanted material and remain in business. Furthermore, ISPs and hosts were exposed to risk as a result of content authored by parties with whom they most often had no contractual relationship. The *LICRA v Yahoo!* case also raised freedom of expression concerns for many in civil society.

Finally Internet intermediaries in some countries argued that they were mere conduits, not content providers, and thus that it would be inequitable to hold them liable (Sutter, 2003). Their aim was to be treated not as creators or facilitators of content but as conduits like the postal service and phone companies which, in the United States, are not liable for content carried and are required to respect confidentiality. They did not want to be classified as publishers, because of the risks raised by making the content available to the public.[8]

From the mid-1990s, then, Internet intermediaries in the United States, Europe and elsewhere vigorously, and largely successfully, maintained that they should face only limited liability under certain circumstances, as established under statute. In the United States, in addition to Section 230, which established exemptions from limited liability, the DMCA in 1998 established caveats to the liability exemptions, in the form of "safe harbours" regarding copyright infringement. In Europe, the European Commission challenged the argument for limited liability of Internet intermediaries, based on their understanding of the role that ISPs and hosts could play in controlling online pornography, spam, libel and other forms of undesirable content. This was a policy goal not only for obvious reasons, such as child protection, but also as part of a general drive to improve public trust and confidence in the Internet as a safe space for economic activity.

Before 2000, a rough consensus had emerged in both Europe and the United States that a balance needed to be struck. While recognising at a general level that different categories of ISPs perform different functions and require specific responses, ISPs should in principle be guaranteed exemption or limited exemption from liability for content authored by third parties. The consensus also held that, to benefit from this liability limitation, ISPs should in many cases be prepared to co-operate when asked to remove or block access to identified illegal or infringing content. Such liability limitation, or, "safe harbour", as it is known in the United States, was implemented in Europe in the ECD and in the United States in the DMCA (copyright infringing material only). These regimes were to prove critically important to the ISP, e-commerce and emerging user-generated content (UGC) industries.

Global safe harbour regimes or ISP/intermediary liability limitations

As a result, most OECD countries adopted regulations from the late 1990s through the early 2000s that define specific liability regimes for actors such as Internet access providers, hosts and, less consistently, other Internet intermediaries. In most cases, they are organised around two broad principles: *i)* intermediaries are not responsible, in principle, for third-party content distributed or conveyed on the Internet or for transactions taking place, nor do they have a general monitoring and surveillance obligation; but *ii)* intermediaries nevertheless have specific obligations, which may vary by country, such as identifying users, preserving traffic data in response to qualified requests, removing ("taking down") content upon receipt of a valid notice, etc.

Over the years, legal frameworks for Internet intermediaries were developed, structured around two types of regulation: *i)* "horizontal" regulation such as Section 230 and the ECD which deals specifically

with the liability of intermediaries in various domains; and *ii)* "vertical" regulation which lays down rules for special domains (copyright, protection of children, personal data, counterfeiting, domain names, online gambling, etc.). Examples of the latter include the US Internet gambling law, the UK *Defamation Act* 1996, the US DMCA (see below), and the French *Code monétaire et financier* for online fraud with a payment card.

Some key distinctions made in various countries, to varying degrees, to regulate the liability of Internet intermediaries include:

- The intermediary's level of passivity. Generally speaking, the more an intermediary acts as a mere conduit, the less likely it will be considered responsible for actions of third parties using its platform.
- The nature of the relationship between originator or author of problematic content/activity and the Internet intermediary, and notably whether a contractual relationship exists (as between ISP and subscriber) or not (as between search engine and casual searcher).
- Whether there was any modification of the transmitted information. In the ECD, for example, activities which involve the modification of transmitted information do not qualify for limitation of liability.
- Whether the intermediary had "knowledge" of the online activity. Whether knowledge must be actual or may be constructive (drawn from facts and circumstances), and how it is obtained by the intermediary, has been a controversial issue (see below).
- Whether the intermediary acted "expeditiously" when notified of illegal activity. The ECD, for example, requires intermediaries to act expeditiously to remove or to disable access to such information on their systems or networks, if they are to avoid liability after obtaining actual or constructive knowledge of infringing or illegal activities.

In the United States, two separate limited liability regimes were created for ISPs and hosts, one relating to all types of liability material except intellectual property (IP) and the other relating to liability for material infringing copyright. The former is found in Section 230(c), which provides a potentially broad granting of immunity from secondary liability in a variety of circumstances, except those relating to intellectual property or federal criminal liability, as long as the content in question was provided by a party other than the service provider (Lemley, 2007). The second regime, found in the DMCA, Title 17, Section 512, limits the remedies available in copyright infringement actions against Internet service providers who are eligible for safe harbours. These limits include immunity from monetary damages and a partial limitation on injunctive relief. Certain conditions apply to the limitation of liability and remedies, such as the disclosure of the identity of alleged infringers who have stored information on Internet intermediaries' platforms or networks upon receipt of a subpoena, subscription to a detailed code of practice relating to notice, take-down and put-back, and a requirement to adopt a policy for the termination of accounts of repeat infringers in appropriate circumstances determined by the Internet intermediary. The regime is described below.

In Europe, the ECD contains a harmonised "horizontal" regime, covering liability for all kinds of content, except gambling and privacy/data protection, which are exempted. Cases across Europe have covered material infringing copyright or trademark, which is in contempt of court, and which is blasphemous or racist, antisemitic or hate speech, etc. Some of these topics are explored in more detail in the case studies section of the present report. The ECD regime is described in detail below.

Variations in liability regimes according to the roles and policy issues involved

Different types of Internet intermediaries may have different legal responsibilities under the various national or supranational regimes. Both the DMCA and the ECD divide service providers into useful categories by function. The most common categories are mere conduits (or communications or access providers), hosts, providers of caching services, and search engines (or information location tools) or other linking intermediaries.

1. United States

In 1996, Congress passed the *Communications Decency Act* (CDA) in an effort to prevent minors from accessing adult speech. In that act, Congress responded to concerns that ISPs making efforts to filter out adult content would render themselves liable as publishers and would discourage editorial activity by ISPs. To address this concern, Section 230(c) was passed, providing that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.... No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." Section 230(c) has been interpreted broadly to apply to many forms of Internet intermediaries, including ISPs, hosting providers, mailing lists, and online auction and listing sites, and in many types of "publication tort" including defamation, privacy or inducing prostitution. Its breadth has been criticised as unfair to true victims, *e.g.* of online libel. However, many commentators justify this breadth on grounds that freedom of speech would otherwise be "chilled", *i.e.* constrained; they consider that Section 230 enables Internet intermediaries to enjoy limited liability and promote the free flow of information, while also making business choices about content deemed offensive by users.

In contrast to the broad immunity of Section 230(c) for offenses regarding the content of online communications, the 1998 DMCA creates a limited liability regime for copyright liability. Title II of the DMCA, the *Online Copyright Infringement Liability Limitation Act* (OCILLA), creates a safe harbour for Internet service providers against copyright liability if they adhere to and qualify for certain prescribed safe harbour guidelines and promptly block access to allegedly infringing material (or remove such material from their systems) if they receive a notification claiming infringement from a copyright holder or the copyright holder's agent.[9] Four classes of intermediaries are given immunity on certain terms known as safe harbours: mere conduits such as telephone companies, which simply transmit packets sent by A to B without modifying them; hosts that store or cache content authored by another; and linking tools, which includes search engines and hyper-linkers (*e.g.* price aggregators) [Section 512 (a, b, c, d)]. Because these classes were set in 1998, their application to technologies developed later, such as peer-to-peer networks and online auction sites, has not always been clear [*MGM v Grokster* 545 U.S. 913 (2005)]. Importantly, most of these protected classes of intermediary benefit from the safe harbour only if they establish, publicise and implement both a "notice and take-down" (NTD) system for removing content when copyright owners complain, and a policy for terminating the accounts of "repeat infringers" in appropriate circumstances determined by the Internet intermediary, and only if they accommodate technical measures. The DMCA, like the ECD, and unlike the CDA, also allows suit for injunctive relief against an intermediary.

2. The European E-Commerce Directive (ECD) regime

Intermediary service providers: definition

Articles 12-15 of the EC E-Commerce Directive (ECD) introduced throughout Europe a harmonised regime on the liability of Internet intermediaries.[10] The regime affects not just ISPs but also ISSPs, *i.e.* information society service providers, or, as the title of Section 4 of the ECD calls them, intermediary

service providers. An information society service is defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service".[11] Recipient of a service is defined as "any natural or legal person who … uses an information society service".

Broadly, the ECD intermediary service provider liability regime covers not only the traditional ISP sector, but also a much wider range of actors involved in: selling goods or services online (*e.g.* e-commerce sites such as Amazon and eBay); offering online information or search tools for revenue or not for revenue (*e.g.* Google, BBC News website, MSN); and "pure" telecommunications, cable and mobile communications companies offering network access services.[12]

The ECD notes explicitly that although a service may be free to the recipient, this does not mean that the provider of that service necessarily falls outside the scope of the ECD if the service broadly forms part of an economic activity. Given that a successful intermediary revenue model is to give away a major product or service but then make money out of it in lateral ways on two-sided markets (*e.g.* search engines, which give away search services but generate revenue from associated advertising), the ECD definition of a service provider is generally interpreted widely.[13]

The ECD also excludes from its remit certain relationships not provided wholly at a distance, as well as activities such as taxation, competition law, activities of notaries and gambling. Liability for privacy or data protection breaches is also excluded from the ECD scheme.

Limitation of Liability/Notify and Take-Down Approach

The ECD, as noted above, takes a horizontal approach to intermediary service provider liability. Furthermore, rather than giving wide immunity in all circumstances, like the US CDA Section 230(c), its approach is to address their various activities separately.

When intermediary service providers act as a *mere conduit, i.e.* as a relay transmitting content originated by and destined for other parties, the ECD, in Article 12, regards them as basically absolved from all liability, as long as the service provider does not initiate the transmission, does not select the receiver of the transmission or does not modify the information contained in the transmission.

When service providers *cache* material, they are not liable for it under the same conditions. In addition, the cached copy must be updated regularly according to industry practice and the intermediary service provider must take down cached copies once it obtains actual knowledge that the original information has been removed or access to it disabled, or that a competent court or authority has ordered the removal or blocking of access.

Discussion in the EC regime has mainly centred on the hosting provisions in Article 14, which deal with circumstances in which intermediary service providers host or store more than transient content originated by third parties. Under Article 14, they are exempt from criminal liability in respect of the storage of information provided by a recipient of their services, so long as they have no "actual knowledge" of "illegal activity or information"; and they are immune from civil liability as long as they have no such actual knowledge and are not aware of "facts and circumstances from which the illegal activity or information is apparent".

In addition, Article 15 provides that EC member states are not to impose any general monitoring requirement on intermediary service providers, and especially "a general obligation actively to seek facts or circumstances indicating illegality". This has generally been taken to mean that intermediary service providers cannot be required to look for and filter out illegal content on a constant, ongoing basis, since this would counteract the notice and take-down limited liability paradigm.

Recital 48 provides however that it is still possible for states to require intermediary service providers "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". For example, UK service providers are asked to monitor and intercept transmissions under the *Regulation of Investigatory Powers Act 2000* for purposes of crime prevention and national security. However, some argue that duties of care should not be read as extending to duties under private rather than public or criminal law, since that would negate the point of Article 15 on general monitoring obligations (Bagshaw, 2003).

In practice, the main debate to date in countries such as the United Kingdom around Articles 14 and 15 has concerned not constructive knowledge but actual knowledge and the effect of notice and take-down on free speech. In the future, however, as discussed below, the main issue may be whether rights holders find that notice and take-down is enough to meet their claims or whether the regime should in some cases require intermediaries to take proactive measures, such as monitoring and filtering in advance.

3. Other countries

Similar rules are found in other OECD countries. Canada has passed legislation relating only to copyright and giving service providers a similar "mere conduit" liability limitation: "a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public".[14] The Canadian Supreme Court interpreted this provision of the *Copyright Act* to exempt a service provider from liability when it acted as a mere conduit.[15] In that case the court also interpreted the statute to require something akin to the notice and take-down provision of the DMCA.[16]

In Australia, an online intermediary liability regime relating only to adult content has received significant international attention. The *Broadcasting Services Amendment (Online Services) Act 1999*, amending the *Broadcasting Services Act 1992*, requires Australian service providers and mobile operators to remove from their servers content officially classified as adult or unsuitable for minors by the Australian Communications and Media Authority (ACMA, formerly the Australian Broadcasting Authority, ABA) on receipt of a take-down notice from that body.[17] Attempts to extend this regime to require ISPs to block access to similar material identified on foreign servers were on hold in mid-2010 (see the case study on illegal content and child-inappropriate content).

Korea regulates liability of Internet intermediaries for both copyright and illegal content. The Korean *Act on Promotion of Information and Communications Network Utilization and Information Protection (...)*, as amended in 2002, and the *Copyright Act* of April 2009, exempts online service providers from liability, fully or in part, provided they take down illegal content on notice, temporarily make inaccessible (place "provisional blindings") content that is deemed harmful (*e.g.* defamation), or "attempt to prevent or stop reproduction and interactive transmission" of content deemed to infringe copyright. Internet intermediaries may post a response if they disagree with the notification.

Iceland proposed a parliamentary resolution in June 2010, the Modern Media Initiative, which aims to turn Iceland into a supportive and attractive jurisdiction for the publication of investigative journalism and other threatened online media, with the world's strongest press and whistleblower protection laws. The relevance is that it includes rules on the protection of intermediaries based on the prevalent ECD model.[18]

Many developing countries still have no rules but tend to regard the DMCA and ECD as potential models. Some enhanced engagement countries have rules.

China regulates liability for material infringing copyright and other types of intellectual property. The Regulation on Protection of the Right to Network Dissemination of Information of 2006 grants limitations of liability to network service providers, including search and linking providers, for hosting IP-infringing material on certain terms. In addition to the online copyright law, the Central Bank of China issued on 21 June 2010, a first set of regulatory measures for Chinese non-bank third-party payment processors. These rules are expected to affect profoundly China's third-party payment services, an important feature and integral part of e-commerce. Eventually not only will third-party payment service providers be affected, but e-commerce itself.

India introduced "for the avoidance of doubt" a wide provision in its IT Act 2000 that "no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention". This mainly related to the cybercrime offences defined by the Act. The *IT Amendment Act 2008* refines the section to correspond more closely to the DMCA/ECD model of near-total immunity for mere conduits and notice and take-down for hosts.

Legal uncertainties and jurisdictional variations

Since legal regimes concerning Internet intermediaries were established, the scope, activities and actors in the Internet landscape have continued to evolve, creating ongoing regulatory challenges and a large quantity of case law. This is leading several OECD countries to consider how best to reconcile current liability regimes with emerging issues or ongoing issues that have increased in scale. Questions include, for example, the responsibility of auction platforms for preventing counterfeiting on their platforms, the role of social networking sites in responding to child protection issues on their networks, or whether sellers of advertisements and other advertising intermediaries must monitor the content of these advertisements for trademark infringement or misleading advertising. Issues in this section include:

- *The meaning of expeditious take-down in the ECD*, *e.g.* whether expeditious means one hour, one day or one week.
- Distinguishing *hosts* from *content providers*. In the world of social networking sites, online marketplaces and video platforms, whether intermediaries, especially some of the newer types, are hosts or content providers.
- *Legal uncertainties:* Sometimes case law by two courts differs on the same issue in the same country. For example, different courts in France have categorised video-hosting sites (see below) as hosting providers or as publishers.
- The impact of *notice and take-down on freedom of speech* and whether there is abuse of NTD systems that may result in "chilling", *i.e.* restraining, speech.
- The status of *search engines and hyperlinks:* The ECD, for example, does not explicitly mention a separate safe harbour provision for search engines, although these play a key role in the Internet economy. Countries such as the United States (for copyrighted material), Bulgaria and Romania have explicitly included search engines in national legislation; elsewhere, case law attempts to fill in.
- *Linking liability and peer-to-peer:* whether a sharp line can be drawn between sites that enable users to search for and locate copyright-infringing material (*e.g.* with BitTorrent technology) to separate "good" hyper-linkers that link only to legal content and deserve limitations of liability, from "bad" ones, which do not.

Meaning of expeditious take-down in the ECD regime

The ECD provides that as long as an intermediary service provider "acts expeditiously to remove or to disable access to the information" it hosts, it retains immunity even after notice. The directive gives no guidance as to what expeditious means, however, and whether it allows enough time to check a claim's validity or consult a legal expert before taking down. In the UK *Mumsnet* case, for example, the defendants settled, apparently because they were unsure whether even removal within 24 hours was expeditious.[19]

National implementations of the ECD often provide no further guidance, although in the United Kingdom, the specialised Electronic Commerce Directive Regulations 2007, which provide specific immunities for service providers from offences under the *Terrorism Act 2006*, do prescribe that take-down must take place within two days. Take-down periods vary from 24 hours to about a week, depending on the type of content and the size of the organisation (Edwards, 2007). In large organisations, it may take some time to find the right employee or to locate the page on a large website, while in small intermediary service providers it may be difficult to identify the employee responsible. The German Multimedia Act provides for liability to arise only after the intermediary service provider has failed to take "reasonable steps".

Distinguishing hosting providers from content providers: the roles of knowledge and financial gain

When the ECD was originally debated, the distinction between an online hosting service provider and a content provider was quite clear. Since then, the growth of participative networking platforms and interactive marketplaces has blurred this distinction, with owners encouraging subscribers to use platform facilities to publish and share their own user-generated content (UGC) to generate advertising revenue (Perset, 2010).[20]

Over 500 million users had Facebook accounts and 2 billion videos were served on YouTube daily as of July 2010.[21] This raises the question of whether a site that gains financial or other benefit from hosting illegal or infringing content should be at least partly liable for infringement or other offenses associated with distributing the content. A further question concerns the role that knowledge of illegal or infringing activity should play in establishing intermediary liability. When a so-called neutral intermediary bases its business model on hosting large amounts of UGC, some of which is anecdotally well known to be illegal or actionable, should it bear some responsibility, even when no notices have been served? This is the "constructive knowledge" provided for by the ECD in relation to civil, though not criminal, liability in Article 14. For some IP right holders, these issues have become crucial to their economic survival. So far, however, the legal response from the courts has varied. Some key areas are discussed below.

Online marketplaces and liability for trademark infringement

Online marketplaces are known to have listings that advertise counterfeit goods. For trademark holders, the first response is to give notice of listings which attempt to sell counterfeit goods. Online marketplaces usually take down listings expediently to avoid contingent liability. However, policing such a notice and take-down policy takes significant vigilance by brands, which inevitably act after the fact.

For trademark holders, a more desirable solution would probably be to compel online marketplaces to filter out listings containing infringements in advance. The typical argument is that online marketplaces must have some degree of knowledge of, and control over, their listings because their revenue comes from commissions on listed sales, and because they provide software for automated categorisation of, and search for, items. Consequently some have argued that online marketplaces must have "constructive knowledge" of infringement that disqualifies them for immunity under Article 14. Accordingly, in *Louis Vuitton Moët Hennessy (LVMH) v eBay*, a French court found, despite the immunity provisions of the ECD as

implemented in French law, that eBay was responsible for failing to prevent the sale of counterfeit luxury goods on its site.[22]

However in a very similar dispute in the United States, eBay won and Tiffany lost.[23] The case was argued under the rules of US trademark and unfair competition law. The US District Court held that it was "the trademark owner's burden to police its mark and companies like eBay cannot be held liable for traders based solely on their generalised knowledge that trademark infringement might be occurring on their websites". In the United Kingdom, eBay won another decision in 2009, but the merits of the case with regard to intermediary service provider liability were not dealt with in detail pending a referral to the European Court of Justice (ECJ) that was outstanding in July 2010.[24] Until the ECJ reaches a final determination, or the ECD is revised, the outcome of such cases is likely to be uncertain.

In the Google "AdWords" case, the question was whether Google was liable for trademark infringement because it allowed companies to advertise on its site using trademarks owned by competitors.[25] The court held that Google was entitled to claim immunity under Article 14 of the ECD if Google's role [was] "neutral in the sense that its conduct is merely technical, automatic and passive pointing to a lack of knowledge or control of the data which it stores". It stated (paragraph 116) that "the mere facts that the referencing service is subject to payment, that Google sets the payment terms or that it provides general information to its clients cannot have the effect of depriving Google of the exemptions from liability provided for in Directive 2000/31". Therefore, the key issue seemed to be *knowledge or awareness* rather than *financial gain*.

The case of *Viacom v YouTube* is another example, from the United States, of a UGC intermediary generating revenue from hosting content supplied by others, some of which is infringing, not of trademarks but of copyright. In 2007, Viacom, owner of the rights to numerous entertainment television programmes and movies, sued Google, as owner of YouTube, for copyright infringement involving the unauthorised posting of clips from properties owned by Viacom (such as MTV videos, or TV comedy clips).[26] In US law, the DMCA, Section 512(c)(i), holds a service provider immune from liability for copyright-infringing content if it does not have actual knowledge of such content, or is not aware of facts and circumstances which make such infringing activity apparent if the infringing material is taken down or access blocked expeditiously. In June 2010, a US district court decided at first instance that YouTube was entitled to the safe harbour of the DMCA[27] and granted Google's motion for summary judgment.[28] The court held that loss of immunity required "knowledge of specific and identifiable infringements of particular individual items" and that "mere knowledge of such activity *in general* is not enough". Viacom filed a notice of appeal with the Second Circuit appellate court in August 2010.

In the meantime, YouTube has worked with the content industry to develop an automated system, known first as "Claim Your Content" and now as Content ID, which enables both copyright holders and YouTube to generate advertising revenue from copyright-protected content that is uploaded to YouTube. More specifically, Content ID enables holders of IP rights to submit the content they want protected to YouTube, which embeds a "watermark" hash against which user-supplied videos are compared. If the content to be uploaded matches a known copyright item, then the rights holder can ask YouTube to block it entirely, to monetise it by placing ads next to it, with the rights holder sharing in the revenue, or alternately to gather statistics on who views the content and where.[29] YouTube thus appeared to have voluntarily made available the pre-emptive filtering solution which Tiffany had proposed in the eBay case. YouTube's Content ID solution is automated and thus economically feasible for them while rights holders must do the work of identifying their content to YouTube.

Host or publisher?

Some European courts have tended to avoid the immunity provisions of the ECD (as locally implemented) in contentious web 2.0 cases, by classifying a site as a "publisher" rather than an "intermediary". In the French *MySpace* decision of 22 June 2007, a French cartoonist whose sketches had been posted without his authorisation successfully sued MySpace for infringement of his author's rights and personality rights.[30] The court found that MySpace should be classified as a publisher because it provided "a presentation structure with frames, which is made available to its members" and "broadcasts advertising upon each visit of the webpage, from which it profits". As a result MySpace did not benefit from the hosting immunity provision of Article 6.I.2 of the *Law on Confidence in the Digital Economy*.

Instead, in another French case, *Dailymotion*, the court found that Dailymotion, a French video platform, was *not* a publisher.[31] Nonetheless, the court reached the same decision as in the MySpace case. It ruled that Dailymotion, although classed as a hosting provider, was still liable for providing Internet users with the means to commit copyright infringement, because "the success of Dailymotion's website depended upon the broadcast of famous works because ... these works captured larger audiences and ensured greater advertising revenues". The court also found that Dailymotion should have exerted prior restraint on access to copyright infringing works, that is, it should have installed effective filtering tools. Since it had not, it was liable.

Such decisions in France and elsewhere show that every case depends on the facts at hand and that the ECD is interpreted differently across jurisdictions in the European Union and indeed within the same member state. These differences are compounded by differences between the European Union, the United States and other jurisdictions. An additional reason for the persistent lack of consistency in web 2.0 jurisprudence is that litigation may simply not occur, not because there may be no grounds for liability, but because business sense leads to negotiated settlement or overlooking the issue.

Freedom of speech and potential "chilling effects" of the notice and take-down paradigm

Many have claimed that NTD regimes can exert a potential "chilling effect" on freedom of speech. In the early UK case of *Godfrey v Demon Internet*, a British physicist, Lawrence Godfrey, alleged that an anonymous hoax message posted in a newsgroup, soc.culture.thai, in 1997 was libellous. Godfrey asked the ISP, Demon, which carried the newsgroup in question, to remove the offensive posting. When Demon did not comply, Godfrey sued Demon, as publisher, for libel. In essence Demon pleaded that it did not know the text was libellous.[32] However the court held that because Demon had been notified and had not removed the post, it lost the benefit of its statutory immunity as host.

The interpretation of *Godfrey* by many United Kingdom ISPs was that, to avoid the risk of litigation, they should remove or block access to *any* notified item without detailed investigation. Cyber-liberties groups protested that this meant any competitor or pressure group could censor text posted on the Internet simply by complaining to the intermediary service provider.

A factor that might deter an intermediary service provider from taking down is the fear that unfounded take-down could lead the content provider to claim breach of contract, although acceptable use clauses in subscriber contracts can help control this risk. In the US DMCA, when an intermediary service provider takes down in good faith, it is protected from any such liability. Such protection does not exist in the ECD; however, it is a minimum harmonisation, so that states have discretion to introduce it. European intermediary service providers likely still regard default take-down on demand as their safest and easiest option. UK and US research shows that the incentive to take down content upon receipt of a NTD request weighs more heavily than the potential costs of not doing so.[33] In the United States, one study concluded

that almost a third of take-down requests made by rights holders under the DMCA were substantively or procedurally flawed and over half of demands for link removal came from competitor companies.[34]

In the United States, the DMCA builds in a number of safeguards to discourage arbitrary NTD. Any take-down notice *must* be notified to the content provider, which can file counter-notice to object to the removal of the material. In this case it can be put back by the service provider, although it is not *required* to do so.[35] If the original notifier continues to dispute the legality of the content, and the content provider to assert it, the argument must be taken to the courts. While the dispute is in progress, the service provider is given safe harbour to keep the content up, free from liability, even if in the end a court decides the content is illicit or actionable. Nothing in the EC regime requires notification to the site whose content is taken down; this is largely a matter for each intermediary service provider's contractual rules and internal procedures. The DMCA also has strict rules to ensure that the person demanding take-down properly identifies himself as the person with the right to demand take-down (using digital signature identification if requesting take-down by email) and specifies details to enable the offending content to be easily located. This discourages fraudulent, unauthorised or over-broad complaints. For example, Section 512(f) of the DMCA allows Internet users whose content has been wrongfully removed to bring a lawsuit against a party that "knowingly materially misrepresents … that material or activity is infringing" for damages or an injunction. In one instance, a US court found that a copyright holder violated § 512(f) by sending take-down notices regarding documents posted under the fair use exemption.[36]

Search engines and hyper-linkers

Linking liability is another issue expressly dealt with by the DMCA but not addressed in the ECD. It is particularly critical for search engine sites, which create links to material over which the search engine has neither legal nor practical control. Hosting as detailed in ECD Article 14 requires storage, which seems to imply that merely making a hyperlink to content may not constitute hosting. The DMCA by contrast expressly limits immunity when a link is made to infringing material under certain conditions.[37]

Although the European Commission specifically instructed countries to investigate linking liability on an ongoing basis by Article 21(2) of the ECD, only a few states have so far created special linking immunities. This creates inconsistency across Europe.[38] Since the drafting of the ECD, aggregators – which essentially make links to a wide variety of upstream content over which they have no editorial control and may or may not have technical control to remove individual links – have also become important Internet intermediaries. Aggregator sites, like search engines and tagging sites, are generally seen as a public good in terms of promoting access to knowledge, information management, consumer choice and competition.[39] Many have therefore suggested incorporating immunity from linking liability into the ECD intermediary scheme in future to reduce business risk and to harmonise within Europe and with the US DMCA scheme. [40]

However, the argument for not doing so is the fact that very few cases in Europe have created problems by ascribing liability to search engines in respect to links made.[41] The ECJ has looked at the liability of Google as a *host* but not as a linking intermediary.[42] The question of linking liability in the European Union thus remains a matter for the domestic law of each member state. This issue is significantly complicated by the operations of clearly infringing sites (such as Pirate Bay) which operate by providing links to infringing materials, rather than hosting and distributing the content directly.

Linking liability and the illicit P2P file-sharing problem

When downloading and file sharing became a major issue for the content industry in 2000-05, litigation was pursued globally against sites such as Napster[43] and Grokster for authorising or promoting copyright infringement. These applications based on peer-to-peer (P2P) technology did not host infringing

files themselves, but pointed to such files held by others. Napster originally aided unauthorised file sharing by providing a centralised database index to music files hosted by others; later, P2P-powered client sites, such as Grokster, provided software that helped locate the uploaders. The Supreme Court in *Grokster* held that there was liability for inducement of infringement. It based its analysis of the technology provider's culpability not on the distribution of the technology, but on the provider's intent to induce infringement.

Modern decentralised protocols such as BitTorrent make it difficult to find a critical central chokepoint intermediary to sue, but still depend on intermediary sites, such as the well-known Pirate Bay,[44] which host files known as "torrents". Torrent files are text files which, when installed on a P2P software client, point to other users using the same P2P client and network, from whom parts of the desired file can be downloaded. Combating illegal P2P file sharing would be easier if torrent hosts were considered to be infringers of copyright; such a ruling was made for the first time in a Swedish court, in 2009. The courts found that the operators of Pirate Bay had criminally infringed Swedish copyright law, and sentenced them to a year in jail and a GBP 2.4 million fine.[45] Some argued that Pirate Bay merely provided links to offending files, and did nothing more than search engines like Google, but the Swedish court found that both their "awareness of illegality" and their acts were very different. Since Pirate Bay posted take-down letters sent by copyright owners on its site to ridicule them, the court determined they had actual knowledge of copyright infringement but failed to take action. Furthermore the court found financial complicity, given that the Pirate Bay operators generated sizeable revenue from advertising on the site. In addition, the majority of files Pirate Bay linked to were protected by copyright, an indication that their business model was substantially based on infringement.

As a matter of policy, the question arises as to whether a clear theoretical line can be drawn between "good" hyper-linkers, which deserve limitations on their liability, and "bad" hyper-linkers, which do not. The question is how to make an objective assessment: by revenue models (both Pirate Bay and search engines generate revenue from site advertising), by the type of content accessed (the Swedish court emphasised that most content linked to by Pirate Bay torrents was infringing, while content search engines link to a mix of infringing, licensed and non-copyright work); or by the intention of the site operators and the intention of their users.

As seen in the US *Viacom* case, which is however currently under appeal, the district court decided that YouTube's fulfilment of its notice and takedown provisions absolved it from liability under the DMCA, despite more subjective claims that YouTube had knowledge of infringement on its network. In another case, the ECJ seemed willing to engage in more "subjective" factors by introducing in the *Adwords* case the notion of the "neutral" intermediary. Disagreement seems to be emerging as to whether the "new" types of intermediaries should be structurally independent of their users in order to warrant immunity from liability.

Pressure to filter *ex ante* rather than take down *ex post*

Overall the preceding discussion has suggested some pressure, supported by luxury goods trademark holders, publishers, and video or music rights holders, to move from the currently prevalent NTD solution, which only obliges intermediaries to remove illegal or actionable content *ex post*, to filtering solutions, which monitor content and if needed reject it.

This trend can be observed in the intellectual property field, and in some countries Internet intermediaries are asked to take action against repeat infringers rather than merely asked to remove infringing works. Several roles have been proposed and some enacted for ISPs, such as disclosing the identities of file sharers, with or without a court order;[46] notifying file sharers that their illegal downloading has been observed; blocking access to known P2P sites; traffic prioritisation; and operating a policy of

"notice and disconnection", *i.e.* eventually removing or suspending the repeat offender's Internet access if the alleged infringing activity continues after several notifications (known as "graduated response").

There is support from some law enforcement agencies (LEAs) and child protection agencies for ISPs to be required to filter out online child pornography (see the case study on Illegal Content and Child sexual abuse material). Yet another area in which ISPs are being encouraged by some to help fix problems is Internet security (see the case study on ISPs and Malicious Software (Malware) Security Threats). Such cases reflect an evolution of the view that Internet intermediaries should not be liable without specific notice for content created by third parties, nor made liable if they refuse to filter it, monitor it, investigate it, etc.

An evolving view of Internet intermediary liability

Three factors were once put forward by the emergent ISP industry to secure regimes of immunity from or limitations on liability: *i)* if ISPs were held liable, the consequences for the public interest in terms of growth and innovation in the Internet economy could be harmful; *ii)* ISPs could not exercise effective factual or legal control over the content or activities of others; and *iii)* ISPs were not morally responsible for the content or acts of others.

By 2010, it had become appropriate to consider whether and how these factors have evolved across all sizes of enterprises. However, with access to and ability to use the Internet increasingly indispensable to fully function in society, ensuring that intermediaries are able to provide these essential services may be more important than ever, and this may involve continuing to limit their liability for the wrongful conduct of third parties.

Today, the Internet economy is more mature. Internet service industries are well established, multinational and often now part of larger business entities. Special "start-up" immunities may seem less necessary for large established entities, although they might still benefit new start-up Internet service entities.

A significant change has been technological. Automated filtering of some infringing material, such as hosted content but not necessarily content in transit carried by ISPs, is increasingly possible, even though this raises serious technical and practical problems for many small-scale intermediaries. Without the co-operation of rights holders, as in YouTube's Content ID, such technologies still appear very demanding in terms of resources and subject to a degree of inaccuracy. When determination of illegality is contextual and subjective, such as libellous or obscene content, filtering is likely to remain impossible to automate in any foreseeable future. Even schemes for blocking obscene content which claim success, such as the UK Internet Watch Foundation (IWF), are based on blacklists built from human complaints and scrutiny, or classified by expert humans, as in the Australian system, and thus block only a tiny percentage of the obscene content accessible on the Internet. Even in areas such as copyright, which are more amenable to automated detection, defences of fair use and fair dealing raise issues that need to be considered and may be difficult to fit into automated systems.[47] Systems, such as PhotoDNA, promise improvements in filtering of child abuse images, but the technology cannot be extended to other types of content.[48] If filtering could to some extent be automated, the question would then shift to whether it should be mandated, given the possibilities of error, scope creep and effects on free speech, as well as the costs imposed on intermediaries and copyright holders. The required degree of accuracy, the level of costs that is justified, what can be reasonably be expected from intermediaries and what trade-offs are acceptable in terms of free speech, privacy, due process and restraints on access to knowledge, and who decides what the trade-offs should be are all critical questions.

Finally, there is the argument that the intermediary should not be held responsible for the wrongs of third parties. There are in fact no proposals to hold intermediaries responsible for the wrongs of third parties. Rather, consideration of the appropriate burden on intermediaries relates to determinations about the duty of care to be exercised in conducting their business. Lawsuits against large intermediaries, such as eBay and YouTube, indicate a relative weakening of the mere conduit argument in some countries. This can be attributed to the decline of the simple access provider, the development of services offered at no direct cost to users through advertising, and the sense that some intermediaries are engaged in a "common enterprise" with their infringing users. However, the revenues of many ISPS or hosting providers come directly from delivering hosting and Internet access services, rather than advertisements. Many are not large companies. These actors include important industries such as server farms and "cloud computing" service providers whose needs must also be considered.

At the same time, incentives to place liability burdens on intermediaries seem to have increased. Consequently, the concept of safe harbours is sometimes interpreted more flexibly, as courts in some OECD countries attempt to take new circumstances into account. Even in the jurisprudence of the US Communications Decency Act, Section 230(c), which generally grants not limited but total immunity to online service providers in respect of publication torts, this immunity has been questioned in cases such as *Grace v EBay*,[49] *Fair Housing Council* v *Room Mates,*[50] *Doe v Friendfinder*[51] or *Barnes v Yahoo!*[52]

Overall, in 2010 in the United States, there seemed to be no real drive towards reform of the DMCA or the CDA Section 230, although judicial interpretation was critical. In Europe, ways of getting around intermediary immunity allowed under the ECD, *e.g.* the seeking of injunctive relief and demands to reveal the identity of anonymous or pseudonymous content providers, were used more and more by rights holders and other aggrieved parties. Attempts had been made to find intermediaries liable on the basis of constructive as well as actual knowledge.

In many OECD countries, there had been pressure on non-traditional intermediaries such as e-commerce payment intermediaries at least to self-regulate to help control illicit content. ISPs rely more and more on technical methods of access prevention (Edwards, 2005). In Europe, the immunity provisions of the ECD in Articles 12-15 were, after some delay, to be reviewed, with a consultation launched in August 2010 by the European Commission and a communication expected before the end of 2010.[53] In the meantime a large number of references for clarity on Articles 12-15 were pending at the ECJ. With or without supranational legislative or judicial intervention, there seemed to be a move towards piecemeal European laws as interpreted by national courts, national legislatures and industry sector regulators.

REFERENCES

Bagshaw, R. (2003), "Downloading Torts: An English Introduction to On-Line Torts", *E-Commerce Law*.

Edwards, L. (2000), "Defamation and the Internet" and "Pornography and the Internet" in Edwards L. and C. Waelde, eds., *Law and the Internet: A Framework for Electronic Commerce*, Hart.

Edwards, L. (2007), "From Casual Censorship to Cartelisation? ISP Control of Illegal and Harmful Content", *3rd IDP Conference on Internet, Law, and Politics,* Barcelona.

Edwards, L. (ed.) (2005), *The New Shape of European Electronic Commerce*, Hart.

Lemley, M. (2007), "Rationalising Safe Harbors", 6 J. On Telecomms and High tech L 101, at 102-105.

Perset, K. (2010), "The Economic and Social Role of Internet Intermediaries", OECD Digital Economy Papers, No. 171. doi: 10.1787/5kmh79zzs8vb-en.

Sutter, G. (2003), "Don't Shoot the Messenger? The UK and Online Intermediary Liability", 17 *Intl Rev L, Computers and Technology*.

BUSINESS PRACTICES AND SELF OR CO-REGULATORY CODES

Even in the absence of legal compulsion, many intermediaries have adopted policies and practices designed to restrict the use of their system for specific illegal activities, adapting their response to the nature of the illegal activity. Business practices of intermediaries and the development of self-regulatory industry codes differ depending on the intermediary's role and the illegal activity involved, as do legal regimes. In practice, regulators have become increasingly adept at securing voluntary agreements, partly out of intermediaries' desire to forestall more intrusive regulation. Self- and co-regulation addresses many of the same issues and offers some advantages and some risks compared to traditional government regulation.

Business practices: Internet intermediaries as platform regulators

Most Internet intermediaries take the position that they that they do not "police" content and that they do not assume responsibility for content created or posted, goods sold, websites referenced or applications downloaded on their platforms. At the same time, many platforms and communities have adopted community standards and associated rules to reduce inappropriate content and actions. Internet intermediaries generally have a strong interest in preserving the trust of their users and/or customers.

Research shows that Internet intermediaries, as platform managers, have incentives to adopt policies and practices to preserve the integrity of their platform (Boudreau and Hagiu, 2009). Providers of two-sided platforms – economic networks with two distinct user groups that provide each other with network benefits, such as eBay or PriceMinister – regulate access to and interactions on their platforms through combinations of legal, technological, informational and other instruments, including price setting (Perset, 2010). The self-regulatory role played by multi-sided platforms is often at the core of their business models (Boudreau and Hagiu, 2009).

Legal instruments, namely contracts, are often a way for platforms to enforce managerial decisions. For example, Apple's iPhone application developers have to accept to abide by a set of rules and procedures which enable Apple to make the final decision on the applications available to its customers on its online store. Similarly, as Facebook grew, it developed a set of refined conditions for the applications developed for its platform.

Legal instruments are frequently underpinned by technological design choices and business innovations. A widely cited example is the deployment of content recognition technology by UGC platforms such as YouTube, MySpace and DailyMotion. The technology provides copyright holders with a tool to control the use of their content on UGC platforms. Google, as a UGC platform, allows rights holders, through their content identification system Content ID, to choose to create revenue from their content or to promote it or to block unauthorised uses. If copyright holders block use of content, end users can state that their use is lawful and contest this. UGC platforms may or may not have a legal obligation to provide this type of tool. But through partnering with content providers, platforms can potentially increase the legal copyrighted content on offer on their platform and therefore the advertising revenue from such content and, at the same time, minimise their liability risk.

Intermediaries' business decisions can meet policy objectives when there are incentives to gain (or avoid losing) market share in competitive marketplaces or to expand into new high-growth markets in concentrated markets. Apple's iPhone platform, for example, does not allow any unapproved application to run on its devices; this can be seen as an attempt to enhance the value of the platform through quality

assurance. This strategy is different from Google's for its Android platform. Moreover, technology firms adopting a platform strategy often leverage partner firms to develop complementary products and services to increase the number of applications using the platform technology and ultimately, platform product sales. Thus, Google's Android operating system or Apple's iPhone OS support and encourage application development on their platforms (Gawer and Cusumano, 2002). Internet intermediaries often pursue similar strategies when setting the system architecture on their platforms and co-ordinating technological innovation within and around their platform domain.

Price-setting is another important instrument, especially to influence adoption on the different sides of the market served by a platform. For example, on one side of the market, Apple subsidises use of its iPhone OS, and, on the other side, pricing on the App Store traditionally had two clear pricing boundaries: USD 0.99 and USD 9.99, although it should be noted that Apple's pricing strategy has recently evolved. At either extreme, applications were less likely to generate revenue. At the bottom end applications were free, and at the top end customers were unlikely to purchase the application since USD 9.99 was seen as the ceiling.[54] Platform firms can also complement "hard" pricing incentives with soft power, *i.e.* co-ordination by means of communication, signalling and relational contracting (Boudreau and Hagiu, 2009).

Policy goals and the balance between the needs of the two sides in the context of market-based intermediaries

The economics of platform intermediaries are such that they pursue strategies to attract different classes of customers at the same time, *i.e.* the two sides of the market. In order to gain customers from one market side (*e.g.* advertisers), they may seek personal information on the other side of the market. These incentives make platform intermediaries particularly subject to public scrutiny by consumer protection agencies. If users can switch at ease to alternative platforms, competition, along with sound regulation, may help ensure that intermediaries maintain adequate standards of consumer protection.

The extent of the alignment between Internet intermediaries' incentives and public policy goals depends on the issues. For example, while cyber-security is a common goal of stakeholders, incentives and capabilities do not always align. In protecting privacy on the Internet, intermediaries whose business model relies on monetising users' personal information to finance services offered at no direct cost need to take into account the policy goal of protection of personal information. Similarly, public policy goals related to protecting intellectual property rights – both copyright and trademarks – are not necessarily directly aligned with intermediaries' goals of encouraging and monetising platform use. By contrast, the safety dimensions of consumer policy are considered an area in which intermediaries' market incentives are aligned with the objectives of policy makers, since online marketplaces and payment providers have a strong incentive to meet consumers' concerns about security and payment systems to gain repeat purchases.

Experience shows that business practices can attempt to improve the level of consumer protection or the level of security in the absence of formal public intervention. For example, intermediaries may consider that guaranteeing the security of consumer transactions is in their best interest if they face market (and/or political) pressure.

Many intermediaries do not operate in traditional market contexts

Although much of the focus of this report is on major market players that operate as intermediaries in some way, it is important to recognise that a majority of online intermediaries operate in a non-financial or a minimally financial context. Any individual who operates a blog for his or her friends or local community (using, for example, a blogging platform such as blogger.com) can be considered an Internet intermediary operating a platform that helps to enable communication. Indeed, blogs "give access to, host,

transmit and index content originated by third parties", as do websites that allow users to post comments (including the websites of NGOs, governments, news sites, etc.). Recent statistics indicate that more than 140 million blogs are currently operating on the Internet and there are tens (if not hundreds) of millions of websites that allow user comments.[55] These numbers are far greater than the number of ISPs, search engines, social networks and other commercial platforms.

Although some individual and non-commercial blogs and websites also run simple advertisements, the presence of ads does not transform the site into a commercially focused or driven operation. The focus and goal of these sites is generally not to maximise ad revenue, but to provide a communication forum for a select group of people.

Thus, any consideration of liability, incentives or other obligations on intermediaries must take into account the fact that many intermediaries are non-commercial sites operated by individuals or small organisations that lack the resources to comply with many legal or liability-based constraints.

Internet intermediaries' self- and co-regulatory approaches can help advance public policy goals

Self-regulation occurs when non-governmental actors co-ordinate their conduct in order to respond to policy objectives or forestall regulation. Codes of conduct, best practices or seal of approval programmes have often been developed, *e.g.* to set out procedures for users to collaborate on participative networks, for Internet providers to exchange traffic, for ISPs to implement notice and take-down or to help combat spam, etc.[56] Self-regulation offers benefits, but also presents risks (Table 1).

Table 1. Benefits and risks of self-regulation

Benefits of self-regulation	Risks of self-regulation
- Key benefits to business flow from the flexibility and adaptability of self-regulatory mechanisms, and their ability to harness specialist industry knowledge to ensure a good "fit" with the problems they need to address. Self-regulation allows business to take control, and provides an opportunity for sharing the costs of reputation building. It can also be a valuable tool for businesses seeking to improve the reputation of an entire industry or sector. - Self-regulation can, in some instances, reduce regulatory burdens and obviate the need for more heavy-handed and formal controls. - For consumers, key benefits flow from the degree of commitment that industry control engenders. This helps to increase compliance with the law, and may in some cases encourage business to raise the bar and reach higher standards. - Self-regulatory mechanisms often provide the means by which consumers can identify businesses that are committed to delivering high standards, thus helping to build consumer confidence. They may also provide efficient resolution of consumer complaints, and an effective means of consumer redress.	- Self-regulatory mechanisms cannot provide a complete solution to all problems within a market. Their largely voluntary nature means that they are unlikely to provide full coverage. - Protection for consumers afforded by the rules may not, for a number of reasons, prove to be as effective as intended or claimed. - Self-regulation may raise standards to a level higher than some consumers actually want. This can reduce consumer choice and make the market inaccessible to some groups of consumers. There should also be a minimum level of protection afforded. - Self-regulation can provide businesses with the opportunity to restrict competition, whether intentionally or not. Co-operation may lead to anti-competitive practices such as creating barriers to entry or allowing the co-ordination of decisions on output or pricing. Self-regulatory initiatives must be designed and maintained in such a way as to avoid anti-competitive consequences.

Source: Policy statement: The role of self-regulation in the OFT's consumer protection work, September 2009, www.oft.gov.uk/shared_oft/reports/consumer-policy/oft1115.pdf.

Co-regulatory action is the result of the interaction of self-regulatory initiatives and explicit governmental mandates based on statutory provisions. It provides explicit legal authority and safeguards that guarantee regulatory intervention if industry players are unable to set up and adopt a self-regulatory system. Self- and co-regulation are established in many Internet markets and frequently involve some degree of public sector endorsement (RAND Europe, 2008).

Performance drivers for self- and co-regulatory schemes

Several institutional and industry factors support effective self- and co-regulatory arrangements (Ofcom, 2008):

- *Stakeholder incentives:* whether or not they are aligned with the interests of citizens and consumers.
- *Industry structure*: Market structure, as well as the number of firms producing identical services, influences the level of co-operation by Internet intermediaries. Markets without clear leaders, *i.e.* fragmented or low-concentration markets with many small operators, are less conducive to self- and co-regulation because no large actor will take responsibility for industry practices. In contrast, intermediary platforms that are leaders on their market, such as eBay or Amazon in online marketplaces, are likely to face considerable pressure to regulate activities on their platforms.
- *Level of homogeneity* of Internet actors engaged in the self-regulatory effort and whether they belong to the same jurisdiction. Both factors facilitate the emergence of a sense of community among Internet intermediaries, which can favour identification of regulatory objectives and co-ordinated and sustained action in pursuing such goals.
- *Pace of change*: Technological progress and the speed at which some business models evolve on the Internet means that reaching stable, established business practices is difficult. This points to the challenges for establishing legislation and the advantage of self-regulation which can respond more rapidly and efficiently.
- *Level of technical complexity*: If technical complexity is very great, it can complicate the agreement to and implementation of any scheme.
- *Representative bodies* when well-established (*e.g.* ISP associations) can help to generate trust in self- and co-regulatory schemes.
- *Incentives not to participate or not to comply with the agreed codes*. When such incentives exist, a self-regulatory solution can be inappropriate as it would lead to free-riding by some members.
- *Review and assessment* as an important part of effective self-regulation.

The performance of self- and co-regulatory solutions can be assessed by examining processes of development, membership, rule making, monitoring, enforcement, sanction and evaluation (RAND Europe, 2008). Understanding the regulatory options available to policy makers can help the design and implementation of self- and co-regulation: *i)* an increased focus on self- and co-regulation can strengthen the analysis of normal regulation by enabling policy makers to identify and quantify the costs and benefits of regulatory arrangements other than statutory regulation; *ii)* appreciating the variety and rationales of existing self- and co-regulatory arrangements, many of which have developed without top-down design, can help government policy initiatives to tailor their regulatory approach to specific issues; and *iii)* policy makers can best adopt and promote industry regulatory solutions by taking into account the extent to which a specific industry setting is conducive to effective self- and co-regulation. Building upon a case review and the analysis of conditions that promote or hinder the potential for self- and co-regulation, Ofcom developed a set of good practice criteria to guide the establishment of new self- and co-regulatory schemes (Table 2).

Research shows that policy makers frequently contribute to the development of self- and co-regulatory schemes once they have been established. Overall, self-regulation is most likely to be effective when the industry has a collective interest in doing so; when it is able to establish clear objectives for a self-regulatory scheme; when the likely solution matches legitimate consumers' and citizens' needs; and when the self-regulatory or co-regulatory schemes yield rules that are enforceable through either contracts or private legal actions or government enforcement actions, or both.

Table 2. Good practice criteria for self- and co-regulation and their rationales

Good practice criterion	The criterion ensures that:
Public awareness	Citizens acknowledge their rights, *e.g.* the right to redress; it is also beneficial when reputational benefits accrue to firms participating in the scheme and consumers can choose between firms which are members of the scheme and those which are not.
Transparency	Stakeholders' confidence is required to guarantee the success of a scheme. A degree of public accountability (*e.g.* publishing annual reports and wide public consultation) can complement openness in operations.
Significant numbers of industry players are members	Firms' private incentives neither conflict with the public interest nor induce free-riding on reputation built by other members; the scheme can therefore be influential across the whole industry and act independently of individual members.
Adequate and proportional resource commitments	Sufficient resources are available for the effective operation of the scheme; a proportionate cost distribution is important not to discourage smaller players from joining, while staff skills and numbers are attuned to the type and quantity of work.
Enforcement measures	Punishment mechanisms are a sufficient threat against members cheating on their obligations; incentives to comply are reinforced by transparent disclosure of information from members and intelligible association of sanctions to breaches.
Clarity of processes and structures	Defined terms of engagement are shared from the outset, specifying the terms of reference, funding and decision-making arrangements, institutional structures and, where appropriate, time limits to achieve the objectives set.
Audit of members and scheme	Key performance indicators (KPIs) for each member's conduct are met consistently across the industry; this is complemented by setting and publishing KPIs for the overall scheme, which eases reviews of the scheme under evolving circumstances.
System of redress in place	Adequate standards for handling complaints, which can feed into an independent appeals mechanism for effective and quick resolution and disclosure of outcomes.
Involvement of independent members	The scheme is respected by other stakeholders such as citizen or consumer groups, parliament or government; this may be less relevant when the scheme affects the interest of consumers/citizens only indirectly or deals with detailed technical issues.
Regular review of objectives and aims	Monitoring of whether the remit and operation of the scheme is sufficient to meet citizen/consumer needs, as stakeholders' expectations or market conditions may evolve.
Non-collusive behaviour	Compliance with competition law statutes, by means of sufficient approval and transparency built into the scheme. This is necessary to demonstrate to third parties industry members' commitment to non-collusive behaviour.

Source: OFCOM (2008).

REFERENCES

Boudreau, K. and A. Hagiu (2009), "Platforms Rules: Multi-Sided Platforms as Regulators", in Gawer, A. (ed.), *Platforms, Markets and Innovation*, Edward Elgar, Cheltenham and Northampton, MA.

Gawer, A. and Cusumano, M. (2002). Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation. Harvard Business School Press Books.

Ofcom (2008), Identifying appropriate regulatory solutions: principles for analysing self- and co-regulation, Statement, 10 December 2008, http://stakeholders.ofcom.org.uk/binaries/consultations/coregulation/statement/statement.pdf.

Perset, K. (2010), "The Economic and Social Role of Internet Intermediaries", OECD Digital Economy Papers, No. 171. doi: 10.1787/5kmh79zzs8vb-en.

RAND Europe (2008), Options for and Effectiveness of Internet Self- and Co-Regulation, Prepared for European Commission DG Information Society & Media, www.rand.org/pubs/technical_reports/TR566.html.

CASE STUDIES IN DIFFERENT POLICY AREAS

Intermediaries raise policy issues related to the nature and extent of their role and potentially their legal responsibilities for actions made possible by the use of their systems. These case studies look into several intermediary liability policy areas: free flow of information, privacy and security, illegal content and child inappropriate content, illegal online gambling, copyright and counterfeiting, and the safety dimensions of consumer protection. In each of these policy areas the role or practices of one or two specific types of intermediaries are discussed (Table 3). As platform providers in two-sided markets, certain Internet intermediaries raise other policy issues, namely competition issues, which the report acknowledges but does not discuss in detail.

Table 3. Case studies of intermediary practices to advance specific policy issues

Internet actors / Policy issues[1]	ISPs Internet service providers	HOSTS Data processing & hosting	SEARCH Search engines & portals	E-COMMERCE Online marketplaces	PAYMENT E-commerce payment	WEB 2.0 Participative Web platforms
Free flow of information	Y	Y	✓			✓
Security threats	✓	✓	Y	Y	Y	Y
Illegal content and child-inappropriate content	Y	✓	Y	Y	✓	Y
Illegal Internet gambling		Y	Y		✓	✓
Copyright	✓	✓	✓	✓	Y	✓
Counterfeiting	Y	Y	✓	✓	Y	Y
Consumer protection in e-commerce payments		Y	Y	✓	✓	Y
Other issues (competition)	Y	Y	Y	Y	Y	Y

Note: ✓: explicitly mentioned in the report.

Y: issues exist but the present report does not detail them.

1. The policy issues in the table were given highest priority by delegations in the ICCP Volunteer Group on Internet intermediaries. Issues such as defamation and taxation were excluded on the basis of the ranking.

GLOBAL FREE FLOW OF INFORMATION

Introduction

Policy principles for Internet intermediaries should take account of social development aspects, particularly human rights and democratic rights. In some cases, government policies require or pressure intermediaries to monitor the information they transmit or to remove certain information; this raises concerns about risks of censorship and violation of freedom of speech. Risks are also involved when intermediaries are asked to reveal personal information about users of their platforms. Companies may find themselves trying to reconcile their obligation to respect the law with their general responsibility to protect the rights of their users. To help them manage such situations, self-regulatory initiatives such as the Global Network Initiative (GNI), which requires its members to conduct *ex ante* civil rights impact assessments and to adopt strategies to mitigate risks to human rights, are viewed by many as best practice.

The Internet enables users to access, share and create information in new ways. The volume of information and the speed at which it is created and accessed continue to increase. The open and transparent architecture of the Internet allows it to function as a single, global platform. Many citizens are using tools such as blogs, social networks and video-sharing sites to express their political views and to access information of everyday social, political, and economic concern. By vastly expanding individuals' ability to communicate and enhancing the public's capacity to obtain such communication, the Internet has proven itself to be a platform that can help advance freedom of expression, freedom of association, the free flow of information, the growth of communications, and economic growth.

What is the free flow of information?

With regard to the Internet and information technology, the free flow of information refers to the right to freedom of expression. It relates more broadly to the commitment to defend and advance freedom of expression, freedom of association and access to information through all media and regardless of frontiers. It builds upon the concept of freedom of expression, recognised as a human right under Article 19 of the UN Universal Declaration of Human Rights adopted in 1948:[57] "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[58] Freedom of information, like political and economic freedom, can provide an impetus to economic growth and benefit society through access to information and services. Privacy, in addition to being a fundamental right in itself, also enables free expression; preserving anonymity an important policy objective in appropriate contexts. There are, however, longstanding and accepted exceptions to free expression under law, such as inciting to violence, defamation, slander or copyright infringement.

All OECD member states must grapple with certain challenges to the free flow of information. According to Freedom House, these challenges are increasing and have become more diverse.[59] One involves demands by governments for Internet intermediaries to censor political speech or to obtain users' personal information in order to limit their right to free expression. As of mid-2010, several OECD governments, including the United States and Sweden, were actively investigating strategies to protect freedom of speech on the Internet by identifying threats to freedom of speech, looking for common ground on principles to protect and promote Internet freedom, and discussing potential solutions to mitigate threats to freedom of expression on the Internet. The United States Department of State created the Global Internet Freedom Task Force to track the issue and engage with foreign governments, and the US Commerce Department has created an Internet Policy Task Force to conduct a comprehensive review of the links between privacy policy, copyright, the global free flow of information, cyber-security and innovation in the Internet economy.[60]

Harm caused by censorship

More countries are imposing forms of censorship and surveillance on the Internet (Box 1). In particular, some governments pressure intermediaries to block or filter Internet content or communications either without any evidence of illegality or based on rules that may be unclear, unexplained or enacted without adequate due process or transparency.[61] Some countries have erected electronic barriers, notably filters, that prevent users in their countries from accessing portions of the world's networks in ways that run counter to the spirit of internationally agreed norms such as the Universal Declaration on Human Rights.[62] Many of these policies oblige intermediaries, directly or indirectly, to monitor and police the information and ideas transmitted over their networks. In some countries governments may even use this policy to, in effect, delegate censorship to the private sector. Other policies require intermediaries, which have large amounts of data on individuals' online activities, to provide this information to authorities as a way to limit free expression on the Internet. It can be difficult for intermediaries to operate in such environments and respect fundamental rights.

State-mandated filtering by Internet service providers has increased, and, as the Internet becomes more pervasive around the world, there is also increasing evidence of Internet filtering at other points in the network. Of particular interest are intermediaries that host social networking services (these also facilitate freedom of association), blogs and websites. Because so many Internet users depend on Internet intermediaries to publish content, censorship of these entities by governments has the potential to exercise a powerful control on online speech. Legal authorities may also seek sensitive information about users from intermediaries.

Box 1. Categories of censorship

Three broad categories of threats to Internet freedom are identified: obstacles to access, limits on content and communication, and violation of users' rights.

Obstacles to access. These reflect governmental efforts to block specific applications or technologies.

Limits on content. These include filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; diversity of online news media; and use of digital media for social and political activism.

Violations of user rights: These concern restrictions on online activity; surveillance; privacy; and repercussions of online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

Source: Based on Freedom House, Freedom on the Net, April 2009.

The problem of censorship has been depicted in many ways – as an ethical issue, a drive for new markets, an international legal issue, an Internet governance issue, a trade barrier (blocking access to goods and services), or an organisational issue.[63] In addition to presenting a challenge for companies and contravening the Universal Declaration on Human Rights, censorship can also negatively affect wider economic interests**.** Filtering of news and information can affect the confidence of corporate decision makers over the medium and long term.

Freedom of expression can also be unintentionally eroded as various actors pursue an array of valid objectives, such as the security of networks or the protection of children. Freedom of expression can in fact be either diminished or reinforced by these competing and legitimate policy objectives, which often involve assigning liability to intermediaries and/or building technical surveillance systems. Policies creating intermediaries' liability for activities of their users may threaten to constrain expression by creating incentives for intermediaries to restrict the use of their services for content that may be considered controversial or to limit the pseudonymous or anonymous use of these services. Furthermore, once surveillance systems are implemented for legitimate purposes, strong political and legal safeguards are

needed to avoid misuse or use of these systems for other purposes. In general, it is critically important that governments and other stakeholders carefully consider policies and practices which impose liability on Internet intermediaries because of the potential impact on basic human rights. In addition, initiatives to promote freedom of expression on the Internet should be as holistic as possible and take a whole-of-government approach.

To support informed policy making, benchmarking at the international level is essential to indicate the scope and scale of censorship. Google already discloses data on government take-down requests.[64] It would be valuable if other companies also provided information on take-down requests.

The Global Network Initiative (GNI)

Corporate strategies to address barriers to the free flow of information

Global companies have chosen to address barriers to the free flow of information, goods and services in different ways and in different venues. Some act on their own, by developing individual relationships with governments of countries in which their affiliates operate. Others engage in informal discussions with other companies in their sector to share experience and best practice. Some companies collaborate or work jointly with non-governmental stakeholders to develop principles that seek to uphold freedom of expression and privacy on the Internet and to respect the Internet's open and transparent nature.

The Global Network Initiative is an example of such collaborative effort. It is a multi-stakeholder group of companies, academics, investors and NGOs which was launched in December 2008. GNI has developed a set of voluntary principles to combat threats to Internet freedom which other stakeholders can also adopt; it is rooted in the rights defined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[65] GNI provides a framework for its participants to uphold these rights. If companies choose to operate in markets where freedom of expression and privacy may not meet internationally recognised standards, GNI recommends that they adopt measures that help ensure respect for basic rights to freedom of expression and privacy.

Assessing the impact of policies on human rights and setting up safeguards

The GNI helps companies to plan ahead and incorporate human rights assessments into plans for new products or plans to enter new markets. Measures include the development of risk assessment and mitigation strategies when entering markets; seeking clarification or modification from authorised officials when government restrictions appear excessively broad; acknowledging the importance of proportionate initiatives to prevent access to illegal online activity such as child exploitation; and, critically, being transparent with customers, the general public and users about their rights and responsibilities and the requirements placed on companies.

The GNI's structure and approach are defined by four documents covering: *i)* the principles; *ii)* the implementation guidelines (the guidelines); *iii)* the governance, accountability and learning framework (the framework); and *iv)* the governance charter (the charter). The principles support international standards of expression and privacy. GNI participants commit to protecting expression and privacy rights both generally and in the face of laws and government demands that seek to undermine them.[66] The implementation guidelines provide concrete guidance on respecting the principles in practice and as institutional knowledge develops. The framework describes initial expectations of a supporting organisation and its accountability and learning regimes. The charter establishes a governance structure and defines organisational elements of the GNI.

One of the principles that GNI participants adhere to is to respect and protect the freedom of expression of their users by seeking to avoid or minimise the impact of government restrictions on freedom

of expression. Another is to respect and protect users' rights when confronted with government demands, laws, and regulations to suppress freedom of expression, remove content or otherwise limit access to information in a manner inconsistent with internationally recognised norms. Companies need to be transparent with users about what is censored, why and how and they should inform users about how their personal data are stored and with whom they can be shared. For example, Google initiated the practice of appending a warning to filtered search results that notes the removal of certain results according to local law, which was subsequently adopted by other search engines. The goal of transparency measures is to inform users and enable them to make informed choices about how and when it is safe or reliable to use these services.

GNI participants also acknowledge narrow but potentially substantial limitations to the rights outlined in Article 19 of the International Covenant on Civil and Political Rights (ICCPR).[67] Limitations on freedom of expression – *e.g.* for incitement to hatred, defamation, invasion of privacy, paedophilia, cybercrime – should be necessary and proportionate for the relevant purpose.

GNI's guidelines provide guidance to ICT companies on how to put the principles into practice, describe the actions that constitute compliance, and provide the framework for collaboration among companies, NGOs, investors and academics. Companies are expected to train employees and boards on approaches and procedures, to provide whistle-blowing mechanisms for employees, and to encourage business partners and others to adopt the GNI principles. With a view to preventing incidents, participants agree to undertake human rights impact assessments to identify circumstances in which expression and privacy rights may be jeopardised or advanced (*e.g.* entering new markets; designing and introducing new technologies, products, or services; selecting partners; or responding to policy change) and to develop steps to mitigate risks and to leverage opportunities.

In the GNI framework, following a human rights impact assessment, a company may decide to make it harder for hosting servers offshore to reach its data. It may also try to reduce its vulnerability to external pressure by minimising the number and responsibilities of staff (hiring only local sales teams, who do not have operational control), and implementing other policies to limit avenues for government to abridge human rights.

The guidelines also specify how participating companies should respond to government demands to remove or limit access to content or restrict communications. They should encourage governments to make requests in writing, providing the legal basis for the request and the name of requesting official; they should interpret laws and requests narrowly and communicate actions to users when legally permissible; and they should challenge practices that appear inconsistent with domestic law and procedures or international human rights laws and standards on expression or privacy. Companies also document these requests and ask to permit tracking and review. These processes enable a responsible approach to engagement with markets in which restrictions on rights are in tension with international norms.

Much of the value of the initiative comes from activities described in the framework, which include the GNI's organisational structure and responsibilities, along with those of participating companies and independent assessors.[68] Independent monitoring supports corporate accountability, remediation where necessary, development of good practice among participants, and continued evolution and refinement of the GNI.

Opportunities

Self-regulation with industry codes of practice or guidelines (Box 2) to protect the free flow of information on the Internet presents an advantage over legal instruments of governments. The advantage is mainly greater adaptability to changes in technology, to evolving business models, to unanticipated user

behaviour, to unpredictable government action, as well as to cultural differences and jurisdictional issues. In addition, self-regulation may better support continued innovation and creativity in intermediary markets.

If widely adopted or recognised, industry self-regulatory initiatives such as the GNI have the potential to make two important contributions to the global free flow of information on the Internet: *i)* to increase transparency as to restrictions placed on the free flow of information through processes to address harmful restrictions and track efforts; and *ii)* to provide a model environment in which relevant industry sectors agree on basic principles that support human rights on line, along with a process to enable individual companies to assess and be held accountable for their own compliance with those principles.

Governments are not members of GNI, but are encouraged to support the principles and encourage their adoption.[69] The creation of multi-stakeholder institutions such as the GNI can be an effective way to craft public policy recommendations to help companies and governments alike to address ethical and business challenges on the Internet. Many of the concepts developed by the GNI, such as voluntary adherence to clear principles, self-governing structure, auditing and rights-based risk assessments, already serve as models for stakeholders, individually or in groups, to combat threats to Internet freedom.

Challenges

The GNI would benefit from additional cultural and geographic diversity. As of mid-2010, only US companies were represented, although they operate worldwide and have a culturally diverse management and staff. GNI has investor, academic and NGO participants from Europe and counts experts on Asia among them, but it would benefit from additional non-industry perspective as well. It does not have members from many industry sectors and it has no small company members.[70] Although the foundational principles and guidelines of the GNI were drafted with the input of European telecommunications operators, in mid-2010, GNI's industry participants consisted of Google, Microsoft and Yahoo!. No new companies had joined in the two years since the GNI's creation. Many large and small companies cite the cost of GNI membership and the significant GNI auditing and compliance requirements as barriers to membership. However, even though GNI's current industry membership represents only a segment of the Internet industry and not the technology industry as a whole, its member companies have been some of the most frequent targets for actions by repressive regimes. The GNI continues to conduct broad outreach with companies based outside the United States and across the technology industry to expand membership.

While most stakeholders agree that it is good practice for companies to have norms and codes of conduct relative to freedom of expression, the requirements associated with implementing codes of conduct in several different areas should be noted. For example, many companies already adhere to codes such as the OECD Guidelines on Multinational Enterprises, ISO 2600, or the World Economic Forum's global agenda on corporate responsibility, or have adopted their own code of conduct. [71] Companies must train all their employees to respect the code of conduct.

Box 2. The joint industry-Council of Europe guidelines on the protection of human rights on the Internet

In 2008, the Council of Europe, in close co-operation with European online game designers and publishers and with Internet service providers, launched two sets of guidelines that aim to encourage respect and promote privacy, security and freedom of expression when accessing the Internet, using e-mail, participating in chats or blogs, or playing Internet games.

The Interactive Software Federation of Europe (ISFE) and the European Internet Service Providers Association (EuroISPA), concerned by the need to raise awareness about human rights and to build confidence on the Internet, worked with the Council of Europe, which has a mandate to protect these rights in Europe, to create two sets of guidelines for their respective sectors. Building on existing self-regulation or projects, these guidelines offer simple and practical guidance to the operators concerned on making the Internet a more open and safe place for users and to ensure users' right to access, entertainment and creation.

The guidelines for online game providers signal the importance of raising awareness of the positive use of games, balanced with the need to secure freedom of expression and to protect users, children in particular, from unsuitable, violent or racist content. They also recommend applying independent labelling and rating systems for games, such as the Pan European Game Information (PEGI) system or PEGI Online, and offering guidance to users and parents on risks such as the excessive use of games, bullying or harassment, and providing personal data.[1]

The guidelines for ISPs recommend that companies ensure that information is available to Internet users about the risks to privacy, security and freedom of expression they incur on line. One of the key aims of the ISP Guidelines is to complement the work already carried out by operators to help protect children from harmful or illegal content and other risks. They also deal with risks to data integrity such as viruses or worms, and to privacy, such as the collection of personal data without the user's consent.[2]

This new approach complements the Council of Europe's work on promoting human rights. It acknowledges that every stakeholder, including the private sector, has a role to play. It helps Internet companies to advance human rights in their daily activity.

1. Guidelines for the Online Games Providers, www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)008_en.pdf.

2. Guidelines for the Internet Service Providers, www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf.

Source: Based on Council of Europe press release of 03/10/2008, www.isfe-eu.org/index.php?oidit=T001:96dec7f314175b346499b34f5ad64fda.

Lessons learned

- Policies to make intermediaries liable for activities of their users may risk "chilling" (*i.e.* restraining) expression by creating incentives for intermediaries to restrict the use of their services. Governments and law enforcement should consider policies that involve intermediaries in monitoring or policing information carefully in light of the potential impact on basic human rights such as freedom of expression.
- Whole-of-government approaches are needed to consider issues related to freedom of expression.
- While norms and instruments in the area of freedom of expression exist, their applicability to the Internet may warrant clarification. Public-private partnerships can be an effective way to clarify these norms and instruments and advance freedom of speech objectives.
- Measures impeding the free flow of information, goods and services on the Internet should be evaluated for their possible unintended negative impact on economic growth and innovation. Freedom of expression on the Internet is a social principle which has the potential to create economic value and long-term financial benefits for both industry and individual citizens.

- There seems to be an emerging consensus that self-regulatory initiatives such as the Global Network Initiative, which requires its members to conduct *ex ante* civil rights impact assessments, are currently a good practice model to follow.
- Technical measures to block content may have unintended negative effects on access to legitimate content and should only be used sparingly and transparently and with adequate monitoring to ensure their effectiveness and adequate protection of due process.ISPS AND MALICIOUS SOFTWARE (MALWARE) SECURITY THREATS

Introduction

Cybersecurity threats are a global issue that affects economic activity and the security and privacy of end users. Estimates of the direct damage caused by Internet security incidents vary wildly, but typically range in the tens of billions of US dollars a year for the United States alone (US GAO, 2007). While this damage is related to a wide variety of threats, the rise of malware and botnets is seen as one of the most urgent current security threats (OECD, 2008 and forthcoming).

Internet hosts – in particular home computers – can be compromised by malware, *i.e.* infected with malicious code that is controlled by criminals remotely. They can be used as "zombie hosts" to contaminate computer systems and remotely commit various types of fraudulent and harmful actions – sending spam or phishing emails, stealing an individual's identity, participating in distributed denial of service (DDoS) attacks, and even, in some cases, attacking critical infrastructures (Edwards and Brown, 2008). Since security comes at a cost, market players make their security-related decisions based on the perceived costs and benefits to them of a course of action (OECD, 2008; Michel *et al*., 2008). In many cases, a security breach does not affect the home user as much as it does the target of the attack. In fact, computer users often do not know that their machine is compromised, which contributes to the problem. Furthermore, home users are not necessarily capable of evaluating risks or stopping a security threat. More broadly, economic research and policy analysis has found that in some cases there are gaps between the private and social costs and benefits of security. Involving ISPs in preventing, detecting or helping to fix infection of home PCs is increasingly viewed as a way to realign interests and internalise negative externalities, *i.e.* costs that result from a decision to act (or not act), but are incurred by parties who are not responsible for the decision. Involving ISPs may, however, require significant amounts of time and imply costs.

According to estimates, 5% of the world's computers may be compromised (Moore *et al*., 2009). In 2008, Symantec, a provider of anti-virus solutions, identified over 1.5 million new malicious programmes, an increase of 165% from 2007. Associated costs include the money spent by end users to purchase software to avoid security problems, the time spent repairing damaged computers, and the lost value of computers made slower or inoperable. The risk of bot-infected computers is also relevant to countries' security because the more domestic computers are compromised, the more vulnerable a country is to cyber attacks from "within" (*i.e.* a cyber attack, even if launched from abroad, would appear to come from domestic sources). Security experts claim that attacks by networks of compromised computers (botnets) are increasing.

Tackling Internet insecurity is a complex task. As one potential measure, ISPs could take a voluntary but co-ordinated and standardised role in enhancing the security of compromised machines attached to their network, by notifying users whose computers are suspected of being infected, giving them guidance on how to clean their system, and in some cases quarantining their computer until it is disinfected. The market seems to be moving towards ISPs providing more security to their customers, and the Internet community, industry groups and governments are increasingly aware of the role ISPs can play in helping to address cyber-security issues (ENISA, 2008). The OECD ICCP Working Party on Information Security and Privacy (WPISP) and the Asia-Pacific Economic Co-operation Telecommunications and Information

Working Group (APEC TEL) are carrying out co-ordinated projects on the role of ISPs in enhancing the security of the Internet by working with governments, each other and their customers and by assisting customers to resolve problems with malicious software.[72]

Advantages to such approaches include the fact that detecting malware is relatively objective (compared to detecting defamation or illegal content, for example), that ISPs have a certain level of market incentives to try to limit these problems in view of the extra bandwidth requirements of malware as well as "IP reputation" costs (when suspicious activity, such as spam or viruses, originating from their IP addresses is detected), and that subscribers are generally likely to react positively to help in identifying security problems on their machines. However it is not clear whether customers are willing to pay for such ISP service.

Depending on how the framework is designed, issues involved may include the cost to ISPs, particularly smaller ones, of the security monitoring to keep up with emerging cyber threats, the fear that providing more security could increase liability in the case of a security breach, the difficulty of identifying the transmissions that cause the problem, the level of intrusiveness of this mechanism and associated privacy considerations, and the need for international co-operation given the cross-border nature of cyber-security threats.

Individual market initiatives

Collaborative efforts by the Internet Engineering Taskforce (IETF) and the Messaging Anti-Abuse Working Group (MAAWG) have produced sets of best practices for the remediation of bots in ISP networks.

Most ISPs provide security or, at a minimum, online security guidance for their customers, and virus and spam filters to incoming email. A number of ISPs propose products and services to their customers, such as free antivirus, firewall and sometimes anti-spyware software. For example, in the United States in 2009, both AOL and Comcast had formed partnerships with the software security firm McAfee to offer free McAfee software to their home Internet customers. Customers were often left to install and operate the software on their own. In other cases, ISPs deploy their own security measures, such as monitoring suspicious activity (for example, an ISP might investigate a user or a group of users and possibly confiscate temporarily their email sending privileges).

Some experts question whether there is sufficient market demand for commercial security services by ISPs, and whether there are sufficient market-based incentives for ISPs to provide increased security (Rowe *et al*., 2009). They also ask how much ISPs can be expected to do, given the sophistication and seriousness of the problem and their business models based on high volumes and low cost.

Self-regulatory and co-regulatory efforts

An international network

The London Action Plan (LAP), formed in 2004, is an international network to combat spam and other online threats. It is an example of a public-private initiative to promote international co-operation on spam and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses. Consumer protection, data protection, and telecommunications agencies around the world are members of the network, and industry also participates. The LAP builds on efforts by the OECD and other international organisations to achieve international co-operation on spam enforcement and education. Among other things, the network focuses on investigative training and establishing points of contact in each agency to respond quickly and effectively to enforcement inquiries. Many Internet intermediaries

participate voluntarily in the LAP, including ISPs, payment system providers, domain name registrars and registries, and providers of alternative dispute resolution services.

The Cyber Clean Centre effort in Japan

Japan's Cyber Clean Centre (CCC) is a long-running example of a public-private endeavour by ISPs and governments to help address the problem of malware and botnets. It is an initiative by the Japanese Computer Emergency Response Team Co-ordination Centre (JPCERT) and 76 Japanese ISPs which together cover 90% of Japan's Internet users.[73] The Cyber Clean programme is funded by the Japanese government. Its steering committee is chaired by the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI). The Cyber Clean Centre and programme are operated by the Japanese CERT (JPCERT) and Trend Micro, an anti-virus vendor and computer security firm which is under contract. JPCERT conducts the malware analysis and tests the signature developed by Trend Micro. Trend Micro develops specific file signatures to clean computers infected with specific types of malware referred to them.

The key function of the Cyber Clean programme is to analyse, test and develop specific file signatures for malware. Its goal is to help prevent direct harm to owners and users of compromised computers, since bot malware often seeks to steal valuable information from compromised computers to engage in identity theft and associated fraud. In addition, the programme establishes a procedure to clean compromised computers so as to prevent their use to support further cyber-crimes and attacks.[74]

The programme requires the co-operation of Japanese ISPs, which notify and communicate with customers whose computers are infected with bot malware and direct them to the Cyber Clean Centre. Participating ISPs receive infection notices from the government-operated and -funded CCC project. ISPs then follow their own procedures to contact their subscribers. For example, ISPs can send users an email or a letter via postal mail and direct them to the Cyber Clean Centre website to download and run a cleanup tool developed by JPCERT in co-ordination with Trend Micro.

In terms of cost to ISPs, the programme is voluntary and arguably provides a benefit to ISPs who bear some communications costs but do not bear costs of monitoring security, operating a security website, or helping customers to clean their computers. Because the Cyber Clean Centre provides tailor-made solutions for specific malware on specific computers, security experts consider that it is more effective than relying on users' anti-virus software.

Japan has had positive results from its scheme. Between December 2006 and November 2009, Japan's CCC claims to have helped over a million customers remove bot infections from their PCs. On average, around 40% of users who receive an infection report forwarded by their ISP access the CCC website and about 30% download the CCC's cleaner removal tool. At the end of 2009, about 10 000 warning emails were being sent monthly to about 5 000 subscribers and 3 500 types of security threats were concerned. There has reportedly been very little negative feedback.[75] There is little information, however, on the programme's cost.

Germany

Eco, the Association of the German Internet Industry, has built on the Japanese initiative and developed a central botnet disinfection centre project in close co-operation with the Federal Agency for Security of the Internet in Germany. This project is a public-private partnership, as the Federal Agency for Security of the Internet is not only funding the project but is also contributing to its set-up phase. The German government is establishing and funding a call centre to which ISPs can direct customers in need of support to disinfect their computers.

Korea

The Korean Computer Emergency Response Co-ordination Centre (KrCERT/CC) is part of the government agency KISA (Korea Internet & Security Agency). In 2005, KrCERT/CC initiated a public-private partnership with Korean ISPs to combat malware infecting the computers of Korean users. KrCERT, acting as a trusted clearing house for malware, collects and verifies information on malware infection vectors (*e.g.* command and control servers or malware-embedded websites). KrCERT operates a Domain Name Service (DNS) "sinkhole" which redirects traffic from these malicious and unwanted hosts and domains and shares this information with ISPs. Almost all major Korean ISPs voluntarily apply the sinkhole information in their DNS servers. This prevents their customers' computers from accessing these malicious hosts and domains using the ISP's DNS services.[76] The Korean government provided funding to launch the programme and it is implemented through a public-private partnership between KrCERT and Korean ISPs.[77]

Korea's nation-wide sinkhole system has lowered the botnet infection rate in Korea and prevented malicious botnet activities such as denial-of-service (DDoS) attacks. Between early 2005 and early 2008, the percentage of bot-infected computers in Korea was more than halved from 26% of infected computers in 2005 to under 10% in 2008.[78] According to Symantec, Korea ranked sixth among the economies with the most bot-infected computers in 2005, but dropped to fifteenth place by 2008.

In 2010, Korea also began a quarantine service for Internet users with several co-operating ISPs. If a participating ISP subscriber's computer is infected, the ISP restricts the subscriber's Internet connection to a specialised site offering tools to remove malware until the malware is removed.

Initiatives in Australia, the Netherlands, Germany, the United Kingdom and the United States

In 2010, ISPs in the Netherlands launched a self-regulatory "treaty" to fight malware and both Germany and Australia were trialling voluntary co-regulatory schemes to see if the ISP industry would offer assistance to end users by notifying customers of suspicious activity originating from their computers and providing information on preventive and remedial action on a voluntary basis.[79] Either ISPs or government-funded centres monitor Internet traffic and identify infected computers.

Australia

Through the Australian Internet Industry Association, Australia worked with ISPs to develop a non-regulatory, voluntary code of practice for industry self-regulation in the area of cyber-security; the "esecurity code". [80] The code of practice provides ISPs an industry benchmark for best practice to service customers if their computers become compromised by malware.[81] It supports the Australian Internet Security Initiative (AISI) launched by the Australian Communications and Media Authority (ACMA) in 2005 to help address the emerging problem of compromised computers.[82] The AISI collects data from various sources on computers with bot behaviour on the Australian Internet and the ACMA provides daily reports to ISPs on IP addresses on their networks that have been reported in the previous 24-hour period. ISPs can then inform their customers that their computer appears to be compromised and provide advice on how to fix it.

The programme's first pilot was launched in November 2005 with six ISPs. The pilot was assessed in 2006 and found to be of merit. In 2009, 2.7 million reports were being provided annually by the AISI to participating ISPs. As of May 2010, 76 ISPs, as well as hundreds of virtual ISPs, participated in the programme.[83] Participating ISPs covered an estimated 90% of Australian residential Internet users.

The Australian ISP service esecurity code of practice is designed to generate consistency in cyber-security messages and remedial practices between ISPs and their customers. The four elements of the code

are: *i)* a notification management system for compromised computers; *ii)* a standardised information resource for end users; *iii)* a comprehensive resource for ISPs to access the latest threat information; and *iv)* a reporting mechanism in cases of extreme threat back to a computer emergency response team (CERT).

Under this framework ISPs do not bear any cost of monitoring traffic, perhaps to take into account the fragmentation of the Australian ISP market in which more than 80 providers of various sizes compete. In addition, the framework protects the trust relationship between ISPs and their customers since the identity of the customers behind IP addresses reported by AISI as compromised is not provided to any third party. In contrast to the Japanese CCC which provides help to end users, the Australian ISPs' customers are responsible for, and bear the cost of, removing malware from their computers. However, detecting and cleaning compromised computers is not always straightforward. Much malware is installed on computers furnished with up-to-date anti-virus programmes, and once malware is installed, anti-virus programmes have limited ability to detect and remove it. Professional expertise may be required and can be costly and time-consuming.

The Netherlands

In 2009 Netherlands ISPs launched a joint effort to fight malware-infected computers and botnets. This effort involves 14 ISPs representing 98% of the consumer market and includes: *i)* the exchange of relevant information among co-operating ISPs; *ii)* the quarantine of infected computers to ensure that they no longer participate in criminal activity or infect others; and *iii)* the notification of end users by their ISPs so they can take action (Evron, 2009). End users bear the cost of cleaning their computers.

United Kingdom

In 2010, the Office of Cyber Security and Information Assurance (OCSIA), BIA and the Cyber Security Operations Centre (CSOC) were in the preliminary stages of developing a proposal with industry on a draft code of conduct for ISPs to combat botnets. The proposal is loosely modelled on the Australian initiative. ISPs would educate consumers on the need to protect their PCs with appropriate software, inform them if their machines are detected as having been compromised and provide some guidance to consumers as to how to clean their machines.

United States

In September 2010, the United States' Federal Communications Commission also issued a notice of inquiry seeking public comment on a Cybersecurity Roadmap examining best practices for ISPs to respond to infected computers.[84] The Department of Commerce has also issued a Notice of Inquiry, which seeks comment on a wide range of issues concerning incentives, including ISPs' incentives, to improve cyber-security.[85] The Computer Security, Reliability and Interoperability Council (CSRIC) of the Federal Communications Commission has organised a working group to focus on ISP Network Protection Practices, to discuss best practices for ISPs to consider in responding to compromised computers.[86] In December 2010, the Council issued a series of best practices, Internet Service Provider (ISP) Network Protection Practices, to address the botnet problem.[87]

Lessons learned

- Improving security is a common goal of stakeholders although those who are in a position to fix security problems (namely, end users) may not have an incentive to do so as they may not directly suffer the consequences or may not have the expertise to remedy the problems without significant external assistance.

- The trend seems to be for ISPs to provide more security to their customers. ISPs can help improve cyber-security and are being called upon to do so by the Internet community and governments.
- Countries such as Japan have had positive results which the Netherlands, Germany and Australia are also trying to achieve by establishing public-private partnerships. Although the practical details vary, these partnerships involve voluntary industry codes of conduct with standard processes for ISPs to notify and communicate with subscribers whose computers are suspected of being infected by malware.
- A variety of barriers exist, particularly regarding costs and who should pay. More information is needed on customers', ISPs' and governments' willingness to pay for security, as well as on the benefits of greater security to each of these groups to motivate faster and more widespread ISP security provision.
- Frameworks involving Internet intermediaries in improving cyber-security should take into account market realities so as not to disrupt competition (for example, they should not impose proportionally higher costs on small ISPs).
- Security systems/frameworks should be technically or organisationally designed so as to protect privacy, as part of the design of the framework. Privacy should be built in to minimise the additional security risks which involving Internet intermediaries in improving cyber-security could potentially generate, through the development of surveillance systems that could potentially invite abuse. It is essential to preserve the trust relationship between ISPs and their customers and between citizens and the government.
- Successful models seem to involve a government role as a convener or in funding some of the costs (set-up and/or running costs) of cyber-security programmes. Frameworks involving Internet intermediaries in improving cyber-security should be developed through multi-stakeholder partnerships. Involving governments, industry and civil society in policies to improve security is a good way to address issues of privacy and other fundamental rights as well as competition concerns.

REFERENCES

Edwards, L. and I. Brown (2008), *Macafee Virtual Criminology Report 2008*, *passim,* www.mcafee.com/us/research/ criminology _report/virtual_ criminology _report/index.html.

ENISA (2008), *Security, Economics, and the Internal Market*, March, www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.

Evron, G. (2009), Dutch ISPs Sign Anti-Botnet Treaty, www.darkreading.com/blog/archives/2009/09/dutch_isps_sign.html

Michel, J., G. van Eeten and J.M. Bauer, "Economics of Malware: Security Decisions, Incentives and Externalities", *STI Working Paper 2008/1*, www.oecd.org/dataoecd/53/17/40722462.pdf,

Moore, T., R. Clayton and R. Anderson (2009), "The Economics of Online Crime", *Journal of Economic Perspectives* 23(3), pp. 3-20.

OECD (2008), *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, at www.oecd.org/document/16/0,3343,en_2649_34223_42276816_1_1_1_1,00.html.

OECD (2008), Economics of Malware: Addressing the Security Externalities of End-Users, OECD Science, Technology and Industry Working Papers 2008/1, OECD Publishing, at www.oecd.org/dataoecd/53/17/40722462.pdf.

Rowe, B., D. Reeves and M. Gallaher (2009), "The Role of Internet Service Providers in Cyber Security", Institute for Homeland Security Solutions, June.

US GAO (2007), "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats", United States Government Accountability Office, www.gao.gov/new.items/d07705.pdf

ILLEGAL CONTENT AND CHILD-INAPPROPRIATE CONTENT

Introduction

The OECD has constructed a typology of the risks to children as Internet users, breaking them down into: *i)* risks that affect children as Internet users, *i.e*. where the Internet is the medium through which the child is exposed to content or where an interaction takes place; *ii)* consumer-related risks to children online, *i.e.* where the child is targeted as a consumer online; and *iii)* information privacy and security risks, *i.e.* online risks every Internet user faces but children form a particularly vulnerable user group (OECD, forthcoming). Within the category of risks to children as users, there is a further distinction between content risk and contact risk, the latter relating for example to improper interactions between adults and children (*e.g.* cybergrooming), online harassment or cyberbullying. This case study describes efforts by Internet intermediaries to control two types of content risks: graphic images of child sexual abuse and age-inappropriate content in virtual worlds.

Child sexual abuse material

Internet intermediaries generally take steps to protect children against the distribution of child sexual abuse material. These protective measures vary depending on the type of intermediary activity. Some are voluntary practices based on individual firm policies, some are pursued in voluntary co-ordination with other industry players and with law enforcement authorities, and yet others are required by law. Under voluntary policies, the following actors adopt some of the following measures:

- Internet service providers in some countries block websites and newsgroups containing child sexual abuse content.
- Web-hosting providers routinely have policies that forbid uploading child sexual abuse content. Blogger, for example, states that it will terminate the accounts of any user publishing or distributing child pornography.[88]
- Search engines often remove child sexual abuse content sites from the results of search queries and do not accept sponsored ads for child sexual abuse content (*e.g.* Google).[89]
- E-commerce intermediaries usually do not allow child sexual abuse content on their platforms (*e.g.* eBay).[90]
- E-commerce payment systems, in particular large players and international card brands (*e.g.* Visa, MasterCard, American Express or PayPal), do not allow their cards to be used for transactions related to child sexual abuse content.[91]
- Participative networking platforms also prohibit child sexual abuse content**.** Video-hosting sites such as YouTube forbid uploading of child sexual abuse content or other sexually explicit material.[92] Virtual worlds such as Second Life ban any depiction of sexual acts involving or appearing to involve children.[93]

Individual and co-operative efforts

Co-operative efforts to control child abuse material have developed over the last several years. These efforts usually involve industry groups, law enforcement agencies, as well as organisations that compile lists of child sexual abuse sites. One effort, by the financial services industry, attempts to disrupt the payment mechanism for the commercial distribution of child sexual abuse material. Another is the filtering of their systems by Internet service providers, hosts and search engines to remove child sexual abuse material.

Payment card networks work closely with law enforcement to detect and expel any merchants involved in child pornography on their networks. They also actively screen merchants and monitor their systems for this illegal activity without legal compulsion to do so and without waiting for complaints from law enforcement or other parties. They also use external firms to search the Internet for child pornography websites that appear to be accepting their payment cards. When detected, child pornography merchants are expelled from the payment systems.[94]

Such individual efforts against child pornography have been supplemented by collective action. In March 2006, at the request of several legislators, payment systems and financial institutions in the United States, along with the National Center for Missing and Exploited Children (NCMEC), formed the Financial Coalition against Child Pornography (FCACP). The group shares information and takes collective action against child pornography merchants identified by complaints to the NCMEC hotline or resulting from Internet searches. This effort has achieved some positive results in curtailing the activities of child pornographers; it has also led to a shift away from recognised payment brands and towards less traditional payment mechanisms.[95]

Some have argued that such websites have become more difficult to detect and are using payment systems which are more difficult to track; however, at the end of 2009, FCACP reported the following indications of success:[96]

- A 50% drop in the number of unique websites with commercial child sexual abuse content reported to the US CyberTipline, a hotline operated by NCMEC.
- A trend on these websites towards directing buyers away from traditional payment tools and methods, such as credit cards, and towards multi-layered, alternative payment schemes.
- Some sites containing commercial child sexual abuse content stated they could not accept credit cards from the United States.
- There has been a significant increase in the price of child sexual abuse content. When the FCACP was launched in 2006, common subscription prices were USD 29.95 a month. By end of 2009, price points had increased dramatically and it was not unusual to find sites costing up to USD 1 200 a month, and rare to find sites for much less than USD 100 a month

Similar co-operative efforts are under way in Europe. The European Financial Coalition against Commercial Sexual Exploitation of Children Online was formed in March 2009. The coalition is led by the Child Exploitation and Online Protection (CEOP) Centre, a non-governmental organisation for protecting children from sexual exploitation. Funded by the European Commission and based in the United Kingdom, it targets the funding mechanisms of commercially distributed images of child sexual abuse. A key role of the coalition is to identify the payment mechanisms used, to identify how to improve co-operation between law enforcement and payment processors, and to identify best practice for payment processors.[97]

Since 1996, the Internet Watch Foundation (IWF) has operated a notice and take-down programme with hosting companies based in the United Kingdom, under which child sexual abuse content is removed following a notice from IWF to the hosting provider. As a result, the proportion of child sexual abuse content hosted in the United Kingdom and known to the IWF has dropped from 18% in 1997 to less than 1% since 2003 (IWF, 2010). A voluntary notice and take-down system is also effective in the Netherlands, where ISPs and hosts receive complaints from the public and concerned organisations and take down material, including child sexual abuse content, after review.[98]

In 2004, British Telecom (BT) and the IWF formed a partnership under which the IWF provides a list of websites of child abuse material to BT so it can block its subscribers' access to the reported sites. The partnership proved successful and, with some government encouragement, spread to most ISPs in the

United Kingdom. IWF now provides an updated list of URLs containing child sexual abuse images twice a day to Internet service providers, mobile operators, search providers, filtering companies, national and international law enforcement agencies, and a group of international hotlines (INHOPE) (IWF, 2010, p. 10). The model was soon followed in Canada, Denmark, Finland, Germany, the Netherlands, Norway, Sweden and Switzerland.

The filtering of websites based on blocklists has improved over time. Some filtering products are almost 100% successful in blocking the targeted material and have with low over-blocking rates; network disruption can be kept to a minimum.[99] Nevertheless, there are limitations. Technologies to circumvent network-level filtering are available, so that people who seek to access material on prohibited URLs can find ways to do so. Moreover, network-level URL blocking is not effective against non-web modes of distribution such as instant messaging and peer-to-peer systems. For this reason, network-level filtering is a way to reduce the prevalence of, but not to eliminate, child sexual abuse material and is most effective against inadvertent access to such material.

Some countries do not require intermediaries to take specific action against child sexual abuse material. For example, in the United States, a 2004 court decision overturned a Pennsylvania law requiring ISPs to block child access to pornography sites.[100] The court ruled that mandatory filtering is not consistent with first amendment guarantees of free expression. On a voluntary basis, however, many ISPs in the United States have signed agreements with state attorneys general to take action against child sexual abuse material. For instance, the New York State Attorney General reached an agreement with most major ISPs to block access to newsgroups that host child sexual abuse content and to purge their servers of websites identified by NCMEC as child sexual abuse content.[101]

Legal regimes

Legal regimes to help control child sexual abuse content build upon the voluntary measures adopted by individual firms and industry groups. They almost always outlaw the production and distribution of child sexual abuse material. Some jurisdictions impose legal obligations on intermediaries to control child pornography. Italy, Korea, New Zealand and Turkey require mandatory network-based filtering by ISPs. Turkey's *Law on the Internet No. 5651* (2007) allows the Telecommunications Communication Presidency (TIB) to request ISPs to take down certain categories of online content, including content involving child sexual abuse. In the case of content deemed obscene or to exploit children sexually, the law empowers the state-run Telecommunications Board to prevent access to the website without recourse to a court decision; for most other offences, a court ruling is required (Deibert *et al*., 2010, pp. 347-351; OSCE, 2009; O'Byrne, 2009).

Concerns are often raised about the process of deciding which sites are to be included on blocklists, whether maintained by private-sector bodies or by law enforcement agencies. The lists themselves are kept secret so that the public does not know how to access the material. There is also the issue of additional material being added to these lists without public accountability. Legislation such as the 2010 German law calling for ISP blocking of child sexual abuse sites continues to give government law enforcement agencies a role in selecting the sites to be blocked (DW-World.de, 2010).

Under the 2009 Interpol Resolution, "Combating sexual exploitation of children on the Internet using all available technical solutions, including access-blocking by INTERPOL member countries", a worldwide list of URLs of websites that publish child abuse material of "severe nature" is maintained and disseminated. Technical assistance in tackling such sites is provided.[102] In March 2010, the European Commission proposed a directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse content. Article 21 of the proposed directive called for filtering the Internet for child

sexual abuse content and removing the content when located.[103] If approved, this EC directive would establish mandatory Internet filtering for child sexual abuse content in Europe.

Australia is also moving towards mandatory Internet filtering of material rated "refused classification" (RC), which includes child sexual abuse material. Currently, such material is available to Australian Internet users only through websites or hosting services located outside Australia. It is proposed to compile a list of RC content to be blocked based on a review of complaints from the public to the Australian Communications and Media Authority (ACMA) as well as a review of international lists of overseas-hosted child sexual abuse material compiled by reputable overseas organisations.[104] A pilot test was conducted to assess the proposed ISP filtering programme, using the existing ACMA blacklist. The test concluded that "ISPs can effectively filter a list of URLs such as the ACMA blacklist with a very high degree of accuracy and a negligible impact on Internet speed".[105]

To ensure transparency and accountability in the selection of sites for the RC list, the government proposed certain measures.[106] These include requiring that all material on the list be referred to the Australian classification board, notifying the affected offshore web hosts, displaying a blocking notification to Internet users who try to access a site, reviewing content from international lists, and having procedures reviewed by independent experts and by industry groups.

In July 2010, the mandatory RC filtering programme was delayed, pending a review of the RC system. Pending the review, three major Australian ISPs, which together account for 70% of Australian Internet users, agreed to block voluntarily a list of child abuse URLs compiled by ACMA.[107] The Australian government confirmed that the programme would include transparency and accountability safeguards.

Dynamic filtering though "deep packet" inspection techniques that read more than just the header information which contains routing directions (DPI) is also under consideration, but no reasonably accurate dynamic filtering system is feasible at this time.[108] With dynamic filtering, ISPs would compare computer files – movies, photographs, documents – with lists of prohibited child sexual abuse images to block prohibited content. However, such a system suffers from a trade-off between accuracy and the time and computational power needed to identify a transmission as prohibited content. The techniques involved also raise privacy and free expression issues.

Age-restricted content in virtual worlds

Many Internet intermediaries have voluntary policies to restrict access by minors to adult-oriented content or activities: *i)* ISPs provide user-level filters which parents can use to block content that is inappropriate for children; *ii)* web-hosting providers generally have terms of service that deal with access to adult content and restrict access for minors; *iii)* e-commerce intermediaries often require members to provide credit card information or alternative verification before they can view adult-only listings;[109] i*v)* e-commerce payment systems, in particular payment card networks, state in their rules that Internet merchants may not use their cards to provide adult-only material to minors; and *v)* participative networking platforms such as video-hosting sites or virtual worlds restrict some content that would be inappropriate for younger viewers.[110]

In December 2009, the US Federal Trade Commission (FTC) presented a report to the Congress on explicit content in virtual worlds. The Commission's study found some form of explicit content on 70% (19 out of 27) of the virtual worlds reviewed. One sexually explicit site aimed at adults was restricted to those over 18 years old, but analysis of its traffic indicated that 18% of its users were under 18.

The sexual or violent content found in online virtual worlds is usually not provided by the site operator, but is user-generated content chosen by and implemented by users. The site operator provides the tools, including the ability to customise the appearance of an online persona (avatar), but does not create the content. However, site operators often voluntarily try to protect children in online virtual worlds by trying to ensure that explicit material is not available to children. No US industry codes of conduct or best practices currently exist. The FTC (2009), given the important first amendment concerns in this area, has urged operators of virtual worlds to take a number of self-regulatory steps to keep explicit content away from children and teenagers by:

- using more effective age-screening mechanisms to prevent children from registering in adult virtual worlds;
- using or enhancing age-segregation techniques to make sure that people interact only with others in their age group;
- re-examining language filters to ensure that they detect and eliminate messages that violate rules of behaviour in virtual worlds;
- providing more guidance to community enforcers in virtual worlds so they are better able to review and rate virtual world content, report potential underage users, and report users who appear to be violating rules of behaviour;
- employing specially trained moderators equipped to take swift action against rule violations.

Some participative networking sites and hosting providers verify age by credit card. However, it is easy to use a parent's or relative's card or one of the new forms of pre-paid credit cards to circumvent this. Payment networks therefore require merchants selling age-restricted products such as alcohol or tobacco to take specific measures, including the use of age-verification technologies, to restrict the sales of these products.

There is an important distinction between age verification services designed to determine that a person is an adult and one designed to determine that a person is a minor. Adult age verification services rely on public databases, government sources and commercial information to determine that a person is an adult. They are more reliable than those designed to determine that a person is a minor, as there is little available public record information on children (FTC, 2008). Consequently, age verification services are considered more useful for keeping minors out of adult-only sites than for creating "walled gardens" for children only.[111] Moreover, many believe that it is not economically feasible to authenticate users on websites that do not sell a product or charge for the use of their services. Authentication may however be a feature of some government services for which users have a national ID or similar identifier.

Legal requirements for age verification vary and are not the norm everywhere. France, Germany and the United Kingdom appear to have legal requirements requiring providers of specific online services and ISPs (in France) to verify users' age. Germany requires the use of age verification technologies by providers of adult content and prescribes a state pre-approval mechanism for age verification technologies and providers (European Commission, 2008).

Lessons learned

- Most Internet intermediaries have terms of service that prohibit the use of their systems for child sexual abuse content. In addition, some use age verification procedures to try to limit access to adult-only material.

- The industry has co-operated with law enforcement and private-sector organisations to prevent sites with child sexual abuse content from being able to use standard payment means and to prevent access to child sexual abuse content sites through voluntary efforts.
- Filtering for child sexual abuse content has become more prevalent, with blocklists provided both by private organisations and by government agencies.
- Technical studies on the effectiveness and costs of filtering technologies, including dynamic filtering and filtering for non-web-based distribution channels, are important to help inform industry actions and policy decision.
- Where in use, mandated filtering should provide for due process, accountability and transparency.
- Age verification and identity verification services are considered more effective for preventing minors from accessing adult-only content than for keeping child-safe venues free of adults. Further technical development and assessment is important.
- Co-operation on cross-border enforcement to detect and close down child sexual abuse content sites is important. While local jurisdictions can take action against child sexual abuse content hosted in their jurisdictions, they have limited ability to control websites elsewhere. This shows the need for information exchange between law enforcement authorities.

REFERENCES

ACMA (2008), "Closed Environment Testing of ISP Level Internet Content Filtering", Report to the Minister for Broadband, Communications and the Digital Economy, June www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf.

Deibert, R., J. Palfrey, R. Rohozinski and J. Zittrain (2010), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press, Cambridge, MA.

DW-World.de (2010), "German child pornography law hits snags", 23 February, www.dw-world.de/dw/article/0,,5278471,00.html.

European Commission (2008), "Background Report on Cross Media Rating and Classification and Age Verification Solutions", http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/reportageverification.pdf.

Federal Trade Commission (2008), *Self-Regulation in the Alcohol Industry*, Report of the Federal Trade Commission, June, www.ftc.gov/os/2008/06/080626alcoholreport.pdf n.104.

Federal Trade Commission (2009), *Virtual Worlds and Kids: Mapping the Risks,* December, www.ftc.gov/opa/2009/12/virtualworlds.shtm.

IWF (2010), *Annual Report*, May 2010, www.iwf.org.uk/documents/20100511_iwf_2009_annual_and_charity_report.pdf.

O'Byrne, D. (2009), "Turkey to Face European Court over YouTube Ban", *Financial Times*, 30 November www.ft.com/cms/s/0/5333cbbc-ddc9-11de-b8e2-00144feabdc0.html?SID=google.

OECD (forthcoming), Protecting Children Online: Risks Faced by Children Online and Policies to Protect Them, OECD, Paris.

OSCE (2009), "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship", December, www.osce.org/documents/rfm/2010/01/42294_en.pdf.

ILLEGAL INTERNET GAMBLING

Introduction

Local laws regulating gambling may be circumvented by individuals using the Internet to gamble on websites in other jurisdictions. Intermediaries may be the logical source of response to this challenge. Individual gamblers are numerous and diffuse, and controls necessarily raise privacy concerns. Gambling merchants in other jurisdictions are beyond the practical reach of local law enforcement. However, intermediaries such as Internet service providers (ISPs) and payment systems are needed to complete an Internet gambling transaction, and they have international reach and local operations that are under local control. This case study focuses on the policy issues surrounding the use of intermediaries to control illegal Internet gambling in Australia, the United States, Norway, France, the United Kingdom and the European Union. It also describes how one virtual world operator dealt with the issue of gambling on its platform.

Australia

In 2001 Australia passed legislation prohibiting the provision of interactive gambling services to customers in Australia.[112] The law focused on Internet gambling merchants rather than individual gamblers. It applied to games of chance, or games of mixed chance and skill, including roulette, poker and blackjack, but not to online wagering on sporting events or to online lotteries. The legislation was reinforced by a complaint system which allowed local police officials to investigate allegedly illegal local gambling sites. It also allowed local regulators to place offshore sites found to be hosting Internet gambling services on a blacklist maintained by filter vendors (Australian Department of Families Housing Children and Indigenous Affairs, 2009, Chapter 3). The law was supported by a co-regulatory industry code for Australian ISPs which commits them to provide subscribers with commercial filtering software that can be used to prevent access to the blacklisted offshore Internet gambling sites (Internet Industry Association, 2001).

The law also authorised the government to use financial institutions to enforce the ban so that an agreement to pay for the supply of a prohibited Internet gambling service would have no effect. However, the government did not choose to impose such a regulation, arguing that "Australian card-issuing institutions would probably respond to the introduction of such regulations by blocking the use of their cards for all gambling-related transactions, including wagering and lottery services permitted under the IGA" and that "the size of the population participating may be too small to justify major changes in regulation" (Australian Department of Families Housing Children and Indigenous Affairs, 2009, Section 3.4).

A government review of the effectiveness of the law in 2009 concluded that: "While prohibition of Internet gambling services appears to have been effective in blocking the development of Australian-based Internet gambling websites which would offer services directly to Australians, there are weaker controls on accessibility of overseas-based websites for Australians." (Australian Department of Families Housing Children and Indigenous Affairs, 2009, Section 3.4) The review called for further research to assess Australians' participation in international Internet gaming sites, since the prohibition made it difficult to measure access to these sites (Australian Department of Families Housing Children and Indigenous Affairs, 2009, Chapter 7). It concluded that the effectiveness of offshore restrictions depended in part on the success of Internet gambling regimes in other jurisdictions, including the United States and the United Kingdom (Australian Department of Families Housing Children and Indigenous Affairs, 2009, Chapter 5).

The US Unlawful Internet Gambling Enforcement Act

The US Congress began to consider how to react to illegal Internet gambling in the late 1990s (GAO. 2002). One early proposal would have placed an enforcement burden on ISPs by requiring them to stop providing services to domestic Internet gambling merchants and to block foreign Internet gambling merchants at the request of law enforcement.[113] This proposal did not pass, in part because of concerns about the effectiveness and appropriateness of placing an enforcement burden on ISPs.[114]

The *Unlawful Internet Gambling Enforcement Act* (UIGEA) of 2006 focused instead on payment intermediaries.[115] Financial institutions were required to establish and maintain policies and procedures reasonably designed to prevent the use of their payment systems for illegal Internet gambling transactions. The traditional card payment networks developed a coding and blocking system which the law recognised as satisfying this requirement. Each gambling merchant in the payment system was required to identify itself using a four-digit "merchant category code" in each authorisation message. In addition, Internet merchants were required to use an electronic commerce indicator to identify themselves. The presence of this information in the authorisation message meant that a transaction involving an Internet gambling merchant could be identified and blocked in real time by the payment network that transmitted the authorisation message or the issuing bank that received it. The system was also able to accommodate conflicting laws in different jurisdictions.

UIGEA defines illegal Internet gambling as any gambling that is illegal under current US state or federal law. It does not resolve uncertainties regarding the illegality of certain Internet gambling activities. Financial intermediaries have the discretion to block or not to block these transactions based upon their own judgment and the strength of the legal arguments presented to them. UIGEA also provides them with protection from liability if they over-block Internet gambling sites that are actually legal. As part of an effort to balance the need for precision in blocking with concerns about legal liability, Visa and MasterCard appear to have developed a special code for betting involving horse racing and dog racing that would allow issuing banks to continue to process these transactions while blocking other transactions coded with the traditional 7995 code. The current law thereby places substantial discretion in the hands of the payment companies.

The costs associated with the programme are substantial. One-time costs of setting up the coding and blocking system have already been incurred by the payment networks, but ongoing enforcement costs remain. The implementing regulations require procedures for ongoing monitoring or testing by the card system operator to detect potential restricted transactions, including conducting testing to ascertain whether transaction authorisation requests are coded correctly; and monitoring and analysing payment patterns to detect suspicious payment volumes from a merchant customer.

The law has been controversial at international level. While the United States has long considered Internet gambling illegal, the WTO ruled in 2005 against the United States in a complaint by Antigua alleging that US law contravened US trade commitments.[116] The European Commission arrived at a similar conclusion in 2009 (European Commission, 2009). These cases were based on a disagreement over what the United States had committed to in the General Agreement on Trade in Services. In deciding whether Antigua was denied the trade benefits granted to them through the WTO agreements, consideration of the underlying legal regime for Internet gambling in the United States was critical, but harm to Antiguan Internet gambling merchants due to the payment system enforcement mechanism embodied in UIGEA was also an important element.

UIGEA has led to the withdrawal of foreign companies from the US market, loss of share value for Internet gambling companies, and a decline of Internet gambling in the United States. The effect of the

simultaneous increase in enforcement by the US Department of Justice cannot be discounted. Still, the independent effect of the passage of UIGEA is clear.

A large percentage of non-US companies that derived extensive revenues from their operations in the United States left the market after the passage of UIGEA (Morse, 2007, p. 447). These included all of the European companies that had been active in the US market (European Commission, 2009, p. 59). Immediately after the law was passed, 25% of all Internet gambling merchants stopped accepting bets from US customers. By mid-2007, the figure had risen to 50% (Williams and Wood, 2007, p. 10). By December 2008, all publicly trade online gambling firms had left the US market, although most of the private firms remained (Casino City, 2009).

Three major European online gambling merchants lost USD 3 billion in 2006 from their withdrawal from the US market (European Commission, 2009, p. 79).Measured traffic at particular sites declined as well. In September 2006, Party Poker, for example, which derived much of its traffic from the United States, had an average of about 12 000 active players. By November 2006, that number had dropped to about 4 000.[117] Moreover, shortly after UIGEA was signed into law in October 2006, analysts estimated that the value of British Internet gambling stocks had declined by USD 7.6 billion (Pfanner and Timmons, 2006).[118] The share value of PartyGaming fell 57%, shares of Sportingbet lost 60%, 888 was down 33% and bwin.com fell 24%.[119] In the nine months between 1 January and 1 November 2006, just after the passage of UIGEA, three major European online gambling firms lost an estimated 75% of their value, or approximately EUR 8.3 billion (European Commission, 2009, p. 83).

According to a European Commission estimate of the likely evolution of the US market in the absence of the specific restrictions imposed in 2006, based on an assumption of 3% yearly growth, US Internet gambling would rise from about USD 5.8 billion a year in gross revenue in 2006 to almost USD 14.5 billion in 2012. Following the passage of UIGEA, annual revenue dropped to about USD 4 billion in 2006 and was estimated to be worth only USD 4.6 billion by 2012 European Commission, 2009, p. 19).

A different way to estimate the effect of UIGEA is to look at the size of the US market under a licensing regime. H2 Gambling Capital, a consulting firm, estimated that a legalised US gambling market would have reached USD 13.4 billion by its fifth year.[120] This is substantially larger than the USD 4-5 billion estimated by the European Commission and roughly comparable to the trend it projected before the passage of UIGEA.

Alternative ways to require payment intermediaries to respond to Internet gambling are under consideration in the US Congress. H.R. 2267 would create a regulatory and licensing regime for all varieties of Internet gambling. Payment intermediaries would have to block transactions from unlicensed Internet gambling merchants and would be allowed to process transactions on behalf of licensed Internet gambling merchants. The lack of clarity about which merchants and transactions are legal would be resolved through the licensing process. The system would rely on a list of approved gambling entities which payment networks could check to determine whether to approve gambling transactions from particular Internet merchants.[121]

Developments in Norway

On 19 February 2010 the Norwegian government enacted a payment processing ban for online gambling. The Payment Act is similar to UIGEA in that it holds banks and financial institutions responsible for stopping illegal Internet gambling transactions between its citizens and illegal Internet gambling merchants. It defines illegal gambling sites as those that do not have a Norwegian gambling licence and is similar in that respect to the alternative Internet gambling law now under consideration in the

United States.[122] A financial institution processing a transaction from an unlicensed Internet gambling site would be guilty of "accessory involvement" in illegal Internet gambling. The law took effect on 1 June 2010 and has been controversial. The European Free Trade Association Surveillance Body warned that such legislation would "constitute an unjustified restriction of the freedoms of the internal market for gambling services".[123]

Developments in France

On 6 April 2010 France adopted a law that would open its market to online gambling. The law set up an administrative agency, ARJEL (Autorité de régulation des jeux en ligne), to issue licences and to publish a list of licensed Internet gambling merchants. The law calls for taxing Internet gambling services at rates of 7.5% on online sports and horseracing wagers and 2% on online poker wagers. An objective was to be able to continue to collect about EUR 5 billion a year in taxes from the gambling industry. The decision followed a communication from the European Commission calling for an opening of the closed French market.[124] The law contains no provisions for enforcement by intermediaries, although an amendment was considered that would have authorised ARJEL to issue blacklists of illegal online gambling sites for filtering by ISPs.

Developments in the United Kingdom

In the United Kingdom, the Gambling Act of 2005 took effect in September 2007.[125] It provided for the licensing of Internet gambling activities, both sports betting and casino-style gambling, by the UK Gambling Commission. It also made it an offense for licensed online gambling operators to enable citizens of jurisdictions in which gambling is forbidden to participate in online gambling. It permitted offshore online gambling merchants to offer services to British citizens if they complied with the licensing requirements of their host countries. It also provided for advertising by approved licensees. In August 2007, the Department of Culture, Media and Sport (DCMS) released a "white list" of Internet gambling merchants allowed to advertise their services.

Despite the complex legal structure of domestic licensing and the approval of offshore gambling operations licensed by their host countries, enforcement in the United Kingdom is entirely in the hands of government agencies. No intermediary enforcement mechanisms are provided for in the law.

In 2006, the British culture minister, noting that the industry "has been very hard hit by the U.S. ban" and that the Internet is a "global marketplace", urged "action at the global level" (Pfanner and Timmons, 2006). Britain was seeking to develop a consensus on a global standard to legalise and regulate Internet gambling. The US UIGEA went in the opposite direction by taking unilateral action to use Internet intermediaries to prevent illegal Internet gambling.

European Union

The European Commission is in the process of preparing a "green paper" on illegal Internet gambling (EuroActiv, 2010). Enforcement mechanisms under discussion include the use of payment systems to block unlicensed online gambling merchants and the use of white lists of legal sites and blacklists of unlicensed sites.[126] A resolution of Parliament in March 2009 addressed the jurisdictional issues raised by Internet gambling, noting that "online gambling operators must comply with the legislation of the Member State in which they provide their services and the consumer resides".[127] An intermediary tasked with an enforcement burden would be responsible for ensuring that an Internet gambling transaction is in compliance with both the law applicable to the merchant and the law applicable to the customer.

Virtual worlds

Although virtual worlds are not payment systems, they are Internet intermediaries linking participants through the shared use of their software platforms. One of them has become involved in the prohibitions on Internet gambling under US law and the payment processing obligations under UIGEA.

Second Life is a virtual world operated by Linden Labs, a company based in the United States. The operator provides a software platform for users, called residents, who are able to engage in a variety of activities that mimic real-world activities, from going to shopping centres to building homes. One activity made possible in Second Life was going to virtual casinos. Residents were able to exchange their local currency for Linden dollars and then use the virtual currency to gamble at in-world casinos or sports books. Any winnings could then be converted back to local currency. These activities by residents exposed the platform operator to legal liability both as a provider of Internet gambling services and as a payment processor under UIGEA (Dougherty, 2007).

In April 2007, it was reported that, at the request of Linden Labs, US authorities had been looking into gambling activities in Second Life (Pasnick, 2007). At around the same time Linden Labs announced that they would "not accept any classified ads, place listings, or event listings that appear to relate to simulated casino activity" (Linden, 2007a). Then, in July 2007, Linden Lab adopted a policy banning all gambling activities from Second Life.

The ban was comprehensive. It banned all games that "rely on chance or random number generation to determine a winner, OR (b) rely on the outcome of real-life organised sporting events, AND (2) provide a payout in (a) Linden Dollars, OR (b) any real-world currency or thing of value". The rationale was the need to comply with US law: "Second Life Residents must comply with state and federal laws applicable to regulated online gambling, even when both operators and players of the games reside outside of the U.S." Rather than ensure that residents were obeying their local laws, this decision ensured that Linden Labs was in full compliance with the laws applicable to an intermediary platform operator. They might have been able to interpret the laws of all the countries in which residents actually lived and authorise residents based in countries that permitted Internet gambling to continue to use in-world casinos, while banning US residents from doing so. It is not easy to see how they could have implemented such a targeted approach, and they clearly did not want to do so: "Because gambling activities may be controlled by the law where the bettor lives in some places, and in others affect the operators of wagering games, we have decided to take a broader approach by prohibiting all games that meet the criteria in our policy." (Linden, 2007b; see also Clayburn, 2007).

Lessons learned

- Intermediary enforcement need not be perfect to be effective. UIGEA has significantly diminished the potential size of the US gambling market.

- Intermediaries are often well placed to monitor their own systems for business activity of a certain type, but not for detecting the illegal nature of activity on their systems. The point arises in the context of Internet gambling because the codes used by financial institutions reflect the business activity of gambling, not its status as legal or illegal. The result is that the policies and procedures adopted by payment systems to comply with UIGEA can over-block, thereby preventing legal activity from taking place.

- Providing for intermediary enforcement of ambiguous laws creates significant problems for the intermediary and for other market participants affected by the legal ambiguity and the enforcement by the intermediary. The legal ambiguity in the United States concerning whether the law applied to

sports betting and horse racing created uncertainty in the merchant community and provided payment systems with substantial discretion to decide how to resolve these legal uncertainties. Clear licensing rules or prohibitions accompanied by white lists of licensed operators or blacklists of illegal sites can alleviate these difficulties.

- An intermediary liability system that works in the short term and for a few countries could be unworkable if many countries attempt to use it to enforce local law. If governments involve intermediaries in enforcing Internet gambling rules, they should co-operate internationally to try to harmonise these rules. A practical way forward in the case of Internet gambling might be an international agreement recognising licensing arrangements in different countries as long as they satisfy certain agreed minimum standards.

REFERENCES

Australian Department of Families Housing Children and Indigenous Affairs (2009), "Review of current and future trends in Interactive gambling activity and regulation", Chapter 3 in *Regulation of Interactive Gambling in Australia,* www.fahcsia.gov.au/sa/gamblingdrugs/pubs/review_trends/Documents/chap3.htm

Casino City (2009), Online Gambling in the United States Jurisdiction, http://online.casinocity.com/jurisdictions/united-states/

Chan, S. (2010), "Congress Rethinks its Ban on Internet Gambling", *The New York Times*, 29 July, www.nytimes.com/2010/07/29/us/politics/29gamble.html

Clayburn, T. (2007), "Second Life Gambling Ban Gets Mixed Reaction", *Information Week*, 27 July, www.informationweek.com/news/internet/showArticle.jhtml?articleID=201201441.

Dougherty, C. (2007), "Virtual Gambling: Betting on 'In-World' Events", *World Online Gambling Law Report*, Vol. 6, No. 11, November, http://ssrn.com/abstract=1092287.

E. Pfanner and H. Timmons (2006), "U.K. Seeks Global Rules for Online Gambling", *International Herald Tribune*, 2 November, www.nytimes.com/iht/2006/11/02/technology/IHT-02gamble.html.

EuroActiv (2010), "Barnier to seek coherent EU rules on gambling", 10 February, www.euractiv.com/en/sports/online-gambling-debate.

European Commission(2009), Examination Procedure Concerning an Obstacle to Trade, within the Meaning of Council Regulation (EC) No. 3286/94, Consisting of Measures Adopted by the United States of America Affecting Trade in Remote Gambling Services, 10 June 2009 (EU Gambling Report), http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143405.pdf.

General Accounting Office (2002), *Internet Gambling: An Overview of the Issues*, December, www.gao.gov/new.items/d0389.pdf.

Internet Industry Association (IIA) (2001), Internet Interactive Gambling Industry Code, www.acma.gov.au/webwr/aba/contentreg/codes/internet/documents/gamblingcode.pdf.

Linden, R. (2007a), "Advertising Policy Change", Blog Post, 7 April https://blogs.secondlife.com/community/features/blog/2007/04/06/advertising-policy-changes.

Linden, R. (200b7), "Wagering in Second Life: New Policy", Blog Post, 26 July, https://blogs.secondlife.com/community/features/blog/2007/07/26/wagering-in-second-life-new-policy.

Morse, E.A. (2007), "The Internet Gambling Conundrum: Extraterritorial Impacts of Domestic Regulation" in *Cyberlaw, Security and Privacy*, in S.M. Kierkegaard (ed.), International Association of IT Lawyers. Available at SSRN: http://ssrn.com/abstract=1192202

Pasnick, A. (2007), "FBI checks gambling in Second Life virtual world", Reuters, 3 April, www.majorwager.com/forums/mess-hall/147318-fbi-checks-gambling-second-life-virtual-world.html

Williams R.J. and R.T. Wood (2007), "Internet Gambling: A Comprehensive Review and Synthesis of the Literature", Report prepared for the Ontario Problem Gambling Research Centre, August, www.uleth.ca/dspace/bitstream/10133/432/1/2007-InternetReview-OPGRC.pdf.

COPYRIGHT INFRINGEMENT

Introduction

Copyright infringement on the Internet presents a sizeable challenge. The International Federation of the Phonographic Industry (IFPI) estimated that 95% of all music downloads in 2008 were unlicensed and that 40 billion files were unlawfully shared online in 2008 alone. It removed 3 million links to such files in 2008, up from 500 000 in 2007 (International Federation of the Phonographic Industry, 2009). In 2007, the OECD estimated that the consumption of pirated digital goods was widespread (OECD, 2007). A 2010 report by the US Government Accountability Office (GAO) did not make a quantitative estimate of the extent of the problem, but stated that it is "sizable" (General Accountability Office, 2010). To collect objective quantitative information on the size of illegal file sharing, the European Commission decided to establish a European Observatory on Counterfeiting and Piracy.[128]

Copyright owners can and do take action against direct infringers. But there are many direct infringers and litigation is costly and does not easily scale to address the extent of the issue. As a result, copyright owners use laws covering secondary liability to involve intermediaries in helping to control copyright infringement on the Internet, in particular by identifying users who post infringing materials or host sites on which infringement occurs. In the United States, for example, ISPs have revealed account holders' names to copyright holders to support their infringement procedures pursuant to private "John Doe" complaints (Anderson, 2010). The following is a discussion of voluntary agreements between Internet intermediaries and rights holders and indirect liability regimes for copyright infringement in selected countries. It examines arrangements that provide for intermediaries to take down infringing material after notice ("notice and take-down"), arrangements under which intermediaries pass on infringement notices to their users ("notice and notice"), and legal requirements or agreements for intermediaries to take increasingly strong deterrent measures against repeat infringers, possibly including suspension of service ("graduated response").

Some proposals related to filtering and site blocking are also reviewed. They call for Internet service providers (ISPs) to block access to specific websites that are alleged or have been determined to host infringing material, or to inspect Internet traffic for signs of infringing content and to block traffic containing suspected infringing material.

Notice and take-down

Many Internet actors, including hosts, search engines, online marketplaces and social networks, respond to complaints of copyright violation through notice and take0down procedures. Legal frameworks such as the European Union E-Commerce Directive (ECD) or the US *Digital Millennium Copyright Act* DMCA create a safe harbour from liability for copyright infringement for various Internet actors when they meet certain conditions. One of the common elements of these regimes is that intermediaries must respond when they receive notice of an alleged infringement from the rights holder or his or her representative, by expeditiously removing the alleged infringing content. Issues involved include:

- verification of information about allegedly infringing material;
- the form of the notification from an authorised sender, from a simple notification by a private party to an official notification by court order;
- cost and effectiveness in reducing copyright violations;
- regulatory framework for action;
- self-regulatory initiatives, *e.g.* codes of conduct, labelling, user controls or best practices;

- means of ensuring compliance with either regulatory or self-regulatory initiatives;
- relationship between the intermediary and the user (*e.g.* contractual relationship, terms of service, anonymous relationship);
- issues arising from data protection legislation;
- the intersection of copyright protection and free expression;
- safeguards to limit the risk of legitimate material being taken down and existence of "put-back" procedures;
- speed of the process and how this influences the effectiveness of the system;
- how to deal with repeated reappearance of infringing content which has been taken down.

United States

The US DMCA of 1998 provides a safe harbour from copyright liability for certain Internet intermediaries. Internet service providers that meet conditions relating to the automatic processing and distribution of third-party content, that do not interfere with technologies employed by copyright owners to protect their content, and that maintain appropriate policies with regard to the termination of accounts of repeat infringers are given a limitation on liability when they act as "mere conduits" by providing only transitory communications such as transmission, routing or connections. Other safe harbours are provided for caching of materials and information location tools such as links to third-party materials. Web hosts and search engines receive a separate safe harbour provided they comply with a specific notice and take-down procedure. If they become aware of infringement, or if they receive proper notification of claimed infringement, service providers must expeditiously take down or disable access to the material or lose the statutory safe harbour.[129]

The DMCA also allows recipients of notices to challenge them by way of a counter-notice procedure. Upon receipt of a counter-notice, service providers are required to reinstate the allegedly infringing material unless the rights holder has filed an infringement lawsuit. Service providers are exempt from liability for good faith removal of material following a notice. The DMCA also provides for penalties if a rights holder files a notification that knowingly misrepresents that the material is infringing (17 U.S.C. § 512). Finally, it requires service providers to have procedures to respond to "repeat infringers", including termination of accounts in appropriate circumstances [17 U.S.C. § 512 (i)]. Some intermediaries attempt to educate users of their platforms about the consequences of repeat infringement and warn them, "If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate."[130] Other intermediaries rely on courts to determine whether someone is a repeat infringer (Sandoval, 2009a). Universities are required to inform students that unauthorised distribution of copyrighted material is illegal, and provide a summary of legal penalties and university disciplinary actions for copyright violations.[131]

European Framework

The European framework for copyright liability under the ECD also provides for a notice and take-down procedure (Angelopoulos, 2009). Article 14, for example, applies to websites that host content and imposes a notice and take-down system by providing that the host is not liable for the information placed on its system by a user on condition that: *i)* the provider does not have actual knowledge of the activity or information and is not aware of facts or circumstances from which the illegal activity or information is apparent; or *ii)* the provider, on obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[132]

As is the case of the DMCA, this limitation of liability extends only to monetary damages. Injunctive relief is available and national states may establish procedures that require certain intermediaries to remove infringing material [Article 14(3)]. Annex 2 lists member countries' transposition of two relevant directives into national law.

Effectiveness and cost of notice and take-down

There is little public information on the number of take-down notices filed. IFPI estimates that the number of links to sites containing allegedly infringing content taken down was 3 million in 2008, up sharply from 500 000 in 2007.[133] The increase appears attributable to more widespread implementation of automated notification methods. The number of take-downs in response to these notices is not known, but some evidence suggests that service providers honour almost all complaints.[134] Additional issues for consideration include the timeliness of service providers' response, which varies, and measures by service providers to prevent infringing content that has been taken down from being re-uploaded by the same person. The number or percentage of counter-notices requesting put-back of allegedly infringing material is not known, although there are some high-profile examples. Because there are legal risks associated with knowingly filing wrongful notices or counter-notices and because the burden upon alleged infringers who file counter-notices is substantial,[135] it is likely that these notices and counter-notices will be filed only when the complainants are reasonably confident of their legal position and have some financial wherewithal.

Copyright owners lose revenue as a result of copyright infringement. Under notice and take-down regimes, copyright owners also bear the costs of monitoring for infringement, preparing the notice of infringement and transmitting it to the service provider. The costs associated with receiving the notice, taking down the allegedly infringing material and handling counter-notices are borne by the service providers. In addition, service providers could bear the subsequent loss of revenue resulting from these processes, or could pass the costs on to the consumer. Unlike the costs for notice and notice systems and for graduated response systems, neither the costs to copyright owners nor the costs to the service providers of complying with the notice and take-down requirements have been publicly estimated.

The application of the DMCA safe harbours has been the subject of significant litigation. For example, in 2007, Viacom sued YouTube for copyright violation, asserting that YouTube wilfully allowed infringing videos to be posted on its site and, by profiting from this infringement, had thereby lost its DMCA safe harbour. In June 2010, a district court agreed with YouTube's response that it did not knowingly allow infringing posts, and was protected by DMCA (Box 1).[136] Many service providers welcomed the decision, while rights holders have criticised it. The decision has been appealed.[137]

To deal with issues concerning commercial sites that earn revenue from user-generated content (UGC) which might include infringing material, a group of copyright owners and UGC-hosting services proposed a set of UGC principles in 2007. These principles encourage the use of technology to block content before posting, as well as measures to remove it after posting.[138] Many of the major UGC sites signing these principles adopted the use of these technologies. Today, all of the major UGC sites hosted in OECD countries use content-recognition technologies (OECD, 2009, p. 33). The principles also mention that such technologies should accommodate fair use. Around the same time, a group of non-governmental organisations released a set of principles for protecting fair use on UGC video-hosting sites. These principles include respect for legitimate transformative uses of copyrighted material, notification of users before take-down or serving ads on the copyrighted content, use of the DMCA protections of counter-notice, and reinstatement upon counter-notification (Electronic Frontier Foundation, 2007).

Many believe that a robust and appropriately managed notice and take-down mechanism is a workable and balanced approach to issues involving certain types of hosted sites (Deibert *et al*., 2010, p.

378; Zittrain, 2008, p. 119). However, this mechanism does not deal effectively with infringement through peer-to-peer systems or through cyber-lockers and websites in other jurisdictions. Moreover, notice and take-down regimes can result in over-blocking of non-infringing content. Within its area of effectiveness, however, a notice and take-down system provides copyright owners a mechanism to respond to infringement online without necessarily the need for costly court proceedings. For intermediaries it provides an after-the-fact mechanism to protect from copyright liability for infringements by their users. The advantage for the general public is continued and increasing access to a wide variety of non-infringing content. Expeditious notice and take-down is, and remains, an element of an effective strategy for dealing with online infringement, but policy makers, copyright holders and intermediaries are exploring further approaches to addressing the full range of online infringement.

Content ID

In 2007, after many of the major UGC sites hosted in OECD countries introduced content recognition technology, YouTube introduced an automated process to screen uploaded content for copyright infringement (Chen, 2007; Stone and Helft, 2007), In this programme, copyright owners provide audio or video files to YouTube and directions on what they want to happen if YouTube finds a match between content protected by copyright and content uploaded to the platform. If a match is found, the user is notified with a note next to the video saying that the video contains copyrighted material. This is not a formal complaint from the copyright owner under DMCA. The user can submit a response to the Content ID notification and YouTube will reinstate the material. In that case, the copyright owner is notified and can submit a formal DMCA complaint. YouTube has a programme allowing for termination of a user's account after a determination that he or she is a repeat offender.[139]

If user-uploaded material is found to match the material provided by a copyright holder, the copyright holder's preferences are applied. He or she has the option of blocking, tracking or monetising his/her content.[140] Content that the copyright owner wants deleted is removed from the site. Tracking the content means that YouTube will issue reports to the copyright owner about the number of views per video. Monetising the content means that YouTube will insert advertisements alongside the content and share the advertising revenue with the rights holder.

In 2008, about 300 content companies began to use these systems, including CBS, Universal Music, Lionsgate and Electronic Arts (Stelter, 2008). YouTube indicated in 2008 that 90% of the claims created by its Content ID system had been monetised (King, 2008). By August 2009, 9% of the videos on YouTube were accompanied by advertisements Learmonth, 2009). By autumn 2010, more than 1 000 entities were using Content ID, including every major US network broadcaster, movie studio and record label. There were 2 billion views a day on YouTube, up 50% from 2009, and there were 2 billion monetised views a week, a gain of 50% over 2009. Hundreds of YouTube partners earn at least USD 100 000 a year, and the number of partners making over USD 1 000 a month grew by 300% in the first nine months of 2010.[141]

Limitations of notice and take-down regimes

Notice and take-down regimes cannot be used to reach across borders to restrain web hosts in other jurisdictions. Nor are they effective for services such as cyber-lockers or linking services in which new infringing links or content can be put up as quickly as some are taken down, or for non-hosted content such as peer-to-peer (P2P) file transfers for which there is no content for an ISP to take down.

Notice and notice

Canada

Canada does not have a notice and take-down regime. However, since 2001 it has had a voluntary programme, called "notice and notice", under which copyright owners send a notice of an alleged violation to an ISP and the ISP forwards that information to its subscriber. All the major Canadian carriers, including Bell Canada, Telus and Rogers, participate in the programme.

Use of the programme is growing. In 2007, Telus claimed it was forwarding 4 000 notices a month (CBC News, 2007). The Business Software Alliance reportedly sent a total of 60 000 notices in 2006. In 2009, Bell Canada was receiving 15 000 complaints a month. Complaints early in the programme were largely from recording interests in the United States. In 2010 the complaints came mostly from movie studios and software companies.[142]

The effectiveness of the programme is difficult to measure. Some anecdotal reports suggest that the programme is working (CBC News, 2007). Copyright owners, however, claim that "no evidence that the voluntary 'notice and notice system' in which some Canadian ISPs participate has had any appreciable impact on online infringements" (International Intellectual Property Alliance, 2010).

A study by Industry Canada in 2006 estimated the cost of a single notification to be CAD 11.73 for larger Internet providers (more than 100 000 subscribers) and CAD 32.73 for smaller Internet providers. The overall cost to all ISPs for administering this programme would thus be tens of millions of Canadian dollars (Industry Canada, 2006). Copyright owners bear monitoring costs and administrative costs for sending notice requests to ISPs, although these are increasingly automated. For their part, ISPs bear the capital and operating costs associated with sending the notices to the alleged infringers.[143]

Proposed legislation in Canada to implement the WIPO Internet Treaties would codify the notice and notice system and would allow the government to set a maximum fee to be paid by copyright owners for using the system.[144]

The United States and the United Kingdom

In early 2009, many US ISPs began to participate in a voluntary notice and notice programme. They forwarded letters from content owners alleging infringement to their subscribers. Some added a cover letter of their own, noting that they reserved the right to terminate service. One ISP estimated that it had sent 2 million notices (Sandoval, 2009b). Verizon has indicated that 70% of the notices it processed were for customers receiving their first notice.[145] AT&T has developed an Automatic Customer Notification Service to forward notices of alleged copyright infringement and thinks the programme is "highly effective".[146]

In 2008 six UK ISPs joined a programme with copyright owners to forward notices to subscribers involved in unauthorised peer-to-peer file sharing (Eaglesham and Fenton, 2008). A 2008 study by Wiggin and Entertainment Media Research found that seven out of ten people surveyed said they would stop downloading unauthorised content if they received a notice from their ISP. A later survey suggests, however, that only 33% of UK consumers would stop piracy after a warning (Anderson, 2009a).

Graduated response

Graduated response procedures involve ISPs taking increasingly strong deterrent measures in response to alleged or adjudicated repeated copyright violations by their subscribers. The French HADOPI law, the regime in Korea, and the new Digital Economy Law 2010 in the United Kingdom are examples of this approach. An Irish ISP has agreed to a graduated response regime as part of the settlement of a

copyright infringement case.[147] New Zealand has introduced a draft graduated response law.[148] Japan is considering how to implement a graduated response mechanism to curtail illicit peer-to-peer file sharing that infringes copyright (Anderson, 2008; Intellectual Property Strategic Programme, 2009, p. 10). Implementation of this mechanism varies from country to country and only a few have so far adopted a graduated response mechanism.[149] Germany[150] and Spain (Llewellen, 2009) appear to have decided against a graduated response regime for the time being. Sometimes the approach is negotiated between particular ISPs and copyright holders. In some cases, these negotiations are overseen by governments. Plaintiffs in several jurisdictions have asked the courts to require a graduated response process through the interpretation of current statutes.[151]

The common procedure in graduated response mechanisms is a report by a copyright owner that a particular ISP's subscriber is violating copyright, followed by notification by the ISP to the subscriber of the complaint. After several such notifications, some regimes offer the possibility to suspend the subscriber's Internet access or otherwise deter future alleged infringement. Issues involved in these regimes include:

- the involvement of public authorities in determination of infringement;
- the proportionality and effectiveness of the suspension remedy compared with a regime that would require only notification of alleged infringement;
- the privacy rights of users and disclosure of personal data in the context of civil proceedings;
- the allocation of costs, *e.g.* who pays for the notifications and follow-up costs associated with the process;
- the level of proof required from rights holders, how illegal file sharers are identified and with what degree of certainty, and whether the volume of files shared is known;
- adjudication issues, for example the creation of a "rights agency", its independence and status *vis-à-vis* government, its role and its funding;
- adjudication processes, including due process and redress mechanisms, which allow affected users the opportunity to contest allegations, appeal sanctions, and have the ability to defend against graduated response claims;
- issues of scope, including to whom the suspension applies, the length of the suspension, the ability of the subscriber to regain access to service;
- respect of rights holders, the free flow of information, innovation and user rights;
- the use of notification to educate consumers about Internet security, such as the securing of WiFi routers;
- the benefits of such enforcement mechanisms for reducing online piracy.

United States

As noted above, under agreements negotiated with rights holders, some US ISPs will pass on infringement notices and some take additional steps involving services to alleged infringers, including the possibility of suspending services (McBride and Smith, 2008). There is little public information about the extent to which suspensions have occurred; some US ISPs may have suspended subscribers' Internet access for alleged copyright violations. AT&T maintains, however, that without a court order they do not cut off subscribers solely on the basis of multiple allegations of infringement. While they have legal authority to use account suspension as a means of enforcing their contractual terms and conditions with subscribers, they argue that it would be inappropriate for a private party to decide on such a procedure in

case of alleged copyright infringement, that it could create substantial liability for them, and that it appears to run counter to other government objectives of universal broadband access. They argue instead for an expedited process of civil infringement adjudication which would enable copyright holders and alleged infringers an opportunity to file charges and provide a defence.

Korea

In April 2009, Korea passed legislation providing for a graduated response to copyright infringement (Anderson, 2009b). The law would allow the Minister of Culture, Sports and Tourism to order an ISP to suspend the user account of an alleged infringer who has been warned at least three times about transmitting infringing content and to suspend websites that have been warned at least three times about hosting infringing content**.** The law also allowed the government's Copyright Commission to recommend that ISPs send notices to alleged infringers and to web hosts telling them to cease transmission or to delete infringing material. The rule took effect in July 2009. By the end of July 2010, no individual subscriber or web host had been suspended by order of the Ministry. However, ISPs had suspended the accounts of 31 subscribers for less than one month upon the recommendation of the Copyright Commission. The Copyright Commission had recommended that ISPs send warning notices to 32 878 subscribers, out of a total of broadband Internet subscribers of 15 million as of mid-2009, *i.e.* to about 0.1% of Internet subscribers.[152] They had recommended that the ISPs delete, or cease to transmit, infringing material in 32 209 cases. Compliance with these recommendations was virtually 100%.[153] Elements of a notice and notice system and a notice and take-down system were used. The remedy of suspension was used in a small number of cases.

European Union

The European Union has set out a framework for consideration of national graduated response laws. In November 2009, the European Parliament, in considering a package of reforms on telecommunications policy, addressed the issue of restrictions on Internet access as part of attempts to enforce copyright law. In a compromise measure, Parliament agreed that: "Restrictions on a user's internet access may 'only be imposed if they are appropriate, proportionate and necessary within a democratic society', agreed MEPs and Council representatives. Such measures may be taken only 'with due respect for the principle of presumption of innocence and the right to privacy' and as a result of 'a prior, fair and impartial procedure' guaranteeing 'the right to be heard (...) and the right to an effective and timely judicial review', says the compromise text on the electronic communications framework directive. 'In duly substantiated cases of urgency' appropriate procedural arrangements may be made provided they are in line with the European Human Rights Convention. In future, internet users may refer to these provisions in court proceedings against a decision of a Member State to cut off their internet access."[154] The laws passed by member states in this area would need to be consistent with this statement of principle, but the details of how the principles should be applied in national laws have not been developed.

France

In October 2009, France adopted a law that would empower a new government agency (HADOPI) to receive complaints from copyright owners about online infringement and forward them to French ISPs for distribution to their subscribers. Subscribers who are the subject of three infringement complaints could have their Internet access suspended for up to a year (Pfanner, 2009).

No direct evidence of the law's effectiveness is yet available. Notifications began in autumn 2010. In October 2010, it was reported that rights holders were reporting 25 000 copyright infringements related to music to HADOPI every day (Picheyin, 2010). Other reports indicated that HADOPI had begun forwarding complaints from copyright owners to ISPs and expected to send 2 000 notices a day through the

end of 2010.[155] A recent study suggests that French Internet users are responding by shifting to different technologies to escape its requirements (Anderson, 2010a; Dejean *et al*., 2010). A survey conducted after the law passed found that only 15% of peer-to-peer software users have stopped using these networks, and that two-thirds of those abandoning peer-to-peer networks had shifted to streaming technologies or other ways to illegally download material. The increases in the use of these alternatives reportedly outweigh the declines in peer-to-peer usage.

Some information on the costs of this programme is available. According to documents made available during parliamentary debate, the government estimated that the law could result in sanctions against 50 000 persons a year (Pfanner, 2009). HADOPI has an annual budget of EUR 6.7 million.[156] The cost to ISPs to respond to the programme is estimated by the government at EUR 70 million for 2009-12 and by the telecommunications industry at EUR 100 million.

United Kingdom

In April 2010, the UK Parliament passed the Digital Economy law, which contains a version of graduated response. It provides for the communications industries regulatory agency, Ofcom, to co-operate with industry to draft a code of practices requiring UK ISPs to forward notifications of alleged copyright violations to their users and provide lists of identified subscribers to copyright owners. Subscribers who receive multiple notifications could have their Internet service suspended or other technical measures applied after review by an independent body and the possibility of an appeals process. However, the possibility of suspensions has been delayed for a year pending a review of the effectiveness of the notice-forwarding regime.[157] Measures that had been under consideration such as requiring ISPs to block websites that are allegedly involved in copyright violation were not adopted.

As the law is still in the process of being implemented, it is too early for direct evidence of its effects. However, costs and benefits have been estimated in an impact assessment done by the government when considering the bill. Estimated benefits of this graduated response regime consist of increased recorded music, film and video game sales. A key variable in estimating the benefits of a graduated response programme is the number of those who would need to get a second or third letter. For those who do not need a further letter, it is assumed that they stopped the infringing activity.

The UK government estimates that approximately GBP 400 million is lost annually to copyright infringement. Based on the survey data reported earlier, it estimated that 70% of the 6.5 million infringing users would stop after receiving a single notice. Drawing on data from the voluntary ISP notice effort, it estimated that these users account for 55% of the volume of infringing downloads. The study therefore concluded that the graduated response measure could reduce displaced sales by approximately GBP 200 million (Department for Business, Innovation and Skills, 2010, p. 68).

The UK government estimated the cost to ISPs to be between GBP 290 million and GBP 500 million over ten years although Ofcom is still evaluating the actual costs. These include the cost of identifying subscribers, notifying them of alleged infringements, running call centres to answer questions, and investing in new equipment to manage the system. The government noted that if the cost were passed on to broadband subscribers, the findings of a study on the elasticity of demand of broadband customers by SPC Network in 2008 indicated that there would be a permanent decline in demand for broadband connections of between 10 000 and 40 000. As a result the ISPs could lose between GBP 2 million and GBP 9 million a year. [158]

A study prepared by LECG on behalf of BPI argued that was economically efficient and equitable for content owners to bear the costs associated with detecting infringement and notifying ISPs and for ISPs to bear the costs associated with sending further notices and applying additional sanctions (LECG, 2009). The

British government has now stated that copyright owners will pay 75% of the ISPs' notification costs and of Ofcom's regulatory costs and that ISPs will pay 25%. Ofcom will set a flat fee per notification at a level intended to meet this cost-sharing formula. The parties would bear similar proportions of the regulatory costs of Ofcom. Subscribers will not pay a fee to appeal a notification, although the agency noted that it had the power to introduce one if a large number of vexatious appeals are filed.[159]

Ireland

In January 2009, the Irish ISP, Eircom, agreed with record companies to implement a graduated response programme as part of the settlement of a lawsuit against them.[160] The programme would work with complaints provided by the record companies. These complaints would contain the IP addresses which the record companies had identified as having been involved in allegedly illegal downloading. Eircom would send notices of copyright infringement to the subscribers at those addresses, and after several such warnings it would disconnect service. In June 2009, copyright owners brought an action against other ISPs seeking to require them to join the graduated response programme (Collins, 2009). In April 2010, an Irish court ruled that this arrangement did not violate the privacy rights of Internet subscribers (Carolan, 2010). In May 2010, Eircom agreed to process complaints involving about 50 IP addresses a week as part of a three-month pilot programme. There is no court review, and the programme is not required by Irish law. Other Irish ISPs have not agreed to the programme, and face ongoing legal challenges alleging that participation in a graduated response programme is required for ISPs to avoid being liable for infringing actions by their users. [161]

Australia

In February 2010, an Australian court ruled that ISPs do not have liability under current Australian law and do not have to implement a graduated response programme. Responding to a suit by copyright owners, the judge ruled that ISPs are not indirectly liable for copyright infringement committed on ISPs' network using the BitTorrent service. The conclusion was based on the fact that liability requires providing the "means" to commit the infringement, and mere provision of facilities is not sufficient.[162] The court also expressed reservations about whether suspension outside of judicial review of the facts would be reasonable or proportional (Anderson, 2010b). The decision, which is under appeal, does not prevent the development of a graduated response regime through new legislation, but it makes it unlikely that such a regime could be adopted as an interpretation of current Australian law.

Site blocking and filtering

Several blocking and filtering methods have been proposed for use by ISPs as a way to reduce online copyright infringement. One proposal is for the ISP to block connections between its subscribers and websites that are involved in online copyright infringement. Another involves examining Internet traffic in transit for indications of infringing material and to prevent the delivery of suspected material identified in this way. These are very different methods and raise different policy issues.

European courts have at times required ISPs to block access to specific infringing websites. For example, in 2008, Italian ISPs were ordered to block access to Pirate Bay, a Swedish site that indexes BitTorrent files. After several court decisions lifting the blocking orders, in February 2010, the Italian Supreme court required all Italian ISPs to block access to Pirate Bay. It should be noted that despite the court decision, the website was made available again immediately under the name "La Baia dei Pirati". In 2008, a court in Denmark required ISPs to block access to the same site.[163] Danish ISPs were also required to block access to infringing websites located in Russia. In March 2010, AT&T indicated support for a procedure that would allow law enforcement to compile and maintain lists of infringing websites and to require ISPs to block access to websites that have been found to be infringing.[164]

Content filtering was required in the *SABAM v Scarlett* case. In June 2007 a Belgian trial court ordered a Belgian ISP to install filtering software to prevent the ISP's users from accessing unauthorised music downloads via peer-to-peer systems. The cost would be borne by the ISP and was estimated by the court, based on an expert's technical report, as not exceeding EUR 0.5 a month per user. The system would require technology that identifies protected musical content in P2P streams, as provided by Audible Magic, which is used by social networks such as MySpace (Hughes *et al*., 2007). This system would perform a function similar to that of the Content ID used by hosting sites such as YouTube to screen content uploaded to their site, with the important difference that the ISP would have to apply the filter to traffic in transit through its system. The ISP was given six months to comply and subjected to fines of EUR 2 500 a day for non-compliance. In 2008, the court delayed implementation of the order, pending a technical feasibility test of content filtering at the network level (Angelopoulos, 2009). In January 2010, the case was referred to the European Court of Justice to determine, among other things, whether an injunction requiring Scarlett to filter would be consistent with Article 15 of the European E-commerce Directive which forbids a general duty to monitor (Linx Public Affairs, 2010). Other European directives are also involved in this legal assessment (Angelopoulos, 2009).

International agreements

For several years a group consisting of the United States, Australia, Canada, the European Union and its 27 member states, Japan, Mexico, Morocco, New Zealand, Singapore, Korea and Switzerland have been negotiating an agreement, called the Anti-Counterfeiting Trade Agreement (ACTA), to increase enforcement efforts against piracy and counterfeiting. These negotiations have dealt with the role of online service providers in enforcing copyright. ACTA includes provisions on digital environment enforcement measures, including remedies against the circumvention of technological protection used in the digital environment and trade in circumvention devices, which are important to ensure a safe Internet marketplace for digital products. ACTA also calls on parties to address the widespread distribution of pirated copyright works on digital networks while preserving fundamental principles such as freedom of expression, fair process and privacy. The Agreement was concluded in November 2010 and a final text was published on 3 December 2010. Participants then engaged in domestic processes prior to opening the agreement for signature on 31 March 2011.[165]

Lessons learned

- Copyright infringement on the Internet is a threat to creativity and legitimate innovative business models. Governments and industry alike are experimenting with different collaborative approaches which involve intermediaries to combat this growing problem and its negative impact on industry, governments and consumers.
- Various organisations have assessed the problem of online copyright infringement and concluded that the problem is sizeable. Quantitative information on the extent of the problem is limited, however. More quantitative information and analysis would be useful.
- The notice and take-down regimes established in many jurisdictions appear workable and balanced, but are limited in their application and effect for many of the principal forms of online infringement. They do not address cross-border and peer-to-peer infringement. Other approaches such as notice-based graduated response, filtering and blocking are being tested as more proactive solutions.
- Private arrangements among parties THAT go beyond notice and notice may be efficient, but issues related to an ISP's liability for suspension of service should be reviewed and addressed.
- Official determination of copyright infringement should be relied upon as much as possible before imposing sanctions, with consideration given to developing an expedited adjudication process. To the extent that sanctions of Internet users are not based on official determinations of copyright

infringement, expeditious procedures should be developed that afford users notice of such action and the opportunity to contest it.

- If proposals for mandatory filtering that require ISPs examine Internet traffic in order to detect signs of copyright infringement are developed, they should include an objective, independent and transparent analysis of technical feasibility as well as of potential effects on free expression, privacy, rights holders' interests and effective enforcement.
- An assessment should be made of the feasibility, costs and benefits of having governments compile and maintain lists of websites found to be infringing and of any requirement for ISPs and other intermediaries to block access to these sites or to deny service to them, including the costs of potential over-blocking, any potential effect on the free flow of information, as well as the potential impact on effective enforcement.
- Governments should engage in analysis before adopting or maintaining any intermediary liability policy. Such analyses should consider the impacts on all interested parties, including rights holders, ISPs and other intermediaries, users and governments.
- Further assessment of the equity of cost sharing is needed.
- Law enforcement also has a role to play in making sure that the most egregious offenders are investigated and prosecuted as appropriate.

REFERENCES

Anderson, N. (2008), "IFPI: 'Three strikes' efforts hit worldwide home run", *ArsTechnica*, 19 August, http://arstechnica.com/tech-policy/news/2008/08/ifpi-three-strikes-efforts-hit-worldwide-home-run.ars. See

Anderson, N. (2009a), "Stern letters from ISPs not enough to stop P2P use after all", *ArsTechnica*, 10 June, http://arstechnica.com/tech-policy/news/2009/06/stern-letters-from-isps-not-enough-to-stop-p2p-use-after-all.ars.

Anderson, N. (2009b), "South Korea fits itself for a '3 strikes' jackboot", *Ars Technica*, 15 April, http://arstechnica.com/tech-policy/news/2009/04/korea-fits-itself-for-a-3-strikes-jackboot.ars.

Anderson, N. (2010), "RIAA? Amateurs. Here's How You Sue 14,000+ P2P Users, *Ars Technica*, 1 June, http://arstechnica.com/tech-policy/news/2010/06/the-riaa-amateurs-heres-how-you-sue-p2p-users.ars.

Anderson, N. (2010a), "Piracy Up in France After Tough Three Strikes Law Passed|, *ArsTechnica*, 23 March, http://arstechnica.com/tech-policy/news/2010/03/piracy-up-in-france-after-tough-three-strikes-law-passed.ars.

Anderson, N. (2010b), "Studios Crushed: ISPs Can't Be Forced To Play Copyright Cop", *ArsTechnica*, 4 February, http://arstechnica.com/tech-policy/news/2010/02/studios-crushed-isp-cant-be-forced-to-play-copyright-cop.ars

Anderson, N. (2010c), "AT&T wants 3 strikes tribunal, government website blacklist", *Ars Technica*, 30 April, http://arstechnica.com/tech-policy/news/2010/04/att-calls-for-us-3-strikes-tribunal-web-censorship.ars.

Angelopoulos, C. (2009), "Filtering the Internet for Copyrighted Content in Europe", *IRIS Plus*, March, www.obs.coe.int/oea_publ/iris/iris_plus/iplus4_2009.pdf.en

Carolan, M. (2010), "Filesharers to have internet cut", *Irish Times*, 16 April 2010, www.irishtimes.com/newspaper/breaking/2010/0416/breaking56.html

CBC News (2007), "E-mail warnings deter Canadians from illegal file sharing", 15 February 2007, www.cbc.ca/consumer/story/2007/02/14/software-warnings.html

Chen, S. (2007), "The State of our Video ID Tools", Google Blog Post, 14 June, http://googleblog.blogspot.com2007/06/state-of-our-video-id-tools.htm.

Cheng, J. (2009), "Germany says 'nein' to three-strikes infringement plan", *Ars Technica*, 9. February, arstechnica.com/tech-policy/news/2009/02/germany-walks-away-from-three-strikes-internet-policy.ars.

Collins, J. (2009), "Major music labels in court move to force internet providers to act on downloads", *Irish Times*, 20 June, www.irishtimes.com/newspaper/finance/2009/0620/1224249188923.html

Deibert, R. *et al.* (2010), "United States and Canada Overview", in *Access Controlled*, MIT Press, Cambridge, MA.

Dejean, S. T. Pénard and R. Suire (2010), "Une première évaluation des effets de la loi Hadopi sur les pratiques des internautes francais", http://recherche.telecom-bretagne.eu/marsouin/IMG/pdf/NoteHadopix.pdf

Department for Business, Innovation and Skills, the Department for Culture, Media and Sport, and the Intellectual Property Office, Digital Economy Act 2010, Impact Assessments, April 2010, http://interactive.bis.gov.uk/digitalbritain/wp-content/uploads/2010/04/Digital-Economy-Act-IAs-final.pdf, p. 68.

Eaglesham, J. and B. Fenton (2008), "UK deal to fight internet piracy", *Financial Times*, 23 July, www.ft.com/cms/s/0/f929aa9e-5901-11dd-a093-000077b07658.html

Electronic Frontier Foundation (2007), "Fair Use Principles for User Generated Video Content", 31 October, at www.eff.org/issues/ip-and-free-speech/fair-use-principles-usergen

General Accountability Office (2010), "Intellectual Property, Observations on Efforts to Quantify the Effects of Counterfeit and Pirated Goods|, April, www.gao.gov/new.items/d10423.pdf.

Hughes, J. *et al*. (2007), English Translation of Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels, 29 June 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1027954

Industry Canada (2006), Internet Service Providers Report, 20 January, www.ic.gc.ca/eic/site/ippd-dppi.nsf/eng/ip01430.html.

International Federation of the Phonographic Industry (2009), *Digital Music Report 2009* pp. 22 and 30, www.ifpi.org/content/library/dmr2009.pdf.

International Intellectual Property Alliance (2010), *2010 Special 301: Canada Report*, 18 February, www.iipa.com/rbc/2010/2010SPEC301CANADA.pdf

Japan (2009), Intellectual Property Strategic Program 2009, 24 June, www.kantei.go.jp/jp/singi/titeki2/keikaku2009_e.pdf.

King, D. (2008), "Making Money on YouTube with Content ID|, Google Blog Post, 27 August, http://googleblog.blogspot.com/2008/08/making-money-on-youtube-with-content-id.html

Learmonth, M. (2009),"YouTube Moving the Needle on Ad Sales", *Advertising Age*, 8 April, http://adage.com/digital/article?article_id=135859.

LECG (2009), "An economic assessment of the impact of cost allocation with regard to proposed measures to address illicit peer-to-peer file-sharing", December, Unpublished. .

Linx Public Affairs (2010), "*SABAM v Scarlet* sent to European Court", 5 February, https://publicaffairs.linx.net/news/?p=1306.

Llewellyn, H. (2009), "Spanish Govt Rules Out Three-Strikes Law", Billboard.biz, 5 November, www.billboard.biz/bbbiz/content_display/industry/e3i6391eb52691ab08c796782a0a307ec43.

McBride, S. and E. Smith (2008), "Music Industry to Abandon Lawsuits", 19 December, http://online.wsj.com/article/SB122966038836021137.html.

OECD (2007), *Economic Impact of Counterfeiting and Piracy*, www.oecd.org/dataoecd/13/12/38707619.pdf.

OECD (2009), Piracy of Digital Content, p. 33, www.oecd.org/document/35/0,3343,en_2649_34223_43394531_1_1_1_1,00.html.

Pfanner, E. (2009), "France Approves Wide Crackdown on Net Piracy", *The New York Times*, 22 October, www.nytimes.com/2009/10/23/technology/23net.html?_r=1.

Pfanner, E. (2010), "U.K. Approves Crackdown on Internet Pirates", *The New York Times*, 8 April, www.nytimes.com/2010/04/09/technology/09piracy.html?scp=1&sq=digital%20economy%20bill%20uk&st=cse

Picheyin, A. (2010), "French Anti-Piracy Scheme's 25,000 Daily Reports", *Billboard*, 22 October, www.billboard.biz/bbbiz/content_display/industry/e3i1c1499752deb3a60a1584400533395b0.

Sandoval, G. (2009a), "Is ATT Violating DMCA by not Booting Repeat Infringers?", CNet, 1 April, http://news.cnet.com/8301-1023_3-10208747-93.html.

Sandoval, G. (2009b),"Comcast, Cox cooperating with RIAA in anti-piracy campaign",CNet.com, 25 March, http://news.cnet.com/8301-1023_3-10204047-93.html

See Chen, J. (2008), "Pirate Bay to IFPI: Danish Ban Has Led to More Traffic", *Ars Technica*, 12 February, http://arstechnica.com/tech-policy/news/2008/02/pirate-bay-to-ifpi-danish-ban-has-led-to-even-more-traffic.ars.

Sparh, W. (2009), "German Government to tighten copyright law", Billboard.biz, 27 October, www.billboard.biz/bbbiz/content_display/industry/e3i018a992ff2ce5f8eae092e04cb24039e.

Stelter, B. (2008), "Some Media Companies Choose to Profit from Pirated YouTube Clips", *The New York Times*, 15 August, www.nytimes.com/2008/08/16/technology/16tube.html

Stone, B. and M. Helft (2007), "New Weapon in Web War Over Piracy", *The New York Times*, 19 February, www.nytimes.com/2007/02/19/technology/19video.html.

Zittrain, J. (2008), *The Future of the Internet and How to Stop It*, Yale University Press, New Haven, CT.

ONLINE MARKETPLACES AND THE SALE OF COUNTERFEIT GOODS

Introduction

Counterfeit goods are products that are manufactured or first sold with a trademark but without the authorisation of the trademark owner. The key issue is the deceptive use of a trademark to connect an unauthorised item with the source of a genuine item. Companies register their trademarks to protect their economic interests in the goods they manufacture or merchandise through licensing agreements. Trademarks enable buyers to identify the source of merchandise and provide an assurance of quality. Like other forms of intellectual property protection, trademarks are linked to innovation and economic growth. Counterfeiting reduces sales and lowers prices of authentic products in the short term. In some cases, such as counterfeit pharmaceuticals, they can also threaten consumers' health and safety, in that they are not produced or distributed according to the same codes, laws and safety regulations as genuine goods. Longer-term harm includes damage and loss of trademark and brand value, quality control and company reputation, investments in plant, equipment, and research and development that cannot be recouped, as well as lower incentives for expansion and innovative activities. Countermeasures to detect and prevent counterfeiting are themselves costly and divert resources from more productive uses.

The services of online marketplaces, search engines, independent websites and social networks can be misused by third parties who list or advertise counterfeit goods and infringe well-known brands. Counterfeiting is a growing concern of trademark owners and others in the Internet community.[166] The OECD and government bodies recommend further actions to "keep the Internet from becoming an even more prominent distribution channel for counterfeit and pirated products" (OECD, 2007, p.7).This case study discusses steps that some intermediaries are taking, envisages voluntary best practices and investigates legal obligations.

It is hard to determine the extent of the counterfeit goods issue. The OECD estimated that international trade in counterfeit and pirated goods could have accounted for up to USD 200 billion in 2005. An updated estimate suggests that counterfeit and pirated goods in international trade grew steadily over 2000-07 and could have reached up to USD 250 billion in 2007. The share of counterfeit and pirated goods in world trade is also estimated to have increased from 1.85% in 2000 to 1.95% in 2007. These figures do not include domestically produced and consumed products or non-tangible pirated digital products. The OECD recognised the difficulty of developing these estimates, but noted that the new estimates seemed to show that the problem was growing (OECD, 2009, p. 1). A recent report from the US Government Accountability Office noted that widely cited figures from US government agencies of USD 200 billion in losses from counterfeit goods could not be substantiated. Nevertheless, it concluded that the problem is "sizable" (GAO, 2010).

Factors that contribute to the online distribution of counterfeited goods include the Internet's worldwide reach, the use of online payments, and the relative online anonymity that helps counterfeiters to convince consumers to purchase counterfeit goods (OECD, 2007, "Executive Summary").

Some voluntary steps taken by Internet intermediaries

Online marketplaces provide the platforms for buyers and sellers to transact. Intermediary online marketplaces do not themselves own, produce, buy, sell or inspect physical goods sold on their platforms and are not necessarily able to determine whether or not they are counterfeit. They typically earn revenue from commissions on all sales that take place on their platform and from advertising based on traffic to their sites. This could potentially provide a disincentive for them to combat counterfeiting on their platforms, since they could profit from the sale of undetected infringing items. On the other hand, market forces also provide online marketplaces with a strong incentive to prevent sales of counterfeit goods

because counterfeit goods may discourage repeat purchases, increase customer complaints and harm the reputation of the marketplace as a reliable shopping venue.

Intermediary platforms usually forbid the sales of counterfeit goods or the unauthorised use of trademarks under acceptable use policies, although this alone rarely deters sellers or infringers.[167] According to court findings, eBay spends USD 20 million a year, and invests significant human and technological resources, to promote safety and trust in its website.[168] It conducts manual reviews of listings in an effort to remove those that are likely to offer counterfeit goods. It also has an automated system designed to filter for and detect descriptions of products that are likely to be counterfeit. eBay also maintains and administers the Verified Rights Owner (VeRO) Program, a notice and take-down programme for brand owners to ask eBay to suspend specific auctions of counterfeit goods speedily.[169] Rights holders can use a notice of claimed infringement (NOCI) form to report a problem. According to US court findings, eBay's practice is to remove reported listings within 24 hours of receiving a NOCI, but in fact it deletes 70-80% within twelve hours of notification. It also suspends from its website tens of thousands of sellers suspected of having engaged in infringing conduct. It suspends repeat infringers, but also suspends sellers after the first violation if multiple infringing items were involved and it is clear that the seller's purpose was to traffic in counterfeit goods.

Search engines have also taken voluntary steps to control counterfeit sales. Google, Yahoo! and Bing recently updated voluntary protocols designed to prevent the sale of sponsored results for unlawful businesses selling counterfeit medications online. These protocols use a "white list" of approved Internet pharmaceutical sellers which includes verification by the National Association of Boards of Pharmacy's Verified Internet Pharmacy Practice Sites (VIPPS) or certifications from the original manufacturers of legitimate and FDA-approved pharmaceuticals (Office of the US Intellectual Property Enforcement Coordinator, 2010, p. 18).

These voluntary efforts are supplemented by a list of best practices suggested by the International Trademark Association (INTA). Policy makers are encouraging these co-operative efforts, believing that agreements among those directly involved will provide practical and efficient solutions. The best practices described by INTA call for increased co-operation between rights holders and various intermediaries, including payment systems, search engines and online marketplaces:

- Best practices for search engines include adopting and enforcing a policy against counterfeiting activities by advertisers, with a publicly available process to deal with counterfeiting, collaboration with rights holders to target counterfeiting through measures such as "blocking or flagging for heightened review certain suspect terms that may be indicative of counterfeiting activity", and education of rights holders about their policies and practices for dealing with counterfeiting.

- Best practices for marketplaces and shopping sites include actively informing users that sales of counterfeit goods are not permitted and that failure to follow this rule can result in permanent loss of access to the site and referral to law enforcement.

- Best practices for payment providers include having a way to respond to complaints about the use of a payment brand for sales of counterfeit goods. Trademark owners would provide information such as identification of the allegedly counterfeit transaction and evidence that the payment system brand was involved, and the payment system would look into the allegation and take action in accordance with a public stated policy, which may include suspension of the merchant involved. Trademark owners would agree to indemnify payment systems for steps taken and for legal risk.[170]

Online marketplaces and liability for trademark infringement

The first response of trademark holders who notice the presence of counterfeit goods listings using their brand on an online marketplace is to give notice. Online marketplaces usually comply and take down listings expeditiously to avoid contingent liability. However, policing such a notice and take-down policy takes significant vigilance by brand owners, who inevitably act after the fact. For trademark holders, a more desirable solution may seem to be to compel online marketplaces to filter out in advance listings containing infringing trademarks. Yet effective identification of counterfeit goods often requires in-depth, confidential brand-specific knowledge and even laboratory testing by a brand owner. Still, some have argued that auction sites – whose revenues are derived from commissions on sales, and which provide software to facilitate categorising and researching items – must have "constructive knowledge" of infringement, disqualifying them for immunity under Article 14.

Accordingly, in *Louis Vuitton Moët Hennessy (LVMH) v eBay*, a French court found, despite the immunity provisions of the E-Commerce Directive (ECD) as implemented in French law, that eBay was responsible for failing to prevent the sale of counterfeit luxury goods on their site.[171] The French court found "serious faults" in eBay's processes and fined it GBP 31.5 million and prohibited the sale of some luxury perfumes on its site.[172]

By contrast, in a similar dispute in the United States, eBay won and Tiffany lost.[173] The case was argued under the rules of United States' trademark and unfair competition law and without reference to a generalised safe harbour law. Tiffany argued that eBay had generalised knowledge of the sale of fake Tiffany jewellery on its site, and that eBay's notice and take-down programme for intellectual property rights holders was inadequate to prevent fraud. The US District Court held however that it was "the trademark owner's burden to police its mark and companies like eBay cannot be held liable for traders based solely on their generalised knowledge that trademark infringement might be occurring on their websites". The district court stated that eBay had a responsibility under trademark law to avoid providing its services to sellers it knew to have infringed trademark by using measures including an effective voluntary notice and take-down programme, but ruled that eBay had satisfied this responsibility. In addition this responsibility did not extend to a positive duty to monitor its auction site. Tiffany's request for eBay to police listings of "Tiffany" branded goods pre-emptively on its site was rejected.[174] The US Court of Appeals for the Second Circuit confirmed the district court's conclusion that eBay should not be secondarily liable for third-party sales of counterfeit Tiffany products on its site.

Other decisions in France, Belgium and Germany reached different conclusions and protected eBay from liability under Article 14 of the ECD, which shields hosting intermediaries from liability if they do not have actual knowledge of illegal activity and are not aware of facts or circumstances which make illegal activity apparent or if they act expeditiously to remove or to disable access to the illegal activity once they have been informed.

In the United Kingdom, eBay won yet another decision in 2009, but the merits of the case with regard to intermediary service provider liability were not dealt with in detail pending a reference to the European Court of Justice (ECJ) that was still outstanding in July 2010.[175] Until and unless the ECJ reaches a final determination on the matter, or the ECD is reformed (a matter also under discussion in mid-2010, with public consultation launched in August 2010[176]), the outcome of such cases is likely to remain uncertain.

Elements of an economic analysis

To the extent that the harmonisation of legal standards proceeds, it is useful to look at this issue from an economic perspective. Who should bear the cost of controlling the sale of counterfeit or other infringing goods? One answer is the owners of trademarks, since they most proximately profit from enforcement by

maintaining the reputation of their brand. The costs of enforcement might arguably be lower when an online marketplace can automate the process of filtering out some or all of the counterfeit listings. Since May 2002, eBay has had an automated fraud engine dedicated to ferreting out illegal listings, including counterfeit listings.[177] However, there are significant technical differences between filtering systems that can detect copyright violations by inspecting an uploaded digital good such as a music or video file, and a filtering system that has to try to detect trademark violations by inspecting the descriptions of physical goods and other indicators of possible infringing activity such as IP addresses. Any such filtering system might be able to detect the most blatant attempts to sell counterfeit goods, but it would probably have a substantial error rate (either positive or negative) which might have negative consequences for users and the marketplace. For example, some automated processes could prevent legitimate resale of original goods. Another consideration is that the costs of controlling listings pre-emptively are likely to be passed on to consumers (*e.g.* resulting in higher rates for listing items by online marketplaces or in higher prices for goods sold by brand owners) thus producing a less competitive online marketplace, regardless of who bears the costs. Such arguments are almost impossible to resolve without empirical economic evidence, which is rarely available.[178]

An economic analysis of the responsibilities of Internet intermediaries for controlling counterfeit sales starts with the argument that they may be well positioned to take some steps to control this illegal activity. While they do not have expert knowledge enabling them to determine when an article for sale is counterfeit, they do have access to and control over the users of their system. They can locate and take action against counterfeiters far more efficiently than brand owners. It is therefore sometimes argued that, as the "least cost avoider", they should bear the responsibility of controlling counterfeit sales (Mann and Belzley, 2005).

However, others argue that such a "least cost" perspective is limited because it assumes that any level of enforcement activity by Internet intermediaries is legitimate if it has some effect on reducing counterfeit sales. Still others have argued for a social cost-benefit analysis whereby enforcement efforts to stop the harm due to counterfeiting should continue until mitigation efforts cost more than they save.

Applying a cost-benefit analysis is difficult. It is hard for external parties to have sufficient knowledge to determine the point at which enforcement efforts are worth it. Brand owners and Internet intermediaries have this knowledge, but their incentives are misaligned. Brand owners have an incentive to call for as much enforcement as possible as long as it has some effect on reducing counterfeiting. Internet intermediaries only have an incentive to contain reputational damage from counterfeit sales, even if further efforts would save more in counterfeit losses than they would cost. Both parties react to their costs and benefits rather than to overall social costs and benefits.

Negotiations between the affected parties to reach a mutually satisfactory outcome could provide guidance for policy makers as to an adequate balance. These would concern both the level of effort involved and the sharing of the costs associated with mitigation efforts. Transaction costs, at least for major players, do not seem to be so high as to block an efficient arrangement, although they might prove significant if online marketplaces needed to negotiate with substantial numbers of brand owners.

Negotiated arrangements would need to be public and to be supervised by public authorities to ensure that the public interest is protected. For instance, an agreement between a brand owner and an online market to stop selling the brand owner's product entirely in return for a regular payment might need to be reviewed by competition policy agencies. These voluntary arrangements could be the basis for industry-wide best practices and for codification into statute or regulation if necessary.

In the United States, voluntary arrangements to limit the sale of counterfeit pharmaceuticals have been established, with the government playing the role of convener. After meetings hosted by the Office of the

Intellectual Property Enforcement Coordinator (IPEC), a number of Internet intermediaries announced that they would take appropriate voluntary action against illegal online pharmacies. Online pharmacies are generally required to demand a prescription before selling a prescription drug online. Those that do not are often involved in the sale of counterfeit pharmaceuticals. The IPEC worked with agencies across the US government to host a series of meetings with private Internet intermediary companies to help increase co-operation among themselves and with law enforcement in regard to these illegal online pharmacies. On 14 December 2010, IPEC disclosed that "a group of private-sector partners – American Express, eNom, GoDaddy, Google, MasterCard, Microsoft, Paypal, Neustar, Visa, and Yahoo! – announced that they will work to form a new non-profit entity with other private sector participants to take appropriate voluntary action against illegal pharmaceutical websites".[179]

Lessons learned

The lessons learned from this case can be summarised as follows:

- Intermediaries are voluntarily responding to complaints and taking some proactive steps.
- Legal requirements for further proactive steps vary by region.
- International harmonisation would be helpful to prevent overlapping and conflicting requirements.
- Governments and courts should take into account the costs of intermediaries' steps to prevent counterfeit sales as well as their effectiveness in determining the appropriateness of intermediary enforcement action.
- Voluntary negotiations might be the best way to achieve this goal, since transaction costs that would prevent efficient agreements seem to be small. However, if voluntary negotiations fail, government action may be necessary.
- Some voluntary efforts in the area of Internet pharmacies engaged in the sale of counterfeit pharmaceuticals are under way and appear promising.

REFERENCES

General Accountability Office (2010), "Intellectual Property, Observations on Efforts to Quantify the Effects of Counterfeit and Pirated Goods", April, www.gao.gov/new.items/d10423.pdf.

Lemley, M. (2007), "Rationalising Internet Safe Harbors" 6 *Jnl of Telecomm, & High Tech L* at 112.

Mann, R.J. and S.R. Belzley (2005), "The Promise of Internet Intermediary Liability", *William and Mary Law Review* 239.

OECD (2007), Economic Impact of Counterfeiting and Piracy, www.oecd.org/dataoecd/13/12/38707619.pdf.

OECD (2009), Magnitude of Counterfeiting and Piracy of Tangible Products: An Update, November, www.oecd.org/dataoecd/57/27/44088872.pdf.

Office of the US Intellectual Property Enforcement Coordinator, Executive Office of the President (2010), "2010 Joint Strategic Plan on Intellectual Property Enforcement, www.whitehouse.gov/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf (Joint Strategy).

CONSUMER PROTECTION IN E-COMMERCE PAYMENTS

Introduction

In recent years, e-commerce has developed rapidly. Payment systems have helped to support this growth, providing consumers with effective and secure ways to purchase products, while also providing means to address problems consumers may experience with vendors when, for example, unauthorised charges occur or products do not meet expectations or are delayed in delivery. This case study focuses on the role of payment providers in enhancing consumer protection in e-commerce transactions. It draws on work conducted by the OECD on consumer protection in online and mobile payments as part of the review of the 1999 *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* ("1999 Guidelines").

Payment systems are intermediaries that link online merchants with online customers by enabling the transfer of customers' funds to merchants to pay for e-commerce transactions. E-commerce payment intermediaries include: *i)* payment systems that employ credit/debit or use a bank account to enable e-commerce transactions (*e.g.* card payment networks such as Visa or Mastercard or payment methods based on online banking); *ii)* alternative (non-card and non-bank) payment systems provided by non-bank institutions operating on the Internet which are associated with a payment card or bank account, either directly (*e.g.* Google Checkout or Checkout by Amazon) or indirectly (*e.g.* Paypal); and *iii)* mobile payments, which include both mobile contactless or point-of-sale (POS) payments and remote payments made with mobile devices.[180]

Payment cards, with over 90% of e-commerce retail transactions in Europe in 2009, over 80% in the United States, and over 74% in Mexico, remain the dominant payment mechanism in e-commerce. Online-banking-based Internet payments are a growing category, particularly in Europe.[181] Alternative (non-card and non-bank) Internet-based payment methods (*e.g.* PayPal or Google Checkout) have been gaining significant market share. For example, PayPal, which dominates the online alternative payments market, was projected to account for 11% of the global e-commerce market by 2011, up from 9% in 2008.[182] Mobile payments are a new and rapidly-growing alternative payment method for e-commerce retail sales, particularly in Asia.[183] Mobile payments are projected to represent 5% of global ecommerce retail sales by 2014.[184]

With respect to payments, e-commerce raises two main types of consumer policy issues. The first is unauthorised payment charges, that is, the unauthorised use of a payment instrument to undertake an online purchase. The key issue in this case is the party responsible for the resulting loss. Traditional card and bank-based payment systems and online merchants address issues of unauthorised payment charges with measures to reduce online fraud and with processes to resolve online disputes. The second issue, in which payment intermediaries are only indirectly involved, relates to disputes between merchants and customers regarding the receipt, nature or quality of the good or service purchased. Some payment providers have implemented measures to resolve online disputes of this type. While some countries legally require such measures, in others they are private. Public policy considerations include the adequacy and efficiency of private-sector measures and of current legal rules.

Regulatory regimes to protect consumers engaging in online payments

There are significant differences among the various legal regimes covering consumer protection for payment users. Protection differs depending on the country, the type of problem (*e.g.* unauthorised payment charges, non-delivery or non-conformity), the medium (*e.g.* online, offline or mobile), as well as the type of payment (*e.g.* debit, credit, prepaid card or mobile phone). While most countries have specific provisions for unauthorised payment charges and processing errors for traditional (card and bank-based)

payment users, fewer have specific provisions for non-delivery or non-conformity of goods and services (OECD, 2006). Users of alternative payment means, such as mobile payments or prepaid cards, may not have any regulatory protection.

Traditional payment mechanisms

Unauthorised payment charges

Unauthorised payment charges include: *i)* fraudulent charges on a consumer's account following loss or theft of payment information, *e.g.* through a data breach; and *ii)* intentional or unintentional billing errors. Most OECD countries have specific legal or regulatory provisions deal with unauthorised charges to payment cards and chargeback (refund) mechanisms to protect consumers, by law or through self-regulation (OECD, forthcoming). These apply to online as well as offline transactions. In the United States, the *Truth in Lending Act* protects consumers from liability for charges resulting from unauthorised use of their credit card, and the *Electronic Fund Transfer Act* provides consumer protection for the use of debit cards. In 30 European countries, the Payment Services Directive (PSD) protects consumers by providing refund rights to consumers by payment service providers in the event of unauthorised or incorrect debits.[185]

In general, online consumer payments are significantly more prone to fraud than offline payments. For example, in France in 2009, the fraud rate on online purchases was seven times higher than the offline rate. In Spain, it was 13 times higher (Box 1). Payment cards are particularly vulnerable to fraud as they were not originally designed for Internet use and contain valuable information on cardholders' identity and account numbers. Furthermore, they cannot be inspected in e-commerce transactions and many different parties are involved in their processing. Experts estimate that occurrences of online payment fraud may increase rapidly owing, paradoxically, to increased security at physical points of sale, in particular due to the EMV (Europay, MasterCard and VISA) "chip and PIN" standard (Sullivan, 2010; Innopay, 2010). In markets where the use of chip and PIN is widespread, offline card fraud is at record low levels.[186] According to Visa Europe, during 2009 environments not protected by EMV, including e-commerce, accounted for some 75% of total fraud losses for Visa Europe membership. Online card fraud gradually increased even as the total volume of fraud decreased.

Box 3. Box 1. Cost of payment fraud to online merchants and payment providers in selected OECD countries

A general lack of detailed and comparable data on the extent and characteristics of payment fraud for many OECD countries makes it difficult to draw conclusions about the cost of online payment fraud and the efficiency of industry strategies or policy responses. *E-commerce merchants* incur substantial fraud-related costs. In addition to direct revenue losses, the cost of stolen goods and associated delivery and fulfilment costs, they incur costs in prevention efforts such as compliance with data security standards, rejecting orders that are in fact valid, deploying automated monitoring systems, staffing manual reviews, and administering fraud claims, in addition to reputation costs. For *card networks*, processing disputes between cardholders and merchants, particularly through chargeback systems, involves significant costs. For *payment issuers*, online payment card fraud costs include monitoring, reissuing of cards, notification, reputational damage and customer dissatisfaction. Available data show that online fraud is much more prevalent than offline fraud and varies significantly among countries.

In the United States and Canada in 2009, on average 1.2% of merchants' online revenues were lost to payment fraud.[1] This represented a decline from the previous year. Total estimated online revenues lost to fraud fell 18% from a peak of USD 4 billion in 2008 to USD 3.3 billion in 2009. Chargebacks (bank refunds) in the United States and Canada in 2009 accounted for about half of these fraud losses. The remaining half represented credit issued by merchants to reverse charges following consumers' claims of fraudulent account use. Overall, payment fraud losses fall most heavily on Internet merchants because most of their payments are card-not-present (CNP) transactions.

In the United Kingdom in 2009, e-commerce merchants expected to lose an average of 1.8% of their online revenue to payment fraud in 2009, or GBP 400 000 on average in lost revenue across all sizes of business.[2] In the first half of 2009, the United Kingdom experienced its first drop in CNP fraud. According to Financial Fraud Action UK, a main reason was the growing use of industry countermeasures by online retailers and consumers. UK e-commerce merchants continued to rank online fraud as the greatest threat to their business (57%) and were increasingly aware of and concerned about the threat of customer data theft (from 6% in 2007 to over 50%).

In France, the fraud rate on online purchases increased in 2009 to 0.263%, from 0.235% in 2008, for a total cost of EUR 51.9 million. The fraud rate on online purchases was seven times higher than the card-present fraud rate of 0.038%. Distance payments, which represented 7% of French transactions, accounted for 57% of the total.[3] Internet payment abroad remained much riskier with fraud rates about 5.5 times higher than the fraud rate in France, at 1.44% compared with 0.235% in France.

In Spain in 2009, fraud at online merchants represented 0.4% of purchases from domestic merchants, while for merchants abroad fraud was 0.34%, compared to an overall fraud rate of just 0.0306% of total sales in Spain.[4]

1. CyberSource (2010a), *Online Fraud Report*, 11th Annual Edition, http://forms.cybersource.com/forms/FraudReport2010NACYBSwwwQ109

2. CyberSource (2010b), *6th Annual UK Online Fraud Report,* http://img.en25.com/Web/CyberSource/uk_online_fraud_report_2010%20web.pdf.

3. Banque de France, Observatoire de la sécurité des paiements, *Rapport Annuel 2009*, www.banque-france.fr/observatoire/rap_act_fr_09.htm.

4. Servired (2010), *Annual Report 2009*, www.servired.es/ingles/pdf/annual_report09.pdf.

Non-delivery of goods or non-performance of services, or non-conformity of goods and services

Some OECD member countries have legal or regulatory provisions to protect traditional cardholders in cases of non-delivery, partial delivery or late delivery of goods purchased online, non-performance of services or non-conformity of goods and services. Among these are Finland, Greece, Japan, Korea, Norway, the United Kingdom and the United States (OECD, 2006).They aim to provide consumers with some ability to avoid liability for charges incurred if goods are not delivered in a timely manner. To provide an indication of the scale of the issue, a majority of complaints handled by the European Consumer Centres' Network in 2009 concerned delivery problems (40%), while 30% concerned problems with the product or service (ECCNET, 2010).

Alternative payment systems

Alternative payment providers (APPs) are not, in many countries, subject to specific regulatory supervision and consumers' level of legal protection varies depending on the type of payment method used.[187] For example, prepaid cards are often not currently required by law to offer consumers' protection

against fraud or billing disputes. For most alternative Internet-based payment services (*e.g.* Paypal, BidPay, Google Checkout or Checkout by Amazon), consumers who settle transactions with their credit or debit card obtain the same protection as if they had paid with their card directly.[188] However, if consumers settle these transactions with a bank or cash account or when Internet-based payment services do not allow the use of credit or debit cards for payment (*e.g.* eBillme or Bill Me Later), online payment services promise some protection, but this is not required by law and varies significantly depending on the provider.[189]

Some of the new mobile payment services can be provided by a number of different actors, including financial institutions (offering mobile payment options), software development companies (such as developers of mobile parking meter payment applications) or telecommunications providers (such as mobile operators that provide their own mobile financial services to their customers). Determining which regulatory framework (*e.g.* financial regulations, consumer protection or telecommunication regulations) governs each type of transaction can be difficult. In some cases, payment may be provided directly by a mobile operator and charges appear on a mobile phone bill. In such cases, e-commerce purchases may not be entitled to standard user protection. If a mobile operator requires a prepaid deposit to cover future charges, consumer protection may also be lacking.[190] For example, the Japan Association of Consumer Affairs Specialists (JACAS) compared the services and contract terms of mobile payment providers, and found that consumers are not protected for unauthorised payments using "registered" mobile payment services until they request that the payment provider stop processing payments. In addition there are no redress mechanisms for users of pre-paid mobile payments whose device is lost and stolen.

The complexity of the structure under which some payment transactions now take place has resulted in legal uncertainty. Consumers, merchants and regulators do not always know which regulations apply, which authorities to contact or which types of redress may be available. These issues, which are perceived by consumers and merchants as major barriers to the development of online shopping, can discourage stakeholders from engaging in e-commerce, in particular across borders (OECD, forthcoming). Many consumer protection authorities and organisations are calling for more uniformity of consumer protection with new payment providers, particularly mobile.

Measures by payment providers to protect consumers in e-commerce

In addition to legal protection, some payment systems afford significant consumer protection voluntarily. The major card networks impose obligations on their issuing banks to provide protection that may exceed what is required by national laws and can give cardholders important benefits.[191] In addition, industry codes of conduct and policies instituted by alternative payment providers can be extremely useful owing to the lack of legal protection in many countries. However, codes of conduct may not provide consumers with adequate protection and may not be enforceable, and some payment providers may not adhere to them. In addition, the protection they afford varies significantly and this can be confusing to consumers.

Measures by traditional payment providers to prevent and detect online payment fraud

Legal and contractual liability rules often prevent merchants and payment providers from imposing the costs of unauthorised use of payment cards on cardholders. As a result, payment networks and financial institutions have introduced measures to reduce payment card fraud and online merchants have adopted them. Online merchants and cardholders are making growing use of fraud prevention measures and online merchants and banks are using more efficient online fraud detection tools. Fraud prevention measures include the use of data security standards such as PCI DSS to help prevent the theft of static authentication information (such as payment card number, expiration date and security code). In addition, a growing fraud prevention practice is the use of real-time dynamic authentication information or of additional layers of

authentication. Additional security measures such as MasterCard SecureCode and Verified by Visa are increasingly, albeit slowly, being implemented. Fraud detection helps identify fraudulent incoming orders in e-commerce and cancel them before the orders are filled by checking compliance with risk parameters set by card issuers or merchants (such as sufficient funds in an account).

Protecting cardholder data to prevent fraud: The PCI DSS standard

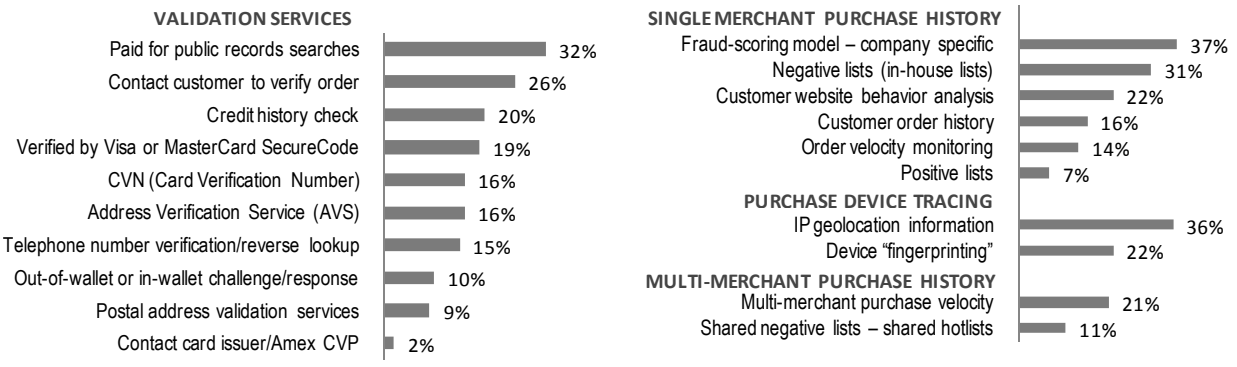
As payments become more computerised, attention has turned towards protecting not just the physical cards, but the data that travel through the payment system, for both offline and online transactions. Since 2004, substantial industry efforts have been made to develop and implement a harmonised security standard that applies to organisations that hold, process or exchange cardholder information from any card from one of the major card networks. The Payment Card Industry Data Security Standard (PCI DSS) helps prevent credit card fraud through better information security processes. It consists of 12 basic requirements involving computer system security, network security and personnel management issues (such as who has access to cardholder data) to prevent theft of useful payment information.[192] Compliance by merchants with this standard is widespread (MacCarthy, 2010).

Fraud detection tools

In the United States and Canada in 2009, 97% of online merchants used one or more of the automated validation tools provided by card associations to help authenticate cards and cardholders. The tools most often used by merchants were the Address Verification Service (AVS) and the Card Verification Number (CVN). AVS compares numeric address data with information on file from the cardholder's card-issuing bank. CVN is a three-digit security code on the back of most types of credit cards that helps ensure the genuine card is being used when buying online.[193] The tools most used by merchants were not necessarily those viewed as the most efficient. For instance, 36% of merchants in the United States and Canada considered IP geolocation tools, which attempt to identify the geographic location of the device from which an online order was placed, as very efficient (Figure 1).

Figure 1. . Perceived effectiveness of fraud management tools in the United States and Canada

Percentage of merchants with at least USD 25 million in online revenue using the tool and selecting it as one of their "top three" most effective



Source: Cybersource (2010a), *Online Fraud Report*, 11th Annual Edition, http://forms.cybersource.com/forms/FraudReport2010NACYBSwwwQ109.

As merchants employ growing numbers of *fraud detection tools*, they increasingly look to automated order-screening systems to evaluate incoming orders in real time. Based on merchants' business rules and results from the fraud detection tools, these systems determine whether a transaction should be accepted, rejected or suspended for review. For example, if an order exceeds a certain amount, or if the billing and shipping addresses do not match, the order is flagged as potentially fraudulent and placed in a "review queue" in the merchant's order management system for further inspection. In 2009 in the United States,

automated order decision/screening systems were used by 67% of merchants (up from 25% in 2005) and by 87% of large online merchants (CyberSource, 2010a). Most merchants use *manual fraud review* for some orders after initial automated screening. Over the past five years an average of about one out of four online orders enter manual fraud review in the United States and Canada. However, reliance on manual review is expensive: over half of fraud management budgets are spent on review staff costs.

Some payment card companies have also adopted *payer authentication schemes* known as "3D Secure Internet security protocol" for Internet-based card payment transactions. These schemes are offered to customers as the Verified by Visa, MasterCard SecureCode or American Express SafeKey services. They add an additional cardholder authentication step for online payments: the issuing bank (the cardholder's bank) prompts the buyer for a password that is known only to the bank and the buyer. However, only 29% of merchants in the United States and Canada used a payer authentication service in 2009. In Europe in 2009, some 300 000 retailers, accounting for 37% of e-commerce transaction volume, supported the service with over 50 million cardholders enrolled.[194] In addition, Visa for example had initiatives to drive down fraud rates for transactions authenticated by Verified by Visa by reducing the reliance on static passwords and migrating to dynamic passcodes.[195]

Externalities, costs and liability allocations for online payment fraud

Default liability allocation under public law and private rules of the payment systems can be simplified as follows: *i)* consumers rarely bear meaningful liability for fraudulent transactions unless they benefited from the fraud; *ii)* card issuers typically bear liability for fraud losses in card-present transactions; and *iii)* merchants generally bear liability for fraud losses in e-commerce transactions (Douglass, 2009).The question of whether the current allocation of fraud liability results in efficient outcomes has been raised, that is, whether each party has appropriate incentives in the form of risk of fraud liability to take reasonable steps to minimise fraud losses from the perspective of the payment system as a whole. While merchants are usually liable for online payment fraud, they are less centralised and may be less able to co-ordinate their actions than the card networks are to co-ordinate the actions of their member banks. Merchants may therefore not be in the best position to improve the payment system. Indeed, innovation in fraud control technology often rests with financial institutions and payment networks.

Card network rules stipulate that merchants bear much of the liability for losses associated with online fraud,[196] but also provide that implementing payer authentication programmes (*e.g.* Verified by Visa or MasterCard SecureCode) shifts risk of fraud liability from the merchant back to the card issuer.[197] Card issuers may lack sufficient incentives to require cardholders to participate in such fraud prevention efforts, as the benefits would accrue primarily to the merchant, while they would spend resources, risk cardholder dissatisfaction, and become liable for fraud. This appears to explain the low adoption of card networks' payer authentication programmes.[198] Despite significant interest by merchants in implementing payer authentication systems over the past few years, adoption has been slow since its introduction in 2003.[199]

Payment providers' measures to resolve consumer disputes

In case of a dispute, consumers are generally encouraged to try first to settle it by contacting the merchant directly. If a settlement cannot be reached between a merchant and a consumer, several third-party options can be pursued at government or at industry level. Protection provided by payment organisations to consumers represents an important avenue for consumer redress. This section focuses on schemes to provide consumers with dispute resolution mechanisms for cases of unauthorised charges, non-delivery and late delivery, or non-conformity.

Consumers can ask the payment organisation to reverse the charge or debit to the merchant. This is known as a "chargeback" (the return of funds to a consumer, initiated by the consumer's issuing bank). In

some jurisdictions, traditional payment providers allow cardholders to bring claims against e-commerce merchants involving disputes such as "non-delivery of goods" or "item not as described", but chargebacks for "fraud" or "billing errors" are the most common (Philiips, 2010). The merchant's bank can dispute the chargeback on behalf of its merchant using the "representment" process.[200] Ultimately, card networks (*e.g.* Visa or Mastercard) often resolve disputes that are not settled directly between the issuer bank and merchant bank. Chargeback mechanisms are viewed by many as an easy and convenient channel to resolve problems associated with the purchase of goods or services online (OECD, 2002, 2006). Paypal also implements chargebacks that are initiated and handled by the buyer's credit card issuer and therefore follow credit card issuer regulations and timeframes.

There are also *dispute resolution schemes* in which payment organisations may play a direct or indirect role. They are sometimes part of trustmarks or other types of self-regulatory schemes. More traditional mechanisms, such as litigation, can be time-consuming, expensive and inappropriate for low-value online consumer transaction disputes. Online dispute resolution (ODR), defined as "a means of dispute settlement whether through conciliation or arbitration, which implies the use of online technologies to facilitate the resolution of disputes between parties", is gaining momentum as a desirable extra-judicial (alternative dispute resolution or ADR) procedure to settle low-value or cross-border disputes. For example, Ebay/Paypal have built an ODR system that handles approximately 60 million disputes a year (Rule and Nagarajan, 2010). Some private companies and governments have built efficient online dispute resolution schemes, such as ConciliaNet (http://concilianet.profeco.gob.mx) run by PROFECO in Mexico. The Organization of American States (OAS) has been exploring the issue of building a dispute resolution scheme for small-value online transactions for several years. In 2010, the United States has proposed the establishment of a working group to consider online dispute resolution at UNCITRAL, whereby payment card issuers would consider consumer claims against vendors for unauthorised charges, non-delivery or non-conformity of goods and services.[201]

However, several challenges remain. First, consumers may not be adequately informed of the availability of such offline or online procedures, particularly when there are complex chains of contracts involving several stakeholders.[202] Another challenge is mechanisms able to handle problems involving cross-border transactions. Yet another is to design processes that are viable for low-value transactions.

Voluntary codes of conduct for alternative payment providers

Consumers incur intangible costs related to inconvenience, worry and time lost as a result of online fraud or disputes with merchants. But while consumers' financial liability for the unauthorised use of their payment card is limited if they use traditional payment mechanisms, it may not be if they use alternative payment providers. Depending on the modalities of their rights to redress, they may in some cases incur substantial tangible costs (Federal Trade Commission (2005).[203]

Many OECD countries have voluntary codes of conduct or voluntary best practices for alternative, including mobile, payment providers. In the United States for example, the wireless industry has developed a set of voluntary best practices for mobile financial services providers. The CTIA (Wireless Association) guidelines call for mobile financial services providers voluntarily to create policies that, at a minimum, limit customer liability. CTIA states that, is cases of unauthorised use of the mobile device, "[s]uch policies should, at a minimum, comply with liability caps required under existing legal requirements (*e.g.* 50 USD or other applicable liability cap for unauthorised credit card transactions or electronic funds transfers)".

However, the guidelines are voluntary and do not have the force of law. Moreover, there are wide variations between industries and between jurisdictions, as well as significant loopholes. For example, some claim that the CTIA guidelines on the issue of dispute resolution are vague. Many consumer

advocates argue that the same level of consumer protection should be guaranteed for any payment service, regardless of the technology or business organisation involved (MacCarthy and Hillebrand, 2010). Others take the view that there are benefits to allowing these new payment systems to develop and innovate without the same legal requirements.

Lessons learned

Overall, the policy objectives of policy makers and online payment intermediaries are often aligned, as both have a strong interest in developing a robust online marketplace. Payment intermediaries may wish to allay consumers' concerns about security and redress so as to trigger repeat purchases. In addition, payment system intermediaries are often in a position to detect and deter payment fraud and to provide dispute resolution and redress mechanisms that raise consumer confidence. The increasing development and deployment of new types of online payment mechanisms may nonetheless raise new challenges for policy makers, merchants, consumers and other actors in the online marketplace.

For *online payment fraud*, the main lessons learned from this case study are:

- Online fraud is increasing as traditional payment systems implement measures such as chip and PIN in some jurisdictions to increase the security of offline transactions.
- More detailed information is needed on the nature and extent of online payment fraud. Lack of detailed and comparable data on the extent and characteristics of online payment fraud makes it difficult to develop effective industry strategies and policy responses. There is a role for policy making in monitoring how the payment industry co-ordinates security efforts in the online context.
- Most OECD countries limit the liability of users of traditional payment systems for unauthorised payment, but do not have similar liability limitations in place for alternative payment systems.
- While alternative payment systems' voluntary practices and codes of conduct help to limit consumer liability for unauthorised use, countries should consider whether to harmonise and extend limitations on consumer liability for unauthorised use to all payment systems involved in e-commerce.
- In online transactions, traditional payment systems assign liability for unauthorised use to e-commerce merchants. Several industry measures are available to help reduce online fraud**,** often developed by payment card networks and financial institutions and implemented by online merchants. Further development of means of fraud prevention and reduction for all types of payment systems is desirable.
- When examining current liability regimes for all types of online payment mechanisms, policy makers should focus on aligning risks with the parties best able to make efficient decisions on how to mitigate them, so that all parties have adequate incentives to invest in online payment fraud reduction.

For *dispute resolution and redress* the main lessons are:

- Legal requirements to provide dispute resolution and redress vary by type of payment mechanism and by jurisdiction. Governments should consider whether and to what extent it would serve policy objectives to extend and harmonise consumer protection for different types of payment mechanisms, including mobile, and across jurisdictions, and to what extent consumer protection should be tailored to the different types of payment mechanisms and legal frameworks.
- Voluntary codes of conduct can offer important protection for consumers. However, variations in the protection customers are entitled to can make it difficult for them determine the protection that applies to new payment services.

- Legal requirements for payment card companies to provide processes for resolving disputes between cardholders and merchants have given the industry an incentive to develop effective business-to-consumer (B2C) dispute resolution mechanisms.
- Payment card chargeback mechanisms that implement these legal requirements can provide an effective method of redress for consumers in the online marketplace.
- Online dispute resolution (ODR) is considered a promising way to provide effective (easy-to-use, less expensive, faster) consumer redress, in particular for cross-border and low-value transactions.

REFERENCES

Banque de France, Observatoire de la sécurité des paiements, *Rapport Annuel 2009*, www.banque-france.fr/observatoire/rap_act_fr_09.htm.

CyberSource (2010a), *Online Fraud Report*, 11th Annual Edition, http://forms.cybersource.com/forms/FraudReport2010NACYBSwwwQ109.

CyberSource (2010b), *6th Annual UK Online Fraud Report,* http://img.en25.com/Web/CyberSource/uk_online_fraud_report_2010%20web.pdf.

Douglass, D. (2009), "An examination of the fraud liability shift in consumer card-based payment systems", Federal Reserve Bank of Chicago.

ECC NET (2010), *The European Online Marketplace: Consumer Complaints 2008 – 2009*, August, www.consumenteninformatiepunt.nl/bin/binaries/13-102-ecc_brochure2010-final-lage-resolutie--2-.pdf.

Federal Trade Commission (2005), "BJ's Wholesale Club Settles FTC Charges", 16 June www.ftc.gov/opa/2005/06/bjswholesale.shtm.

Focus (2009), *Pocket Shopping*, www.consumerfocus.org.uk/assets/1/files/2009/06/Pocketshopping.pdf.

Innopay (2010), "Online payments 2010 - Increasingly a global game", http://www.europeanpaymentscouncil.eu/knowledge_bank_download.cfm?file=Online%20payments%202010%20-%20Report%20Innopay.pdf.

MacCarthy, M. (2010), "Information Security Policy in the U.S. Retail Payments Industry", http://works.bepress.com/cgi/viewcontent.cgi?article=1002&context=mark_maccarthy.

MacCarthy, M. and G. Hillebrand (2010), "Mobile Payments Need Strong Consumer Protections", *American Banker Tuesday*, 10 August, www.defendyourdollars.org/2010/08/mobile_payments_need_strong_ru.html.

OECD (2002), "Report on Consumer Protections for Payment Cardholders", OECD Digital Economy Papers, No. 64, OECD Publishing. http://dx.doi.org/10.1787/233364634144

OECD (2006), "Consumer Dispute Resolution and Redress in the Global Marketplace", www.oecd.org/dataoecd/26/61/36456184.pdf.

OECD, "Consumer Protection in Online and Mobile Payments", internal working document.

Philips, T. (2010), "Friend and Foe? Combating E-Commerce 'Friendly Fraud'", *E-Commerce Times*, 17 August, www.ecommercetimes.com/story/70630.html.

Rule, C. and C. Nagarajan (2010, "Leveraging the Wisdom of Crowds: the eBay Community Court and the Future of Online Dispute Resolution", *ACResolution Magazine,* Winter, http://ec.europa.eu/consumers/ policy/developments/acce_just/acce_just07workdoc_en.pdf.

Servired (2010), *Annual Report 2009*, www.servired.es/ingles/pdf/annual_report09.pdf.

Sullivan, R. (2010), "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options", *Kansas City Fed, Economic Review* - Second Quarter.

OTHER INTERNET INTERMEDIARY-RELATED POLICY ISSUES / COMPETITION

Internet intermediaries function as platform providers in two-sided markets. Numerous economic analyses have shown that their markets are subject to substantial network effects and economies of scale. Both of these economic characteristics create a tendency toward market concentration. As a result, the application of competition policy will take on a different dimension. These issues, however, are out of the scope of the present report. Competition policy and telecommunications issues are being investigated in more depth by the OECD Working Party on Communication Infrastructures and Services and as part of national initiatives such as the National Broadband Plan in the United States and similar initiatives in other OECD countries.

ANNEX 1.

EXAMPLES OF ISSUES RELATED TO INTERNET INTERMEDIARIES' ROLE

Internet actors	Potential issues	Examples of market, regulatory and self-regulatory questions that may arise	Sample OECD work
Internet access and service providers	Internet access, copyright, security threats, child protection, freedom of speech, due process and privacy, network neutrality	- identifying customers engaged in allegedly illegal or unauthorised activities. - notifying users regarding allegedly unauthorised material. - combating spam and other security threats. - informing customers of data breaches that might affect personal data. - investigating technical measures to block illegal content (*e.g.* child abuse sites) or allegedly infringing content (*e.g.* copyright material).	*Communications Outlook 2009* Ongoing WPISP work on malware
Data processing and web hosting providers[1]	Access to information, copyright, security threats, defamation, child protection, illegal content	- having "knowledge" of unauthorised or illegal character of content diffused on hosts' platforms. - determining legitimate vs. illegal character of content. - investigating technical measures to prevent unauthorised content. - being able to qualify legally different types of hosts *e.g.* the cases in which hosts can also be considered to be "editors", "advertisers", etc.	
Including domain name registrars	Security threats, especially phishing and spam,[2] consumer protection, trademarks (cybersquatting)	- withdrawing domain name services from users conducting illegal activities,[3] *e.g.* phishing.[4] - prohibiting or minimising the use of fast-flux domains (domains for which the IP address fluctuates rapidly to avoid detection and take-down) to help fight malware.	OECD (2008), "Scoping Paper on Online Identity Theft", [DSTI/CP(2007) 3/FINAL]
Internet search engines and portals	Free flow of information, user choice, trademark, copyright, counterfeiting, security threats, click fraud, defamation, privacy	- developing industry standards and codes of conduct. - excluding some types of content from search results to comply with national legislations' treatment of illegal content. - hyperlinking/providing access to potentially illegal material and activities. - providing thumbnails of allegedly unauthorised material. - abiding by notice and take-down letters for copyright infringements and the effectiveness of counter-notification mechanisms. - advertising companies using third parties' trademarked terms as keywords. - being able to legally qualify participative search engines, *e.g.* as a host and/or as an advertiser or editor.	*Information Technology Outlook* 2008
E-commerce platforms	User choice, consumer protection, counterfeiting, taxation	- developing community standards and associated rules. - determining whether sellers are businesses or individuals (*e.g.* to determine relevant consumer protection and taxation regimes). - identifying counterfeit goods being offered via auction platforms and respective roles of rights owners, notices and auction platforms in reducing their availability. - informing customers of data breaches that might affect personal data. - being able to legally qualify auction platforms.	Ongoing CCP work in reviewing e-Commerce Guidelines
E-commerce payment systems	Illegal gambling, security threats, child protection, identity and privacy	- cutting off payment to merchants engaged in illicit activity; *e.g.* to e-casinos in jurisdictions where online gambling is illegal or to merchants storing allegedly improper/infringing content or engaging in fraud. - informing customers of data breaches that might affect personal data.	Ongoing WPISP work on malware
Participative Web platforms	Copyright, identity and privacy, defamation, child protection	- developing community standards and associated rules. - being able to legally qualify participative web platforms (*e.g.* as a host and/or as an editor).	OECD (2007), "Participative Web: User-created content"

1. Providers strictly of data processing services face a different set of issues from hosting providers.

2. Research has shown that most spam and malware originates from just a few registrars

3. Domain name registrars have standard domain name registration agreements prohibiting domain name use for 'illegal purposes'. *E.g.*, the eNom Registration Agreement at www.enom.com/terms/agreement.asp.

4. See www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf.

ANNEX 2

TRANSPOSITION OF THE 2000 EC E-COMMERCE DIRECTIVE INTO NATIONAL LAW

OECD COUNTRIES	LEGISLATIONS
Belgium	Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information
Denmark	Electronic Commerce Act 22 April 2004
Finland	Act of June, 5, 2002
France	Loi n° 575 du 21/6/2004 pour la confiance dans l'économie numérique
Greece	Administrative measures 131 FEK A n°116 16 May 2003
Ireland	European Communities (Directive 2000/31/EC) Regulations 2003
Italy	Legislative decree 9 April 2003. Implementation of Directive 2003/31/EC on certain legal aspects of information society services in the internal market.
Luxemburg	Loi du 14 août 2000 relative au commerce électronique
Poland	9 September 2002
Portugal	Decree-Law No.7/2004 of January 7
Spain	Law 34/2002, 11 July, services of the information society and electronic commerce
Sweden	Law on Electronic Commerce and other Information Society Services of 26 June 2002
United Kingdom	The Electronic Commerce Regulations of August, 21st, 2002

TRANSPOSITION OF THE DIRECTIVE ON THE HARMONISATION OF CERTAIN ASPECTS OF COPYRIGHT AND RELATED RIGHTS IN THE INFORMATION SOCIETY OF MAY 2001

OECD COUNTRIES	LEGISLATIONS
Austria	1 July 2003
Belgium	Loi du 22 mai 2005 transposant en droit belge la Directive européenne 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information
Denmark	Act no 1051 of 17 December 2002
Finland	Law 14.10.2005/821, amending the Copyright Act
France	Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information
Germany	Act amending the Law on Copyright and Related Rights 1965 of 10 September 2003
Greece	Article 81 of Law 3057/2002 (Amendment and Completion of Law 2725/1999, regulation of matters pertaining to the Ministry of Culture and other provisions)
Hungary	Act CII amending the Copyright Act 1999
Ireland	Statutory instrument No. 16/2004 (European Communities (Copyright and Related Rights) Regulations 2004
Italy	Legislative decree No. 68 of 9 April 2003 amending the Basic Copyright Law Act (Act No. 633 of 22 April 1941 as amended)
Luxembourg	Act amending the Law on Author's Rights, Related Rights and Databases (18 April 2004)
Netherlands	Act of 6 July 2004 amending the Copyright Act
Poland	Act of 1 April 2004 on the alteration of the Law on Copyright and Neighbouring Rights (2004 Act)
Portugal	Law 50/2004 of 24 August 2004
Slovakia	Act No. 618/2003 of 4 December 2003
Spain	Ley 23/2006 de 7 julio, B.O.E. num. 162, 8 julio 2006
Sweden	Government Bill no 2004/2005:110, amending Act 1960:729 on Copyright in Literary and Artistic Works of 30 December 1960
United Kingdom	Statutory Instrument SI 2003/2498 ("The Copyright and Related Rights Regulations 2003)

NOTES

1 OECD(2010), The Economic and Social Role of Internet intermediaries, at www.oecd.org/dataoecd/49/4/44949023.pdf. Not all entities that provide Internet-based services to third parties are intermediaries between third parties, for example financial intermediaries.

2 *Cubby v CompuServe* 766 F Supp 135 (SDNY, 1991), was one of the earliest cyberlaw cases to be decided, in 1991.

3 For historical context, see earlier discussion of these issues by Edwards (2000).

4 Secondary liability, or indirect infringement, arises when a party materially contributes to, facilitates, induces or is otherwise responsible for directly infringing acts carried out by another party.

5 BT Internet estimated in 1999 that to effectively monitor just news-group traffic, they would have had to hire 1 500 new employees working 24 hours a day. See *WIPO Workshop on Service Provider Liability*, Geneva, 9-10 December 1999, paper by Janet Henderson, Rights Strategy Manager, BT Internet.

6 Technology has evolved over the past decade, and new technologies such as audio fingerprint technology digital file identification are now available.

7 *LICRA et UEJF vs Yahoo! Inc and Yahoo France* (20 November 2000, Tribunal de Grande Instance de Paris, Superior Court of Paris). Around 70% of user's country of origin could be established from IP address and the remaining 20% or so could be obtained by asking users to fill in a form declaring country of origin.

8 In fact the US courts took a middle way in two early decisions. See discussions in *Cubby v CompuServe* 766 F Supp 135 (SDNY, 1991) *and Stratton Oakmont Inc v Prodigy Services* LEXIS 229 (NY Sup Ct, Nassau Co., 1995).

9 OCILLA is sometimes colloquially called "Section 512", which is its statutory citation in the US Code, 17 U.S.C. § 512.

10 2000/31/EC, passed 8 June 2000. The ECD was implemented in the United Kingdom via the Electronic Commerce (EC Directive) Regulation 2002, SI 2002/2013, largely taken verbatim from the European English text.

11 Article 2(a) of the ECD refers back to the definition in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. The definition is discussed further in Recitals 17 and 18 of the ECD.

12 However the requirement that an information society service be offered "at the individual request of the recipient" means that TV and radio broadcasters do not fall within the remit of the ECD liability regime, although sites that offer individually on-demand services such as video-on-demand or email are included. See Recital 18, ECD.

13 A UK court upheld the view that Google, the search engine, qualified as an information society service provider in *Metropolitan v Google* [2009] EWHC 1765 (QB). A French court has found Wikipedia, the free online encyclopedia, to be deserving of intermediary service provider immunity: see OUT-Law news report of 6/11/2007, at www.outlaw.com/page-8615.

14 Copyright Act, R.S.C., ch. C-42, §2.4(1)(b).

15 *Society of Composers, Authors and Music Publishers of Can. v Canadian Assoc. of Internet Providers*, [2004] S.C.C. 45, 240 D.L.R. (4th) 193, ¶92.

16 Proposed Bill C-32 would significantly modify the current system in Canada.

17 See www.aph.gov.au/parlinfo/billsnet/99077.pdf.

18 See http://en.wikipedia.org/wiki/Icelandic_Modern_Media_Initiative.

19 This case was settled so no opinion was given.

20 The growth of the advertising revenue model is discussed in Perset, 2010.

21 www.facebook.com/press/info.php?statistics; www.youtube.com/t/fact_sheet, accessed July 2010.

22 OUT-Law, 1/07/2008, available at www.out-law.com/page-9225.

23 *Tiffany (NJ) Inc v eBay,* US District Court of NY, SD Ny, No 04 Civ.4607(RJS). The United States Court of Appeals, Second Circuit affirmed: *Tiffany (NJ) Inc. v eBay Inc*., 08-3947-cv, Apr. 1, 2010.

24 *L'Oréal v eBay* [2009] EWHC 1094 (Ch) (22 May 2009). Although the case is still pending as a reference to the ECJ, the questions asked of the ECJ by the English court have been finalised, www.cpaglobal.com/newlegalreview/4213/ecj_reveals_terms_ebay_probe.

25 *Google France, Google, Inc. v Louis Vuitton Malletier (C-236/08), Viaticum SA, Luteciel SARL (C-237/08), Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08), etc, Joined cases,* Judgment of the Court (Grand Chamber), 23 March 2010, http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-236/08.

26 Original Complaint, *Viacom International v YouTube*, Inc No 1:2007- CV- 02103 (S.D.N.Y Mar 13, 2007). See case documents at http://news.justia.com/cases/featured/new-york/ nysdce/1:2007cv02103/302164.

27 *Viacom International v YouTube Inc* 2010 WL 2532404 (SDNY June 23, 2010).

[28] www.nytimes.com/2010/06/24/technology/24google.html?scp=1&sq=YouTube%20viacom&st=cse. screen.html?_r=1&nl=technology&emc=techupdateema1.

[29] www.youtube.com/t/contentid.

[30] www.twobirds.com/english/publications/newsletters/upload/43288_1.htm.

[31] In a decision dated 13 July 2007 of the Tribunal de Grande Instance of Paris.

[32] [1999]4 All ER 342. The case preceded implementation of the ECD but was dealt with under a similar set of rules in the UK Defamation Act 1996, section 1. 1996 Act, section 1(1)(c).

[33] Discussion in C. Ahlert, C. Marsden and C. Yung, "How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation" ("*Mystery Shopper*") at http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf.

[34] Urban J. and L. Quilter, "Efficient Process or 'Chilling Effects'? Take-down Notices Under Section 512 of the Digital Millennium Copyright Act: Summary Report", http://mylaw.usc.edu/documents/512Rep-ExecSum_out.pdf.

[35] Because OSPs are encouraged to remove content upon receipt of a notice alleging infringement, but are not required to put back content that may have been removed due to mistake or mischief, some claim that the DMCA's notice and take-down regime provides an asymmetric level of protection to rights holders. www.chillingeffects.org.

[36] Online Policy Group v Diebold, Inc., 337 F. Supp. 2d. 1195 (N.D. Cal. 2004).

[37] S 512 (d) Information Location Tools.

[38] See UK *Consultation document on the electronic commerce directive: the liability of hyperlinkers, location tool services and content aggregators - Government response and summary of responses* DTI, December 2006.

[39] See for example Pasquale F., "Copyright in an Era of Information Overload: Towards The Privileging of Categorisers" (2007) 60 *Vand. L Rev* 135.

[40] A French court (the Tribunal de Grande Instance de Nanterre) is believed to be the only European court to have found a website liable for reproducing an RSS feed of content which was found to be in breach of privacy rights, 18/04/2008, www.out-law.com/page-9058.

[41] Arguably one of the few such examples is the Belgian copyright case of *Copiepresse. Copiepresse v Google* [2007] ECDR 5, Brussels Court of First Instance (TGI), 13 February 2007.

[42] Google as a host in *Google v LVMH* (C-236/08).

[43] *A&M Records, Inc v, Napster Inc*, 239 F3d 1004 (9th Cir, 2001).

[44] http://thepiratebay.org.

[45] *Sony and Ors v Neij*, Stockholm District Court, Division 5, Unit 52, VERDICT B 13301-06, 17 April 2009 handed down in Stockholm, Case no B 13301-06. Unofficial English translation commissioned by the IFPI, available at www.ifpi.org/content/library/Pirate-Bay-verdict-English-translation.pdf.

[46] See ECJ decision in *Promusicae v Telefonica* C-275/06 Judgment (OJ) OJ C 64 of 08.03.2008, p.9.

[47] There have already been complaints that YouTube's Content ID system wrongly blocks videos from being uploaded which only contain a small portion of an infringed original, or where it is used in some transformative way *e.g.* in a remix, which US fair use would sometimes allow.

[48] Microsoft researchers teamed with Hany Farid of Dartmouth University to develop a technique to calculate the distinct characteristics of a digital image to match it with other copies of that same image, even if the image has been altered such as through re-sizing or editing. PhotoDNA is now in use by NCMEC to assign a unique signature, called a hash, to each image of child abuse. The hash data are shared with online service providers to match against photos found on their services and tag them for removal.

[49] 2004 WL 1632047 (Cal App 2nd Dist, 22 July 2004). EBay was sued for defamatory remarks made on its auction site by a disgruntled bidder in respect of another user of the site. But although eBay lost on CDA immunity, having been found not to be a publisher of information but a distributor, they still were held not liable because their contractual terms successfully excluded liability.

[50] *Fair Housing Council of San Fernando Valley, et al. v Roommates.com* LLC 489 F.3d 921, CV-03-09386-PA (9th Cir., May 15, 2007) aff'd en banc 2008 WL 879293 (9th Cir., April 3, 2008).

[51] *Doe v Friendfinder Network, Inc.*, 540 F.Supp.2d 288 (D.N.H. 2008).

[52] *Barnes v Yahoo!, Inc.*, 2009 WL 1232367 (9th Cir. May 7, 2009).

[53] http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.

[54] www.geek.com/articles/apple/apples-app-store-success-hasnt-stopped-prices-tumbling-20090225/#ixzz0qAKsKkXV

[55] http://blogpulse.com/

[56] In practice, self-regulatory activity has also taken place in cases where some form of statutory law is present. Regulators have become increasingly adept at securing voluntary agreements in areas relevant to public policy, partly out of intermediaries' desire to forestall more intrusive regulation.

[57] Universal Declaration on Human Rights, Article 19, www.un.org/en/documents/udhr/index.shtml#a19 and UN's Millennium Development Goals, www.un.org/millenniumgoals.

[58] http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021808.htm.

[59] Freedom House (2009), Freedom on the Net, March.

[60] www.ntia.doc.gov/internetpolicytaskforce.

[61] Laws in OECD countries regarding the blocking or removal of copyright infringing material do not generally fall into this category. Statutory provisions to facilitate action against Internet piracy and other illegal activity are an appropriate part of a balanced legal intellectual property framework.

[62] Universal Declaration on Human Rights, Article 19, op-cit.

63 OpenNet Initiative, Access Controlled, April 2010, C.M. Maclay, Chapter 6, "Protecting Privacy and Expression Online, Can the Global Network Initiative Embrace the Character of the Net?", www.access-controlled.net/wp-content/PDFs/chapter-6.pdf.

64 www.google.com/governmentrequests.

65 International Covenant on Civil and Political Rights, Article 19, www2.ohchr.org/english/law/ccpr.htm.

66 www.globalnetworkinitiative.org/principles/index.php.

67 Including "actions necessary to preserve national security and public order, protect public health or morals, or safeguard the rights or reputations of others", related interpretations issued by international human rights bodies, and the Johannesburg Principles on National Security, Freedom of Expression, and Access to Information.

68 www.globalnetworkinitiative.org/governanceframework/index.php.

69 Congressional Research Service (2010), U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology, April, http://assets.opencrs.com/rpts/R41120_20100405.pdf.

70 OpenNet Initiative, Access Controlled, April 2010, C.M. Maclay, Chapter 6, "Protecting Privacy and Expression Online, Can the Global Network Initiative Embrace the Character of the Net?", www.access-controlled.net/wp-content/PDFs/chapter-6.pdf.

71 Comments by Dominique Lamoureux from THALES at the Conference on "Internet et liberté d'expression", organised in Paris on 8 July 2010 by the French and Dutch Ministries for Foreign Affairs.

72 APEC project proposal, http://aimp.apec.org/Documents/2010/TEL/TEL41-SPSG-WKSP1/10_tel41_spsg_wksp1_006.pdf.

73 http://krebsonsecurity.com/2010/03/talking-bots-with-japans-cyber-clean-center.

74 House of Representatives Standing Committee on Communications – Inquiry into Cyber Crime, Supplementary submission from AusCERT, Australia's National Computer Emergency Response Team, www.auscert.org.au/download.html?f=498.

75 http://krebsonsecurity.com/2010/03/talking-bots-with-japans-cyber-clean-center.

76 When a client asks to resolve the address of such a host or domain, the sinkhole returns a non-routable address or another address that is not the real address.

77 The Korean government through the Korea Communications Commission (KCC).

78 Report on July DDoS attack in Korea and Korea's countermeasure, KISA and KrCERT/CC, 26 January 2010, http://elec.sch.ac.kr/inco-trust/pt/20100126-77ddos%20presentation-YoungBaekKim.pdf.

79 www.oecd.org/document/62/0,3343,en_2649_34223_44949886_1_1_1_1,00.html#position.

80 The Australian Federal Department of Broadband, Communications and the Digital Economy.

81 www.iia.net.au/index.php/section-blog/90-esecurity-code-for-isps/757-esecurity-code-to-protect-australians-online.html. Draft code available at www.iia.net.au/images/resources/pdf/esecurity_code_consultation_version.pdf.

82 www.acma.gov.au/WEB/STANDARD..PC/pc=PC_310317.

83 Presentation by Bruce Matthews at the APEC TEL 41 Workshop on Cyber Security Voluntary ISP Codes of Practice of 6 May 2010, from ACMA on the Australian Internet Security Initiative.

84 www.fcc.gov/Daily_Releases/Daily_Business/2010/db0809/DA-10-1354A1.pdf.

85 US Dept. of Commerce, Notice of Inquiry on Cybersecurity, Innovation, and the Internet Economy, 75 Fed. Reg. 44216, July 28, 2010.

86 www.fcc.gov/pshs/advisory/csric/wg-8.pdf.

87 www.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

88 Blogger content policy available at www.blogger.com/content.g

89 Testimony of Nicole Wong, Associate General Counsel, Google Inc., before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, United States House of Representatives, 27 June 2006.

90 eBay, Adult Only category policy, Items that can't be listed at all, http://pages.ebay.com/help/policies/adult-only.html.

91 For example, Visa International Operating Regulations at 4.1.C.5.b, http://usa.visa.com/download/merchants/visa-international-operating-regulations.pdf.

92 YouTube, Community Guidelines, www.youtube.com/t/community_guidelines.

93 Keeping Second Life Safe, Together, https://blogs.secondlife.com/community/features/blog/2007/06/01/keeping-second-life-safe-together; http://blogs.secondlife.com/community/features/blog/2007/11/14/clarification-of-policy-disallowing-ageplay#more-1379.

94 Testimony by Visa and MasterCard at United States House of Representatives, Committee on Energy and Commerce, Subcommittee on Oversight and Investigation, "Deleting Commercial Child Pornography Sites from the Internet: The U.S. Financial Industry's Efforts to Combat This Problem", 21 September 2006. (House Hearing)

95 See Senate Testimony of Ernie Allen, Chairman of the National Center for Missing and Exploited Children, United States Senate, Committee on Banking, Housing and Urban Affairs, "Combating Child Pornography by Eliminating Pornographers' Access to the Financial Payment System", 19 September 2006.

96 Financial Coalition against Child Sexual Abuse Content, Backgrounder, December 2009, www.missingkids.com/en_US/documents/FCACPBackgrounder.pdf.

97 See the description of the coalition, www.ceop.police.uk/efc/piwg/.

98 Dutch Notice-and-Take-Down Code of Conduct, October 2008, www.samentegencybercrime.nl/UserFiles/File/NTD_Gedragscode_Opmaak_Engels.pdf.

99 ACMA (2008, p. 46). The Internet Safety Technical Task Force did not evaluate network-level filtering. Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social

Networking of State Attorneys General of the United States, December 2008 Appendix D, p. 10, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_D_TAB_and_EXHIBITS.pdf.

100 *Center for Democracy & Technology v Pappert* Case No. 03-5051 (E.D. Pa. Sept. 10 2004).

101 Office of Attorney General of New York State, Attorney General Cuomo Announces Unprecedented Deal with Nation's Largest Internet Service Providers to Block Major Sources of Child Sexual Abuse Content, 10 June 2009 www.nystopchildporn.com/press_releases/2008/june/10a.html.

102 www.interpol.int/Public/ICPO/GeneralAssembly/AGN78/resolutions/AGN78RES05.pdf.

103 Article 21, European Commission, Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child sexual abuse content, repealing Framework Decision 2004/68/JHA, 20 March 2010 p. 24, http://ec.europa.eu/justice_home/news/intro/doc/com_2010_94_en.pdf.

104 Department of Broadband, Communications, and the Digital Economy ISP Filtering, 10 March 2010 www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering.

105 www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot.

106 www.dbcde.gov.au/funding_and_programs/cybersafety_plan/transparency_measures/consultation_paper.

107 Senator Stephen Conroy, Minister for Broadband, Communications, and the Digital Economy, Media Release, 9 July 2010, www.minister.dbcde.gov.au/media/media_releases/2010/068.

108 Internet Industry Association Feasibility Study – ISP Level Content Filtering, February 2008, www.dbcde.gov.au/__data/assets/pdf_file/0006/95307/Main_Report_-_Final.pdf.

109 eBay, Adult Only Category Policy – Additional Information, http://pages.ebay.com/help/policies/adult-only.html#additional.

110 YouTube, "Inappropriate Content: Age-Restricted Videos", http://help.youtube.com/support/youtube/bin/answer.py?answer=117432&topic=10551.

111 Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, December 2008, p. 29, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

112 Internet Gambling Act 2001, at www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/current/bytitle/0A26E04ABE95D0BBCA25702600018A62?OpenDocument&mostrecent=1.

113 H.R. 3125, http://thomas.loc.gov/cgi-bin/query/D?c106:2:./temp/~c106mktqmw.

114 See the floor debate on H.R. 3125 CR H6057-6068, 17 July 2000.

115 Unlawful Internet Gambling Enforcement Act of 2006, enacted as Title VIII of the Security and Accountability for Every Port Act of 2006, on 12 October 2006, Pub. L. No. 109–347, 120 Stat. 1884, and codified at 31 U.S.C. 5361–5367.

116 United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services - AB-2005-1 - Report of the Appellate Body, WT/DS285/AB/R, 05-1426, 7 April 2005.

117 WhichPoker.com, www.whichpoker.com/stats/UIGEAEffects.

118 Pfanner and Timmons (2006). The basis for this decline in share value was the withdrawal of these firms from the lucrative US market and the perception that they would not be able to recover the revenue lost from non-US customers.

119 Associated Press, *Online Gambling Shares Fall as Congress OKs Bill*, Foxnews.com, 3 October 2006 www.foxnews.com/printer_friendly_story/0,3566,217039,00.html.

120 H2 Gambling Capital at www.h2gc.com/news.php.

121 Chan (2010). The text of the revised legislation is available at http://financialservices.house.gov/Media/file/markups/7_28_2010/Amendments--HR%202267/Frank12.pdf.

122 In the United States under current law gambling licences are issued by the states and are limited to a specific geographic area. Internet gambling is inherently interstate which brings in the national government.

123 Olswang LLP, "Gambling News, News from Around Europe", 22 March 2010, www.olswang.com/newsarticle.asp?sid=110&aid=2926.

124 Bloomberg News, "France opens gambling industry to competition with online betting licenses", 7 April 2010, www.financialpost.com/scripts/story.html?id=2771459#ixzz0ksP7o285.

125 United Kingdom Gambling Act, Chapter 19, www.opsi.gov.uk/acts/acts2005/ukpga_20050019_en_1.

126 Council of Europe, French EU Presidency Report, Gambling and betting: legal framework and policies in the Member States of the European Union 27 November 2008, register.consilium.europa.eu/pdf/en/08/st16.

127 European Parliament resolution of 10 March 2009 on the integrity of online gambling at www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0097+0+DOC+XML+V0//EN&language=EN.

128 http://ec.europa.eu/internal_market/iprenforcement/index_en.htm.

129 17 U.S.C. §512, www4.law.cornell.edu/uscode/17/512.html.

130 *E.g.* Facebook Statement of Rights and Responsibilities,t www.facebook.com/terms.php.

131 Higher Education Opportunity Act, PL 110–315 (14 August 2008), Section 488(a)(1)(E).

132 Article 14 (1), Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF.

133 IFPI, Digital Music Report 2009, www.ifpi.org/content/library/dmr2009.pdf.

134 "Three Strikes Rule: Sleeping for Seven Months", Heesop's IP Blog, 10 March 2010, http://hurips.blogspot.com/2010/03/three-strikes-rule-sleeping-for-seven.html.

135 Persons who misrepresent that material is infringing are liable for damages. The burdens on filing counter-notices are procedural and legal. Those contemplating filing a counter-notice must be prepared for legal action. Under the DMCA, a person who files a counter-notice must include contact information, a signature, a statement under penalty of perjury that the "material was removed or disabled as a result of a mistake or misidentification", and consent to the jurisdiction of his/her local federal court (if the copyright owner elects to sue), www.eff.org/issues/intellectual-property/guide-to-youtube-removals.

136 *Viacom International v YouTube Inc* 2010 WL 2532404 (SDNY June 23, 2010).

137 http://news.viacom.com/news/Pages/summaryjudgment.aspx.

138 Press Release, Internet and Media Industry Leaders Unveil Principles to Foster Online Innovation While Protecting Copyrights, 18 October 2007, www.ugcprinciples.com/press_release.html.

139 See YouTube Terms of Service, Account Termination Policy, www.youtube.com/t/terms.

140 YouTube Copyright Policy: Video Identification Tool, www.google.com/support/youtube/bin/answer.py?answer=83766.

141 Testimony of Derek Slater, Senior Policy Analyst, Google, Inc., before the National Academy of Sciences Committee on the Impact of Copyright Policy on Innovation in the Digital Age, 15 October 2010.

142

143 Presentation by Bell Canada, Copyright Consultations, 27 August 2009, www.ic.gc.ca/eic/site/008.nsf/eng/h_04034.html, note 8.

144 Sections 41.25-27 of CB-32, introduced 2 June 2010, www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4580265&file=4.

145 Comments of Verizon in Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement: Request of the Intellectual Property Enforcement Coordinator for Public Comments Regarding the Joint Strategic Plan (Federal Register Volume 75, Number 35 – FR Doc. 2010-3539), 24 March 2010.

146 Comments of AT&T in Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement: Request of the Intellectual Property Enforcement Coordinator for Public Comments Regarding the Joint Strategic Plan (Federal Register Volume 75, Number 35 – FR Doc. 2010-3539), 24 March 2010, www.whitehouse.gov/omb/IPEC/frn_comments/AT_T.pdf (Comments of AT&T).

147 www.irishtimes.com/newspaper/frontpage/2009/0129/1232923373331.html.

148 The Telecommunication Carrier's Forum has released a draft of their Internet Service Provider Copyright Code of Practice for public consultation, www.tcf.org.nz/library/2e53bf81-d6c4-4735-9ed0-740e8b2c6af3.cmr.

149 For example, the Italian Data Protection Authority has ruled that the activity of monitoring peer-to-peer users for the purposes of prosecuting alleged copyright infringements is illegal.

150 Cheng (2009). Their proposed copyright initiative in October 2009 specifically excluded graduated response (see Sparh, 2009)

151 An ongoing court case filed in 2009 in Ireland seeks to establish a graduated response regime in this fashion. In 2010, an Australian court declined to do this.

152 OECD Broadband statistics, www.oecd.org/sti/ict/broadband.

153 "Facts and Figures on Copyright Three-Strike Rule in Korea", Heesop's IP Blog, 24 October 2010, http://hurips.blogspot.com/2010/10/facts-and-figures-on-copyright-three.html.

154 European Parliament, Press Release, Telecoms package conciliation: MEPs and Council representatives agree on internet access safeguards, 10 November 2009, www.europarl.europa.eu/news/expert/infopress_page/052-63798-309-11-45-909-20091105IPR63793-05-11-2009-2009-true/default_en.htm.

155 "L'Hadopi veut envoyer jusqu'à 2 000 mails par jour d'ici la fin de l'année", *Le Monde*,, 26 October 2010, www.lemonde.fr/technologies/article/2010/10/26/la-hadopi-veut-envoyer-jusqu-a-2-000-mails-par-jour-d-ici-la-fin-de-l-annee_1431496_651865.html

156 Budget 2009, Ministère de la Culture et de la Communication 26 septembre 2008 p. 43, www.culture.gouv.fr/culture/actualites/conferen/albanel/budget2009.pdf.

157 Pfanner (2010). The text of the law can be found at www.statutelaw.gov.uk/content.aspx?parentActiveTextDocId=3699621&ActiveTextDocId=3699682.

158 www.spcnetwork.co.uk/uploads/Broadband_Elasticity_Paper_2008.pdf.

159 Department for Business, Innovation and Skills, HM Government Response To The Consultation On Online Infringement Of Copyright (Initial Obligations) Cost Sharing, September 2010, www.bis.gov.uk/assets/biscore/business-sectors/docs/o/10-1131-online-copyright-infringement-government-response.

160 "Downloaders face disconnection after Eircom Settlement", *Irish Times*, 1 January 2009, www.irishtimes.com/newspaper/breaking/2009/0128/breaking81.html?via=rel.

161 See, for example, *EMI Records (Ireland) Limited et al. v. UPC Communications Ireland Limited*, High Court, Charleton J, 11 October 2010, www.scribd.com/doc/39104491/EMI-v-UPC.

162 BitTorrent is a peer-to-peer file sharing programme used to distribute very large files. It creates efficiencies by spreading the file downloading function among many different users of the programme.

163 In this case, there is some evidence that the ban was ineffective. Traffic from the ISP blocking the site was the same before and after the imposition of the ban, suggesting that users had used proxy servers or other ways to circumvent the blockages. See Chen, 2008)

164 Comments of AT&T in Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement: Request of the Intellectual Property Enforcement Coordinator for Public Comments Regarding the Joint Strategic Plan (Federal Register Volume 75, Number 35 – FR Doc. 2010-3539), 24 March 2010, www.whitehouse.gov/omb/IPEC/frn_comments/AT_T.pdf. See also Anderson (2010c).

165 See text and explanatory material at www.ustr.gov/acta.

166 INTA Submission on the Request for Public Comment Regarding the Joint Strategic Plan for IP Enforcement, for the Office of the Intellectual Property Enforcement Coordinator (IPEC) through the Office of Management and Budget, 24 March 2010, www.whitehouse.gov/omb/IPEC/frn_comments/InternationalTrademarkAssociation.pdf (INTA Submission).

167 See eBay's IP policy for a seller which excludes counterfeit goods available, http://pages.ebay.com/help/policies/intellectual-property-ov.html.

168 See the discussion of eBay's countermeasures in *Tiffany (NJ) Inc. v EBay Inc*. United States Court Of Appeals for the Second Circuit Docket No. 08-3947-Cv, 1 April 2010.

169 Testimony of Mr. Robert Chesnut, Senior Vice President, Rules, Trust and Safety, eBay, Inc., at the hearing, Organized Retail Theft Prevention: Fostering A Comprehensive Public-Private Response before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, US House Of Representatives, 25 October 2007, p. 26.

170 These best practices are described in INTA, "Addressing the Sale of Counterfeits on the Internet", September 2009, available as attachment 3 in the INTA Submission.

171 See account at OUT-Law, 1/07/2008, www.out-law.com/page-9225. See report at OUT-Law, 12/09/2007, www.out-law.com/page-8463.

172 But a Paris court seems to have reached the reverse decision in a very similar action by L'Oreal against eBay in respect of sale of counterfeit perfumes, reported 15 May 2009, www.guardian.co.uk/technology/2009/may/13/ebay-loreal-court-paris-counterfeit.

173 *Tiffany (NJ) Inc. v. eBay, Inc.,* No. 04 4607 (S.D.N.Y. July 14, 2008) (eBay District case).

174 eBay District case p. 2-3.

175 See *L'Oréal v eBay* [2009] EWHC 1094 (Ch) (22 May 2009). Although the case is still pending as a reference to the ECJ, the questions asked of the ECJ by the English court have been finalised: see www.cpaglobal.com/newlegalreview/4213/ecj_reveals_terms_ebay_probe.

176 http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm.

177 eBay District case p. 9.

178 See a critical assessment of this suggestion of "no safe harbour" for web 2.0 sites, in Lemley (2007).

179 Office of the US Intellectual Property Enforcement Coordinator, Intellectual Property Spotlight, December 2010, p. 1, www.whitehouse.gov/sites/default/files/omb/IPEC/spotlight/IPEC_Spotlight_December2010.pdf

180 Mobile contactless/point-of-sale payments can be thought of as a technological replacement of a consumer's wallet, whereas mobile remote payments are online payments through the tool of a mobile device. These two types of payments using mobile phones raise significantly different concerns, both in terms of usability and security and the consumer protection issues they raise.

181 E-Commerce Report 2009, *Trends in Consumer and Payment Behaviour in E-Commerce on the Basis of Real-Life Transactions*, Deutsche Card Services. Javelin Strategy & Research, February 2010, "Online Retail Payments Forecast 2010 ? 2014: Alternative Payments Growth Strong but Credit Card Projected for Comeback", https://www.internetretailer.com/2010/02/19/credit-cards-are-losing-some-luster-with-online-shoppers. In Mexico, according to the study annually carried out by the Mexican Association of Internet (AMIPCI) on e-commerce, credit cards are the primary mean of payment for online purchases at 74% of total payments in 2008.

182 http://paymentsviews.com/2009/03/11/ebay-analyst-day-paypal-world-domination/ and https://www.paypal-apac.com/sg/why-use-paypal/if-you're-selling.aspx. In the United States for example, PayPal accounted for 15.9% of online purchases in 2009 and was expected to account for nearly 20% of online purchases by 2014. PayPal had more than 87 million active registered accounts out of a total of 224 million total accounts. *The Internet Retailer*, 2010.

183 In South Korea for example, Danal allows consumers to purchase goods and services online by charging their regular mobile phone bills. Up to 60% of all online digital content purchases in Korea are now billed directly to mobile accounts. http://news.vzw.com/news/2010/03/pr2010-03-19m.html.

184 In April 2010, Juniper Research predicted that almost half of global mobile subscribers – both developed and developing nations – will pay by mobile for physical and digital goods and services (such as ticketing) by 2014, with the volume of m-payments representing 5% of global ecommerce retail sales by 2014 or some USD 630 billion, up from USD 170 billion in 2010, http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats#m-payments.

185 PSD, 2007/64/EC, which became law on 1 November 2009 for the European Union, Iceland, Norway and Liechtenstein. Korea and Mexico also have specific legal or regulatory provisions dealing with unauthorised charges to payment cards.

186 In the UK for example, the replacement of the swipe card by "chip and pin" led to a gradual decrease in the proportion of offline card fraud in 2009.

187 In the United Kingdom, for example, while the Office of Fair Trading licenses credit providers and the Financial Services Authority licenses deposit-taking institutions, payment providers do not necessarily fall into either of these categories and therefore are not eligible for licences and not subject to the supervision of these authorities.

188 It should be noted that in Europe PayPal is classified as a bank, while in the United States it is not.

189 *Consumer Reports Money Adviser* issue, May 2010. For example, EBillme offers refunds up to 90 days after the purchase date, but only for items that cost less than USD 500. It does not refund taxes or shipping costs.

190 MacCarthy and Hillebrand (2010). In Korea for example, Article 8 of the 2002 Consumer Protection Act on Electronic Transaction provides some obligations that apply to all payment providers (issuer of e-payment and e-settlement service provider) http://ftc.go.kr/data/hwp/no6687.doc. In Japan, the "Act Regulating Advanced Payment Certificates" provides some consumer protection for mobile payment services.

191 For example, Visa USA advertises a "zero liability" policy for US cardholders, which promises protection against liability for certain unauthorised credit or debit charges. Visa International has a global policy that requires issuers to implement a chargeback (refund) process for certain kinds of complaints.

192 The PCI version is available on the PCI website, https://www.pcisecuritystandards.org/index.shtml.

193 CVN, also known as CVV2 for Visa, CVC2 for MasterCard, and CID for American Express and Discover

194 Visa Europe, *Annual Report 2009*, www.visaeurope.com/en/about_us/annual_report.aspx.

195 Another example of a dynamic authentication payment security scheme is offered by Visa's *e-Carte Bleue* launched in France in 2002: each time a consumer wishes to purchase products online, a one-time fictitious credit card number is generated for disclosure to the merchant, who does not have access to the actual credit card number. In July 2010, Visa launched a new type of card ("*Visa CodeSure",* incorporating a tiny keypad and LCD-screen) which generates a dynamic passcode when a cardholder enters his PIN number for shopping online or logging in to an online banking service.

196 Merchants are liable for fraud unless they: *i)* performed an address verification at the time the transaction was authorised (*i.e.* verified that the person conducting the transaction could validate the billing address associated with the payment card being used); *ii)* delivered the purchased merchandise to an address that matches the address validated through the address verification; and *iii)* obtained proof that the purchased goods were delivered to the verified address.

197 For certain fraud-related chargebacks relating to the verified transaction, http://usa.visa.com/download/merchants/Visa_e-commerce_cross-border_handbook-Chapter_9-July_2010.pdf.

198 CyberSource (2010) comments on the relatively slow adoption of payer authentication programmes.

199 CyberSource (2010) found that 20% of merchants were interested in deploying these systems in the next 12 months as a new tool to manage fraud.

200 Cybersource (2010a). About half of fraud-coded chargebacks were contested by online merchants in the United States from 2005 to 2009, with merchants reportedly winning, on average, 42% of the chargebacks they disputed.

201 The proposal includes establishing: *i)* an online dispute resolution (ODR) initiative for electronic resolution of cross-border e-commerce consumer disputes; and *ii)* a draft model law for alternative dispute resolution of cross-border B2C e-commerce claims in which payment card issuers would be responsible for considering the claims of consumers against vendors for unauthorised charges, non-delivery or non-conformity of goods and services.

202 Research indicates that 46% of merchants do not provide information about responsibility rules for handling consumer disputes. See Consumer Focus (2009), p. 8.

203 The European Payment Services Directive (PSD) for example sets a limit of up to EUR 150 to be borne by consumers in a pre-notification period (Article 61 of PSD). In some countries, additional considerations such as consumer negligence can also lead to consumer liability.