PERSPECTIVES ON POLICY RESPONSES TO ONLINE COPYRIGHT INFRINGEMENT

An Evolving Policy Landscape

Internet Society

Table of Contents

INTRODUCTION . . . 1
THE INTERNATIONAL AND REGIONAL LANDSCAPE . . . 2
OVERVIEW AND OBSERVATIONS . . . 9
THE INTERNET SOCIETY'S ROLE . . . 12
BACKGROUND AND OBJECTIVES . . . 13
THE ISOC COPYRIGHT WORKING GROUP . . . 14
THE ANALYSIS . . . 15
COPYRIGHT INFRINGEMENT VIA THE INTERNET . . . 16
EMERGING INTERNET-FOCUSED POLICY RESPONSES . . . 18
DETECTING INFRINGEMENT AND IDENTIFYING INFRINGERS . . . 19
SUSPENSION OF INTERNET ACCESS . . . 22
- Graduated response . . . 22
- Infringement notices . . . 23
- National approaches . . . 26
- International negotiations . . . 38
- Examining suspension of Internet access as an enforcement measure . . . 42

TRAFFIC SHAPING . . . 50
- National approaches . . . 50
- Examining traffic shaping as an enforcement measure . . . 51

BLOCKING (IP address, URL, port and protocol) . . . 60
- Approaches to blocking . . . 60
- Examining blocking as an enforcement measure . . . 63

CONTENT IDENTIFICATION AND FILTERING . . . 75
- Examining content identification and filtering as an enforcement measure . . . 76

MANIPULATING THE DOMAIN NAME SYSTEM . . . 81
- Examining the use of the Domain Name System as an enforcement measure . . . 84

COPYRIGHT TAXES AND LEVIES . . . 91
FINAL COMMENTS . . . 93

INTRODUCTION

1. Technological innovations and the widespread adoption of the Internet[1] present new challenges for the protection of copyright, principally because:

   - Copyright content can be easily reproduced and cheaply transported in digital form all over the world via the Internet using any number of different protocols and distribution models.

   - The Internet does not distinguish between lawful and unlawful traffic.

   - There is no truly uniform global copyright law (e.g. what is illegal in one country may be legal in another) or approach to enforcement.

   - Infringers may be numerous, pseudo-anonymous and located outside national borders (i.e. beyond the reach of local law enforcement).

   Social developments such as the advent of "mash-ups" also challenge traditional concepts of what is "fair use". However, underlying all this is a human element—attitudes such as "downloading a film is okay even if it is not legal" and perhaps even a misunderstanding or lack of knowledge as to what is permissible and what is not.

2. Online copyright enforcement gained prominence in the Internet governance space in 2009-2010 with the introduction of the highly publicised French Hadopi law, other national proposals to use technical measures to enforce copyright online, and negotiations on the digital content provisions of the proposed Anti-Counterfeiting Trade Agreement.

3. These various proposals apply specifically to copyright infringement in the online environment. Proponents argue that laws applying in the offline world (e.g. traditional legal remedies for copyright infringement) are not effective when applied to the online environment. Opponents disagree and contend such proposals are, or could be, detrimental to the Internet and its users (e.g. breaching a fundamental right to privacy through traffic monitoring). Further, they argue against the need for Internet-specific laws.

4. This is the time of exploration. Countries around the world, both individually and collaboratively, are exploring and experimenting with new solutions to strengthen enforcement and curtail online copyright infringement. There is also increasingly international interest in harmonising and/or reforming digital copyright law and enforcement. It is too soon to say what is the appropriate or preferable enforcement approach. Further research and careful consideration of the potential ramifications is needed. Looking 10 years into the future, it is likely that a number of today's proposals will have been discarded, perhaps because they are ineffective, too expensive, unreasonably impact the Internet and its users, or are no longer considered necessary (e.g. if other initiatives are successful in reducing infringement).

1 The Internet is a global system of interconnected networks (a "network of networks") that communicate and transport data.

THE INTERNATIONAL AND REGIONAL LANDSCAPE

5. There is a long history of international laws and agreements concerning copyright, starting in 1886 with the *Berne Convention for the Protection of Literary and Artistic Works* ("the *Berne Convention*").[2] Significantly, the Convention gave mutual copyright protection among the signatories (i.e. works created in one country were protected in the other countries to the same degree as works created by citizens of those countries) and set minimum standards.[3]

6. The World Trade Organisation ("WTO") administers the 1994 *Agreement on Trade Related Aspects of Intellectual Property Rights*[4] ("*TRIPS Agreement*"). This agreement is intended to specify the minimum standard of Intellectual Property protection that WTO members are required to provide in their national laws.[5]

7. The *World Intellectual Property Organization ("WIPO") Copyright Treaty*[6] was adopted by WIPO member states in 1996. As at January 2011, there were 88 parties to the treaty.[7] The *WIPO Copyright Treaty* supplements the *Berne Convention* and was intended to update international law on copyright in light of technological and other developments.[8] Notably, the treaty explicitly extends copyright protection to computer programs (article 4) and compilations of data (article 5). It also imposes obligations on parties to the treaty to provide effective legal remedies against the circumvention of technical measures to protect copyright and electronic rights management information (articles 11 and 12).

8. In the European Union, the objective of *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights* is to "… approximate legislative systems so as to ensure a high, equivalent and homogeneous level of protection in the internal market".[9]

World Intellectual Property Organization

9. WIPO "... is a specialized agency of the United Nations. It is dedicated to developing a balanced and accessible international intellectual property (IP) system, which rewards creativity, stimulates innovation and contributes to economic development while safeguarding the public interest. WIPO was established by the WIPO Convention in 1967 ... to promote the protection of IP throughout the world through cooperation among states and in collaboration with other international organizations".[10] The organisation administers 24 intellectual property treaties, including the *Berne Convention*, the *WIPO Copyright*

2 http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html
3 http://www.wipo.int/treaties/en/ip/berne/summary_berne.html
4 http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm
5 See article 1(1) http://www.wto.org/english/docs_e/legal_e/27-trips_03_e.htm
6 http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html
7 See http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16
8 See preamble http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html
9 See paragraph 10 of the preamble http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R%2801%29:EN:NOT
10 http://www.wipo.int/about-wipo/en/what_is_wipo.html

Treaty and the *WIPO Performances and Phonograms Treaty*. WIPO covers Internet-related copyright issues through its Standing Committee on Copyright and Related Rights and the work of the Advisory Committee on Enforcement.

10. In 2011, WIPO launched the "International Music Registry"[11], a "... project aimed at facilitating licensing in the digital environment by providing easier access to reliable information about musical works and sound recordings"[12]. "As a first step, WIPO is facilitating a dialogue among stakeholders in the music sector, with a view to defining the purpose, scope and main features of the future IMR." [13]

Anti-Counterfeiting Trade Agreement

11. In 2008-2010, Australia, Canada, the European Union and its 27 member states, Japan, Mexico, Morocco, New Zealand, the Republic of Korea, Singapore, Switzerland and the United States of America negotiated the text for a new pluri-lateral agreement regarding counterfeiting and enforcement of intellectual property rights ("IPR"), known as the *Anti-Counterfeiting Trade Agreement* ("ACTA"). The text of the agreement was finalised in late 2010 and will be open for signature from 31 March 2011.[14] The objective the agreement is stated by the parties as follows:

> ACTA aims to establish a comprehensive international framework that will assist Parties to the agreement in their efforts to effectively combat the infringement of intellectual property rights, in particular the proliferation of counterfeiting and piracy, which undermines legitimate trade and the sustainable development of the world economy. It includes state-of-the-art provisions on the enforcement of intellectual property rights, including provisions on civil, criminal, border and digital environment enforcement measures, robust cooperation mechanisms among ACTA Parties to assist in their enforcement efforts, and establishment of best practices for effective IPR enforcement.[15]

ACTA would, among other things, create a new inter-governmental forum responsible for administering the agreement, i.e. responsible for enforcement of IPR in the international environment. Given the much broader breadth of its membership and specialist expertise in intellectual property rights issues, some forces are advocating for WIPO to take over international discussions on online IPR enforcement issues. (Further details regarding ACTA appear later in this document.)

12. The ACTA negotiations are one example of recent trends towards international harmonisation of IPR enforcement approaches, particularly with regard to the online environment.

---

11 http://www.wipo.int/imr/en
12 http://www.internationalmusicregistry.org/portal/en/index.html
13 http://www.wipo.int/imr/en
14 Article 39 of the ACTA text dated 3 December 2010 (available for download from http://www.ustr.gov/acta)
15 Joint statement on finalising ACTA text dated 16 November 2010 http://www.dfat.gov.au/trade/acta/Final-Press-Release.html

Organisation for Economic Co-operation and Development

13. The Organisation for Economic Co-operation and Development ("OECD") "… explores the role of Intellectual Property Rights (IPRs) in stimulating the diffusion of knowledge and fostering innovation. It studies the economic impact of IP regimes in high-tech industries and in public research; assesses policies and institutional practices for IP management and exploitation; and develops indicators to assess the effectiveness of technology transfer."[16]

14. In 2005, "[r]esponding to concerns in governments and the business community, the OECD launched a project … to assess the magnitude and impact of counterfeiting and piracy. The objective of the project is to improve factual understanding and awareness of how large the problem is and the effects that infringements of intellectual property rights have on governments, business and consumers in member countries and non-member economies"[17] ("the project on counterfeiting and piracy").

15. In June 2009, the OECD produced a report on the Piracy of Digital Content.[18] This was phase II of the project on counterfeiting and piracy, covering "… infringements of the intellectual property rights that are described and defined in the WTO Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS)".[19]

16. The Working Party on the Information Economy ("WPIE") of the OECD's Committee for Information, Computer and Communications Policy ("ICCP") has also been examining the delivery of digital content under the Work Plan on Digital Broadband Content.[20] As part of that work, the WPIE produced a report on entitled *Digital Broadband Content, Digital Content Strategies and Policies*.[21]

17. For the OECD Ministerial Meeting on the Future of the Internet Economy (Seoul, Korea 2008), the OECD produced *OECD Policy Guidance for Digital Content*.[22]

18. The ICCP's work on Internet Intermediaries is also relevant to online copyright issues.

Asia-Pacific Economic Cooperation

19. The APEC Anti-Counterfeiting and Piracy Initiative was endorsed by the Asia-Pacific Economic Cooperation ("APEC") Ministers Responsible for Trade in 2005.[23] Its goals include:

16 http://www.oecd.org/topic/0,2686,en_2649_34797_1_1_1_1_37417,00.html
17 http://www.oecd.org/document/50/0,3746,en_2649_34223_39542514_1_1_1_1,00.html
18 http://www.oecd.org/document/35/0,3746,en_2649_34797_43394531_1_1_1_1,00.html
19 http://www.oecd.org/document/50/0,3746,en_2649_34797_39542514_1_1_1_1,00.html
20 http://www.oecd.org/document/62/0,3746,en_2649_34223_32160190_1_1_1_1,00.html
21 Available for download via http://www.oecd.org/document/62/0,3746,en_2649_34223_32160190_1_1_1_1,00.html
22 Available for download via http://www.oecd.org/document/62/0,3746,en_2649_34223_32160190_1_1_1_1,00.html
23 http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Intellectual-Property-Rights-Experts-Group

- "Promote the enacting of appropriate legal regimes and enforcement systems to curtail online piracy and to undermine the online trade in counterfeit goods. This includes the development of guidelines to prevent Internet sales of counterfeit goods".

- "Increase operational contact and the sharing of information between customs and law enforcement agencies to combat counterfeiting and piracy networks."

- "Increase Member Economies' ability to develop and manage effective anti-counterfeiting and piracy enforcement systems through education and training throughout the region."[24]

APEC's Intellectual Property Rights Experts' Group ("IPEG") has developed model guidelines on intellectual property rights and has a program of work to:

- "Deepen the dialogue on intellectual property policy.

- Survey and exchange information on the current status of IPR protection and administrative systems.

- Study measures for the effective enforcement of IPR.

- Fully implement the TRIPS Agreement.

- Facilitate technical cooperation to help economies implement TRIPS." [25]

European Union

20. On 1 March 2010, the Council of the European Union by resolution invited "… the Commission, in accordance with Article 18 of Directive 2004/48/EC and in close collaboration with the Member States, to analyze the application of that Directive, including an assessment of the effectiveness of the measures taken, and, if necessary, propose appropriate amendments to ensure a better protection of intellectual property rights"[26] in the European Union.

21. On 22 December 2010, the European Commission published a report on the "Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights".[27] A staff working document compliments the

24 http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Intellectual-Property-Rights-Experts-Group

25 http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Intellectual-Property-Rights-Experts-Group

26 Paragraph 30 of the *Resolution on the enforcement of intellectual property rights in the internal market* available at http://ec.europa.eu/internal_market/iprenforcement/documents_en.htm#council Note: The European Commission in a Communication to the Council, the European Parliament and the European Economic and Social Committee, *Enhancing the enforcement of intellectual property rights in the internal market said "With a principal body of laws in place*, the Commission said it "… now proposes to supplement the regulatory framework with complementary non-legislative measures, in line with Competitiveness Council Resolution of 25 September 2008 on a comprehensive European anti-counterfeiting and piracy-plan." (COM(2009) 467 final)

27 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:EN:PDF

report.[28] In terms of action being taken regarding IPR infringement outside the European Union, the report states:

> Infringements of intellectual property rights taking place outside of the EU also constitute a major source of concern. The Commission is addressing them in different ways, for instance by including ambitious chapters on intellectual property rights in bilateral trade agreements and through participation in international initiatives, such as the on-going negotiation of the ACTA agreement[7]…[29]

22. On 11 January 2011, the European Commission (DG Internal Market and Services) launched a public consultation[30] with the objective:

> … to prompt the views of other European institutions, the Member States and private stakeholders on the findings reflected in the report on the application of the Directive and the technical paper attached to it. The consultation in particular is aimed at verifying the information provided in the report and at identifying additional issues that should be addressed in the context of a possible review of the Directive.

African Regional Intellectual Property Organization

23. The African Regional Intellectual Property Organization ("APRIPO") has 17 member states: Botswana; Gambia; Ghana; Kenya; Lesotho; Liberia; Malawi; Mozambique; Namibia; Sierra Leone; Somalia; Sudan; Swaziland; Tanzania; Uganda; Zambia; and Zimbabwe.[31] ARIPO's objectives include:

> (a) to promote the harmonization and development of the industrial property laws, and matters related thereto, appropriate to the needs of its members and of the region as a whole;
>
> (b) to foster the establishment of a close relationship between its members in matters relating to industrial property;
>
> (c) to establish such common services or organs as may be necessary or desirable for the co-ordination, harmonization and development of the industrial property activities affecting its members;
>
> (d) to establish schemes for the training of staff in the administration of industrial property law;
>
> (e) to organize conferences, seminars and other meetings on industrial property matters;
>
> (f) to promote the exchange of ideas and experience, research and studies relating to industrial property matters;

28 Available at http://eur-lex.europa.eu/SECMonth.do?year=2010&month=12
29 Footnote 7 refers to the European Union "Strategy for the enforcement of intellectual property rights in third countries" available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:129:0003:0016:EN:PDF
30 http://ec.europa.eu/internal_market/consultations/2011/intellectual_property_rights_en.htm
31 http://www.aripo.org/index.php?option=com_content&view=section&id=11&Itemid=13

(g) to promote and evolve a common view and approach of its members on industrial property matters; …[32]

24. APRIPO's mandate has included copyright since 2002.[33] It's strategic plan for copyright and related rights includes:

> Formulation of policy matters in the field of Copyright and Related Rights that will be the main focus of ARIPO in the short and medium terms;
>
> Sensitisation of the stakeholders in Member States on the new mandate and the explanation of its practical implementation; and
>
> Extensive training of members of staff of the Secretariat of the Organization and officials from Member States, mainly in matters relating Copyright and Related Rights.[34]

Organisation Africaine de la Propriete Intellectuelle

25. The Organisation Africaine de la Propriete Intellectuelle ("OAIP") has 16 member states: Benin; Burkina Faso; Cameroon; Central African Republic; Chad; Congo; Côte d'Ivoire; Equatorial Guinea; Gabon; Guinea; Guinea Bissau; Mali; Mauritania; Niger; Senegal; and Togo.[35] OAIP's mission and objectives include:

> Implement and enforce administrative procedures under the uniform system of protection of industrial property and the stipulations of international conventions in this field to which the Member States have acceded to and services related to industrial property.
>
> … promoting the protection, encouraging the creation of national organizations of writers, etc.
>
> Encourage creativity and technology transfer through the use of industrial property systems.
>
> Make the legal area attractive to private investment by creating favourable conditions for the effective implementation of the principles of intellectual property.
>
> Implement effective training programs to improve the capacity of OAPI to provide quality services. …[36]
>
> [unofficial English translation (Google)]

32 http://www.aripo.org/index.php?option=com_content&view=article&id=19&Itemid=53
33 http://www.aripo.org/index.php?option=com_content&view=article&id=27&Itemid=67
34 http://www.aripo.org/index.php?option=com_content&view=article&id=27&Itemid=67
35 http://www.oapi.int/index.php/en/aipo/etats-membres
36 http://www.oapi.int/index.php/en/aipo/objectifs-et-missions

Observatories

26. The United Nations Educational, Scientific and Cultural Organization ("UNESCO") World Anti-Piracy Observatory ("WAPO"), an online platform for sharing information and best practices was created following the 13th session of the Intergovernmental Committee of the UNESCO Universal Copyright Convention in 2005.[37]

27. The European Counterfeiting and Piracy Observatory was created by the Council of the European Union *Resolution on a comprehensive European anti-counterfeiting and anti-piracy plan* (28 September 2008).[38] The Observatory was "… launched to:

    - improve the quality of information and statistics related to counterfeiting and piracy on the Internal Market of the EU;
    - identify and spread national best practice strategies and enforcement techniques from both the public as well as the private sector;
    - help raise public awareness".[39]

    The Observatory has created a Legal Sub-group comprised of IPR legal practitioners to examine the European IPR legal framework.

28. On 1 March 2010, the Council of the European Union passed the *Resolution on the enforcement of intellectual property rights in the internal market*. This resolution, among other things, "requests the Observatory to facilitate regular experts' meetings, involving representatives from public authorities, private sector bodies and consumer organizations, to promote successful and proportional solutions against counterfeiting and piracy. …".[40]

37 http://portal.unesco.org/culture/en/ev.php-URL_ID=39057&URL_DO=DO_TOPIC&URL_SECTION=201.html
38 Resolution available at http://ec.europa.eu/internal_market/iprenforcement/documents_en.htm#council
39 http://ec.europa.eu/internal_market/iprenforcement/observatory/index_en.htm#what
40 Paragraph 33 of the Resolution available at http://ec.europa.eu/internal_market/iprenforcement/documents_en.htm#council

OVERVIEW AND OBSERVATIONS

29. Technological innovations and the widespread adoption of the Internet present new challenges for the protection of copyright, principally because:

- Copyright content can be easily reproduced and cheaply transported in digital form all over the world via the Internet using any number of different protocols and distribution models.
- The Internet does not distinguish between lawful and unlawful traffic.
- There is no truly uniform global copyright law (e.g. what is illegal in one country may be legal in another) or approach to enforcement.
- Infringers may be numerous, pseudo-anonymous and located outside national borders (i.e. beyond the reach of local law enforcement).

Social developments such as the advent of "mash-ups" also challenge traditional concepts of what is "fair use". However, underlying all this is a human element – attitudes such as "downloading a film is okay even if it is not legal" and perhaps even a misunderstanding or lack of knowledge as to what is permissible and what is not.

30. This is the time of exploration. Countries around the world, both individually and collaboratively, are exploring and experimenting with new solutions to strengthen enforcement and curtail online copyright infringement. There is also increasingly international interest in harmonising digital copyright law and enforcement. It is too soon to say what is the appropriate or preferable enforcement approach. Further research and careful consideration of the potential ramifications is needed. Looking 10 years into the future, it is likely that a number of today's proposals will have been discarded, perhaps because they are ineffective, too expensive, unreasonably impact the Internet and its users, or are no longer considered necessary (e.g. if other initiatives are successful in reducing the level of infringement[41]).

31. This paper draws from the expertise, experience and discussions within the Internet Society Copyright Working Group (2009-2010). It is intended to provide an overview of some of the potential issues for the Internet, Internet technologies, access and Internet use, posed by several main categories of emerging Internet-focused policy responses to online copyright infringement, namely:

- **Suspension of Internet access**

  Preventing an Internet subscriber from using their subscribed Internet connection to access the Internet for a specified period of time

41 For example: Some people argue infringement would be lower if there were more widespread legal sources of affordable digital copyright content.

Note: This measure is being applied as the final step in an escalating "graduated response" process (otherwise known as "three-strikes").

- **Traffic shaping**

  Limiting the bandwidth provided to an Internet user (e.g. the speed or the volume of traffic)

- **Blocking**

  Preventing Internet users from: accessing websites or other sources of content; using protocols (e.g. P2P); using ports

- **Content identification and filtering**

  Identifying content in Internet users' traffic and preventing them from accessing or distributing that content

- **DNS manipulation**

  Preventing Internet users from accessing websites or other sources of content via the Domain Name System ("DNS")

32. As this is a discussion document, the Internet Society does not seek to state a position on the complex and controversial issues canvassed in this paper, but rather we seek to stimulate further dialogue and collaborative examination of these issues at the international, regional and local level.

33. Nonetheless, we offer some observations and "work-in-progress" principles:

- The challenge is to find an enforcement approach which is effective, efficient, replicable across jurisdictions AND proportionate, fair, provides due process, respects fundamental rights and does not unreasonably impact third parties.

- Awareness raising, education and offering affordable legal alternatives are an important aspect of any online copyright enforcement plan.

- Technical measures to combat online copyright infringement can be circumvented: They will not prevent copyright infringement from occurring in the online environment.

  – Infringers can easily avoid solutions that focus on preventing infringement via a subscriber's connection to the Internet through their ISP (e.g. traffic shaping) by shifting to another Internet access point or deploying technical and social counter-measures (e.g. disguising infringing traffic).

  – Infringers can also avoid solutions that focus on preventing access to infringing content via the DNS by using other "addresses" (e.g. IP addresses, alternate DNS).

- A stepped enforcement procedure with an educative element (e.g. warnings followed by a sanction) offers some promise but still has many obstacles to overcome, including ensuring:
  - methods used for detection of infringement and identification of infringers are reliable, accurate and carried out in a privacy-respecting manner;
  - stringent data protection rules and security;
  - the procedure:
    - is linguistically, socially, culturally and economically appropriate;
    - does not unreasonably interfere with the business or activities of ISPs and third parties;
    - does not diminish innovation and development of the Internet, Internet technologies and the spread of Internet access;
    - is applied to proven, not suspected, infringement;
  - any sanctions are proportionate, fair, appropriate, and are applied with due process by an independent suitably qualified third party.

34. We also note that a very important underlying question raised by these emerging Internet-focused enforcement policies is:

    What role (if any) can and should Internet intermediaries and domain name registries play in enforcing copyright in the online environment?

    This question cannot be answered in isolation: before one can begin to answer this question, it is important to consider holistically, among other things, the scope of copyright in the online environment, motives behind online infringement, how copyright is infringed, objectives behind online copyright enforcement, how the Internet functions and develops, how different enforcement policies might operate in practice, and the potential impact they may have.

THE INTERNET SOCIETY'S ROLE

35. The Internet Society is a non-profit organisation, founded in 1992 to provide leadership in Internet-related standards, education and policy. It is a principles-based organisation, dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world.

36. The Internet Society is the organisational home for the Internet Architecture Board ("IAB") and the Internet Engineering Task Force ("IETF") - an open consensus-based group responsible for defining Internet protocols and standards.

37. The Internet Society has more than 100 organisational and 40,000 individual members, and over 80 Chapters around the world. To better serve the regional Internet community, the Internet Society has also created bureaus in Africa, Latin America, Asia, North America and Europe.

38. The Internet Society is accredited with Consultative Status with the United Nations Economic and Social Council ("ECOSOC"). It has formal and strong working relationships with other UN organisations such as WIPO, the UN Educational, Scientific and Cultural Organization ("UNESCO") and the International Telecommunication Union ("ITU"), as well as governmental and inter-governmental organisations, for example, the OECD and APEC.

39. Across the world, the Internet Society engages in policy projects guided by these core values:

- The quality of life for people in all parts of the world is enhanced by their ability to enjoy the benefits of an open and global Internet.
- Well-informed individuals and public and private policy makers are the essential foundation of an open and global Internet society.
- The genius of the Internet is that its decentralized architecture maximizes individual users' power to choose (or create) and use the hardware, software, and services that best meet their needs, and if the Internet is to continue to be a platform for innovation and creativity, its open, decentralized nature must be preserved.
- Enduring and sustainable progress toward our vision is best achieved by a combination of global initiatives and activities at a local level that engage people in their home regions.
- Technical standards and Internet operating procedures should be developed and asserted through open and transparent processes, with minimal barriers to participation or access to information.
- The social, political, and economic benefits of the Internet are substantially diminished by excessively restrictive governmental or private controls on computer hardware or software, telecommunications infrastructure, or Internet content.

- Rewarding and productive use of the Internet depends on the ability to trust critical services.[42]

40. One of the Internet Society's key objectives in the policy sphere is to work with governments and partner organisations to foster Internet-friendly policy environments. We strive to deliver reliable and technically-sound perspectives on key and emerging Internet policy topics that will promote good decision-making at all levels – local, national, regional and international.

BACKGROUND AND OBJECTIVES

41. The Internet Society considers that protection of copyright in an online environment is an important and current issue for the Internet community, particularly with the growing interest in Internet-focused enforcement measures and the role that Internet intermediaries could and/or should play in enforcing copyright online. Further, policies developed today to address online copyright infringement have the potential to become precedents for dealing with other unlawful activity or other defined misuses of Internet resources. The Internet Society also considers that enforcement solutions should not endanger the stability of the Internet or limit the development and use of Internet technologies for legitimate purposes.

42. The genesis for this project came from work undertaken by the Internet Society's French Chapter (ISOC-FR) and the Internet Society European Coordinating Council (ISOC-ECC) regarding the then proposed Projet de loi favorisant la diffusion et la protection de la création sur Internet (otherwise known as the "Hadopi law").

43. Our initial objective in this project was to bring together different interested stakeholders from our members to collaboratively explore the possible implications of emerging national policy responses to online copyright infringement. This discussion paper evolved from that initial undertaking.

44. The paper draws from the expertise, experience and discussions within the Internet Society Copyright Working Group (2009-2010). It starts from the premise that online copyright infringement occurs and governments around the world are searching for new solutions to prevent, reduce and/or discourage this conduct. Accordingly, to confine the scope of this paper, we have not examined the definition, scope and extent of online copyright infringement. Nonetheless, these issues are relevant to the question of whether proposed enforcement measures are proportionate and appropriate. We consider that the international dialogue on such measures would benefit from further research in this area.

45. In this paper, we explore some potential implications of emerging Internet-focused enforcement policy responses to online copyright infringement (i.e. infringement of digital content, rather than other forms of IPR infringement that occur via the Internet such as the sale of counterfeit goods). The paper is not intended to provide an exhaustive analysis of all emerging policy responses, or indeed, *all* aspects of each of the policy responses

42 http://www.isoc.org/pubpolpillar/principles.shtml

discussed. Further, our analysis principally focuses on the categories of enforcement (e.g. blocking etc.) rather than the individual national implementations of those policies. In this regard, we note that, in most cases, implementation is still under development (e.g. the Hadopi law in France).

46. Thus, our objective in this paper is to provide an overview of these categories of emerging policies and discuss what impact they might have on the Internet and Internet technologies, access and use. We hope that this paper will inform the international, regional and local debate on online copyright enforcement, and assist policymakers develop appropriate policies in this area.

47. While we have tried to identify the countries where these emerging policies have been adopted or are being considered, there may be countries not mentioned in this report that are also considering similar or other Internet-focused policies.

THE ISOC COPYRIGHT WORKING GROUP

48. Consistent with the Internet Society's belief that a collaborative multi-stakeholder approach is essential to the development of sound Internet policy, the Internet Society's Public Policy team invited all interested members to join a working group to investigate and examine emerging policy responses around the world to online copyright infringement.

49. In response to our call for participation, more than 35 individual and organisational members, and one non-member guest joined the working group from Africa, Asia, Europe, North America, the Pacific, the Middle East and Latin America. The working group drew participants from content and services providers, technical experts, the academic community, end-users, lawyers, Internet Society Chapters and others. We were delighted with the enthusiastic response from our membership.

50. We believe that the diverse expertise and different perspectives that the members brought to the working group, together with a collaborative information-sharing approach, were fundamental to its success. Not surprisingly, given these different perspectives, there was some disagreement in views in the discussions that were the foundation for this document. Accordingly, it should be noted that any opinions expressed in this document are not necessarily shared by all members of that group.

51. The Internet Society would like to express its sincere thanks to the Internet Society Copyright Working Group members for their strong commitment to this pilot project, the many insightful observations and ideas they brought to the discussion, and their ongoing support of the Internet Society's mission to provide technically-sound advice and expertise on key emerging Internet policy issues.

THE ANALYSIS

52. In our analysis of the various identified emerging policy responses to online copyright infringement, we considered the following questions:

(a) What methods of copyright infringement and/or categories of infringers is the policy designed to address?

(b) How effective is the policy likely to be at preventing or reducing copyright infringement?

(c) What solutions might infringers choose or develop in response? What impact would these have?

(d) What impact would the policy have on privacy?

(e) Would the policy discriminate against legitimate uses of applications?

(f) Would the policy discourage or prevent the use of certain technologies and/or development of new communications protocols?

(g) Would the policy alter the basic architecture of the Internet? Are there any unpredictable or identifiably negative consequences?

(h) What impact would the policy have on security?

(i) Would the policy inhibit or enhance users' willingness to access the Internet or obtain access to the Internet?

(j) Would the policy directly or indirectly reduce Internet access or the availability of Internet access?

(k) Would the policy materially raise or lower the costs of Internet access?

(l) Is there any risk of significant or material damage to third parties' use of or access to the Internet?

(m) Would the policy encourage or discourage the use of certain business models?

These questions were not intended to be exhaustive: they were intended to highlight some of the key issues and possible consequences of the various identified policy responses.

COPYRIGHT INFRINGEMENT VIA THE INTERNET

53. There are many ways that copyright content can be accessed, distributed and/or copied without authorisation via the Internet, but they essentially fall into 3 broad categories: client-server; store-and-forward; and peer-to-peer.

54. In the client-server model (for example: a website), copyright content is stored (semi-permanently) on a server (or servers) and clients obtain it from there.

55. With store-and-forward systems (for example: email), copyright content is transmitted by one client to a server and then sent by the server to another client. Servers can also send to other servers, or there may be multiple recipient clients (for example: a mailing list), but the key feature of these systems is that there are still central servers where content distribution can be disrupted, though the material is only stored temporarily as it passes through them.

56. Peer-to-peer ("P2P") systems distribute content directly between "clients", i.e. end user devices, from PCs to "smart phones" and beyond. Early P2P systems incorporated a central server that acted as a directory, informing clients that wanted content where to find the clients that had it (i.e. a directory service). However, later generations of P2P systems distribute the directory service as well as the content among clients.

57. From an online copyright enforcement perspective, it is usually easier to stop illegal or unauthorised distribution of copyright content where such content is stored centrally (for example: in a client-server distribution system or even a store-and-forward system) than one where the content is distributed directly between clients (for example: P2P file-sharing).

58. The Internet does not distinguish between copyright content and non-copyright content. In this sense, copyright content is no different to any other data that might be exchanged between hosts over the Internet.

59. Illegal P2P file-sharing has attained some notoriety, but there are many ways that copyright content can be distributed (legally or illegally). For example:

    (a) Local network exchange (e.g. Windows Networking, Samba etc.)

    (b) Emails (in the message body or as attachments)

    (c) Instant messaging ("chatting") file exchange

    (d) Dedicated file uploading and storage services

    (e) P2P networks

    (f) "Warez" sites (web and FTP)

    (g) "One click" hosting services (known as file lockers or cyberlockers)

(h) Online media/video/music sharing and streaming websites, including user-generated content ("UGC") sites

(i) Leech sites and deep linking sites which provide links to "pirated content" that are disguised on UGC sites

(j) Web and FTP sites using third party servers without the third party's knowledge or permission

(k) Internet Relay Chat ("IRC")

(l) USENET[43].[44]

43 See OECD Document - *Piracy of Digital Content* (Pre-Publication Version) at paragraphs 42-62 http://www.oecd.org/dataoecd/50/22/42619490.pdf

44 a, d, f – j are client-server; b and l are store-and-forward; c, e and k are peer-to-peer. Note: IRC is typically client-server, but IRC file transfers using Direct Client-to-Client (DCC) are peer-to-peer.

EMERGING INTERNET-FOCUSED POLICY RESPONSES

60. The Working Group identified several main categories of emerging technical Internet-focused policy responses being considered around the world to address online copyright infringement, namely:

- **Suspension of Internet access**

  Preventing an Internet subscriber from using their subscribed Internet connection to access the Internet for a specified period of time

  Note: This measure is being applied as the final step in an escalating "graduated response" process (otherwise known as "three-strikes").

- **Traffic shaping**

  Limiting the bandwidth provided to an Internet user (e.g. the speed or the volume of traffic)

- **Blocking**

  Preventing Internet users from: accessing websites or other sources of content; using protocols (e.g. P2P); using ports

- **Content identification and filtering**

  Identifying content in Internet users' traffic and preventing them from accessing or distributing that content

- **DNS manipulation**

  Preventing Internet users from accessing websites or other sources of content via the Domain Name System ("DNS")

Another Internet-focused, but non-technical approach, might be a general "**copyright levy or tax**" on Internet access to collect remuneration for copyright content producers.

We discuss each of these measures in the sections below.

DETECTING INFRINGEMENT AND IDENTIFYING INFRINGERS

61. A preliminary aspect of the various emerging Internet-focused enforcement measures under discussion is the need to be able to accurately detect infringement and identify infringers. Historically, the task of detecting infringement has been principally undertaken by rights holders.

62. Rights holders and their agents use a variety of different techniques to detect copyright infringement in Internet traffic without the assistance of Internet Service Providers ("ISPs") (e.g. by participating in P2P swarms). We do not cover these in detail in this paper.

63. One of the major concerns of both ISPs and Internet users is whether emerging Internet-focused enforcement policies would shift that task (or aspects of it) to ISPs – leading to Internet traffic monitoring in one form or another. In any case, the infringing conduct associated with an Internet Protocol address ("IP address") (date and time used) detected by rights holders and/or their agents needs to be linked to a subscriber – data that is (or could be) collected by the ISP – and then to the infringer (who may or may not be the subscriber).

64. This raises practical difficulties associated with matching the infringer to the infringing conduct. For example, a subscriber's Internet connection may be used by more than one person (even at the same time – e.g. through a wireless router) with or without the knowledge and consent of the subscriber. Further, the widespread use of Network Address Translation ("NAT") and Dynamic Host Configuration Protocol ("DHCP") mean that it is not always possible to uniquely identify the subscriber associated with a particular public IP address, particularly if the complaint from the rights holder does not include both source and destination addresses, and ports. Even with this information, particularly where multiple NATs are involved, it may be impossible for ISPs to identity that subscriber. The depletion of the IPv4 address pool is likely to make these problems more acute.[45]

65. IP addresses can also be spoofed and Internet wireless connections can be hijacked (either because they are unsecure or because they have been hacked)[46].

66. Without a legal requirement to record and retain IP address logs, some ISPs may choose, for one reason or another, to stop logging this information. For example, after Sweden resolved to implement *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights*[47] ("IPRED") which, among other things, provides that rights holders may request details concerning alleged copyright

45 *IETF Internet Draft* – "Issues with IP Address Sharing" (15 October 2010) http://tools.ietf.org/html/draft-ietf-intarea-shared-addressing-issues-02

46 According to NetworkWorld, a "network scrounging device" that can be purchased in The Peoples' Republic of China "… took over an hour to crack the WEP key equivalent to the password "sugar" in a test attack on a personal router set up for the purpose using 40-bit encryption" see *ZeroPaid* "Chinese USB Wifi Crackers Make Three Strikes Laws Obsolete?" (6 May 2010) http://www.zeropaid.com/news/89039/chinese-usb-wifi-crackers-make-three-strikes-laws-obsolete

47 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:EN:PDF

infringers from ISPs, some local ISPs announced they would stop logging subscribers' Internet traffic.[48] Subsequently, the Swedish Minister for Justice presented a bill to the Swedish Parliament that would require, among other things, ISPs to retain Internet traffic data logs for 6 months.[49]

67. Additionally, there are many ways that technically competent infringers could avoid detection by disguising the source, destination and content of their Internet traffic. Thus, in most cases, identifying the subscriber to whom the IP address was allocated at the relevant time will not be sufficient to identify the person that is alleged to have infringed copyright. These practical difficulties have led some to argue that Internet subscribers should be held more responsible for the traffic on their connection (e.g. by password protecting their wireless connection) and/or that Internet access should be less anonymous.

68. There are many reasons why Internet users may choose to remain anonymous and/or encrypt their Internet traffic apart from wanting to avoid detection while engaging in copyright infringement, including: privacy; security; concerns about repercussions for statements made in social media and/or hosting blogs for "cyber-dissidents"; being identified while attempting to access government blocked websites or other content deemed inappropriate; illegal activity; concerns about employer or government surveillance, etc.

69. There are a number of different Internet anonymity service providers. For example, in July 2010, a new ISP (Pirate ISP) started beta testing a model of supplying anonymous Internet access in Lund, Sweden.[50] ItsHidden.com offers a free Virtual Private Network ("VPN") service and does not keep data logs. One year after its launch, ItsHidden.com had 300,000 members. On an average day, more than 55,000 users log in and transfer thousands of Gigabytes of data.[51] Tor (torproject.org) offers a "Hidden Service Protocol" "… for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server. Using Tor 'rendezvous points,' other Tor users can connect to these hidden services, each without knowing the other's network identity".[52] Smarttorrent, reportedly the largest French torrent site, started offering a VPN service for its users (known as SmartVPN) after Hadopi enforcement action commenced.[53] In January 2011, reportedly in response to the upcoming introduction of the Swedish implementation of IPRED, Bahnhof

48 *Ars Technica* – "Online and anonymous: Swedish ISP won't retain Internet data" (16 April 2009) - http://arstechnica.com/tech-policy/news/2009/04/when-isps-dont-retain-data-theres-nothing-to-turn-over.ars and *TorrentFreak* - "Swedish ISPs Obstruct New Anti-Piracy Legislation" http://torrentfreak.com/swedish-isps-obstruct-new-anti-piracy-legislation-090427

49 *Stockholm News* – "Data traffic to be stored" (11 November 2010) http://www.stockholmnews.com/more.aspx?NID=6254 (See also *BoingBoing* – "Swedish ISP will Anonymize all its users' data" (27 January 2011) http://www.boingboing.net/2011/01/27/swedish-isp-will-ano.html

50 *TorrentFreak* – "World's First Pirate ISP Launches In Sweden" (20 July 2010) http://torrentfreak.com/worlds-first-pirate-internet-provider-launches-in-sweden-100720

51 *TorrentFreak* – "Free 'BitTorrent VPN' Grows to 300000 Members in a Year" (6 July 2010) (http://torrentfreak.com/free-bittorrent-vpn-grows-to-300000-members-in-a-year-100706

52 http://www.torproject.org/docs/hidden-services.html.en

53 *TorrentFreak* – "Torrent Site Launches VPN to Counter France's Anti-Piracy Law (27 October 2010) http://torrentfreak.com/torrent-site-launches-vpn-to-counter-frances-anti-piracy-law-101027

(a Swedish ISP) announced it would route customers' traffic through an encrypted VPN (unless they opt-out).[54]

70. On the issue of monitoring, the Article 29 Data Protection Working Party, in a letter to the European Commissioner for Trade regarding the then draft Anti-Counterfeiting Trade Agreement (ACTA) text, said:

> WP29 emphasizes that any form of large scale monitoring or systematic recording of data of EU citizens would be contrary to the provisions of Directive 95/46/EC since that would affect millions of individuals, regardless of whether or not they are under any suspicion.[55]

71. Further, determining infringement in the online environment is not without its difficulties. No one party has the information required to (a) identify with certainty that infringement has taken place and (b) identify the responsible person. ISPs cannot with certainty distinguish a packet that infringes copyright from one that does not (e.g. the packets may be technically identical); rights holders may be able to identify when infringement has taken place (although "fair use" provisions of national laws make even that a less than perfect science), but they do not know ISPs' addressing and routing schemes, or end users' security provisions, so as to be able to accurately identify the person responsible. In such a complex system, some errors of identification are inevitable.

72. Given these evidential difficulties, there has been consideration and debate as to where the onus of proof should lie (i.e. with the rights holder or the Internet subscriber) with proponents on both sides. For example, in New Zealand, a report released by the New Zealand Commerce Committee in November 2010 regarding the draft New Zealand legislation (discussed below) recommended amending the draft to provide that an infringement notice establishes a rebuttal presumption that infringement has occurred (see paragraph 107).

73. ISP collection, retention and use of Internet traffic data is a controversial area even outside the ambit of online copyright enforcement, and views vary across jurisdictions.[56] We have not covered these issues in any detail in this paper but it is a very fundamental issue associated with any enforcement measure that requires content identification, identification of infringers and/or detection of infringing content. Further research and discussion is recommended.

74. In the following sections, we consider some of the potential implications of various emerging Internet-focused online copyright enforcement policies.

---

54 *TorrentFreak* – "Wikileaks ISP Anonymizes All Customer Traffic to Beat Spying" (27 January 2011) http://torrentfreak.com/wikileaks-isp-anonymizes-all-customer-traffic-to-beat-spying-110127

55 (15 July 2010) http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm

56 As, background, see, for example, *Studies on Online Copyright Enforcement and Data Protection in Selected Member States* (November 2009 and April 2010) prepared by Hunton & Williams for DG Internal Market and Services of the European Commission available at http://ec.europa.eu/internal_market/iprenforcement/documents_en.htm

SUSPENSION OF INTERNET ACCESS

75. France, the Republic of China, the Republic of Korea and Chile have passed laws which introduce suspension of Internet access as an enforcement measure for online copyright infringement after at least two notices of infringement (i.e. warning notices) have been sent to the relevant Internet subscriber. The United Kingdom has also passed legislation to permit suspension of Internet access as an enforcement measure, but the relevant provisions will not be effective prior to 2012 and only if the Secretary of State, with parliamentary approval, decides to require ISPs to impose this measure. New Zealand is in the process of adopting legislation.

76. While all the national approaches outlined briefly below use suspension of Internet access as the ultimate sanction in an escalating graduated response enforcement procedure, they vary in their implementation. For example: the Korean legislation provides two schemes for suspension – order by the Minister of Culture, Sports and Tourism and recommendation by the Korea Copyright Commission; In New Zealand, the proposed legislation would require a court order for suspension; ISPs in the Republic of China receive protection from liability if they implement a suspension policy.

Graduated response

77. "Graduated response" enforcement procedures (also known as "three-strikes") have received considerable criticism, principally because such procedures typically have suspension of Internet access as the ultimate sanction. Much of the debate regarding the graduated response approach, therefore, has centred on the whether or not it is appropriate to temporarily preclude individuals from accessing the Internet because they infringed copyright, which in many jurisdictions is a civil, not a criminal offence. Yet, a graduated response procedure does not have to end with suspension of Internet access – other options could be considered.

78. A "graduated response" is, as the term suggests, an escalating approach to enforcement, aimed at deterring further infringement with the minimal enforcement necessary. For example, in an infringement notice model, if an infringer stops after receiving the first infringement notice no further action would be taken under this model, however, if the infringer continues after receiving the first notice, a second infringement notice would be sent, and so forth. In theory, only the most egregious infringers should be subject to the most severe sanctions, rather than all infringers (irrespective of the degree of infringement) being subject to the same sanction.

79. The graduated response approach is also intended to serve an important informational and educational function. For example, infringement notices may inform a subscriber of a shared Internet connection that his or her Internet connection may have been used to infringe copyright. They may also provide information regarding what conduct constitutes copyright infringement and offer suggestions to the subscriber as to how to minimise the risk of the connection being used by others to infringe copyright.

80. There is considerable scope for variation in the procedure applied in a graduated response – some methods will be more privacy-respecting than others, afford more due process and judicial oversight, be more efficient and cost-effective, apply stricter standards for proving infringement and identifying infringers, etc.

81. In some cases, graduated response programs are coupled with other initiatives such as those that provide increased access to legal content (e.g. Eircom's MusicHub[57]).

Infringement notices

82. Each of the national laws and proposed laws discussed in this document that authorise suspension of Internet access require ISPs or another entity to send the subscriber warning notices before suspension can be considered. Infringement notices (as an enforcement tool) are designed to inform the subscriber that: the subscriber's connection was allegedly used to infringe copyright; warn the subscriber of potential action that might be taken if infringement continues; and discourage infringement. The objective is to also provide a process for dealing with relatively low-level infringement by a very large number of people.

83. Copyright infringement notices are not new.[58] What is new is their use as part of a broader enforcement strategy – a graduated response culminating in a new sanction, i.e. suspension of Internet access. More traditional sanctions for civil copyright infringement include court ordered fines and/or damages.

84. Publicising infringement notice campaigns may raise awareness that copyright infringement is unlawful and that those responsible for online copyright infringement can be identified and held to account. (Note, however, that the subscriber may or may not be the infringer and may or may not be aware that his/her/its connection is or was being used for online copyright infringement.) Infringement notices themselves could also be a tool for raising awareness and education about copyright and infringement.

85. At present, there do not appear to be any infringement notice models that require an infringement notice to be sent only to an infringing Internet user. Perhaps this is in part because of the practical difficulties and, indeed in many cases, the impossibility of reliably identifying that person. While, in theory, it would seem preferable to require that infringement notices be sent only to the alleged infringer, such a policy may discourage business models that allow anonymous access to the Internet (a feature that can be indispensible for the exercise of freedom of expression). Further, a legal requirement to always be able to identify a responsible Internet user might make it difficult to continue using NAT and DHCP systems, thereby significantly increasing the demand for IP addresses.

57 *Eircom Press Release* (8 December 2010) – "eircom Launches MusicHub" http://pressroom.eircom.net/press_releases/article/eircom_launches_musichub

58 For example – U.S. Digital Millennium Copyright Act ("DCMA") notices (section 512 of Chapter 5 of Title 17 of the U.S. Code). In July 2010, the Recording Industry Association of America ("RIAA") said that it sent notices to 1.8 million Internet subscribers and 269,609 to colleges and universities in less than 2 years. (see *TorrentFreak* (4 July 2010) – "RIAA Warns 1 Million Copyright Infringers a Year") http://torrentfreak.com/riaa-warns-1-million-copyright-infringers-a-year-100704

86. Thus, in current infringement notice models, the sender does not need to identify the actual infringer before the notice is sent to a subscriber – only that infringement has allegedly occurred via the subscriber's Internet connection. Accordingly, there should be no need under such models for ISPs to disclose the identity of subscribers to rights holders alleging infringement.

87. The onus to challenge the notice (either to assert that he/she/it was not the infringer and/or that infringement did not take place) typically rests with the subscriber. The notice itself usually does not carry punitive consequences, but action might be taken if copyright infringement is detected and proven to have occurred via the subscriber's connection after receipt of two or more notices (e.g. temporary suspension of Internet access). Nonetheless, even receipt of such a notice might be considered by innocent recipients as potentially damaging to their reputation vis-à-vis their ISP, and others if their receipt of a notice became known. Further, there may be privacy issues associated with a shared Internet connection and a subscriber's attempts to identify the infringing party.

88. Some ISPs send out infringement notices on a voluntary basis (at the request of rights holders and their agents), while others send them as required by law. Where infringement notices are part of a government mandated enforcement policy, but ISPs are not legally required to forward such notices, some ISPs may choose not to do so. For example, Free (a French ISP) initially declined to refer warning notices to its customers at its own expense, but started sending them after a government decree on 12 October 2010 that ISPs send the notices within 24 hours.[59]

89. Infringement notice schemes are not without cost. Rights holders need systems and sometimes agents to monitor Internet traffic to detect infringement (e.g. by participating in P2P file-sharing) and notify the relevant ISPs. ISPs need systems to identify the relevant subscribers and send the infringement notices. Although these processes can be automated to some extent, ISPs are likely to need a more manual process for dealing with customer queries about the process and those cases where the allegations are incorrect or incomplete (e.g. because the content was covered by a "fair use" rule, or because the complaint did not contain sufficient information to allow the responsible subscriber to be identified). Estimates of the costs of processing and sending out infringement notices vary[60] as do the models for costs apportionment. For example, the U.K. proposal is to split the cost (estimated by Ofcom[61]) 75:25 between rights holders and ISPs.[62]

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

60 See, for example, *itnews* – "Kiwis put a price on copyright notices: $23" (29 September 2010) http://www.itnews.com.au/News/233676,kiwis-put-a-price-on-copyright-notices-23.aspx

61 "Independent regulator and competition authority for the UK communications industries" http://www.ofcom.org.uk

62 See *The Online Infringement of Copyright (Initial Obligations) (Sharing of Costs) Order 2011 (Draft)* available at http://www.bis.gov.uk/Consultations/online-infringement-of-copyright?cat=open and *Online Infringement of Copyright (Initial Obligations) Cost Sharing: HM Government Response* available at http://www.bis.gov.uk/Consultations/online-infringement-of-copyright?cat=open

90. Accurate detection of infringement and the relevant infringing IP address can also be an issue. There have been some reported incidents where complaints have been sent in error. For example, in 2008, University of Washington researchers released results of a study of BitTorrent on a university network and said:

> … We have conducted the first scientific, experimental study of monitoring and copyright enforcement on P2P networks and have made several discoveries which we find surprising.
>
> - **Practically any Internet user can be framed for copyright infringement today.**
>
> By profiling copyright enforcement in the popular BitTorrent file sharing system, we were able to generate hundreds of real DMCA takedown notices for computers at the University of Washington that never downloaded nor shared *any content whatsoever.*
>
> Further, we were able to remotely generate complaints for nonsense devices including several printers and a (non-NAT) wireless access point. Our results demonstrate several simple techniques that a malicious user could use to frame arbitrary network endpoints.[63]

However, it is important to note that different infringement notice regimes involve different detection techniques and more or less rigor in ascertaining whether infringement has occurred and the identity of the subscriber of that Internet connection (endpoint). For example, in France, under the Hadopi scheme, allegations of infringement asserted by rights holders are independently verified by the Hadopi authority before any infringement notice is sent to a subscriber.

91. Scale is also an issue – too many requests to send infringement notices may place an excessive burden on ISPs.

92. Estimates vary as to how effective infringement notices (with no further action) are as an enforcement remedy, however, some surveys suggest that up to 70% of Internet users would stop infringing copyright in response to a warning.[64] Even the prospect of detection may have some impact. For example, a day after the Swedish Parliament resolved to implement IPRED, Internet traffic in Sweden was reported to have decreased by 30%.[65]

93. As with the other enforcement measures discussed in this document, Internet users might shift to less easily traced methods of gaining access to copyright content, or use encryption

63 *Tracking the Trackers. Investigating P2P Copyright Enforcement*. http://dmca.cs.washington.edu/index.html#papers

64 New Zealand: In a 2009 survey conducted for the NZ Federation Against Copyright Theft 71% of the respondents said they would take notice of ISP warnings and stop infringing (see Movie File Sharing Amongst Young New Zealanders available at http://www.nzfact.co.nz/reports.html); UK: "Results of the Digital Entertainment Survey (2008) suggest that 70% of infringers would stop illegal P2P downloads after being notified by their ISP." *Impact Assessment accompanying the draft statutory instrument "online infringement of copyright (initial obligations) (sharing of costs) order"* www.bis.gov.uk/.../10-1164-impact-assessment-cost-sharing-consultation.pdf

65 The Local - *Anti-piracy law has little effect on internet use* http://www.thelocal.se/25868/20100401

or other techniques to defeat the systems used to detect infringement. Or they may simply ignore the warnings.

94. Using a different approach to providing warnings, in 2007, the University of Michigan launched "Be Aware You're Uploading" (BAYU), an application that automatically sends its network users a BAYU email when they are sharing files via P2P (without examining the content).[66] Reportedly, after BAYU was introduced "the number of copyright infringement notices the university receive[d] .. slowed to a trickle".[67]

95. Unlike the technical measures discussed in this paper, a policy of sending infringement notices (with no further action) should not discriminate against legitimate uses of applications, nor discourage the use of certain technologies and protocols or affect the basic architecture of the Internet, provided there is no demand or need to alter Internet infrastructure to detect infringement. Any impact on Internet access and usage is likely to be driven by infringement detection techniques or the ultimate sanction rather than the notices themselves. It is likely, however, that that circumstance would change dramatically if ISPs disclosed subscriber details to rights holders or others without a court order for the purposes of sending infringement notices.

National approaches

96. In this section, we very briefly outline some policies that include the possibility of suspension of Internet access as a sanction for infringement. Even though such policies have already been incorporated in national laws, such laws are relatively new and their implementation is still in the evolutionary stage.

France

97. France, with its *Loi favorisant la diffusion et la protection de la création sur Internet*[68] (passed in 2009), brought the discussion of the appropriateness of suspension of Internet access as a remedy for copyright infringement to the forefront of the debate, but it is not the only country which has adopted or is considering adopting such a policy.

98. The French law is commonly referred to as the "Hadopi law" because it created a new government authority - Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet (Hadopi) – to administer the new law. This new law introduced new enforcement procedures for online copyright infringement that have come to be known as "graduated response" or "three strikes". (After two or more infringement notices, the third step of the enforcement procedure is suspension of Internet access imposed by a judge.)

99. Although the Hadopi law has, for many, become synonymous with "graduated response" or "suspension of Internet access" for online copyright infringement, the law has other

66 http://bayu.umich.edu/basics.php
67 http://www.businessweek.com/ap/financialnews/D9GMG8K00.htm
68 http://www.senat.fr/dossierleg/pjl07-405.html

objectives such as: encouraging the development of legal content services and relevant expertise. The Hadopi authority has established five "labs" which are:

> … aimed at building a knowledge base accessible to all, combining reference publications written in a collaborative approach, to develop proposals for resolving tensions. Each corresponding to a particular area of expertise and together, they ensure a multidisciplinary approach to address these issues from several complementary angles. (unofficial translation (Google))[69]

The "Hadopi Labs" are intended to operate as multistakeholder "think tanks" in the following fields: Standards and Technology, Digital Economy, Online uses, Intellectual Property Rights, and Internet and Societal issues.[70] Their mission includes fostering the development of legal content models and secure Internet connections. The Hadopi authority will also be establishing a portal with links to legal content and information to help Internet users identify legal content online.[71]

100. The Hadopi law has a relatively long and controversial development history. Being the first authority created at the national level in France to counteract copyright infringement, the French Senate and National Assembly had numerous discussions regarding the proposed law until agreement was finally reached in May 2009.[72]

101. On 10 June 2009, the Constitutional Council of France declared that part of the "first" version of the Hadopi law was unconstitutional and infringed the *Declaration of the Rights of Man and of the Citizen* because it would have allowed a governmental (i.e. non-judicial) body to impose a sanction (i.e. suspension of Internet access). That aspect was held to infringe articles 9 and 11 of the *Declaration,* which gives French citizens the right to the presumption of innocence and the right to freedom of expression and communication.[73] A revised version of the law was approved by the Constitutional Council of France on 22 October 2009.[74] Implementation of the Hadopi law enforcement procedures commenced in September-October 2010.

102. Under the "second" and operating version of the Hadopi law, suspension of Internet access can only be ordered by a judge. Infringement notices are issued by the Hadopi authority based on information it has received from rights holders (evidence of infringement plus details of the IP addresses used for the infringement) and ISPs (names of Internet subscribers using the IP addresses at the relevant time).[75]

---

69 http://www.hadopi.fr/labs-hadopi/les-5-labs-de-l-hadopi.html
70 http://www.hadopi.fr/labs-hadopi/les-5-labs-de-l-hadopi.html
71 http://www.hadopi.fr/usages-responsables/nouvelles-libertes-nouvelles-responsabilites/offres-legales-labellisees.html
72 www.wikipedia.org (Hadopi) as at 13 January 2011 http://en.wikipedia.org/wiki/Hadopi#Legislative_process
73 *Digital Civil Rights in Europe* - "The French Constitutional Council censures the 3 strikes law" - http://www.edri.org/edri-gram/number7.12/3-strikes-censured-council-constitutional. See the opinion of the Constitutional Council of France (in French) at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html
74 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-590-dc/decision-n-2009-590-dc-du-22-octobre-2009.45986.html
75 Unofficial English translation of the Hadopi law http://www.laquadrature.net/wiki/HADOPI_full_translation

103. The Hadopi authority started sending first infringement notices in October 2010. However, as early as January 2010, there were reports that Trident Media Guard ("TMG") had been selected by the French entertainment industry to detect and report illegal file-sharing via P2P.[76] In June 2010, the Société des auteurs, compositeurs et éditeurs de musique ("SACEM") was reported to have confirmed that TMG had been engaged and would be monitoring illegal P2P file-sharing of a set of reference works. It was also reported that SACEM anticipated TMG would be able to provide reports on 50,000 incidents/day (music and audio-visual).[77]

104. Reportedly, in the period from October to December 2010, the Hadopi authority asked ISPs to identify approximately 100,000 infringing IP addresses. Estimates as to the number of email warnings sent by the authority in the same period vary from 20,000-25,000.[78]

New Zealand

105. The New Zealand proposal to temporarily suspend Internet accounts of copyright infringers is intended to be applied through its judicial system. The NZ *Copyright (Infringing File Sharing) Amendment Bill 2010* provides:

> 122O Court order suspending account holder's account
>
> (1) A District Court may, on application by a copyright owner, make an order requiring an ISP to suspend the account of an account holder for a period of up to 6 months if the court is satisfied that—
>
> (a) an enforcement notice has been sent to the account holder in accordance with this Act in relation to infringements against the copyright owner; and
>
> (b) the application for the order is made at least 2 weeks after the date of the most recent enforcement notice sent to the account holder in relation to infringements against the copyright owner; and
>
> (c) suspension of the account is appropriate in the circumstances, given the seriousness of the infringing.
>
> (2) In considering the seriousness of the infringing, the court may consider any evidence put before it by the copyright owner, including any infringement notices relating to infringements against the copyright owner that have been sent to the account holder at any time.

76 *TorrentFreak* – "BitTorrent Spammers Chosen to Spy On French Pirates" (27 January 2010) http://torrentfreak.com/bittorrent-spammers-chosen-to-spy-on-french-pirates-100126

77 *TorrentFreak* – "Scope of French '3 Strikes' P2P Piracy Monitoring Confirmed" (24 June 2010) http://torrentfreak.com/scope-of-french-3-strikes-hadopi-piracy-monitoring-confirmed-100624

78 *TorrentFreak* – "Hadopi Sends 100,000 Warning Emails To Suspected Pirates" (29 December 2010) http://torrentfreak.com/hadopi-sends-100000-warning-emails-to-suspected-pirates-101229

(3) When considering the circumstances, and determining the duration, of a proposed suspension, the matters that the court may consider include, but are not limited to,—

(a) the degree of the account holder's reliance on access to the Internet; and

(b) the identity (if known) of the user who engaged in the infringements identified in the notices; and

(c) any other matter that may be specified in regulations.[79]

106. It appears, despite the title of the Bill, that such an order might be made in respect of other forms of copyright infringement, as "file sharing" is defined as follows:

file sharing is where material—

(a) is downloaded from the Internet; or

(b) is made available on the Internet by a user in a form in which the material may be downloaded by 1 or more other users; or

(c) is transferred, directly or indirectly, via the Internet from one user to another user.

107. A report from the New Zealand Commerce Committee released on 3 November 2010[80] recommended the Bill be passed with certain amendments. In particular:

- reducing the scope of the definition of ISPs "… with the aim of excluding universities, libraries, and businesses that provide Internet access but are not traditional ISPs";

- changing the definition of "file sharing" to include "… reference to downloading or uploading material using networks or applications that allow material to be shared among multiple users … to avoid inadvertently capturing activities such as emailing or downloading that did not involve file sharing…";

  (The report notes that copyright infringement via email or downloading that did not involve file sharing would be covered by existing copyright law.)

- shifting the onus of proof by providing that an infringement notice establishes a rebuttal presumption that infringement has occurred; and

- preventing an application for an order suspending Internet access pending an Order in Council (effectively suspending the operation of the provision).

79 http://www.legislation.govt.nz/bill/government/2010/0119/latest/DLM2764327.html#DLM2764355
80 http://www.parliament.nz/NR/rdonlyres/47ED3168-0231-42D9-9245-F82EEAD38575/164872/DBSCH_SCR_4901_CopyrightInfringingFileSharingAmend.pdf

> Explanation:
>
> If evidence indicated that notices alone (and the remedy through the Copyright Tribunal) were not having the desired deterrent effect, the suspension provisions could be activated by Order in Council. The majority of us believe this approach would create the right incentives, with the remedy of suspension able to be brought into effect if needed. We would expect an appropriate timetable for monitoring and review to be developed in consultation with rights holders. We note that a similar approach was recently adopted in the United Kingdom.

United Kingdom

108. The United Kingdom (U.K.) proposal to temporarily suspend Internet accounts outlined in the then *Digital Economy Bill 2009-2010* was intended to be applied by a direction from the Secretary of State to Ofcom with parliamentary approval[81]. However, in a statement on 23 February 2010, the U.K. Government said:

> We will not terminate the accounts of infringers - it is very hard to see how this could be deemed proportionate except in the most extreme – and therefore probably criminal – cases.
>
> We added account suspension to the list of possible technical measures which might be considered if our measures to tackle unlawful file-sharing through notifications and legal action are not as successful as we hope. This is but one of a number of possible options on which we would seek advice from Ofcom – and others – if we decided to consider a third obligation on technical measures. However what is clear is that we would need a rapid and robust route of appeal available to all consumers if we decided technical measures were needed.[82]

109. The *Digital Economy Act 2010 (U.K)* retains the proposed power to require ISPs to suspend service to subscribers as one of the technical measures:

> … a measure that -
>
> (a) limits the speed or other capacity of the service provided to a subscriber;
>
> (b) prevents a subscriber from using the service to gain access to particular material, or limit such use;
>
> (c) suspends the service provided to a subscriber; or
>
> (d) limits the service provided to a subscriber in another way[83]

81 s.10 and s.11 http://www.publications.parliament.uk/pa/ld200910/ldbills/032/10032.12-17.html#j158
82 http://www.number10.gov.uk/Page22497
83 s.9 *Digital Economy Act 2010 (U.K.)* – For details of the intended scope see paragraph 51 of the *Explanatory Notes to the Digital Economy Act 2010 (U.K.)* at http://www.legislation.gov.uk/ukpga/2010/24/notes?type=en and paragraph 1.6 of the *Consultation Document for the Draft Initial Obligations Code* released by Ofcom on 28 May 2010 at http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf

"for the purpose of preventing or reducing infringement of copyright by means of the internet".[84] However, under the Act, no order may be made by the Secretary of State without parliamentary approval and not before 12 months after an initial obligations code has come into force. A Draft Initial Obligations Code was released by Ofcom for public consultation on 28 May 2010. Ofcom expects the code[85] will come into force in early 2011.[86] Further, as noted in paragraphs 111 to 113, the Act is under review.

110. At present, Ofcom is preparing to implement the infringement notice aspect of the *Digital Economy Act 2010 (U.K.).* In a Department for Culture, Media and Sports new release dated 1 February 2011, Deputy Prime Minister Nick Clegg said:

> Ofcom is currently preparing to implement the Digital Economy Act's mass notification system. This aims to tackle the most prolific form of online copyright infringement by writing to those identified as sharing music, films and other content unlawfully through file-sharing networks.[87]

Review of the Digital Economy Act 2010 (U.K.)

111. On 10 November 2010, the U.K. Parliament Culture, Media and Sport Committee announced an inquiry into the Protection of Intellectual Property Rights Online. That inquiry will consider issues such as:

> The implementation, practicality and likely effectiveness of the relevant measures contained in the Digital Economy Act. In particular:
>
> - Whether the new framework has captured the right balance between supporting creative work online and the rights of subscribers and ISPs.
> - Whether the notification process is fair and proportionate.
> - The extent to which the associated costs might hinder the operation of the Act.
> - At what point, if at all, consideration should be given to introducing the additional technical measures allowed for under the Act.[88]

112. On 11 November 2010, the High Court of Justice granted British Telecommunications PLC and TalkTalk Telecom Group PLC ("the applicants") leave to seek judicial review of s.3–18 of the *Digital Economy Act 2010 (U.K.)* ("the contested provisions"). The hearing

84 See s.9 http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_2#pb2-l1g9
85 Draft code as at 30 July 2010 - http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf
86 http://media.ofcom.org.uk/2010/05/28/draft-code-of-practice-to-reduce-online-copyright-infringement
87 Department for Culture, Media and Sports News Release – "Ofcom to review aspects of Digital Economy Act - http://www.culture.gov.uk/news/media_releases/7756.aspx
88 Committee launches a new inquiry into the Protection of Intellectual Property Rights Online http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/news/committee-announces-new-inquiry

is scheduled for a date to be determined as soon as possible after 7 February 2011. The applicants' grounds of review are as follows:

> The contested provisions:
>
> - contravene the requirements of the Technical Standards Directive[89]
> - are incompatible with the E Commerce Directive[90]
> - are incompatible with the PEC Directive[91]
> - are disproportionate in their effect, in that they unduly restrict the ability of ISPs established in other Member States to provide internet services in the United Kingdom and/or infringe Articles 8 and/or 10 of the European Convention on Human Rights and equivalent provisions found in the EU Charter on Fundamental Rights.[92]

In his reasons for decision, Wyn Williams J said at [3] and [5]:

> The issue in relation to ground 1 is whether the contested provisions of the Communications Act 2003 (introduced by amendment by virtue of the Digital Economy Act 2010) constitute a technical regulation and/or a rule on services within the meaning (sic) Directive 98/34/EC. In turn that depends upon whether one or more of the contested provisions has or have legal effects of its/their own. In my judgment it is open to serious argument that the obligations of internet service providers under sections 124A and 124B of the 2003 Act do have such legal effect.
>
> It is common ground that if the contested provisions constitute a technical regulation they should have been referred to the EU Commission prior to enactment and they were not.[93]

113. With the consent of the parties, a number of interested organisations (including Producers' Alliance for Cinema and Television (Pact), the Motion Picture Association, the British Recorded Music Industry, the Premier League, the British Video Association, the Film

89 *Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations as amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations* – See http://www.etsi.org/WebSite/document/about ETSI/EC_other/Directive_1998_48.pdf

90 *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* – See http://www.etsi.org/WebSite/document/aboutETSI/EC_other/Directive_2000_31.pdf

91 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* – See http://www.etsi.org/WebSite/document/aboutETSI/EC_other/Data_Privacy_Directive.pdf

92 Statement of Facts and Grounds, see paragraphs 49 and following http://www.btplc.com/newsadmin/attachments/statement%20of%20facts%20and%20grounds.pdf

93 http://www.btplc.com/newsadmin/attachments/order%2011%20nov%202010.pdf

Distributors' Association, the British Media & Entertainment Union and the Open Rights Group) have been granted leave to intervene in the proceedings.[94]

Republic of Korea

Orders to suspend accounts

114. Amendments to the Republic of Korea (South Korea)'s *Copyright Act* which took effect on 23 July 2009[95], gave the Minister of Culture, Sports and Tourism ("MCST") the power to require Online Service Providers ("OSPs") to suspend accounts of infringers who had received three or more warnings.[96] OSPs are defined as:

> … the persons who provide others with services that reproduce or interactively transmit works, etc. through information and telecommunications networks.[97]

[Order to give warnings] Article 133-2 (1) (English version) states:

> In the case where reproductions or information infringing on copyrights and other rights protected pursuant to this Act or programs or information circumventing technological protection measures (hereinafter referred to as "illegal reproductions, etc.") are interactively transmitted through information and telecommunications networks, the Minister of Culture, Sports and Tourism may order online service providers to take any of the following measures as prescribed by Presidential Decree after deliberation by the Commission:
>
> 1. Issuing warnings against reproducers and interactive transmitters of illegal reproductions, etc.; and
>
> 2. Deletion or suspension of interactive transmission of illegal reproductions, etc.[98]

[Order to suspend account] Article 133-2 (2) (English version) states:

> If a reproducer or interactive transmitter who received three or more warnings as prescribed under Subparagraph 1 of Paragraph (1) of this Article interactively transmits illegal reproductions, etc., the Minister of Culture, Sports and Tourism may order online service providers to suspend the account [which refers to accounts on usage rights used by online service providers to identify and manage users (excluding email exclusive accounts) and includes other accounts provided by

94 *The Guardian* – "Rights holders alliance to defend Digital Economy Act" http://www.guardian.co.uk/technology/2011/jan/31/rights-holders-digital-act and Open Rights Blog (20 January 2011) "ORG will intervene in DEA Judicial Review" - http://www.openrightsgroup.org/blog

95 http://www.zeropaid.com/news/86703/south-koreas-three-strikes-law-takes-effect

96 See *Copyright Act* which can be downloaded here http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=21

97 See *Copyright Act* which can be downloaded here http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=21

98 See *Copyright Act* which can be downloaded here http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=21

> the corresponding online service providers] of the corresponding reproducer or interactive transmitter within a period of no more than six months as prescribed by Presidential Decree after deliberation by the Commission.[99]

[Advance notice of suspension] Article 133-2 (3) (English version) states:

> An online service provider receiving an order as prescribed under Paragraph (2) shall notify the corresponding reproducer or interactive transmitter of the fact that the corresponding account will be suspended according to Presidential Decree within seven days before suspending the account.[100]

(Email exclusive accounts appear to be exempt from suspension.)

115. With effect from 3 November 2010, the MCST ordered the suspension of 11 subscribers' accounts. Reportedly, these are the first instances (globally) of ordered suspension of Internet access for online copyright infringement.[101] (The affected subscribers' names were published on 4 October 2010 in the Korean Official Government Gazette and afforded 24 days within which to contest the orders. None of the subscribers filed an objection.)[102]

116. MCST Deputy Director Choi said:

> If internet users think that they can violate copyright online despite repeated warning, we will have no choice but to cut off their means of access through their OSP accounts. We are hopeful that the account suspensions will make users appreciate the need to act responsibly.[103]

Recommendations to suspend accounts

117. Amendments to the Republic of Korea (South Korea)'s *Copyright Act* which took effect on 23 July 2009[104], also gave the Korea Copyright Commission (a newly created body) ("the KCC") the power to recommend OSPs send warnings and/or suspend accounts of infringers.[105]

Articles 133-3 (1) – (3) (English version) state:

> (1) When investigating the information and telecommunications networks of online service providers and learning that illegal reproductions, etc. are interactively transmitted, the

99 See the *Copyright Act* which can be downloaded here http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=21
100 See the *Copyright Act* which can be downloaded here http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=21
101 *MPA Int. News Release* - "Korean Government orders suspension of online accounts of copyright infringers" (3 November 2010) http://mpa-i.org/newspress/newspress_korea101103.html
102 *MPA Int. News Release* - "Korean Government orders suspension of online accounts of copyright infringers" (3 November 2010) http://mpa-i.org/newspress/newspress_korea101103.html
103 *MPA Int. News Release* – "Korean Government orders suspension of online accounts of copyright infringers" (3 November 2010) http://mpa-i.org/newspress/newspress_korea101103.html
104 http://www.zeropaid.com/news/86703/south-koreas-three-strikes-law-takes-effect
105 See the *Copyright Act* which can be downloaded here http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=21

Commission may deliberate on such and recommend the online service providers to take correction measures under any of the following:

1. Issuing warnings against reproducers and interactive transmitters of illegal reproductions, etc.;

2. Deletion or suspension of interactive transmission of illegal reproductions, etc.; and

3. Suspension of the accounts of reproducers and interactive transmitters which repeatedly interactively transmit illegal reproductions, etc.

(2) Within five days from receiving a recommendation under Paragraphs (1) and (2) of Article 1 and within ten days from receiving a recommendation under Paragraph (3) of Article 1, online service providers shall notify the Commission of the consequences of carrying out the recommendation.

(3) If online service providers fail to follow a recommendation under Paragraph (1), the Commission may request the Minister of Culture, Sports and Tourism to issue an order under Paragraphs (1) and (2) of Article 133-2.[106]

118. In the period from 23 July 2009 to 31 July 2010 (the first year of operation):

- the KCC recommended OSPs issue warnings against 32,878 account holders[107]
- OSPs, following the recommendations, sent warnings to 32,838 account holders[108]
- 31 Internet subscribers had their accounts suspended by their OSPs for less than one month, as recommended by the KCC[109].

OSPs (with the exception of one unnamed OSP) have followed the KCC's recommendations.[110]

119. Article 133-3 is particularly controversial because it does not require a graduated response – an account holder could have his or her account suspended without the three or more warnings that are required when suspension is ordered by the MCST. Nonetheless, it appears that the KCC's own procedures require three or more warnings to be issued before making a recommendation of suspension.[111]

106 See *Copyright Act* which can be downloaded here http://www.moleg.go.kr/english/korLawEng?pstSeq=52683&pageIndex=21

107 Slide 5 at http://aimp.apec.org/Documents/2010/IPEG/IPEG2/10_ipeg31_033.pdf

108 Figure drawn from TechDirt article – "A Look at How Many People Have Been Kicked Offline in Korea on Accusations (Not Convictions) Of Infringement" (26 October 2010) http://www.techdirt.com/articles/20101025/18093711583/a-look-at-how-many-people-have-been-kicked-offline-in-korea-on-accusations-not-convictions-of-infringement.shtml

109 http://freedomforip.org/2010/10/25/three-strikes-in-south-korea-stats and see also slide 5 at http://aimp.apec.org/Documents/2010/IPEG/IPEG2/10_ipeg31_033.pdf

110 TechDirt – "A Look At How Many People Have Been Kicked Offline in Korea On Accusations (Not Convictions) Of Infringement" (26 October 2010) http://www.techdirt.com/articles/20101025/18093711583/a-look-at-how-many-people-have-been-kicked-offline-in-korea-on-accusations-not-convictions-of-infringement.shtml

111 See note in *Hurips Blog* (24 October 2010) http://hurips.blogspot.com/2010/10/facts-and-figures-on-copyright-three.html

Republic of Chile

120. Amendments to the Chilean *La Ley Propiedad Intelectual* (No. 17336) in May 2010, allow a Court to order the termination of the contract for supply of access to the Internet between an ISP and subscriber whom has been found by the Court to be a repeat infringer.[112] The legislation provides:

> … Any such relief measures shall be issued with due regard for the relative burden to the service provider, to users and subscribers, the potential harm to the holders of copyright or related rights, the technical feasibility and effectiveness of the remedy, and whether less burdensome enforcement methods are available.
>
> These measures shall be ordered after due notice has been given to the service provider, pursuant to paragraphs 3, 4 and 5 of Article 85 Q, except for orders ensuring the preservation of evidence or other orders that are not expected to have an effect on the operation
>
> (Unofficial English version)

Republic of China

121. The Republic of China (also known as "Chinese Taipei" or "Taiwan") introduced amendments to its *Copyright Act* on 13 May 2009 which provide an ISP with protection against liability if, among other things, it "… informs users that in the event of repeat alleged infringements up to three times the service provider shall terminate the service in whole or in part".[113] ISPs are very broadly defined under the Act and include caching service providers, information storage service providers and search service providers as well as connection service providers.[114]

> Chapter VI-1 Limitations on Liability for Internet Service Providers
>
> Article 90quinquies
>
> An Internet service provider shall be entitled to the application of Article 90sexies to Article 90novies regarding the limitation on liability only if the service provider—
>
> 1. by contract, electronic transmission, automatic detective system or other means, informs users of its copyright or plate right protection policy, and takes concrete action to implement it; and
>
> 2. by contract, electronic transmission, automatic detective system or other means, informs users that in the event of repeat alleged infringements up to three times the service provider shall terminate the service in whole or in part; and (sic)

112 http://www.leychile.cl/Navegar?idNorma=28933

113 See the *Copyright Act 2010* which can be downloaded here http://www.tipo.gov.tw/en/AllInOne_Show.aspx?path=2557&guid=26944d88-de19-4d63-b89f-864d2bdb2dac&lang=en-us and TIPO News Release – "ISP Liability Bill Completed Third Reading at the Legislative Yuan on April 21" (24 April 2009) http://www.tipo.gov.tw/en/News_NewsContent.aspx?NewsID=3675

114 See Article 3 Paragraph 19 of the *Copyright Act 2010*

3. publicly announces information regarding its contact window for receipt of notification documents.

4. accommodate and implement the technical measure described in paragraph 3.

A connection service provider that, after receiving notification by a copyright holder or plate rights holder of alleged infringement by a user, has forwarded the notification to that particular user by electronic mail is deemed to have met the requirement in the preceding paragraph, subparagraph 1.

If a copyright holder or plate rights holder has provided technical measures which have been developed based on a broad consensus and are used to identify or protect copyrighted or plate-righted works, the Internet service provider shall accommodate and implement the measures if the technical measures has been ratified by the competent authority.

The procedures for infringement notices are prescribed by *Regulations Governing Implementation of ISP Civil Liability Exemption,* which came into effect on 17 November 2009.[115]

122. A news release from the Taiwan Intellectual Property Office ("TIPO") states:

> … To take advantage of this 'safe-harbor', service providers must, prior to providing their services, clearly inform users of the copyright protection measures they adopt, and also inform users that partial or complete termination of services would be carried out if they have three repeated alleged infringements.[116]

123. The "safe harbour" approach, i.e. conditional liability for ISPs, has existed for some time (e.g. § 512 of Chapter 5 of Title 17 of the U.S. Code[117]), however, requiring a "graduated response" procedure for that protection is a relatively new adaptation.

United States of America

124. Section 512 of Chapter 5 of Title 17 of the *U.S. Code*[118] provides ISPs with protection from liability for copyright infringement where they are acting as "the conduit". However, the limitation of liability is subject to the following provision, (i):

> (1) Accommodation of technology.— The limitations on liability established by this section shall apply to a service provider only if the service provider—

115 Available at http://www.tipo.gov.tw/en/AllInOne_Show.aspx?path=2557&guid=26944d88-de19-4d63-b89f-864d2bdb2dac&lang=en-us See also *TIPO News Release* – "Regulations Governing Implementations of Limitations on the Liability of ISP enters into force November 17, 2009" (25 November 2009) http://www.tipo.gov.tw/en/News_NewsContent.aspx?NewsID=4259

116 *TIPO News Release* – "ISP Liability Bill Completed Third Reading at the Legislative Yuan on April 21" (24 April 2009) http://www.tipo.gov.tw/en/News_NewsContent.aspx?NewsID=3675

117 http://www.law.cornell.edu/uscode/17/usc_sec_17_00000512----000-.html

118 http://www.law.cornell.edu/uscode/17/usc_sec_17_00000512----000-.html

> (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and
>
> (B) accommodates and does not interfere with standard technical measures.
>
> …

Section 512 does not specify what the termination policy should be or how it should be applied. Compared to the "notice and take-down" provisions of § 512 (at paragraph (c)) (otherwise known as "DMCA[119] notices") which have been extensively applied[120], it appears that U.S. ISPs have not generally adopted a termination or suspension policy.[121]

Hong Kong Special Administrative Region of the People's Republic of China

125. In 2009, the Hong Kong Legislative Council Panel on Commerce and Industry released a paper entitled *Proposals for Strengthening Copyright Protection in the Digital Environment* and said, regarding graduated response:

> … Meanwhile, copyright owners have been pressing the Tripartite Forum to introduce a "graduated response" system, as proposed or implemented in France, South Korea, New Zealand etc, into the Code. Under this system, warning notices will be issued to subscribers identified as having engaged in online infringing activities (such as unauthorised downloading or file-sharing activities). Repeat infringers who disregard the warning notices on three occasions could have their Internet access suspended for up to one year. The "graduated response" system is clouded by debates over its implications on civil rights and liberties even in jurisdictions where legislation introducing the system has been passed. Some criticise the system, which effectively deprives users of their Internet connection based on claims by copyright owners, as being disproportionate. Furthermore, the European Parliament recognised access to the Internet as a fundamental right, the limitation of which should be subject to the prior ruling of the Court. **We believe that it is not an opportune time to consider introducing such a system in Hong Kong, especially when its implications are yet to be fully tested in overseas jurisdictions**.[122] (emphasis added)

International negotiations

Anti-Counterfeiting Trade Agreement

126. In April 2010, after the 8th round of negotiations, the then draft consolidated ACTA text was released to the public.[123] One of the proposals under "enforcement procedures in the

119 DMCA – *Digital Millennium Copyright Act*
120 As noted in paragraph 82
121 Although, as noted in paragraph 129, Suddenlink (a U.S. ISP) was reported in September 2010 to have implemented a graduated response procedure.
122 http://www.legco.gov.hk/yr09-10/english/panels/ci/papers/ci1117cb1-341-8-e.pdf
123 http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf

digital environment" was to limit the civil liability of OSPs for online copyright infringement on condition, among other things, OSPs "remove or disable access to infringing material or infringing activity upon obtaining actual knowledge of the infringement …" and meet the requirements of "… adopting and reasonably implementing a policy to address the unauthorized storage or transmission of materials protected by copyright or related rights". OSPs were broadly defined:

> … **online service provider** and **provider** mean a provider of online services or network access, or the operators of facilities therefore, and includes an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.[124]

If such a proposal were to be adopted by the negotiating countries, some OSPs in those countries (and elsewhere) might choose to adopt a "graduated response" process as part of their strategy to avoid liability for online copyright infringement by their subscribers.

127. Further, the then draft ACTA text stated:

> Paragraph 3(a) shall not affect the possibility for a judicial or administrative authority, in accordance with the Parties legal system, requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility of the parties establishing procedures governing the removal or disabling of access to information

i.e. such as that presently in place in France (i.e. the Hadopi law).

128. The Article 29 Data Protection Working Party observed in its letter dated 16 July 2010 to the European Commissioner for Trade[125]:

> To mitigate minor alleged copyright infringement carried out by individuals, the current text would stimulate the signatory states to oblige Internet providers in case of copyright infringements to "terminate or to prevent the infringing act" or "to determine procedures in order to prevent access to information or in order to remove them". We recognize that these wordings may not explicitly provide for Internet access blocking. The (sic) do not provide either for the monitoring of the Internet to enable the identification of alleged infringers. **Nevertheless, they indicate that the … parties to ACTA shall at least be encouraged to voluntarily include Internet access blocking** and to some extend (sic) the monitoring of the Internet to enable identification of alleged infringers as an answer to copyright infringements into national legislation. (emphasis added)

124 See page 21 http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf
125 http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm

129. These are three examples of ISPs that have voluntarily chosen to introduce such a process:

Eircom (Ireland)

- In May 2010[126], Eircom (an ISP in Ireland) introduced a pilot graduated response procedure for its broadband subscribers, focused on the illegal distribution of copyright content via P2P networks. Under the pilot procedure, Eircom stated that Internet access would be suspended for non-business customers for 7 days on the third infringement and disconnected for 12 months on the fourth infringement. Affected subscribers would receive a refund for the 7 days suspension.[127]

- In December 2010, Eircom ended the pilot and announced the introduction of a "graduated response programme" for "customers who deliberately and persistently infringe copyright".[128] The protocol for the program is confidential, but Eircom provided the following overview in its announcement[129]:

> As part of this agreement, IRMA will provide eircom with notifications which will contain among other details, the IP address identified as engaging in illegal music file sharing in breach of copyright along with evidence of the infringement. The IP addresses have been captured in accordance with relevant laws and processed on IRMA's behalf via a third party. eircom on receipt of the notification will:
>
> - Contact identified eircom customers to inform them that their broadband account has been linked to an IP address detected by IRMA, as engaging in illegal music file sharing in breach of copyright. eircom will clearly advise the customer that such acts are illegal and in breach of the terms and conditions of broadband service, and eircom will provide information as to how the customer can avoid repeating the infringement.
>
> - If the customer continues to engage in the illegal file sharing of copyrighted music, eircom will send the customer a second warning letter indicating that unless the infringement ceases the customer's broadband service will be suspended.
>
> - Where there is a third notification of infringement, eircom will write to the customer advising that eircom has received a third notification of illegal filesharing of music and eircom will then proceed to withdraw the customer's broadband service for a period of 7 days.
>
> - The customer will also be informed that should they continue to engage in illegal filesharing of music illegally in breach of copyright and a further

126 *The Irish Times* – "Eircom to cut broadband over illegal downloads" (24 May 2010) http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html
127 See FAQs http://www.eircom.net/notification/legalmusic/faqs
128 *Eircom Statement on Illegal File Sharing* http://pressroom.eircom.net/press_releases/article/eircom_Statement_on_Illegal_File_Sharing
129 *Eircom Statement on Illegal File Sharing* http://pressroom.eircom.net/press_releases/article/eircom_Statement_on_Illegal_File_Sharing

> notification of infringement is received, the customer's broadband service will be disconnected for a 12 month period.

The introduction of this program coincided with Eircom's launch of MusicHub, a free music streaming and pay-for-download service for its broadband customers.[130]

Suddenlink (U.S.A.)

- Suddenlink (an ISP in U.S.A.) is also reported (as at September 2010) to apply a graduated response procedure to its subscribers, suspending subscribers' Internet access for 6 months after receipt of three *Digital Millennium Copyright Act* ("DMCA") notices.[131]

Karoo (Hull, U.K.)

- In July 2009, Karoo (an ISP in Hull, U.K.) received strong criticism for its broadband suspension policy. Karoo, the sole supplier of broadband in the area, initially did not include a graduated response procedure (i.e. infringement notices) before suspension. In response, Karoo advised that it would implement a procedure requiring three notices before suspension.[132] Karoo is then reported to have changed its policy, i.e.:

> We will no longer suspend a customer's service unless we receive a court order from a copyright owner taking legal action. As a result it is the responsibility of the legal system, not Karoo, to ensure the accuracy of the information provided by the copyright owners.[133]

130. There were further negotiations following the April 2010 release of the draft consolidated ACTA text. Another consolidated text was released to the public on 6 October 2010 after the 11th and stated final round of negotiations in Tokyo.[134] The final (legally reviewed) ACTA text was released in early December 2010.[135]

131. The proposal (referred to in paragraph 126 above) that ACTA parties provide ISPs with conditional protection from liability appears to have been removed. However, a new article has been inserted (article 27(3)) which provides:

> Each party shall endeavor to promote cooperative efforts within the business community to effectively address … copyright or related rights infringement ….

Thus, it is not inconceivable that parties to ACTA (governments) might choose to encourage OSPs (a term which is no longer defined in the text) to voluntarily adopt a

130 *Eircom Press Release* – "eircom Launches MusicHub" (8 December 2010) http://pressroom.eircom.net/press_releases/article/eircom_launches_musichub
131 *TorrentFreak* – "US ISP Disconnects Alleged Pirates for 6 Months" (24 September 2010) http://torrentfreak.com/us-isp-disconnects-alleged-pirates-for-6-months-100924
132 *BBC News* – "Plug-pulling ISP changes policy" (24 July 2009) http://news.bbc.co.uk/2/hi/technology/8166640.stm
133 *TorrentFreak* – "Karoo Won't Disconnect Pirates Without a Court Order" (10 August 2009) http://torrentfreak.com/karoo-wont-disconnect-pirates-without-a-court-order-090810
134 http://www.ustr.gov/webfm_send/2338
135 http://www.dfat.gov.au/trade/acta/Final-ACTA-text-following-legal-verification.pdf

graduated response process or other technical measures in return for protection from liability.

132. In any case, although ACTA does not require parties to the agreement to impose Internet-focused enforcement measures such as suspension of Internet access, it does require that:

> … enforcement procedures … are available … so as to permit effective action against an act of infringement of intellectual property rights which takes place in the digital environment, including expeditious remedies to prevent infringement and remedies which constitute a deterrent to further infringements[136]

How this will be implemented remains to be seen.

Examining suspension of Internet access as an enforcement measure

133. In the following paragraphs, we consider the likely effectiveness of using suspension of Internet access as an enforcement measure against online copyright infringement and explore some of the potential issues for the Internet, Internet technologies, access and Internet use. In this discussion, we consider only suspension of Internet access, not the preceding infringement notices which are typically the first part of a graduated response process. These are discussed above at paragraph 82 and following.

What methods of copyright infringement and/or categories of infringers is the policy designed to address?

134. This policy (suspension of Internet access), as a general rule, is intended to be applied as part of a graduated response which incorporates the sending of infringement notices before suspension is contemplated (see the discussion at paragraph 82 and following). It is also generally intended to be applied to repeat infringers irrespective of what method they use to infringe copyright via the Internet. However, as noted above in paragraph 103, it appears that, at least in this introductory period, the Hadopi law will only be applied to copyright infringement via P2P.[137]

135. Suspension of Internet access (the ultimate step in a graduated response process) is a sanction intended to deter the individual (and others) from infringing copyright via the Internet. The earlier steps (i.e. infringement notices) are intended to: raise awareness about copyright and infringement; educate; warn; and influence behaviour (i.e. encourage Internet users not to infringe copyright). Although the application of the policy would prevent an individual from infringing copyright via the suspended Internet connection for a period of time, the real driver for this policy would appear to be its potential specific and general deterrent effect.

136 Article 27(1) – ACTA text available at http://www.dfat.gov.au/trade/acta/index.html
137 Note: the Hadopi law is not limited to infringement via P2P

136. It presently appears that governments which have adopted, or are considering adopting, such a sanction only intend to apply suspension against repeat infringers at the end of a graduated response process. Unless otherwise stated, we have assumed, for the purposes of this discussion, that the policy would only be applied against this category of Internet subscriber.

137. It should be noted that many ISPs' terms of service already provide a contractual right to suspend a subscriber's account for unlawful activity, including infringement of copyright. Indeed, as noted above in paragraph 129, at least a couple of ISPs have already implemented such a policy. Under such voluntary schemes ISPs generally retain the discretion to determine when to suspend or terminate a subscriber's account. In any case, the remedy is for breach of contract rather than for a contravention of copyright law, even though the reason for suspension may be copyright infringement.

How effective is the policy likely to be at preventing or reducing copyright infringement?

What solutions might infringers choose or develop in response? What impact would these have?

138. The policy would prevent copyright infringement via the suspended Internet connection for the duration of the suspension. The connection may or may not be the infringer's only, usual or most convenient access to the Internet. Many users have multiple Internet access points - e.g. fixed line at home; wireless; fixed line and/or wireless at work; wireless access through public WiFi hotspots; 3G mobile phone; Internet-enabled TV, etc. For some users, suspension of their access to one of these access points may be no more than an inconvenience. However, there may be some users who have only one access point and no ability to find an alternative (e.g. due to remote location). In those limited cases, it is likely the policy would successfully prevent that user from engaging in all forms of online copyright infringement.

139. Repeat infringers who have deliberately disregarded warning notices are unlikely to be deterred by temporary suspension of their usual Internet connection. For the policy to have any real deterrent effect, these users would have to be banned from all Internet access points, which may be impossible to enforce. Such users could, among other things, access unsecured WIFI, create their own ISP, or simply use another person's Internet access with their consent. Thus, in practice, the policy's effectiveness is likely to be limited. Nonetheless, if the policy and its application are highly publicised, the threat of disconnection for breach of copyright might discourage more casual infringers.

What impact would the policy have on privacy?

140. We discuss some of the potential privacy implications associated with detecting infringement, identifying infringers, infringement notices and content identification in other sections of this document. Here, we discuss the potential privacy implications of suspending Internet access.

141. If an Internet connection is suspended, all traffic via that connection would cease for the duration of the suspension (assuming the subscriber is not able to circumvent the technical suspension). Nonetheless, the policy may raise some potential privacy issues for the affected subscribers and other users of the connection when they use, or attempt to use, other less secure means to access the Internet for the duration of the suspension (e.g. unsecured WiFi).

142. Proposals for a national list of suspended subscribers to prevent affected subscribers from obtaining Internet access through other ISPs could also raise privacy issues. An earlier proposed version of the Hadopi law contained a proposal but sought to limit access to this personal information as follows:

> In order to guarantee that the suspensive measures decided on are respected, the internet service providers will have to check when agreeing to any new contract, that the contracting party is not part of a list of people, managed by the High Authority, whose subscription has been suspended.
>
> … Furthermore, consultation by the internet service providers of the list of suspended subscribers will be done in the form of a simple query about the presence of the contracting party's name.[138]

(Note: this proposal was not included in the enacted Hadopi law.)

Would the policy discriminate against legitimate uses of applications?

Would the policy discourage or prevent the use of certain technologies and/or development of new communications protocols?

143. Assuming the policy is applied across all subscribed Internet access platforms (fixed, mobile, "smart phone", Internet-enabled TV etc.) it would be technology neutral and would not discriminate between legitimate and illegitimate uses of applications. It would prevent the subscriber and other users of the connection from using all online applications, services and technologies for the duration of the suspension via the suspended Internet connection.

144. If the policy is only applied to certain methods of online copyright infringement such as P2P file-sharing, the policy may discourage Internet users from using those protocols and applications, even for legitimate purposes, out of a concern that their Internet connection may be suspended. However, this is really more of an issue related to detection of infringement.

Would the policy alter the basic architecture of the Internet? Are there any unpredictable or identifiably negative consequences?

145. To avoid the application of the policy (i.e. by avoiding detection in the first place) or perceived privacy intrusions (whether real or not) associated with the various techniques used to detect infringers, users (including innocent users) may alter the way they send and receive data. Such trends may include increased use of encryption, online anonymity solutions and closed private networks.

138 Explanatory Memorandum to the Government Bill promoting the dissemination and protection of creative works on the internet www.culture.gouv.fr/culture/actualites/.../creainterenglish.pdf

146. If ISPs are required to temporarily suspend more than just a few users each year, they may consider it cost effective to develop and implement semi-automatic systems for switching on and off subscribers' connections, and preventing another supplier from reconnecting the subscriber through the same connection (e.g. ADSL or 3G). This could introduce a process-driven uniform technical framework for rapid disconnection. Once there is a semi-automated (and potentially externally controlled or directed) system for connecting and disconnecting a subscriber's connection, such a system could be easily used to disconnect the subscriber for other reasons (e.g. content that is considered inappropriate).

What impact would the policy have on security?

147. The act of temporarily disconnecting a subscriber from the Internet should not impact the security of the Internet as the subscriber's connection (an end-point) is merely disconnected from the network. However, assuming the subscriber cannot circumvent the suspension, he or she would not be able to download operating system security patches and anti-malware/spyware updates for the duration of the suspension. Thus, the subscriber's devices may be exposed to infection upon reconnection until the subscriber is able to download and install them.

148. It is likely that "hardcore" infringers who are threatened with disconnection, or the prospect of disconnection, will simply start using far more sophisticated methods of online piracy (e.g. dynamic proxy servers, private networks etc.) which would make them more difficult to trace. Law enforcement agencies in the UK are reported to have expressed concerns that the policy would make Internet monitoring of criminals more difficult because of the stimulus to encrypt traffic.[139]

Would the policy inhibit or enhance users' willingness to access the Internet or obtain access to the Internet?

149. The policy (suspension of Internet access) is designed to be a temporary "off-switch". As such, it is not likely to have any direct impact on Internet users' *willingness* to access the Internet. However, the continued demonization of certain Internet technologies (e.g. P2P), and some of the sensationalist media coverage around proposals to suspend Internet access for online copyright infringement, risk creating a negative image of the Internet among the mainstream population. This may further deter the strands of society that have yet to take up the Internet (e.g. up to 30% of the UK population[140]) and thereby reinforce the digital divide, even in technologically advanced societies. The threat of detection and disconnection may also drive some users to closed private networks.

139 *The Times* - "MI5 comes out against cutting off internet pirates" (23 October 2009) http://www.timesonline.co.uk/tol/news/uk/crime/article6885923.ece

140 http://www.21stcenturychallenges.org/60-seconds/what-is-the-digital-divide

Would the policy directly or indirectly reduce Internet access or the availability of Internet access?

150. In some jurisdictions, access to the Internet has been recognised as a right (e.g. Article 16.2 of the Ecuador Constitution[141] and Judgment 2010-012790 of Sala Constitucional de law Corte Suprema de Justicia[142], Costa Rica). In Europe, *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services* states, among other things:

> 1) Article 1 shall be amended as follows:
>
> …
>
> (b) the following paragraph shall be inserted:
>
> "3a. Measures taken by Member States regarding end-users access' to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law.
>
> Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to effective and timely judicial review shall be guaranteed."[143]

151. The policy would prevent the subscriber from accessing the Internet via the suspended connection. It may or may not prevent that person from accessing the Internet. The policy may also prevent others who share the suspended connection from accessing the Internet.

141 http://pdba.georgetown.edu/Constitutions/Ecuador/ecuador08.html
142 http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp?param1=XYZ&param2=1&nValor1=1&nValor2=483874&strTipM=T&lResultado=1
143 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=EN&numdoc=32009L0140

The policy may affect their ability to access services, carry on their business, undertake education and carry out other aspects of their daily life. For many people, use of the Internet is part of everyday living, both from fixed and mobile access, and is now considered indispensable in most of today's technologically advanced economies. Without access to the Internet a person cannot send or receive an email, use online banking, access electronic Health records, etc. It may also be more difficult for that person to access other services, information, and communicate with their government and their community.

152. If this policy is extended to public fixed or wireless connections, the potential impact on community Internet access points may be considerable. These are common in libraries, coffee shops, train stations and other public locations. For some users, these may be their only feasible access to the Internet (e.g. due to lack of financial resources, location, mobility restrictions, etc.).

153. Further, the risk of closure of such Internet access points is likely to hinder public and community Internet access deployment, particularly open and free WiFi.

Would the policy materially raise or lower the costs of Internet access?

154. The real costs of the policy (suspension of Internet access) lie with the initial detection of infringement, the identification of infringers, the processing of infringement notices and associated judicial and administrative costs, rather than suspension itself.

155. Suspending an Internet connection that is normally used by multiple users may require those innocent users to incur additional costs to access the Internet (e.g. they may have to pay for a new account with the same or a different ISP).

Is there any risk of significant or material damage to third parties' use of or access to the Internet?

156. Whether there is any risk of significant or material damage to third parties' use of, or access to, the Internet will depend on the circumstances of the temporary disconnection. If the infringer is the only user of the Internet connection and he or she has been correctly identified, there should be no material impact on third parties. However, if there are multiple users of the same connection (as there often are) those users would be adversely affected: the extent will vary according to their individual circumstances (e.g. the reason(s) they use the Internet connection, their ability to access alternative connections, as well as the duration of the suspension and other factors). This could be avoided if an ISP could prevent one user of a subscribed Internet connection from using the connection. While technically possible, by creating separate access credentials for each user, it would be practically impossible to prevent others from sharing their credentials with the banned user.

157. Further, as noted above, if the affected connection is a public Internet connection, suspending that connection could adversely affect many other users who have no relationship with the infringer. It may be difficult to estimate the potential impact of suspending such a connection

as the supplier of that service may not even know who uses that connection, for what purposes and what alternatives they may have.

158. Eircom, in its pilot program (discussed at paragraph 129), stated that it would not suspend or disconnect its business customers. While some may argue that this may have been a commercially motivated exception, it highlights a fundamental point – many Internet connections are shared by multiple individuals for business, communication, learning, etc.

Would the policy encourage or discourage the use of certain business models?

159. A policy to suspend Internet access for copyright infringement may help drive demand for legal content (through education and the threat of disconnection) and thereby demand for legal content providers. For example, Eircom, in December 2010, launched a free music streaming service for its customers the same day that it launched its graduated response programme.[144] In their press release for the MusicHub, Eircom said:

> At the heart of the protocol is the desire to help our customers to avoid illegal copyright infringement by creating awareness about the issues surrounding copyright infringement and illegal file sharing of copyrighted music. eircom is committed to helping its customers get the most from their broadband service and ensuring customers can access the world of digital music in a legal way. Today's launch of eircom MusicHub gives eircom customers a novel, easy, inexpensive and legal way of accessing music online, which is unique in Ireland, and which reflects our commitment to meeting our customers' needs. It is a compelling alternative to illegal file sharing.[145]

160. In many cases, particularly in emerging economies, an Internet connection is a shared resource. Sharing resources enables more people to have access to the Internet and may reduce the overall cost of Internet access for a community because it encourages efficient and maximum use of infrastructure.

161. Unless there are measures to ensure that non-infringing users of a shared Internet connection are not affected by a suspension order against an infringer, subscribers may be less willing to share their connection with others leading to unnecessary duplication of infrastructure and higher Internet access costs.

162. Businesses which offer free WiFi to their customers (e.g. coffee shops, hotels, airports, train stations etc.) may also be discouraged from offering this service if there is a risk that their connection may be temporarily disconnected.

163. If this occurs, it would slow the spread of last mile Internet access, particularly wireless access.

144 *Eircom Press Release* – "eircom Launches MusicHub" (8 December 2010) http://pressroom.eircom.net/press_releases/article/eircom_launches_musichub

145 *Eircom Press Release* – "eircom Launches MusicHub" (8 December 2010) http://pressroom.eircom.net/press_releases/article/eircom_launches_musichub

164. Further, some goods and services are only supplied via the Internet (e.g. VOIP). If those suppliers normally receive income from users who have been prevented from accessing the Internet, those suppliers may lose income from those persons during the period of suspension.

165. Some businesses may see this as an opportunity to promote services to Internet subscribers to prevent users from illegally downloading or distributing copyright content via their connection. For example, in June 2010, Orange (a French ISP) reportedly started offering its customers a service designed to stop illegal downloads via P2P networks.[146] (Unfortunately, it appears that this service may have inadvertently disclosed some of its users' IP addresses on the Web. [147])

Suspension of Internet access voluntarily applied by ISPs

166. A model that provides ISPs with protection from liability provided they suspend or terminate the account of repeat infringers, in effect, shifts the decision-making from a court or a government administrative body to the ISP, in most cases a private entity. If penalties for inaction by ISPs are high, there will be greater incentives for such ISPs to rigorously enforce the policy. But, a preliminary and crucial question is how infringers will be identified and whose responsibility it is to identify them. If the responsibility rests with the ISP, without clear guidance as to what monitoring is appropriate and what is not, subscribers' and others' privacy may be adversely affected. Further, the ISP community is neither equipped nor the appropriate group of entities to be determining culpability and the appropriate remedies for online copyright infringement. Due process and judicial oversight must remain paramount.

167. Cowdroy J in *Roadshow Films Pty Ltd v iiNet Limited* (No. 3) [2010] FCA 24 observed at [435]:

> One need only consider the lengthy, complex and necessary deliberations of the Court upon the question of primary infringement to appreciate that the nature of copyright infringements within the BitTorrent system, and the concept of 'repeat infringer', are not self-evident. It is highly problematic to conclude that such issues ought to be decided by a party, such as the respondent, rather than a court. Copyright infringement is not a simple issue. Such problems as identified are not insurmountable, but they do weigh against a finding that the respondent could conclusively decide that infringement had occurred and that it had the relevant power to prevent by warning, suspension or termination of subscriber accounts, even if it had the technical capability to do so. ....[148]

146 *TorrentFreak* – "ISP attempts to block file sharing results in epic failure" (14 June 2010) http://torrentfreak.com/isp-attempts-to-block-file-sharing-ends-results-in-epic-failure-100614

147 *TorrentFreak* – "ISP attempts to block file sharing results in epic failure" (14 June 2010) http://torrentfreak.com/isp-attempts-to-block-file-sharing-ends-results-in-epic-failure-100614

148 http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/FCA/2010/24.html?stem=0&synonyms=0&query=iinet&nocontext=1

TRAFFIC SHAPING

168. One of the other categories of technical measures to combat online copyright infringement that has been under discussion in the U.K. is "traffic shaping", namely bandwidth capping and bandwidth shaping[149].

169. **Bandwidth capping** and **bandwidth shaping** are defined in the *Digital Britain – Final Report* respectively as:

- "capping the speed of a subscriber's Internet connection and/or capping the volume of data traffic which a subscriber can access"; and

- "limiting the speed of a subscriber's access to selected protocols/services and/or capping the volume of data to selected protocols/services.[150]

For the purposes of this paper, we will use these definitions.

170. In some jurisdictions, ISPs routinely employ bandwidth capping, shaping or a combination of both to manage the services they provide to their subscribers. Further, subscribers may have a choice of Internet access plans with different volume caps and/or speed caps. In some cases, speed is slowed after a volume cap is reached. In other cases, subscribers are charged a higher price to download data in excess of the volume cap.

National approaches

United Kingdom

171. The *Digital Economy Act 2010 (U.K)* gives the Secretary of State the power to order Ofcom, subject to parliamentary approval, to require ISPs, among other things, to limit the speed or other capacity of the service provided to a subscriber or limit the service provided to a subscriber in another way.[151] This would seem to include bandwidth capping and bandwidth shaping. As with suspension of Internet access, these measures cannot be imposed until 12 months after an initial obligations code has come into force.[152] Ofcom expects the code[153] will come into force in early 2011.[154] However, as noted in paragraphs 111 to 113, the *Digital Economy Act 2010 (U.K.)* is under review.

149 *Digital Britain* – Final Report at pages 111-112 http://www.culture.gov.uk/images/publications/chpt4_digitalbritain-finalreport-jun09.pdf
150 *Digital Britain* – Final Report at pages 111-112 http://www.culture.gov.uk/images/publications/chpt4_digitalbritain-finalreport-jun09.pdf
151 See s.9 and s.10 http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_2#pb2-l1g9
152 See s.9 and s.10 http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_2#pb2-l1g9
153 Draft code as at 30 July 2010 - http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf
154 http://media.ofcom.org.uk/2010/05/28/draft-code-of-practice-to-reduce-online-copyright-infringement

United States of America (U.S.A.)

172. The *Higher Education Opportunity Act 2008 (U.S.A.)* ("the HEOA")[155] came into force on 1 July 2010[156]. The HEOA requires institutions to certify that:

> "… the institution—
>
> (A) has developed plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents; and
>
> (B) will, to the extent practicable, offer alternatives to illegal downloading or peer-to-peer distribution of intellectual property, as determined by the institution in consultation with the chief technology officer or other designated officer of the institution."[157]

173. While the legislation does not require universities to deploy bandwidth shaping or capping to achieve compliance, some universities may adopt this approach. For example, the University of California, Los Angeles ("UCLA") bandwidth shapes its network.[158] Unlike the U.K. approach, which is intended to be only applied to repeat infringers, it appears the measures deployed by UCLA and probably other universities would apply to all users (unless exempt).

174. In a submission to the United States Intellectual Property Enforcement Coordinator in March 2010, the American Federation of Television and Radio Artists, the Directors Guild of America, the International Alliance of Theatrical and Stage Employees, the Motion Picture Association of America, the National Music Publishers' Association, the Recording Industry Association of America, and the Screen Actor's Guild recommended that the government encourage network administrators to employ bandwidth shaping and throttling to address infringement on their networks.[159]

Examining traffic shaping as an enforcement measure

175. In the following paragraphs, we consider the likely effectiveness of traffic shaping as an enforcement measure against online copyright infringement and explore some of the potential issues for the Internet, Internet technologies, access and Internet use.

What methods of copyright infringement and/or categories of infringers is the policy designed to address?

176. The policy, as it was proposed by the U.K. government in 2009, focused on copyright infringement via P2P protocols and was intended to be imposed against repeat infringers

155 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ315.110.pdf
156 http://www.copyrightlaws.com/us/college-copyright-policies-on-file-sharing-required-by-heoa
157 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ315.110.pdf
158 http://p2p.ucla.edu/resources/uclaplan.pdf
159 Letter dated 24 March 2010 http://www.mpaa.org/Resources/0c72c549-89ce-4815-9a71-de13b8e0a26f.PDF

if other non-technical measures proved to be deficient in reducing infringement[160]. The intention of this policy seems to have been to prevent (or at least discourage) known infringers from continuing to unlawfully receive and distribute copyright material using P2P protocols. However, it appears that the *Digital Economy Act 2010 (U.K.)*[161] would not restrict the application of technical measures, including traffic shaping, to subscribers who have infringed copyright using P2P protocols.

177. Given the genesis for the proposed law, namely a concern about copyright infringement via P2P protocols, and a widely held view (whether correct or not) that P2P file-sharing is the most popular method for obtaining and sharing unauthorised or illegal copies of copyright material, the following discussion focuses principally on P2P.[162]

How effective is the policy likely to be at preventing or reducing copyright infringement?

What solutions might infringers choose or develop in response? What impact would these have?

Bandwidth capping (volume)

178. Capping data downloads will not affect a subscriber's ability to access the Internet until the total volume downloaded reaches the maximum allowed, and thus would not, of itself, prevent a subscriber from continuing to engage in online copyright infringement by P2P or any other means. It is possible that some subscribers, knowing they are restricted to a maximum download in a given period, may reduce their infringing activity, choosing to first consume their limited data allocation for perceived higher priority uses that are lawful. Such subscribers may be more likely to be casual rather than repeat infringers.

179. Capping downloads without a corresponding cap on uploads would not prevent the subscriber from continuing to act as a seeder in a P2P network provided downloads are kept below the data threshold.

180. Once a subscriber reaches the maximum data threshold, he or she has several options for accessing additional data, with varying levels of associated cost and inconvenience: For example, the subscriber could:

- respect the imposition of the limitation;
- subscribe to another ISP (unless all other available ISPs were prevented from supplying their services to the subscriber);

160 *Government Statement on the Proposed P2P File-sharing Legislation* at page 1 - http://www.berr.gov.uk/files/file52658.pdf

161 See s.9 of the Act http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1

162 Regarding use of P2P protocols: BitTorrent Inc. reported that there are 20 million active users from more than 220 countries/day using BitTorrent or uTorrent. See *TorrentFreak* – "uTorrent & BitTorrent Hit 100 Million Monthly Users" (3 January 2011) http://torrentfreak.com/utorrent-bittorrent-hit-100-million-monthly-users-110103

- use another subscriber's connection with permission (friend, workplace, library, Internet café, etc.) or without permission (e.g. accessing unsecured wireless connections); or

- establish his or her own ISP.

Those options are also available to a subscriber whose connection has been slowed.

181. It may be impossible or, at best, resource intensive and expensive for a regulator to ensure the subscriber does not have the ability to download data in excess of the imposed maximum volume or speed via other connections. However, bandwidth capping may make it more difficult or inconvenient for some infringers.

Bandwidth capping (speed)

182. Whether capping the speed of a subscriber's connection is likely to affect his or her ability and/or willingness to engage in online copyright infringement via P2P or any other means depends on the degree to which the speed is capped. P2P protocols are relatively data speed resilient so capping data speeds is more likely to have a greater and more immediate impact on other protocols and applications that are less bandwidth resilient, such as video streaming.

183. To effectively prevent the subscriber from using P2P protocols, the connection would need to be slower than the speed required for any of the existing, or likely to be developed, P2P protocols. Otherwise, it would only limit the amount of data that could be downloaded or uploaded within a given period. Further, as P2P protocols often select their peers opportunistically, capping the speed may simply shift infringement to another subscriber.

184. It is unlikely that capping data speeds would prevent popular P2P file-sharing protocols from functioning on subscribers' devices as such protocols are still capable of operating at very slow speeds[163]. However, at slow enough speeds, the length of time that it takes to download content may discourage all but the very persistent and patient from continuing to engage in online copyright infringement using those protocols.

Detecting and shaping P2P traffic

185. To be able to bandwidth shape P2P traffic separately, an ISP must be able to detect and differentiate P2P traffic from other traffic.

186. Although the policy (as envisaged in the *Digital Britain Report*[164]) does not appear to distinguish between lawful and unlawful P2P traffic, an ISP could "white-list" lawful sources of P2P traffic and thus exempt them from bandwidth shaping.[165] However, given the extra

163 In theory, as low as 2 bps (the limiting factor being the TCP connection timeout, which is typically 3 minutes)

164 See the definition of bandwidth shaping at pages 111-112 http://www.culture.gov.uk/images/publications/chpt4_digitalbritain-finalreport-jun09.pdf

165 See Ipoque whitepaper on *Bandwidth Management Solutions for Network Operators* at page 2 http://www.ipoque.com/userfiles/file/BW-Management-for-Operators-WP.pdf

labour and cost involved in maintaining white-lists for subscribers who are subject to the policy, ISPs may be reluctant to offer that service. White-lists are also notoriously inflexible and hard to scale to Internet proportions.

187. P2P traffic which uses known fixed port numbers is relatively easy to detect, however traffic can be transported via P2P using dynamic and random port numbers, thus making detection by using port numbers more difficult.[166]

188. Another way unencrypted P2P traffic can be detected is via Shallow Packet Inspection, that is, through inspection of the header of a data packet, however, many P2P networks encrypt their traffic.[167]

189. Various Deep Packet Inspection[168] ("DPI") techniques have been developed to detect encrypted P2P traffic (i.e. to recognise P2P traffic without seeing its contents), including techniques to analyse traffic behaviour. These techniques vary in their effectiveness.[169]

190. Unless the policy requires an ISP to identify and distinguish between lawful and unlawful P2P traffic for the purposes of deploying the policy, it does not matter whether the technological measures could break the content encryption, provided they can reliably detect P2P traffic.

191. If the content of the P2P traffic is irrelevant to the policy, subscribers subject to P2P bandwidth shaping may be more concerned about disguising the fact that they are sending or receiving P2P traffic than they are about encrypting its contents. However, if being detected as "infringers" led to the application of the policy, there may also be a strong incentive to disguise the contents.

192. Internet users who wish to disguise their P2P traffic from third parties have developed and are continuing to develop new methods to prevent third parties from detecting the fact they are using P2P protocols. For example: Message Stream Encryption ("MSE") protocol is intended to disguise BitTorrent P2P traffic by generating what seems to be a random header. It is also designed to work with RC4 (a stream cipher) to encrypt the contents.[170] However, more sophisticated traffic analysis tools are still able to detect P2P even where

166 For example: BitTorrent's User Manual (http://www.bittorrent.com/btusers/guides/bittorrent-user-manual/faq-frequently-asked-questions/network) recommends user do not ".. ports in the 6881-6889 range, as they are commonly throttled by ISPs .." and states "[s]ince no single port has inherent advantages over any other port, you can simply let BitTorrent Mainline pick a random port for you."

167 For example: BitTorrent's Connection Guide at http://www.bittorrent.com/btusers/guides/bittorrent-connection-guide gives users instructions on how to enable protocol encryption.

168 DPI is "is the act of any IP network equipment which is not an endpoint of a communication using non-header content (typically the actual payload) for some purpose" (www.wikipedia.org as at 1 February 2010)

169 For example: in 2008, Italian researchers claimed that "Tunnel Hunter" could detect encrypted P2P traffic with 88.77% accuracy (see *ZeroPaid* – " 'Tunnel Hunter' Detects Encrypted P2P Traffic With 90% Accuracy" (30 June 2008) http://www.zeropaid.com/news/9600/tunnel_hunter_detects_encrypted_p2p_traffic_with_90_accuracy). See also *Peer-to-Peer Filters: Ready for Internet Prime Time?* Author: Carsten Rossenhövel http://www.internetevolution.com/document.asp?doc_id=148803&

170 See The Arms Race in P2P Kevin Bauer, Dirk Grunwald and Douglas Sicker, University of Colorado at page 9 http://www.tprcweb.com/images/stories/papers/kevinbauer_2009.pdf and http://www.azureuswiki.com/index.php/Message_Stream_Encryption and http://en.wikipedia.org/wiki/RC4

MSE and RC4 are used.[171] Another method used to disguise P2P traffic is to send the traffic via an encrypted VPN tunnel that encapsulates the network traffic within encrypted packets between tunnel endpoints.[172]

193. Apart from developing methods to disguise P2P traffic, infringers are also likely to develop means to prevent, or reduce the effectiveness of, bandwidth shaping. For example, Transmission Control Protocol ("TCP") packet resets to delay P2P traffic such as BitTorrent, would not be effective against traffic transported using the uTorrent protocol which operates via the User Datagram Protocol ("UDP"). (As at 2008, BitTorrent Inc's VP of Product Management estimated that 28 million unique users use uTorrent every month.[173]).[174]

What impact would the policy have on privacy?

Bandwidth capping

194. Technical measures that only "count" the volume of data received within a given time and then impose a technological cap should not reveal what content the subscriber is viewing, downloading and/or uploading. Similarly, technical measures that only restrict the speed of a subscriber's connection should not reveal the content of the data being streamed.

Bandwidth shaping

195. If P2P traffic is adequately encrypted and passes through a VPN tunnel, technical measures employed to bandwidth shape that traffic should not reveal what content the subscriber or other user is viewing, downloading and/or uploading. But in this case, the technical measures are unlikely to be effective if ISPs only attempt to shape identified P2P traffic. If ISPs adopt a complimentary policy of shaping unrecognised traffic (e.g. encrypted traffic using an unregistered port), the policy may be more effective, but may adversely affect non-infringing traffic.

196. If P2P traffic is not encrypted, such technical measures may additionally reveal the content and, therefore, potentially reveal considerably more personal information about the subscriber, other peers in the network and/or third parties. For example: the subscriber may use unencrypted P2P to send a video of a family barbeque to other friends on the network.

197. Even if the content of the traffic is not exposed, even the mere presence of P2P traffic, particularly when combined with information about its sources and destinations (i.e. IP addresses) may reveal information about the subscriber's or other users' interests, activities, etc.

171 See *The Arms Race in P2P* (above) at page 10
172 See *The Arms Race in P2P* (above) at page 12
173 http://torrentfreak.com/utorrent-grows-to-28-million-monthly-users-081225
174 See *The Arms Race in P2P* (above) at pages 13-14

Would the policy discriminate against legitimate uses of applications?

198. Bandwidth capping would apply indiscriminately to all Internet use via the capped connection, including lawful and unlawful P2P activity. Some uses of the Internet require faster Internet connection speeds (e.g. video streaming and online games) and/or larger volumes of data traffic (e.g. software and video downloads). The impact this policy would have on legitimate uses of applications will depend greatly on the degree to which speed or volume is capped. However, any degree of bandwidth capping could affect the effectiveness and/or render a bandwidth-intensive application inoperable.

199. By contrast, bandwidth shaping should only affect the targeted protocols – for example, the P2P protocols used by P2P networks – provided those protocols can be identified and distinguished from other traffic. However, data exchanged through P2P file-sharing can be lawful or unlawful. Bandwidth shaping which cannot distinguish between lawful and unlawful file-sharing would prevent the user from using P2P for legitimate purposes.

Would the policy discourage or prevent the use of certain technologies and/or development of new communications protocols?

200. Bandwidth shaping focused purely on P2P protocols is unlikely to discourage or prevent the development of new communications protocols. However, given the difficulty of detecting P2P traffic, there may be incentives for ISPs to apply their traffic shaping policy to all unrecognised traffic. Such a practice would be likely to discourage protocol development.

201. The policy may encourage development of new file-sharing protocols that would not be affected by the proposed bandwidth shaping techniques. It will, however, prevent or discourage the subscriber and other users of the connection from using existing P2P protocols for lawful as well as unlawful purposes unless the technical measures distinguish between the two types of traffic. But, as noted above, there are serious privacy implications associated with attempting to ascertain the content of Internet traffic.

202. Bandwidth capping may discourage or prevent affected Internet users from using “cloud computing” technologies for data storage because data transfer is too slow or uses too much of the capped bandwidth. Users with a volume cap may also be concerned that they may not be able to access the data if they reach the maximum data threshold. Affected users may be more likely to back-up data on local hard drives, disks, flash drives and other storage devices.

Would the policy alter the basic architecture of the Internet? Are there any unpredictable or identifiably negative consequences?

203. By their very nature, bandwidth capping and shaping at the subscriber level will impact the Internet architecture at the edge, since the edge requires that all traffic from a given subscriber must pass through a single point where it can be counted, capped, shaped, etc. While that may be the case in any event, there is still a very clear tension between these technical measures and the desire of some users to have more reliable connections by

having diverse routing. Further, requiring all ISPs to invest in sophisticated DPI at the edge of their networks to enable them to implement a bandwidth shaping policy is likely to inhibit investment in other areas of Internet development and innovation simply because funds that might otherwise have been available have been directed elsewhere.

204. P2P file-sharing offers one particular advantage to the Internet – scalability – i.e. "[i]n general, the more popular the content handled, the more scalable the P2P system is". Unlike a centralised content distribution system, the capacity of content distribution via a P2P network is not limited to the bandwidth speed and processing capacity of the original source of the content, and the quality of service is greater.[175]

What impact would the policy have on security?

205. Bandwidth capping will make it slower or perhaps impossible for the subscriber to download operating system patches which could have a significant effect on the security of the subscriber's devices and, correspondingly, potentially the network. However, a slower Internet connection may protect the subscribers from some bandwidth hungry Internet security threats.

206. Bandwidth shaping may encourage affected subscribers to encrypt data they send and receive because they may be concerned that the technical measures applied to effect bandwidth shaping may inspect the content of their traffic. Such subscribers would, therefore, apply a higher level of security to their traffic. Their demand for encrypted data may drive online service providers to support and provide encrypted traffic. This may in turn make copyright infringement and other illegal activities more difficult to detect.

Would the policy inhibit or enhance users' willingness to access the Internet or obtain access to the Internet?

207. If the techniques deployed to shape the traffic passing through the subscriber's connection involve content inspection, the subscriber and other users of that connection may be less willing to use it, concerned that their activities could be monitored, recorded and disclosed by their ISP to their government and other third parties. Even without content inspection, such users may still be less willing to use the connection, particularly for the exchange of traffic via P2P protocols, if they are uncertain as to which of the applications they use rely on P2P protocols.

Would the policy directly or indirectly reduce Internet access or the availability of Internet access?

208. Bandwidth speed capping would directly reduce Internet access for all users of the affected Internet connection. The impact it would have will depend on the degree to which speed is capped and the services that individual and other users of the connection wish to use.

175 See IETF RFC 5694 *Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability* at http://www.rfc-editor.org/rfc/rfc5694.txt

By contrast, provided P2P protocols can be successfully identified and distinguished from other traffic, bandwidth shaping of P2P protocols should only reduce access to content, applications and services that use those protocols. However, unless lawful P2P traffic can be distinguished from unlawful P2P traffic, bandwidth shaping would directly reduce access to lawful content. Further, it is unlikely to be feasible in "real-time" and, in any case, raises major privacy issues.

209. Capping the volume of a subscriber's connection would prevent the subscriber and other users of the connection from accessing the Internet once the threshold is reached. The effect would be the same as temporarily suspending Internet access.

210. As noted above, the affected subscriber (and other users of the affected connection) could, at least in theory:

- subscribe to another ISP (unless all other available ISPs were prevented from supplying their services to the subscriber);
- use another subscriber's connection with permission (friend, workplace, library, Internet café, etc) or without permission (e.g. accessing unsecured wireless connections);
- establish his or her own ISP.

Nonetheless, all of these steps require the user to take positive steps to obtain alternate Internet access at greater inconvenience and cost.

Would the policy materially raise or lower the costs of Internet access?

211. If the subscriber of the Internet connection that is subject to bandwidth capping or shaping is required to continue to pay the same amount for Internet access, the policy would effectively cause the subscriber to pay more for Internet access. That person may or may not be the infringer.

212. The policy may directly increase ISPs' costs and, therefore, may indirectly raise the costs of Internet access to other users if ISPs are required to purchase and/or develop the software and hardware needed to individually apply bandwidth capping and/or shaping. The cost is likely to be greater in the case of bandwidth shaping because of the complex tools required to analyse disguised and encrypted P2P traffic. DPI deployed at the edge of the network is very expensive[176], a cost that is likely to be passed on to subscribers directly by their ISPs, or indirectly to taxpayers if the cost is subsidised by government.

176 For example, in 2008, a PacketLogic PL10000 DPI unit cost up to $800,000 (see http://arstechnica.com/old/content/2008/05/throttle-5m-p2p-users-in-real-time-with-800000-dpi-monster.ars)

Is there any risk of significant or material damage to third parties' use of or access to the Internet?

213. There is a real risk that the policy would limit innocent parties' access to the Internet – those individuals who are legally entitled to use the same connection as the infringer. Current bandwidth capping and shaping methods generally do not distinguish between users of the same connection. While it may be possible for ISPs to issue separate passwords for different users of the connection and thus different levels of Internet access, such a solution is unlikely to be attractive to regulators because passwords for non-restricted Internet access could be easily shared with the infringer.

Would the policy encourage or discourage the use of certain business models?

214. An application that moves large volumes of data, while being careful not to interfere with any other use, such as online file backup, is likely to be adversely affected by bandwidth capping.

215. Bandwidth shaping of P2P protocols irrespective of the content is likely to discourage new and legitimate uses for those protocols – either because of a concern that users may not be able to access the services or because use of P2P protocols has (*incorrectly*) become synonymous with illegal activity.

BLOCKING (IP address, URL, port and protocol)

216. For the purposes of this paper, **blocking** refers to the range of technical measures capable of being used by an ISP to prevent an Internet user from:

a. accessing particular websites, servers and/or devices (e.g. a web server), specifically;

- URL blocking;
- IP address blocking;
- DNS look-up blocking;

b. using particular protocols (e.g. P2P protocols);

c. using particular ports.

Approaches to blocking

United Kingdom

217. Some of the technical measures under consideration by the U.K. government in 2009 to combat online copyright infringement were IP address, URL, port and protocol blocking.[177] Paragraph (b) of the definition of "technical measures" in s.9 of the *Digital Economy Act 2010 (U.K.)*[178] would seem to be broad enough to encompass these measures:

> A "technical measure" is a measure that—
>
> ….
>
> (b) prevents a subscriber from using the service to gain access to particular material, or limits such use

In any case, subparagraph (d) is even broader – "limits the service provided to a subscriber in another way".[179] As with suspension of Internet access, these measures cannot be imposed by the Secretary of State until 12 months after an initial obligations code has come into force and only if there is parliamentary approval.[180] Ofcom expects the code[181] will come into force in early 2011.[182] However, as noted in paragraphs 111 to 113, the *Digital Economy Act 2010 (U.K.)* is under review.

177 See *Digital Britain* – Final Report at pages 111-112 http://www.culture.gov.uk/images/publications/chpt4_digitalbritain-finalreport-jun09.pdf
178 s.9 http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_2#pb2-l1g10
179 http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_2#pb2-l1g10
180 See s.9 and 10 http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_2#pb2-l1g9
181 Draft code as at 30 July 2010 - http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf
182 http://media.ofcom.org.uk/2010/05/28/draft-code-of-practice-to-reduce-online-copyright-infringement

218. Additionally, s.17 of the *Digital Economy Act 2010 (U.K.)* provides, among other things:

> (1) The Secretary of State may by regulations make provision about the granting by a court of a blocking injunction in respect of a location on the internet which the court is satisfied has been, is being or is likely to be used for or in connection with an activity that infringes copyright.
>
> (2) "Blocking injunction" means an injunction that requires a service provider to prevent its service being used to gain access to the location.
>
> (3) The Secretary of State may not make regulations under this section unless satisfied that—
>
> (a) the use of the internet for activities that infringe copyright is having a serious adverse effect on businesses or consumers,
>
> (b) making the regulations is a proportionate way to address that effect, and
>
> (c) making the regulations would not prejudice national security or the prevention or detection of crime.

Note: s.17(2) does not specify the type of "blocking" that would need to be implemented.

219. The potential scope of such regulations is fairly broad as "service provider" is defined as:

> any person providing an information society service[183]

and 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 …[184]

220. Section 17 also prescribes requirements for the regulations such as:

- "a court may only grant an injunction if the internet location is, or is likely to be, used to host or access a substantial amount of material in infringement of copyright"[185] – s.17(4)
- factors a court must take into account before granting an injunction – s.17(4)
- advance notice to service providers and operators of the location – s.17(6).

183 s.17(12) of the *Digital Britain Act 2010 (U.K.)* http://www.legislation.gov.uk/ukpga/2010/24/section/17 and s.97A of the *Copyright, Designs and Patents Act 1988 (U.K.)* http://www.legislation.gov.uk/ukpga/1988/48/section/97A and para.2 of T*he Electronic Commerce (EC Directive) Regulations 2002* http://www.legislation.gov.uk/uksi/2002/2013/regulation/2/made

184 See para.2 of *The Electronic Commerce (EC Directive) Regulations 2002* http://www.legislation.gov.uk/uksi/2002/2013/regulation/2/made and

185 Explanatory notes to the *Digital Economy Act 2010 (U.K.)*, para.82 http://www.legislation.gov.uk/ukpga/2010/24/notes/division/5/2/15

221. However, before such regulations may be made, the Secretary of State must first go through a legislated process of consultation and parliamentary scrutiny (s.18) and the proposed regulations must be approved by resolution by both houses of Parliament (s.17(11)).[186]

222. On 1 February 2011, U.K. Culture Secretary, Mr. Jeremy Hunt announced that he had asked Ofcom "to assess whether the Act's reserve powers to enable courts to block websites dedicated to copyright infringement could work".[187] In a Department for Culture, Media and Sport news release, Mr Hunt said:

> I have no problem with the principle of blocking access to websites used exclusively for facilitating illegal downloading of content. But it is not clear whether the site blocking provisions in the Act could work in practice so I have asked Ofcom to address this question.
>
> Before we consider introducing site-blocking we need to know whether these measures are possible.[188]

Blocking access to particular websites, servers

223. Since about March 2004, Turkish *Supplemental Article 4 of Law No. 5846 on Intellectual and Artistic Works* has authorised the Public Prosecutor to provide a blocking order if a takedown notice is not complied with in 72 hours. According to media reports, at least 3000 websites have been blocked using this procedure, predominately to block "piracy".[189]

224. There have also been some instances where courts have ordered ISPs to block particular websites which have been proven to be sources of infringing copyright content and/or links to such sources). For example:

- In February 2010, Il Tribunale del Riesame di Bergamo in Italy ordered all Italian ISPs to block their users from accessing www.thepiratebay.org, the static IP address 83.140.176.146 and any future domain names and IP addresses used by The Pirate Bay.[190]

186 *Digital Economy Act 2010 (U.K.)* http://www.legislation.gov.uk/ukpga/2010/24/contents
187 Department for Culture, Media and Sports News Release – "Ofcom to review aspects of Digital Economy Act - http://www.culture.gov.uk/news/media_releases/7756.aspx
188 Department for Culture, Media and Sports News Release – "Ofcom to review aspects of Digital Economy Act - http://www.culture.gov.uk/news/media_releases/7756.aspx
189 *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship* (Prepared by Dr. Yaman Akdeniz, Associate Professor, Human Rights Law Research Center, Faculty of Law, Istanbul Bilgi University.) at page 23 http://www.osce.org/documents/rfm/2010/01/42294_en.pdf
190 http://www.giuristitelematici.it/modules/bdnews/doc/riesame-bis_bg-TPB_lowres.pdf

- In February 2008, the Haifa District Court in Israel ordered:

> … the respondents, that is Israeli internet service providers, to systematically block access to the illicit site, HttpShare, so that surfers cannot enter this site and utilize it in order to impede upon the claimants' copy rights.[191]

225. IP address and/or URL blocking measures are already used by governments in some countries to prevent, or at least discourage, their Internet users from accessing particular websites. For example, YouTube (www.youtube.com) was blocked in Tunisia from November 2007[192] to January 2011.

Port blocking

226. Operating systems and Internet browsers may block ports for security reasons. For example, Mozilla, by default, blocks a number of ports including port 25.[193] Many ISPs use port blocking to stop certain types of traffic and to provide greater security for their subscribers' devices. For example, they block:

- outgoing TCP port 25 to block spam email traffic generated by infected devices;
- unused ports to close off potential third party access to subscribers' devices.

Some ISPs block port 5060 used by Session Initiation Protocol ("SIP"), a common protocol for VOIP applications. Between 2002 and 2004, the Panamanian government banned and port blocked VOIP.[194]

Protocol blocking

227. As noted above at paragraph 172 and following, universities in the U.S.A. have deployed various technical measures to combat online copyright infringement in response to the HEOA. Such measures include P2P protocol blocking.[195]

Examining blocking as an enforcement measure

228. In the following paragraphs, we consider the likely effectiveness of using blocking as an enforcement measure against online copyright infringement and explore some of the potential issues for the Internet, Internet technologies, access and Internet use.

191 http://www.edri.org/edrigram/number6.5/israel-isp-block Note; EDRI-gram reported in that article that HttpShare only contained links to external sites and did not itself host infringing content.
192 http://opennet.net/youtube-censored-a-recent-history
193 See http://www.mozilla.org/projects/netlib/PortBanning.html
194 *CNET* – "Panama cracks down on Net telephony" (8 November 2002) - http://news.cnet.com/2100-1033-965073.html The government required all ISPs to block 24 UDP ports commonly used for VOIP.
195 See for example, Illinois State University http://www.helpdesk.ilstu.edu/kb/index.phtml?kbid=1432 and Western Connecticut State University http://www.helpdesk.ilstu.edu/kb/index.phtml?kbid=1432

What methods of copyright infringement and/or categories of infringers is the policy designed to address?

229. The terms **filtering** and **blocking** are sometimes used interchangeably, particularly in the context of preventing access to particular URLs, as the aim is to "separate" traffic on route, stopping illegitimate traffic and allowing legitimate traffic to reach its destination. Nonetheless, there is a key difference between a policy to "identify content and filter" and a policy to "block":

- **Content identification and filtering** involves "real-time" detection of infringing content on route to the subscriber before preventing access. Its focus is on the content rather than the source.

- **Blocking** prevents access to pre-determined infringing content (e.g. a URL "black-list").

230. Presumably, a policy of blocking IP addresses, URLs and/or DNS look-up is designed to target sources of illegal copies or distribution of copyright content rather than a subscriber who seeks to access this material using his or her Internet connection – by blocking Internet users' access to those third party websites and/or devices. On the other hand, protocol blocking (e.g. P2P blocking) is designed to prevent the subscriber from using that protocol to receive and distribute illegal copies of copyright material irrespective of the source.

231. In a Department for Culture, Media and Sports new release dated 1 February 2011[196], U.K. Deputy Prime Minister Nick Clegg said:

> The site-blocking measures need secondary legislation before they can be introduced, and the review will inform the Government's decision about how to proceed. They are aimed at tackling other forms of online copyright infringement, such as unlawfully streaming live television programmes or other content from sites outside the UK.

How effective is the policy likely to be at preventing or reducing copyright infringement?

What solutions might infringers choose or develop in response? What impact would these have?

Port blocking

232. Port blocking is relatively easy for an ISP to deploy but unlikely to be effective at preventing or reducing copyright infringement via the Internet as traffic that infringes copyright can be transported using dynamic and random port numbers.[197]

196 Department for Culture, Media and Sports News Release – "Ofcom to review aspects of Digital Economy Act - http://www.culture.gov.uk/news/media_releases/7756.aspx

197 See paragraph 186

IP address and URL blocking

233. IP address blocking is also not likely to be very effective at preventing users from accessing, downloading and/or uploading unauthorised copies of copyright content via their subscribed Internet connection because many sources use dynamic IP addresses or interchangeable proxy web servers. Even if those sites typically use static IP addresses, such addresses can be changed.

234. Similarly, URL blocking is unlikely to be very effective because URLs can also be easily changed. Further, if the intention is to block access to a particular website, the URLs for all web pages would need to be blocked individually.

235. There is also the added problem of correctly identifying all sources or potential sources of infringing content when such material may be encrypted or otherwise disguised (e.g. as a site purportedly containing only legal user-generated content). Thus, it may be difficult for ISPs to maintain an accurate exhaustive list of IP addresses or URLs that should be blocked.

236. Additionally, a URL block without a corresponding IP address block could be circumvented by an Internet subscriber typing in the IP address for the specific URL (provided it has a dedicated IP address).

237. In any case, a subscriber also has several options for obtaining access to blocked IP addresses or URLs, with varying levels of associated cost and inconvenience: For example, the subscriber could:

- access the IP address or URL via a proxy server (or servers) or VPN;
- subscribe to another ISP or use another subscriber's connection (unless all other available ISPs blocked the same IP addresses and URLs);
- establish his or her own ISP.

238. Enex TestLab's Report on an Australian *Internet Service Provider Content Filtering Pilot* in 2009[198] observed:

> All participants in the pilot were successful in blocking 100 percent of the ACMA blacklist. …
>
> A technically competent user could, if they wished, circumvent the filtering technology. Testing showed that the filters used for the ACMA blacklist only were more easily circumvented than other more complex filters used to cover a wider range and volume of material. ….

198 http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot

> Telstra found that its filtering solution was 100 percent accurate at blocking a blacklist of 10,000 URLs. Telstra also found there was no discernible performance degradation.
>
> Telstra did not test circumvention, because it considers that filtering can be circumvented by a technically competent user.
>
> … Telstra reported that heavy traffic sites could overload its trial filtering solution if included in the filtering blacklist. This is also the case for all filters presented in the pilot.

239. Some URL blocking solutions may also be vulnerable to oracle attacks and thus have the inadvertent consequence of providing users with an additional way to locate infringing material (i.e. via the blocked list).[199]

240. Another option for a subscriber is to shift to a different source or directory of content. Reportedly, this is what hundreds of thousands of Italian Pirate Bay users did after the website was blocked by Italian ISPs in February 2010.[200]

241. It is relatively easy for persons wishing to circumvent technical measures to block access to websites to find instructions on the Internet. For example, Electronic Frontier Australia, in response to the Australian filtering proposal, produced a short video entitled "5 ways around the filter in 2 minutes" which is publicly available on the Internet.[201]

242. Furthermore, this policy would not prevent a subscriber from uploading unauthorised copies of copyright material to other users, although it may at least temporarily discourage them from using their subscribed Internet connection to upload content to blocked websites or servers.

Blocking DNS look-ups

243. Blocking DNS look-ups for domain names has the enforcement advantage that an ISP can easily block access to all URLs for a particular domain name, but a subscriber can also circumvent this blocking via a proxy server, VPN or changing ISP, or by using alternate DNS servers.

Blocking protocols

244. Many different protocols can be used to infringe copyright, including various protocols for P2P file-sharing. There is no single solution to block all these protocols: Different techniques are needed to block each protocol. Even if an ISP were able to successfully block all known protocols used to infringe copyright, new protocols would be developed by infringers to

199 See, for example, the study by Richard Clayton (University of Cambridge) regarding CleanFeed - *Failures in a Hybrid Content Blocking System* http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf

200 *TorrentFreak* - "Blocked Pirate Bay Users Flock to Other Torrent Sites" (16 February 2010) http://torrentfreak.com/blocked-pirate-bay-users-flock-to-other-torrent-sites-100216

201 http://openinternet.com.au/2010/08/04/5-ways-around-the-filter-in-2-minutes-video

circumvent the blocking measures. With such a policy, there would be a constant need for evolving blocking methods to stay ahead.

245. The Internet Architecture Board in *RFC 4924 Reflections on Internet Transparency* states:

> In practice, filtering intended to block or restrict application usage is difficult to successfully implement without customer consent, since over time developers will tend to re-engineer filtered protocols so as to avoid the filters. Thus over time, filtering is likely to result in interoperability issues or unnecessary complexity. These costs come without the benefit of effective filtering since many application protocols began to use HTTP as a transport protocol after application developers observed that firewalls allow HTTP traffic while dropping packets for unknown protocols.[202]

246. In any case, a user could easily avoid the application of most protocol blocking techniques by routing all traffic through a VPN tunnel, thus masking the content and protocol used to transport the content.

What impact would the policy have on privacy?

247. Data regarding a subscriber's or other individuals' attempts to access blocked IP addresses and/or URLs may contain personal information about the individual such as his or her interests or activities.

248. Technical measures which merely block a subscriber from accessing specified IP addresses (e.g. by advertising a null route) and do not permit ISPs or anyone else to view and collect data as to which blocked IP addresses the subscriber and/or other users of the connection have attempted to access are unlikely to impact their privacy. However, technical measures to block URLs requires the ISP to reassemble the packets to check whether the URL is on the blocked list and even where logging is disabled, there may be privacy leaks, for example, where there is a "you have been blocked" web page from a dedicated server. (Even if the logs of that server are also disabled, unless the traffic is encrypted, the fact that someone using the Internet connection attempted to access a blocked page may be observable.)

249. Technical measures that merely block traffic from being transported via certain protocols without examining the contents of the traffic are unlikely to impact the subscriber's privacy. But that would not be the case if DPI is deployed for the purpose of trying to distinguish between lawful and unlawful traffic, unless the user has successfully encrypted his or her traffic.

250. Where technical measures to block traffic do not distinguish between lawful and unlawful traffic, incorrect and adverse assumptions might be drawn regarding the subscriber's attempt to use a particular protocol. For example, persons might incorrectly assume a BitTorrent user is attempting to illegally download or upload copyright content when in fact that person is using the protocol for legal purposes.

202 http://www.ietf.org/rfc/rfc4924.txt

251. On the other hand, if the blocked sources (e.g. websites) collect personal information about their users without their knowledge or permission (e.g. through spyware), blocking may help protect those users from unauthorised collection, use and disclosure of their personal data (assuming, of course, subscribers do not circumvent the block).

Would the policy discriminate against legitimate uses of applications?

252. Protocol blocking would prevent subscribers and other users of the Internet connection from using the blocked protocol for other purposes, as well as for copyright infringement. This measure, therefore, may prevent or limit those persons' access to applications for legitimate uses. For example, P2P protocols are also commonly used for legal distribution of content. NASA, for example, uses BitTorrent to distribute images from its Visible Earth Catalogue[203]. In its FAQs page, NASA states:

> Why can't I just download the larger files directly?
>
> When the Visible Earth relaunched in 2005, all imagery on the site was available for immediate HTTP download. Unfortunately, this started to generate maintenance problems, as folks downloading the larger Blue Marble imagery (~400M) would be connected to the server for a very long time. Frequently they would be forcibly disconnected for maintenance, causing their downloads to abort. When Blue Marble: Next Generation launched, we had a large influx of files of equal, and LARGER, sizes. Since this would require more people to be dropped regularly, we decided to look for other ways of resolving the download options.

CNN used Octoshape's P2P technology for their Internet broadcast of U.S. President Obama's inauguration.[204]

253. Blocking ports would have the same effect. A port can be used in the transport of content, whether legitimate or not. Further, any port above 1023 may be used on occasions by multiple applications and a number of "well known" ports below 1023 also have multiple designations.

254. IP and URL blocking should not discriminate against legitimate uses of applications provided that the blocked sites and devices do not contain any legitimate content or offer any legitimate applications or services. But, this will not always be the case. For example, a website may offer non-infringing and infringing content via the same URL. Additionally, where two or more websites share the same IP address (i.e. they are hosted on a shared hosting server), blocking that server's IP address may prevent a subscriber from accessing non-infringing websites and accessing the services provided through those sites.

203 http://visibleearth.nasa.gov/faq.php

204 *TorrentFreak* – "CNN uses P2P plugin for its live stream" http://torrentfreak.com/cnn-uses-p2p-plugin-for-its-live-stream-090124

Would the policy discourage or prevent the use of certain technologies and/or development of new communications protocols?

255. IP address and URL blocking is unlikely to discourage or prevent the use of certain technologies and/or the development of new communications protocols, but URL and DNS look-up blocking may encourage owners of sites that deliberately host infringing content to search for cheap and easy ways to quickly and dynamically change their domain names. For example, they might shift their site from one domain to another using domain tasting periods.

256. Routine blocking of particular ports may discourage the use and deployment of technology on those ports. A widespread practice of port blocking may also encourage the use and deployment of applications that operate via dynamic ports.

257. Blocking protocols (e.g. P2P protocols) is likely to discourage or prevent the use of those technologies on the affected connection for legitimate as well as illegitimate purposes. But, it may encourage the development of new protocols that are not affected by existing blocking techniques.

Would the policy alter the basic architecture of the Internet? Are there any unpredictable or identifiably negative consequences?

258. Presumably, dynamic protocol and port blocking would be implemented at the point where the subscriber is connected to the Internet so the key issue is whether ISPs' systems can cope with a large, and rapidly changing, set of rules.

259. URL and IP address blocking would require the ISP to route a subscriber's traffic through a single point, so it may conflict with the desire to make the Internet more reliable by designing in multiple paths. These measures also increase complexity so may themselves reduce the reliability of the Internet.

260. DNS look-up blocking may encourage subscribers to move to alternate DNS servers, which if prevalent could undermine a very fundamental aspect of the Internet – a globally unique public address space. The Internet Architecture Board in *RFC 2826 IAB Technical Comment on the Unique DNS Root* states:

> Put simply, deploying multiple public DNS roots would raise a very strong possibility that users of different ISPs who click on the same link on a web page could end up at different destinations, against the will of the web page designers.
>
> ….
>
> The requirement for uniqueness within a domain further implies that there be some mechanism to prevent name conflicts within a domain. In DNS this is accomplished by assigning a single owner or maintainer to every domain, including the root domain, who is responsible for ensuring that each sub-domain of that domain has the proper records associated with it. This is a technical requirement, not a policy choice.[205]

205 http://tools.ietf.org/html/rfc2826

What impact would the policy have on security?

261. Some open source software, including the Linux operating system, are distributed via P2P. Restricting access to P2P protocols would hamper the ability of end-users to upgrade their operating system and other critical software, thereby compromising the security of their computers and the network.

262. If any of the blocked sources of infringing content are also sources of malware or spyware, the policy may help to protect the subscriber's connection from infection and data-stealing from those websites or devices (assuming the subscriber does not circumvent the block). However, the subscriber and/or other users, in attempting to learn how to circumvent the blocks (e.g. by going to websites offering or purporting to offer solutions), may inadvertently visit infected sites.

Would the policy inhibit or enhance users' willingness to access the Internet or obtain access to the Internet?

263. Port blocking is unlikely to affect users' willingness to access the Internet. ISPs routinely block ongoing TCP port 25 to block spam traffic generated by infected devices and this appears to have no impact on users' willingness to access the Internet.

264. Some users may be inhibited from accessing URL/IP address blocked sites and/or devices, either from a technical point of view (e.g. if they do not know how to circumvent the block) or perhaps because the blocked endpoints have been identified as "bad". For others, the policy probably will have no inhibiting effect. However, some users may be less willing to access unblocked areas of the Internet if the blocked sites are not disclosed in advance, fearing (rightly or wrongly) that their ISP will record their attempt to access a site which has been placed on the "blocked" list. Similarly, some users may be less willing to use P2P protocols if they are not sure which ones have been blocked.

Would the policy directly or indirectly reduce Internet access or the availability of Internet access?

265. IP address, URL and DNS look-up blocking are designed to directly reduce subscribers' Internet access but given the relative ease with which they could circumvent these blocks, it is unlikely that the policy will have any lasting effect on Internet access for many subscribers. Nonetheless, those subscribers who accept the blocks or who are unable to circumvent them will have less Internet access than those who are not subject to the policy. This limitation will also apply to all users of the Internet connection, not just the subscriber. Further, as it may be easier for ISPs to block a whole domain rather than specific URLs, there is a risk of over-blocking and a consequent reduction in Internet access.
.

266. Subscribers and other users of their connection who are prevented from using particular protocols (e.g. P2P protocols) also have more limited Internet access and their overall Internet experience is reduced. "P2P technology enables computer users to share communications, processing power, and data files with other users. Use of P2P technology

can yield significant benefits, such as enhancing efficiency by allowing faster file transfers, conserving bandwidth, and reducing storage needs. Businesses, government agencies, academic institutions, and others use P2P applications for a variety of tasks…". [206]

267. A subscriber who is unable to circumvent a blocked port or ports, which would, but for the blocking, be used to access the Internet, will have reduced access to the Internet. The extent to which access is affected will depend on which ports are blocked. For example, if IRC ports are blocked, a user may be preventing from participating in research discussions conducted via IRC.

Would the policy materially raise or lower the costs of Internet access?

268. ISPs which are required to dynamically block IP addresses and/or URLs for particular subscribers are likely to expend greater costs supplying Internet access given, among other things, the cost of the technologies, and the labour required to maintain up-to-date and accurate block lists. It is not clear how this increased cost would be recouped.

269. Simple fixed port blocking should be relatively easy for ISPs to deploy, but port blocking could become an expensive exercise if ISPs are required to detect and block "real-time" ports used by subscribers who randomly and frequently switch ports.

270. In theory, some ISPs with limited bandwidth capacity may experience some potential cost savings by blocking protocols typically used to exchange large volumes of data (e.g. P2P protocols) as their customers' overall demand for bandwidth may be reduced. However, they would also incur the cost of detecting and blocking protocols.

Is there any risk of significant or material damage to third parties' use of or access to the Internet?

271. Blocking ports, protocols, URLs, etc. on a subscriber's Internet connection would prevent other users of the connection from accessing the Internet via those ports and protocols, and from accessing the content on the blocked websites, thus reducing their Internet access and overall experience of the Internet.

272. With any "black-list" of URLs and IP addresses, there is a risk of over-blocking and under-blocking. Over-blocking access may impact a business and/or its reputation, particularly if the blocking measure diverts the user to a webpage stating the asserted reason for the block (e.g. copyright infringement).

273. Blocking protocols may prevent a third party communicating or exchanging data lawfully with the subscriber and/or another user of the Internet connection via those protocols.

206 *U.S. Federal Trade Commission Press Release* - FTC Issues Report on Peer-to-Peer File Sharing (23 June 2005) (http://www.ftc.gov/opa/2005/06/p2p.shtm)

Would the policy encourage or discourage the use of certain business models?

274. Cisco's Visual Networking Index (VNI) Forecast, 2009-2014 predicts that by 2014, 91% of global consumer IP traffic will be video.[207] Various businesses that supply video via the Internet are exploring cheaper and more efficient ways to distribute such content. One option that some providers are exploring to reduce streaming costs is to make the content available via P2P protocols (thereby shifting and distributing the streaming costs to viewers). For example:

- In June 2010, NPO (Dutch Public Broadcaster) launched a trial, making its latest content available to download or stream via BitTorrent.[208]

- Adobe's new Flash Player 10.1 incorporates P2P technology (Stratus) allowing video to be streamed live or on-demand[209] via peer assisted networking using Real Time Media Flow Protocol (RTMFP). Adobe's website states:

> The most important features of RTMFP include low latency, end-to-end peering capability, security and scalability. These properties make RTMFP especially well suited for developing real-time collaboration applications by not only providing superior user experience but also reducing cost for operators.[210]

- In 2010, Twitter started using a BitTorrent based system to improve data deployment across its servers (called Murder).[211]

- On 27 September 2010, Wikimedia started offering BitTorrent streamed video (using Swarmplayer V2.0), with the following explanation:

> As Wikimedia and the community embark on campaigns and programs to increase video contribution and usage on the site, we are starting to see video usage on Wikimedia sites grow and we hope for it to grow a great deal more. One potential problem with increased video usage on the Wikimedia sites is that video is many times more costly to distribute than text and images that make up Wikipedia articles today. Eventually bandwidth costs could saturate the foundation budget or leave less resources for other projects and programs. For this reason it is important to start exploring and experimenting with future content distribution platforms and partnerships.[212]

207 http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf
208 *TorrentFreak* – "Dutch Public Television Tries BitTorrent Downloads" (29 June 2010) http://torrentfreak.com/dutch-public-television-tries-bittorrent-downloads-100629
209 *TorrentFreak* – "Adobe Flash to Eliminate Bandwidth Costs with P2P" (19 May 2010) http://torrentfreak.com/adobe-flash-to-eliminate-bandwidth-costs-with-p2p-100519
210 http://labs.adobe.com/technologies/stratus
211 *TorrentFreak* – "BitTorrent Makes Twitter's Server Deployment 75x Faster" (16 July 2010) http://torrentfreak.com/bittorrent-makes-twitters-server-deployment-75-faster-100716
212 http://techblog.wikimedia.org/tag/video-labs

- The P2P-Next Project[213], a consortium of 21 partners from 12 countries launched in 2008 with a grant from the European Union, observes on its website:

> P2P still has a somewhat dubious reputation as an illegal file sharing mechanism akin to Napster, Kazaa, Glockster, etc. Nevertheless, today it is considered by many as an efficient, reliable, and low cost mechanism for distributing any media file or live stream, and it is extensively used.[214]

and states:

> Broadcasters and content providers consider P2P as a future-proof, universal, and ubiquitous two-way (interactive) distribution mechanism. Initially, P2P will complement the existing distribution mechanisms such as satellite, cable and terrestrial networks, but ultimately it may supersede them. The P2P-Next Project extends the notion of a conventional media distribution network. It introduces a concept of on-demand, personalised, and social network.[215]

Their objective is to:

> … develop a platform that takes open source development, open standards, and future proof iterative integration as key design principles ...[216]

Thus, a policy to block P2P protocols may discourage the use and development of decentralised content distribution models for legal content.

Additional comments

275. On the question of proportionality of P2P protocol blocking, Charleton J in *EMI Records [Ireland] Ltd & Ors -v- UPC Communications Ireland Ltd* [2010] IEHC 377 said at [29] – [31]:

> **I am not convinced** by the evidence … **that any solution based on blocking all peer-to-peer traffic, or severely constricting it, is reasonable**. ….
>
> …Even if that were not so, **it would not be in accordance with the principle of proportionality to use a blunt instrument for the deterrence, or rendering impossible, of illegal activity, when the effect of that would inevitably lead to the infringement on the right of communication through the internet**.
>
> **Another solution proposed**, by way of injunctive relief, **was to search out the platforms most often used within peer-to-peer sharing protocols for illegal file sharing, to identify them by deep packet inspection, and to severely**

213 www.p2p-next.org
214 www.p2p-next.org/?page=content&id=73F87D854E37E0F75C68C69304535873&mid=EE056556C09ED2492B0FF130393D054B
215 www.p2p-next.org/?page=content&id=73F87D854E37E0F75C68C69304535873&mid=EE056556C09ED2492B0FF130393D054B
216 www.p2p-next.org/?page=content&id=09C723B96E610060C05BD7EFBC4C04C8&mid=0C97B9F7B15A2D9CE4F6EA2CE5076A79

throttle or block these communications. There are two reasons why this also is not proportionate. Firstly, the relevant software may be designed to use a number of applications. Those involved in copyright piracy, would readily, and swiftly, release new applications for downloads. Illegal users would switch to them readily. Secondly, there is no satisfactory evidence upon which I can rely which indicates to me that a list of protocols, such as eDonkey, gNnutella and LimeWire, are not also used legally. **To block these communications would not be proportional. It might have the effect of cutting off a certain amount of illegal peer-to-peer file sharing, but it would also have an effect on the ability of internet users to lawfully communicate with each other**. (emphasis added)[217]

217 http://www.bailii.org/ie/cases/IEHC/2010/H377.html

CONTENT IDENTIFICATION AND FILTERING

276. One of the other technical measures under consideration by the U.K. government in 2009 to combat online copyright infringement was **content identification and filtering**.[218] The definition of "technical measures" in s.9 of the *Digital Economy Act 2010 (U.K.)*[219] would seem to be broad enough to encompass this measure:

> A "technical measure" is a measure that—
>
> (b) prevents a subscriber from using the service to gain access to particular material, or limits such use
>
> …
>
> (d) limits the service provided to a subscriber in another way.

As with suspension of Internet access and blocking, these measures cannot be imposed by the Secretary of State until 12 months after an initial obligations code has come into force and only if there is parliamentary approval.[220] Ofcom expects the code[221] will come into force in early 2011.[222] However, as noted in paragraphs 111 to 113, the *Digital Economy Act 2010 (U.K.)* is under review.

277. In this section of the paper we principally focus on "content identification" as many of the filtering techniques involve some form of blocking, which is discussed in the section above.

278. Identification of the content of Internet traffic for the purposes of detecting copyright infringement involves a process of: (a) looking at data flowing on the network; (b) looking for particular types of data (e.g. data being transported via P2P); (c) checking the fingerprint of the content being shared (or, in the case of streaming content, checking the fingerprint of the content being viewed). A fingerprint is an algorithmically produced summary of a file. There are a number of different providers of video and audio fingerprinting technologies (e.g. Audible Magic's CopySense[223] and Vobile's VideoDNA[224]). Acoustid is an open source project for audio fingerprinting.[225]

279. Watermarking technologies are also used to identify digital content. Unlike a fingerprint, a digital watermark is embedded in the content of the media file.[226] Some watermarks are visible (e.g. the letters "QF" or the word "Qantas" visible on films displayed on Qantas flights) and others are only machine-readable.

---

218 See *Digital Britain – Final Report* at pages 111-112 http://www.culture.gov.uk/images/publications/chpt4_digitalbritain-finalreport-jun09.pdf
219 s.9 http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_2#pb2-l1g10
220 See s.9 and 10 http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_2#pb2-l1g9
221 Draft code as at 30 July 2010 - http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf
222 http://media.ofcom.org.uk/2010/05/28/draft-code-of-practice-to-reduce-online-copyright-infringement
223 http://audiblemagic.com/products-services/contentsvcs/copysense-basic.asp
224 http://www.vobileinc.com/technology.html#fragment-1
225 www.acoustid.org
226 *Digital Watermark Technologies, Applications in P2P Networks* (P2P Digital Watermark Working Group) www.digitalwatermarkingalliance.org/docs/.../dcia_whitepaper_p2p.pdf

Examining content identification and filtering as an enforcement measure

280. In the following paragraphs, we consider the likely effectiveness of using content identification and filtering as an enforcement measure against online copyright infringement and explore some of the potential issues for the Internet, Internet technologies, access and Internet use.

What methods of copyright infringement and/or categories of infringers is the policy designed to address?

281. As noted above (at paragraph 172 and following), universities in the U.S.A. have deployed various technical measures to combat online copyright infringement in response to the HEOA. Such measures include "content identification and filtering".[227] However, we also note that there presently appears to be little interest in requiring ISPs to deploy "content identification and filtering" to enforce copyright online where such ISPs merely provide access to the Internet. The position is different where ISPs host user-generated content: There appears to be increasing pressure for OSPs that host user-generated content to deploy some form of "content identification and filtering".

How effective is the policy likely to be at preventing or reducing copyright infringement?

What solutions might infringers choose or develop in response? What impact would these have?

282. Content identification and filtering has been voluntarily deployed by some user-generated content providers (for example: Google Inc.'s YouTube Video ID and Audio ID which works by comparing user uploaded content with reference files from copyright content owners[228]). Such voluntary measures assist in reducing copyright infringement via these services, but can be burdensome for the provider.

283. Content identification and filtering services (particularly with respect to copyright content – video and music) typically rely on fingerprinting or watermarking technologies that can be recognised in Internet traffic.[229] Multiple tools are needed since copyright content can be transported by many different protocols, not merely P2P and HTML.

284. Real-time content identification and filtering of a subscriber's traffic is complex, difficult and expensive to deploy. The Open Initiative[230] observes on its website:

> Filtering based on dynamic content analysis—effectively reading the content of requested websites—though theoretically possible, has not been observed in our research.[231]

227 See, for example, the University of Utah http://audiblemagic.com/products-services/copysense and West Liberty University which uses OpenDNS web content filtering and security services http://www.westliberty.edu/it/welcome/heoa-compliance
228 http://www.youtube.com/t/contentid
229 See, for example, the services offered by BayTSP http://www.baytsp.com/services/index.html#content
230 http://opennet.net
231 http://opennet.net/about-filtering

285. As fingerprint detection is too slow for high-speed Internet connections[232], "real-time" content identification and filtering is a more of a policy goal rather than a reality. To avoid disruption to the network, content identification technologies are typically deployed on a copy of network traffic created using port mirroring[233].

286. While fingerprinting technologies are more commonly used to identify copyright content in Internet traffic, the Distributed Computing Industry Association's P2P Digital Watermarking Working Group contends that digital watermarks can be used to signal authorisation (or the lack thereof) to download, distribute, copy etc. in P2P networks. They argue that P2P applications could incorporate watermark detection tools and either allow or deny file distribution based on signal authorisation.[234]

287. Competent Internet users are likely to be able to circumvent content identification and/or filtering techniques deployed by their ISP in any case (e.g. by encrypting their data and/or any of the methods described in paragraph 232 and following).

What impact would the policy have on privacy and security?

288. By its very nature, "content identification" raises some very serious privacy concerns, particularly where DPI is deployed for the purposes of identifying whether a subscriber is illegally accessing, uploading or downloading copyright content. Effective DPI may reveal data from which an individual's identity, activities, interests, location, etc. can be inferred – more information than would be necessary to detect and determine infringement. Further, such inspection may also reveal personal data of innocent third parties.

289. Digital fingerprint detection technologies such as CopySense search network traffic for reference fingerprints. Provided these technologies see all other data as "noise" and effectively ignore it, Charleton J's comments in *EMI Records [Ireland] Ltd & Ors -v- UPC Communications* Ireland Ltd [2010] IEHC 377 at [47]:

> On the issue of privacy, the inspection maintained by CopySense on the appliance which mirrors the university network access to the internet does not violate privacy. The university is not looking at content. Instead, similar considerations apply as in the DtecNet solution. There are some instances where the university does monitor the content of communications, but this is not one of them. **There are therefore no implications in respect of privacy**.[235] (emphasis added)

would seem to be applicable. However, a pending ruling of the European Court of Justice regarding a reference lodged by the Rechtbank van eerste aanleg te Brussel (Belgium) on

232 Copyright Protection in the Internet (iPoque) Authors: Klaus Mochalski, Hendrik Schulze, Frank Stummer http://www.ipoque.com/resources/white-papers

233 http://en.wikipedia.org/wiki/Port_mirroring

234 *Digital Watermark Technologies, Applications in P2P Networks* (P2P Digital Watermark Working Group) www.digitalwatermarkingalliance.org/docs/.../dcia_whitepaper_p2p.pdf

235 http://www.bailii.org/ie/cases/IEHC/2010/H377.html

19 July 2010 in *Belgische Vereniging van Auteurs, Componisten en Uitgevers (Sabam) v Netlog NV*, specifically –

> Do Directives 2001/29 (1) and 2004/48, (2) in conjunction with Directives 95/46, (3) 2000/31 (4) and 2002/58, (5) construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: 'They [the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right', to order a hosting service provider to introduce, for all its customers, in abstracto and as a preventive measure, at its own cost and for an unlimited period, a system for filtering most of the information which is stored on its servers in order to identify on its servers electronic files containing musical, cinematographic or audio-visual work in respect of which SABAM claims to hold rights, and subsequently to block the exchange of such files?[236]

should shed more light on this issue.

290. Security is closely connected to the issue of privacy. Internet users are likely to regard their overall Internet experience as being "less secure" if they are aware that third parties are able to inspect their traffic.

291. Some techniques which subscribers might use to hide or otherwise obscure the content of their traffic may increase the security of their data (e.g. encryption tools).

Would the policy discriminate against legitimate uses of applications?

292. In theory, accurate fine-grained content identification and filtering should not discriminate against legitimate uses of applications as only infringing content would be affected, but as noted in the section above, attempts to block access to infringing content are at risk of over-blocking – not merely content, but also applications and services. This risk is greatly increased where blocking is sought to be undertaken in "real-time".

Would the policy discourage or prevent the use of certain technologies and/or development of new communications protocols?

293. Content identification and filtering are likely to discourage the use of open protocols for communication and data transfer via the Internet. Instead, such measures are likely to encourage the use of encryption protocols as well as the development of new "secret" encryption protocols to avoid "back-door" access.

236 Official Journal of the European Union (23.10.2010) http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&numaff=&nomusuel=sabam&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&alldocrec=alldocrec&docor=docor&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoor=docnoor&radtypeord=on&newform=newform&docj=docj&docop=docop&docnoj=docnoj&typeord=ALL&domaine=&mots=&resmax=100&Submit=Rechercher

Would the policy alter the basic architecture of the Internet? Are there any unpredictable or identifiably negative consequences?

294. Content identification and filtering on the network imposes creation of single points of failure and hinders widespread connectivity (less peering points, for example, since some ISPs may need to filter egress traffic). However, some of these issues could be alleviated by deploying content identification off the network using port mirroring.

Would the policy inhibit or enhance users' willingness to access the Internet or obtain access to the Internet?

295. If an Internet user is aware that an ISP may or will be inspecting his or her traffic, that user may be less willing to access the Internet via the affected connection (irrespective of the reason for inspection). Alissa Cooper in *The Singular Challenges of ISP Use of Deep Packet Inspection*[237] said:

> To the extent that Internet users find themselves at ease conversing and transacting online, ISPs' increased use of DPI presents the potential to chip away at that sense of security by introducing a surveillance element where it did not exist previously. ISPs are an important element of the trust that Internet users place in the network, and increased use of DPI calls that trust into question.

Would the policy materially raise or lower the costs of Internet access?

296. In addition to the costs associated with blocking, there is the added cost of developing and deploying techniques to identify infringing traffic in "real-time" (or as close to "real-time" as possible). If the costs are borne by ISPs, these may be recouped through higher Internet access fees.

Is there any risk of significant or material damage to third parties' use of or access to the Internet?

297. In addition to the issues identified in paragraphs 271 to 272 above, content identification which involves DPI may reveal personal data about third parties. Knowing that their Internet traffic may or will be inspected may discourage those persons from using or accessing the Internet, or affect the way they use it.

Would the policy encourage or discourage the use of certain business models?

298. If ISP content identification and filtering for unauthorised distribution of copyright content were widespread, content owners may have additional incentives for expending resources to develop and implement watermarking and fingerprinting technologies to protect digital copyright content.

237 http://www.deeppacketinspection.ca/the-singular-challenges-of-isp-use-of-deep-packet-inspection

Additional comments

299. It is important to distinguish between Internet user-enabled "content identification and filtering" (e.g. Google Inc.'s SafeSearch Filter[238]) and third party imposed "content identification and filtering". Internet-user enabled "content identification and filtering" can help Internet users block content they do not wish to access (e.g. parents blocking access to content or services they consider would not be appropriate for their children).

300. There is also a significant difference between using technology to filter content that Internet users wish to be protected from (e.g. malware, spam) and content that Internet users wish to reach (e.g. copyright content). Using technology to block access to the latter is likely to encourage the development and wider use of circumvention technologies such as proxies and encrypted traffic. By seeking to circumvent such measures, such users may inadvertently expose themselves to content they do not want and that their government is seeking to protect them from (e.g. malware).

301. Once filtering infrastructure is widely deployed within a country (whether centrally controlled or not) to combat online copyright infringement, it would be relatively easy from a technical point of view to amend the filtering rules to prevent access to other content and censor the Internet.

302. It is not our intention to address the complex issue of Internet censorship in this paper, however, in the context of a discussion on content filtering, we wish to note that the Internet Society strongly advocates for the application of Article 19 of the *Universal Declaration of Human Rights*[239]:

> 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.

to the online environment.

238 http://www.google.com/support/websearch/bin/answer.py?hl=en&answer=510
239 http://www.un.org/en/documents/udhr/index.shtml

MANIPULATING THE DOMAIN NAME SYSTEM

303. Typically, Internet-focused policy responses to online copyright infringement (such as those discussed in the preceding sections) would require action by the suppliers of an Internet connection (i.e. ISPs). By contrast, a recent proposal in the U.S.A. (the *Combating Online Infringements and Counterfeiting Bill* ("COICA")) would require action by domain name registrars and registries (as well as ISPs and other entities).

304. The recent "domain seizures" by the U.S. government (discussed below at paragraphs 311 – 313) were reportedly carried out by the relevant registry, in compliance with court orders.

United States of America

Combating Online Infringements and Counterfeiting Bill (COICA)

305. On 20 September 2010, the U.S. *Combating Online Infringements and Counterfeiting Bill* was introduced to the U.S. Senate and referred to the Committee on the Judiciary.[240] This Bill provided, among other things, that the Attorney General may apply for a court order requiring:

For domestic domains (for example: .com)

- a domain name registrar or registry to "suspend operation of, and lock, the domain name" of an Internet site "dedicated to infringing activities" (as defined)[241]

For non-domestic domains (for example: .me)

- a "service provider" or other operator of a DNS server to "take reasonable steps that will prevent a domain name of an Internet site "dedicated to infringing activities" (as defined) from resolving to that domain name's Internet protocol address"[242]

- a service that "serves contextual or display advertisements to Internet sites … take reasonable measures, as expeditiously as practical, to prevent its network from serving advertisements to an Internet site accessed through such domain name"[243]

306. On 18 November 2010, the US Senate Judiciary Committee voted to send an amended version of the draft COICA bill to the full Senate for consideration.[244] This amended bill provides, among other things, that the Attorney General may apply for a court order requiring:

For domestic domains (for example: .com)

- a domain name registrar or registry to "suspend operation of, and lock, the domain name" of an Internet site "dedicated to infringing activities" (as defined)[245]

240 http://thomas.loc.gov/cgi-bin/bdquery/z?d111:s.03804:
241 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s3804is.txt.pdf
242 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s3804is.txt.pdf
243 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s3804is.txt.pdf
244 http://leahy.senate.gov/press/press_releases/release/?id=45b5a544-0f49-46d8-9782-ab7a3fe43a1f
245 http://www.gpo.gov/fdsys/pkg/BILLS-111s3804rs/pdf/BILLS-111s3804rs.pdf

For non-domestic domains (for example: .me)

- a "service provider" or any other operator of a nonauthoritative domain name system server to, as expeditiously as reasonable, take technically feasible and reasonable steps designed to prevent a domain name of an Internet site "dedicated to infringing activities" (as defined) from resolving to that domain name's Internet protocol address[246]

- a service that "provides advertisements to Internet sites … take reasonable measures, as expeditiously as reasonable, to prevent its network from providing advertisements to an Internet site associated with such domain name" [247]

307. On 16 February 2001, the U.S. Senate Committee on the Judiciary held a publicly webcast hearing on "Targeting Websites Dedicated to Stealing American Intellectual Property".[248]

308. COICA does not specify what steps a U.S. based domain name registrar or registry would need to take to "suspend operation of, and lock, the domain name" of a website in compliance with a court order. However, one approach that might be taken (at the registry level) is to change the entries in the authoritative name server so that Internet traffic intended for the website is re-directed by the DNS to a different location. This is allegedly how the recent U.S. government "domain seizures" (see paragraphs 311 – 313) were carried out. Another approach might be to render the domain name administratively inactive and not publish it in the root zone. In this case, Internet users would receive a message from their browser to the effect that it cannot find the server at [the domain name] and/or DNS error.

309. With respect to non-domestic domain names, COICA would seem to require a "service provider" (e.g. a U.S. based ISP) to block DNS look-ups in compliance with a court order. Further, an operator of a DNS server based in the U.S. might also be required to prevent a non U.S. based domain name from resolving to its IP address. As to U.S. based operators of DNS servers located overseas, Verizon, in its written testimony for the U.S. Senate Committee on the Judiciary hearing on "Targeting Websites Dedicated To Stealing American Intellectual Property"[249] said:

> The bill should clarify that judicial orders issued pursuant to it apply only to service providers' DNS servers located in the United States. While Verizon believes that the scope of the bill's domain name restrictions is intended to apply only to a service provider's U.S. customers and operations, some service providers – including Verizon – maintain DNS servers that are located in countries outside our borders that serve customers outside the U.S. …[250]

246 http://www.gpo.gov/fdsys/pkg/BILLS-111s3804rs/pdf/BILLS-111s3804rs.pdf
247 http://www.gpo.gov/fdsys/pkg/BILLS-111s3804rs/pdf/BILLS-111s3804rs.pdf
248 http://judiciary.senate.gov/hearings/hearing.cfm?id=4982
249 http://judiciary.senate.gov/hearings/hearing.cfm?id=4982
250 http://judiciary.senate.gov/pdf/11-2-16%20Dailey%20Testimony.pdf

310. COICA has been the subject of considerable international criticism, particularly because of its likely impact on the Internet and its potential extraterritorial reach.[251] As COICA targets the DNS (a global system) rather than subscribers' Internet connections (through ISPs), it has the potential to affect the Internet experience of users all around the world. A major concern is that other countries may copy this approach for broader categories of content, amplifying the problems outlined below.

Domain seizures

311. On 29 November 2010, the U.S. Immigration and Customs Enforcement agency ("ICE"), announced it had (in coordination with other federal agencies) executed seizure orders against " …82 domain names of commercial websites engaged in the illegal sale and distribution of counterfeit goods and copyrighted works".[252]

312. The practical effect of the execution of the orders was that users attempting to access one of the affected domain names (e.g. torrent-finder.com) would be re-directed to another domain name (seizedservers.com) where a notice to the following effect was displayed:

> This domain has been seized by ICE – Homeland Security Investigations, pursuant to a seizure warrant issued by a United States District Court under the authority of 18 U.S.C. §§ 981 and 2323.
>
> Wilful copyright infringement is a federal crime ….[253]

Allegedly, this was achieved by changes to the entries in the authoritative name server by VeriSign (the operator of the top level domain .com registry).[254]

313. On 2 February 2011, ICE announced that seizure warrants had been issued against 10 websites had been illegally streaming live sporting telecasts and pay-per-view events.[255] The announcement states, among other things:

> The websites seized yesterday were popular "linking" sites - a type of website that provides access, or "links," to other websites where pirated sporting and pay-per-view events are hosted. Users simply click on a link to begin the process of downloading or streaming to their own computer an illegal broadcast of a sporting event from the third party website that is hosting the stream.

---

251 See, for example: Electronic Frontier Foundation – Update: The Case Against COICA https://www.eff.org/deeplinks/2010/11/case-against-coica and Center for Democracy & Technology Memo – The Dangers of S.3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture http://cdt.org/files/pdfs/Leahy_bill_memo.pdf

252 ICE News Release: *ICE seizes 82 website domains involved in selling counterfeit goods as part of Cyber Monday crackdown* http://www.ice.gov/news/releases/1011/101129washington.htm

253 *The Background Dope on DHS Recent Seizure of Domains* http://rulingclass.wordpress.com/2010/11/28/the-background-dope-on-dhs-recent-seizure-of-domains

254 *The Background Dope on DHS Recent Seizure of Domains* http://rulingclass.wordpress.com/2010/11/28/the-background-dope-on-dhs-recent-seizure-of-domains

255 http://www.ice.gov/news/releases/1102/110202newyork.htm

> Linking websites are popular because they allow users to quickly browse content and locate illegal streams that would otherwise be more difficult to find. Visitors to these websites are being redirected to a banner that advises them that the domain name has been seized by the New York office of ICE HSI because of criminal copyright violations.[256]

Anti-Counterfeiting Trade Agreement

314. Although ACTA does not mention the DNS, orders against domain name registries and registrars, such as envisaged in COICA, would seem to fall within the scope of article 8(1) of the final text which states:

> **Each Party shall provide that**, in civil judicial proceedings concerning the enforcement of intellectual property rights, **its judicial authorities have the authority to issue an order against** a party to desist from an infringement, and inter alia, an order to that party or, where appropriate, to **a third party** over whom the relevant judicial authority exercises jurisdiction, **to prevent goods that involve the infringement of an intellectual property right from entering into the channels of commerce**. (emphasis added)[257]

Examining the use of the Domain Name System as an enforcement measure

315. In the following paragraphs, we consider the likely effectiveness of using the DNS as an enforcement measure against online copyright infringement and explore some of the potential issues for the Internet, Internet technologies, access and Internet use.

316. Note: DNS look-up blocking is discussed under Blocking.

What methods of copyright infringement and/or categories of infringers is the policy designed to address?

How effective is the policy likely to be at preventing or reducing copyright infringement?

What solutions might infringers choose or develop in response? What impact would these have?

317. Unlike other Internet technical measures considered in this paper which require action by ISPs, the U.S. ICE "domain seizures" referred to in paragraphs 311 – 313 were reportedly carried out by VeriSign (the operator of the .com registry) in accordance with court orders[258]. While most of the websites offered counterfeit goods for sale, one of the sites (www.torrent-finder.com) allowed users to search torrent search engines and indexes[259]. This "domain

256 http://www.ice.gov/news/releases/1102/110202newyork.htm
257 ACTA text available at http://www.dfat.gov.au/trade/acta/index.html
258 *The Background Dope on DHS Recent Seizure of Domains* http://rulingclass.wordpress.com/2010/11/28/the-background-dope-on-dhs-recent-seizure-of-domains
259 *TorrentFreak* – "US Government Made Painful Mistakes In Torrent-Finder Seizure" (17 December 2010) http://torrentfreak.com/us-government-made-painful-mistakes-in-torrent-finder-seizure-101217

seizure" has been particularly controversial because some argue that search engines such as Google and Bing also allow users to locate torrents[260]. (Note: Google Inc. announced in December 2010, that it would "prevent terms that are closely associated with piracy from appearing in Autocomplete".)[261]

318. Reportedly, although users attempting to access torrent-finder.com by typing the domain name into their web browser were re-directed to seizedservers.com, users who typed the IP address 208.101.51.57 into the browser were still able to access the site.[262] Thus, all a user needs to continue to have access to a "domain seized" website is the IP address of its web server. The operator of an affected site and/or its users could easily and quickly broadcast the IP address on the Internet via Twitter, Facebook and other social media platforms.

319. Enforcement measures which rely on the DNS to prevent or impede access to services offered from particular domain names can be easily avoided by Internet users who do not need to use the DNS (e.g. they know the IP address) or who use an alternative DNS which is not affected by the court order.

320. Furthermore, a number of potential responses to such "domain seizures" are already becoming apparent. For example:

- In late November 2010, the Dot-P2P project was launched.[263] Its goals include:

> By creating a .p2p TLD that is distributed and that does not rely on ICANN to issue domains, or any ISP's DNS service to resolve the domains, and by having this application mimic force-encrypted bittorrent traffic, there will be a way to start combating DNS level based censoring like the new US proposals as well as those systems in use in countries around the world including China and Iran amongst others.[264]

- On 2 December 2010, Demonoid, a BitTorrrent tracker site, announced that it would be moving its services from .com to .me (a registry located in Montenegro[265]).[266]

> The situation is pretty obvious. The US is already seizing .com, .net and .org domains. When and if the COICA bill passes is going to be even worse. We

260 *TorrentFreak* – "US Government Made Painful Mistakes In Torrent-Finder Seizure" (17 December 2010) http://torrentfreak.com/us-government-made-painful-mistakes-in-torrent-finder-seizure-101217
261 Google Public Policy Blog (2 December 2010) http://googlepublicpolicy.blogspot.com/2010/12/making-copyright-work-better-online.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GooglePublicPolicyBlog+%28Google+Public+Policy+Blog%29
262 *The Background Dope on DHS Recent Seizure of Domains* http://rulingclass.wordpress.com/2010/11/28/the-background-dope-on-dhs-recent-seizure-of-domains
263 *TorrentFreak* – "BitTorrent Based DNS To Counter US Domain Seizures" (30 November 2010) http://torrentfreak.com/bittorrent-based-dns-to-counter-us-domain-seizures-101130
264 http://dot-p2p.org/index.php?title=Goals
265 http://www.domain.me/contact-us.html
266 *TorrentFreak* – "Sensing Danger, Demonoid BitTorrent Tracker Ditches .COM Domain" (2 December 2010) http://torrentfreak.com/sensing-danger-demonoid-bittorrent-tracker-ditches-com-domain-101202

don't know if migrating will help, but it won't hurt," Demonoid's owner told TorrentFreak.[267]

- On 8 December 2010, BitTorrent released the latest version of the Tribler BitTorrent client, which, among other things, allows users to search for torrents from peers rather than from a central index, thereby obviating the need for hosted BitTorrent search engines and indexes (such as The Pirate Bay).[268]

- Reportedly, torrent-finder moved its services from torrent-finder.com to torrent-finder.info which resolves to the original IP address for torrent-finder.com.[269]

- "A work around for sites seized by ICE" - http://code.google.com/p/deicer

- "Find the IP address of a seized website" - http://www.hm2k.com/posts/find-the-ip-address-of-a-seized-website

- On 5 February 2011, TorrentFreak published a list of actions provided by an individual identified as "SearchFreak" in an article entitled "How To Stop Domain Names Being Seized by the US Government".[270]

What impact would the policy have on privacy?

321. The intention of the policy to "seize domains" appears to be to block Internet users at large from accessing particular websites. Accordingly, it is difficult see how monitoring attempts to access such sites would be necessary for the implementation of the policy. Yet, reportedly, seizedservers.com utilises website traffic analytic tools - Google Analytics and Piwik.[271]

322. Although Google Analytics and Piwik tracking cookies can be blocked (e.g. by web browser plug-ins such as Ghostery), not all Internet users are aware that such tools exist and may not even be aware that web analytic tools are being used. Furthermore, they would have been re-directed to that web server without their notice or consent.

323. Therefore, from a privacy perspective, simply rendering a domain name administratively inactive (without redirection) would be preferable.

267 *TorrentFreak* – "Sensing Danger, Demonoid BitTorrent Tracker Ditches .COM Domain" (2 December 2010) http://torrentfreak.com/sensing-danger-demonoid-bittorrent-tracker-ditches-com-domain-101202
268 *TorrentFreak* – "Truly Decentralized BitTorrent Downloading Has Finally Arrived" (8 December 2010) http://torrentfreak.com/truly-decentralized-bittorrent-downloading-has-finally-arrived-101208
269 *The Background Dope on DHS Recent Seizure of Domains* http://rulingclass.wordpress.com/2010/11/28/the-background-dope-on-dhs-recent-seizure-of-domains
270 *TorrentFreak* – "How to Stop Domain Names Being Seized by the US Government" (5 February 2011) http://torrentfreak.com/how-to-stop-domain-names-being-seized-by-the-us-government-110205
271 *The Background Dope on DHS Recent Seizure of Domains* http://rulingclass.wordpress.com/2010/11/28/the-background-dope-on-dhs-recent-seizure-of-domains

Would the policy discriminate against legitimate uses of applications?

324. This measure should not discriminate against legitimate uses of applications provided that the affected domain names do not contain any legitimate content or offer any legitimate applications or services. But, this will not always be the case. For example, a website may simultaneously offer non-infringing and infringing content.

Would the policy discourage or prevent the use of certain technologies and/or development of new communications protocols?

Would the policy encourage or discourage the use of certain business models?

Would the policy alter the basic architecture of the Internet? Are there any unpredictable or identifiably negative consequences?

What impact would the policy have on security?

325. Using the DNS as an enforcement measure may also encourage Internet users to move to DNS servers located offshore[272] or to alternate DNS servers, which if prevalent, could undermine a very fundamental aspect of the Internet – a globally unique public address space (see paragraph 259).

326. Causing Internet traffic to be re-directed from one domain name to another may undermine the widespread deployment and confidence in Domain Name System Security Extensions ("DNSSEC"). In a letter to the U.S. Senate Judiciary Committee, .Org said:

> History: The Internet has a history of openness, and a long commitment to addressing security concerns and challenges. Over the years, we have seen spoofing attacks, in which an attacker can fool the DNS system into routing to the wrong website, and "man in the middle attacks" with similar results: sending an Internet user to a website that looks like the bank, e-commerce site, or organization he/she seeks -- but is not. The result is loss of personal data, financial data, money, time, and ultimately, confidence in the Internet.
>
> So the Technical Community, together with Registries and Registrars, responded. At considerable cost of time and resources, we developed a new level of security: Domain Name System Security Extensions (DNSSEC). DNSSEC is a set of DNS extensions which provide 3 basic functions: Data Origin Authentication, Data Integrity, and Authenticated Denial of Existence. DNSSEC works on a chain of trust: passing an "electronic key" to Internet users to verify the address of the website they seek. It allows Internet users to reach the Internet sites they intend; it strengthens confidence in the Internet.

272 .Org Letter to the U.S. Senate Judiciary Committee dated 15 November 2010 http://www.eff.org/files/filenode/coica_files/COICA%20Blocking%20Breaks%20DNSSEC%20-%20.ORG%20Memo.pdf

> But Senate Bill 3804 breaks DNSSEC at this early pivotal time in its roll-out. It requires a blocking that damages and degrades DNSSEC security efforts. …[273]

327. On this issue, IETF Internet Draft *DNS Redirect Use by Service Providers*[274] states:

> … It is critically important that service providers understand that adoption of DNSSEC is technically incompatible with DNS redirect. As such, in order to properly implement DNSSEC and maintain a valid chain of trust, DNS redirect MUST NOT be used any longer. …
>
> When DNSSEC has been implemented in a service provider's resolvers, DNS redirect MUST NOT be used, as it is technically incompatible with DNSSEC and breaks the chain of trust critical to proper DNSSEC validation functionality.

328. Specifically, regarding long-term effects, .Org said COICA will:

- Completely undermine efforts to ensure that people trust their local name servers when looking up their banks, e-commerce sites and search engines – and instead create greater security and stability risks for Internet users and the DNS (Dan Kaminsky, Computer Security Guru, and Finder of the Kaminsky Bug)

- Encourage people to "opt out" of the local domain name system: specifically, to change their resolving name servers to ones located outside their ISP and outside the US – which is easy and fast to accomplish (Dan Kaminsky).

- Undermine the strong cooperative arrangements with law enforcement, legislative and judicial authorities around the globe that we are working to build (Steve Crocker, Chairman of ICANN's Security and Stability Advisory Group).

- Undermine the stability and integrity of the network by creating confusion for the Internet user. If a website is not accessible due to blocking or filtering by an ISP at a court order, is it because the network is broken, someone typed in the wrong name, or something else? There's no easy way to tell, and the result is uncertainty and loss of confidence in the overall system. (Steve Crocker).

- Create a situation which it is difficult or impossible to correct. Even if a site cures itself or is subsequently determined not to be or have been a rogue site, it will be impossibly hard to remove the blockage from all of the ISPs. AsRay Donovan, former Secretary of Labor, said after being acquitted of larceny and fraud charges, "Which office do I go to get my reputation back?" (Steve Crocker)

> Overall, S.3804 will encourage Internet users to opt-out of their DNS filters and shared DNS servers. This, in turn, will disrupt the dynamic balancing and load distribution of the Internet, and bypass the security systems we have installed. Thus,

273 .Org Letter to the U.S. Senate Judiciary Committee dated 15 November 2010 http://www.eff.org/files/filenode/coica_files/COICA%20Blocking%20Breaks%20DNSSEC%20-%20.ORG%20Memo.pdf

274 http://tools.ietf.org/html/draft-livingood-dns-redirect-02#section-6

> Internet systems will not work as efficiently or robustly today – or tomorrow, where there will be far more content to distribute.[275]

329. In a letter to the U.S. Senate Judiciary Committee, various members of the Internet technical community expressed the following views:

> … We are writing to oppose the Committee's proposed new Internet censorship and copyright bill. If enacted, this legislation will risk fragmenting the Internet's global domain name system (DNS), create an environment of tremendous fear and uncertainty for technological innovation, and seriously harm the credibility of the United States in its role as a steward of key Internet infrastructure. In exchange for this, the bill will introduce censorship that will simultaneously be circumvented by deliberate infringers while hampering innocent parties' ability to communicate.
>
> All censorship schemes impact speech beyond the category they were intended to restrict, but this bill will be particularly egregious in that regard because it causes entire domains to vanish from the Web, not just infringing pages or files. Worse, an incredible range of useful, law-abiding sites can be blacklisted under this bill. These problems will be enough to ensure that alternative name-lookup infrastructures will come into widespread use, outside the control of US service providers but easily used by American citizens. Errors and divergences will appear between these new services and the current global DNS, and contradictory addresses will confuse browsers and frustrate the people using them. These problems will be widespread and will affect sites other than those blacklisted by the American government. …[276]

Would the policy inhibit or enhance users' willingness to access the Internet or obtain access to the Internet?

330. Some users may be inhibited from accessing "seized domains" either from a technical point of view (e.g. if they do not know how to circumvent the re-direction) or perhaps because the domain names have been identified as "bad". For others, the policy probably will have no inhibiting effect. However, some users may be less willing to access unaffected areas of the Internet if the re-directed sites are not disclosed in advance, fearing (rightly or wrongly) that their government (or another country's government) will record their attempt to access a site which has been seized.

Would the policy directly or indirectly reduce Internet access or the availability of Internet access?

Is there any risk of significant or material damage to third parties' use of or access to the Internet?

331. The "domain seizure" approach outlined in paragraphs 311 – 313 changes the access of one group of Internet users (those who rely on the DNS to locate the servers at the

275 .Org Letter to the U.S. Senate Judiciary Committee dated 15 November 2010 http://www.eff.org/files/filenode/coica_files/COICA%20Blocking%20Breaks%20DNSSEC%20-%20.ORG%20Memo.pdf

276 http://www.publicknowledge.org/letter-internet-engineers-opposing-coica

affected domain names), but it does not change the access of the other group of Internet users (those who do not rely on the DNS, e.g. because they know the IP addresses of the servers). Further, the first group's devices are re-directed to a web server and content they did not request. Significantly, Internet users from all over the world (not just the U.S.) may fall into either group.

332. Rendering a domain name administratively inactive has the same effect except that there is no re-direction to another web server.

333. Where a DNS server prevents a domain name from resolving to its IP address, it changes the access of one group of Internet users (those who rely on that DNS server to locate the servers at the affected domain names), but it does not change the access of the other group of Internet users (those who do not rely on that DNS server). Unlike the "administratively inactive" approach only users of a particular DNS server would be affected.

334. If any of the affected domain names host legitimate content and/or services, these measures would prevent those who could not circumvent them from accessing that content and services. It would also prevent those content and service providers from accessing potential customers.

335. Where the "domain seizures" involve re-direction to another domain name with an official notice asserting or even mentioning illegal conduct, there is the potential to damage the reputation of legitimate businesses and individuals if the scope is not sufficiently confined.[277]

Would the policy materially raise or lower the costs of Internet access?

336. This is difficult to answer. Unlike other enforcement measures at the ISP level, enforcement via the DNS is most likely to place the cost and administrative burden on domain name registries and/or registrars. Such costs, if more than negligible and uncompensated, are likely to be recouped through domain name registration fees.

277 See *TorrentFreak* – "US Government Shuts Down 84,000 Websites 'By Mistake' " (16 February 2011) - http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216

COPYRIGHT TAXES AND LEVIES

337. A number of countries impose or have sought to impose a tax or levy on digital storage devices to collect remuneration for private copying of media (e.g. music and video). For example, under the Finnish scheme the levy for external hard disks is 5 euro for 250GB to 950GB and 10 euro for 950 GB to 3TB (with effect from 1 January 2011).[278]

338. In France, in 2005, the Alliance Public-Artistes supported by some politicians made a proposal to the French National Assembly to legalise copyright infringement via P2P and impose a fee on Internet broadband subscriptions. While initially supported by the National Assembly, the proposal was dropped in 2006.[279]

339. Last year the Canadian Radio-television and Telecommunications Commission (CRTC) in its Broadcasting Regulatory Policy CRTC 2009-329 (4 June 2009) considered the issue of whether ISPs should pay a levy to contribute to a fund to support new Canadian media broadcasting content and referred "... the question of whether ISPs, when they provide access to broadcasting content, ..." are subject to the Broadcasting Act, to the Canadian Federal Court of Appeal.[280]

340. The Canadian Federal Court of Appeal issued its decision on 7 July 2010 and said:

> Because ISPs' sole involvement is to provide the mode of transmission, they have no control or input over the content made available to Internet users by content producers and as a result, they are unable to take any steps to promote the policy described in the Broadcasting Act or its supporting provisions. Only those who "transmit" the "program" can contribute to the policy objectives.
>
> …
>
> In providing access to "broadcasting", ISPs do not transmit programs. As such, they are not "broadcasting" and therefore they do not come within the definition of "broadcasting undertaking". In so holding, I wish to reiterate as was done in CAIP that this conclusion is based on the content-neutral role of ISPs and would have to be reassessed if this role should change (CAIP, para. 92).[281]

(Note: The CRTC also said in its decision: « ...Although the Commission has determined that funding (and, consequently, a levy) is neither necessary nor appropriate at this time, it considers that the question as to whether ISPs are subject to the Act must be resolved. ...».)

341. A tax on Internet access (levied on the ISP or on the individual subscriber) whether to raise money for artists (or others) would raise the cost of Internet access by the amount of tax plus the cost of administering the tax and associated costs. Raising the cost of Internet access is likely to have a direct and negative impact on access.

278 http://www.hyvitysmaksu.fi/teosto/hymysivut.nsf/0/319D43C6E158F9E5C22577FC003F8693?opendocument
279 http://en.wikipedia.org/wiki/DADVSI#The_.22global_license.22 (as at 20 February 2011)
280 http://www.crtc.gc.ca/eng/archive/2009/2009-329.htm
281 http://www.michaelgeist.ca/content/view/5176/125

342. In any case, it would be impossible to equitably apportion the tax across Internet users (payers) and artists (recipients), particularly artists who are located outside the jurisdiction. Further, requiring Internet users to pay a copyright tax may have the unintended effect of encouraging online copyright infringement as such persons may consider paying the tax entitles them to “free” copies of copyright content.

FINAL COMMENTS

343. We note that some people argue traditional concepts of copyright such as "fair use" need to be revised in light of new technologies and new trends in expression such as user-generated content and "mash-ups". Further, we note that European Commissioner Neelie Kroes, Vice-President for the Digital Agenda, in a speech at Forum d'Avignon - Les rencontres internationales de la culture, de l'économie et des medias on 5 November 2010[282] said:

> … Today our fragmented copyright system is ill-adapted to the real essence of art, which has no frontiers. Instead, that system has ended up giving a more prominent role to intermediaries than to artists. It irritates the public who often cannot access what artists want to offer and leaves a vacuum which is served by illegal content, depriving the artists of their well deserved remuneration. And copyright enforcement is often entangled in sensitive questions about privacy, data protection or even net neutrality.
>
> It may suit some vested interests to avoid a debate, or to frame the debate on copyright in moralistic terms that merely demonise millions of citizens. But that is not a sustainable approach. We need this debate because we need action to promote a legal digital Single Market in Europe.
>
> My position is that we must look beyond national and corporatist self-interest to establish a new approach to copyright. We want "une Europe des cultures" and for this we need a debate at European level.
>
> The Commission will soon make legislative proposals on orphan works and on the transparency and governance of the collective management societies. We will examine again the problem of divergent national private copy levies. We will also look into multi-territorial and pan-European licensing. And we will not stop exploring ideas for as long as the system is not working. …

344. As the international emphasis expands from enforcement to include the scope of copyright, (specifically the appropriate scope of copyright in light of technological developments), it would be also be useful for that debate to be informed by the perspectives and expertise of the Internet technical community.

345. The future of copyright in the online environment should be examined holistically, and include consideration of issues such as: the scope of copyright in the online environment, motives behind online infringement, how copyright is infringed, objectives behind online copyright enforcement, how the Internet functions and develops, how different enforcement policies might operate in practice, and the potential impact they may have, as well as the role (if any) of Internet intermediaries and domain name registries.

346. The Internet Society considers that further dialogue is needed at the international level and at the local level where such Internet-focused technical measures are already beginning

282 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/619&format=HTML&aged=0&language=EN&guiLanguage=en

to be implemented. The Internet Society calls upon the international copyright community to embrace and implement a direct and active multi-stakeholder dialogue on these issues.

347. Finally, the Internet Society would again like to express its sincere thanks to the informal volunteer Internet Society Copyright Working Group (2009-2010), particularly those members that have contributed to the development of this document.

348. Please send any comments you have regarding this report to isoc@isoc.org, mentioning “Copyright Report” in the subject heading.

Date: 20 February 2011

bp-copyrightpolicy-201102-en