REFERENCE SERIES NO. 12

MAPPING DIGITAL MEDIA:
THE MEDIA AND LIABILITY FOR CONTENT ON THE INTERNET

By Cynthia Wong and James X. Dempsey

OPEN SOCIETY FOUNDATIONS

The Media and Liability for Content on the Internet

WRITTEN BY

Cynthia Wong and James X. Dempsey[1]

This paper provides an overview of content liability on the internet, with a focus on the risks to human rights as governments claim extended authority over this unique, borderless medium.

Speakers may be liable for content online in many of the same ways as offline, but additional rules often exist. Many countries are enacting internet-specific speech laws, often imposing enhanced liability for online expression. In addition, some governments are extending broadcast-type regulations to online media, which could create new sources of liability.

The authors also examine new entities that may be subject to liability on the internet. In some countries, internet "intermediaries"—meaning internet service providers (ISPs), webhosts, and other platforms for online expression—can be held responsible for the speech of others, which can lead to self-protective and overly broad "private" censorship. Since most speakers rely on intermediaries to host or disseminate their content, intermediary liability can harm citizens' and media institutions' ability to speak online.

Finally, the internet's borderless nature may complicate any assessment of what content laws apply, and thus what liability risk may arise. Addressing these complex challenges requires attention to several policy areas, including enacting legal protections for internet intermediaries, repealing internet content laws that enhance liability, and opposing further extension of broadcast regulation to the internet.

1. Cynthia Wong and James X. Dempsey work at the Center for Democracy & Technology, Washington, D.C.

Mapping Digital Media

The values that underpin good journalism, the need of citizens for reliable and abundant information, and the importance of such information for a healthy society and a robust democracy: these are perennial, and provide compass-bearings for anyone trying to make sense of current changes across the media landscape.

The standards in the profession are in the process of being set. Most of the effects on journalism imposed by new technology are shaped in the most developed societies, but these changes are equally influencing the media in less developed societies.

The Media Program of the Open Society Foundations has seen how changes and continuity affect the media in different places, redefining the way they can operate sustainably while staying true to values of pluralism and diversity, transparency and accountability, editorial independence, freedom of expression and information, public service, and high professional standards.

The **Mapping Digital Media** project, which examines these changes in-depth, aims to build bridges between researchers and policy-makers, activists, academics and standard-setters across the world.

The project assesses, in the light of these values, the global opportunities and risks that are created for media by the following developments:

- the switchover from analog broadcasting to digital broadcasting
- growth of new media platforms as sources of news
- convergence of traditional broadcasting with telecommunications.

As part of this endeavor, the Open Society Media Program has commissioned introductory papers on a range of issues, topics, policies and technologies that are important for understanding these processes. Each paper in the **Reference Series** is authored by a recognised expert, academic or experienced activist, and is written with as little jargon as the subject permits.

The reference series accompanies reports into the impact of digitization in 60 countries across the world. Produced by local researchers and partner organizations in each country, these reports examine how these changes affect the core democratic service that any media system should provide – news about political, economic and social affairs. Cumulatively, these reports will provide a much-needed resource on the democratic role of digital media.

The **Mapping Digital Media** project builds policy capacity in countries where this is less developed, encouraging stakeholders to participate and influence change. At the same time, this research creates a knowledge base, laying foundations for advocacy work, building capacity and enhancing debate.

The **Mapping Digital Media** is a project of the Open Society Media Program, in collaboration with the Open Society Information Program.

Contents

I. Introduction 6

II. Sources of Content Liability 7

III. Liable Parties 13

IV. Cross-Border Issues 19

V. Policy Reforms 22

I. Introduction

The internet is a powerful platform for expression of all kinds, presenting many opportunities for traditional media while also supporting a wide range of innovative uses. However, as the internet has become more central to the lives and work of individuals and media organizations alike, governments around the world have become more aggressive in seeking to control online content, posing challenges for both content producers and media platforms.

Certain attributes of the internet appear to support especially robust online speech: the internet has a nearly unlimited capacity to enable user participation and interactivity, and its borderless nature defies traditional territorial boundaries. At the same time, other attributes of the internet offer new avenues of control and new ways for governments to stifle dissent. This essay provides an overview of content liability on the internet, exploring the sources of liability, the parties subject to liability, and the challenges of jurisdiction, with a focus on the risks to democratic values as governments claim extended authority over this unique, borderless medium.

As we discuss in section one, speakers are legally liable for content online in many of the same ways they are in the offline world, but additional rules often exist. Liability can be of a criminal or civil nature, or both. Liability can arise from national laws, for example, that prohibit (or permit private lawsuits for) incitement to violence, defamation, hate speech, obscenity or pornography, privacy violations, blasphemy, criticism of the government or government officials, or copyright infringement.

In section two, we examine a special area of concern: in some countries, internet "intermediaries"—ISPs, web hosts, and other platforms and conduits for online expression—can be held responsible for content created by others, which can lead to self-protective and overly broad private censorship. In section three, we explore how the borderless nature of the internet often complicates any assessment of what law applies, and thus of what liability risk a speaker faces: content that is lawful in one country may run afoul of national laws in another country, and governments are increasingly attempting to extend national law in order to reach content originating outside their countries. Section four suggests several policy reforms that would help to protect internet freedom.

II. Sources of Content Liability

In this section, we highlight examples of how governments are using existing or new laws to restrict individuals' use of the internet to access information and engage in expressive activity.

It is important to note at the outset that governmental actions against internet speech may be subject to challenge under the freedom of expression clauses in international and regional human rights treaties, which clearly apply to the internet.[2] These instruments, as well as national constitutions, have been interpreted variously to limit the scope of government power to impose liability for content. For example, the Inter-American Court of Human Rights has ruled that article 13.2 of the American Convention on Human Rights establishes three criteria for any national law limiting freedom of expression: first, the limitation must have been defined in a precise and clear manner by a law; second, the limitation must serve a compelling governmental objective authorized by the Convention; and third, the limitation must be necessary in a democratic society, strictly proportionate, and appropriate to serve the compelling objective.[3]

However, all human rights instruments permit some imposition of liability for some forms of content. Moreover, it is generally accepted that, within the scope of permissible restrictions, national laws will vary as to what kind of speech is proscribed, in part due to legitimate cultural differences. For example, the European Court of Human Rights grants individual national laws restricting expression a certain "margin of appreciation"—a deference to local standards—particularly in the area of morals.[4] The application of international human rights law to the internet requires further concerted attention of both traditional media and internet stakeholders.

---

2. See, e.g., "Report of the UN's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/HRC/14/23 (2010) pp. 12–16 (summarizing the permissible restrictions and limitations on freedom of expression), available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf (accessed 15 November 2010).

3. See "Annual Report of the OAS Special Rapporteur for Freedom of Expression," Volume II of the Inter-American Commission on Human Rights (IACHR) "Annual Report" (December 2009), pp. 233–239, available at http://www.cidh.org/pdf%20files/Annual%20Report%202009.pdf (accessed 15 November 2010). The standard under the European Convention on Human Rights is similar: the European Court of Human Rights has stated that any government measure that infringes on the rights granted in article 10 of the Convention must be prescribed in law, have a legitimate aim, and be necessary in a democratic society to achieve that aim.

4. See, e.g., *Handyside v. United Kingdom*, Series A, no. 24, 1 EHRR 737 (1979).

1. Laws Created to Regulate Online Behavior

1.1 Laws Created to Directly Regulate Online Speech

Some governments have passed specific laws directed at behavior on the internet. One example is the Internet Law of Turkey, known as Law 5651.[5] The government enacted this law in 2007 in response to concerns about YouTube videos containing content that was illegal in Turkey, as well as the availability of pornography and other online materials deemed harmful to children. Although Law no. 5651 does not create new internet speech crimes, it imposes new obligations on content providers, ISPs, and website hosts, and it grants authority to an agency to issue administrative orders to block websites (for content hosted outside Turkey),[6] and to take down eight specific kinds of unlawful content.[7] Also imposing broad data retention requirements on service providers,[8] Law no. 5651 seems aimed both at preventing the particular "harm" caused by prohibited speech when disseminated online and at facilitating its prosecution.

Thailand's 2007 Computer Crimes Act (CCA) is another example of a law specifically targeting the internet.[9] The CCA defines new computer crimes and sources of civil liability and provides broad electronic search and seizure authority to government officials. The CCA, which implicates both intermediaries that transmit or host third-party content and content authors themselves,[10] punishes the online publication or knowing dissemination of "false computer data" that causes injury to another person, the public, or to national security, as well as making "obscene computer data" accessible to the public.[11]

However, the law leaves many of these terms undefined, and the breadth of the language makes it difficult to assess what speech might be judged unlawful. The CCA does not make specific reference to Thailand's *lèse majesté* law, which criminalizes criticism or defamation of the royal family.[12] However, because government

5. Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication, Law no. 5651, *Turkish Official Gazette* no. 26030, 23 May 2007 (hereafter Internet Law of Turkey).

6. Internet Law of Turkey, art. 8. The law provides for some judicial oversight and a process for appealing blocking orders. However, the standard the agency must meet to get a blocking order approved in the first place is low, requiring only "sufficient suspicion" of criminal activity. For a fuller analysis, see Y. Akdeniz, "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship," 2010, available at http://www.osce.org/documents/rfm/2010/01/42294_en.pdf (hereafter OSCE Turkey Report) (accessed 15 November 2010).

7. The specific crimes include obscenity, child abuse images, encouragement of or incitement to suicide, crimes against Atatürk, and the provision of substances dangerous to health. Although Turkish lawmakers consciously decided to limit the scope of the crimes covered by the law, there is already pressure to expand this list. See Y. Akdeniz and K. Altiparmak, "Internet: Restricted Access, A Critical Assessment of Internet Content Regulation and Censorship in Turkey," 2008, available at http://privacy.cyber-rights.org.tr/?page_id=256 (hereafter Akdeniz and Altiparmak, *Internet: Restricted Access*) (accessed 15 November 2010).

8. Internet Law of Turkey, art. 6(1)(b). The data retention requirements track those of the EU Data Retention Directive, 2006/24/EC. However, the Turkish provision has been criticized because it is not subject to the counterbalancing data protection requirements or oversight mechanisms that exist in other Member States. See Akdeniz, *Internet: Restricted Access*, p. 64.

9. Computer Crimes Act BE 2550 (2007), English translation available at http://advocacy.globalvoicesonline.org/wp-content/plugins/download-monitor/download.php?id=2 (hereafter Computer Crimes Act) (accessed 15 November 2010).

10. See section 2.

11. Computer Crimes Act, section 14. Section 16 also specifically penalizes the public online dissemination of digital photographs meant to hurt the reputation of others or expose another person to public hatred or shame.

12. See OpenNet Initiative, "Thailand Country Profile," 2007, available at http://opennet.net/research/profiles/thailand (accessed 15 November 2010).

officials have interpreted *lèse majesté* broadly to amount to harm to national security, the mechanisms created by the CCA have been used to penalize online political dissent or criticism of the government.[13] By imposing liability on intermediaries, the CCA forces service providers to self-censor their services, with results that risk being broader even than direct regulation.[14]

1.2 Electronic Privacy and Data Protection Laws can Create Liability

Content liability does not only arise from laws that directly regulate speech. In Europe, it may also arise from privacy and data protection laws. The EU Data Protection Directive (DPD) requires entities that collect and process personally identifiable information (PII) to take steps to secure it, guarantee its accuracy, handle it responsibly, and get permission from the data subject before making it publicly available.[15] Given that the DPD applies to any PII (including pictures or video in some circumstances), anyone who hosts or disseminates works involving the likenesses of others could face liability under the DPD if they are found to be "controllers" of that data.[16]

For example, an Italian court convicted three Google executives of violating Italy's Data Protection Code after a video depicting cruelty to a disabled teenager was posted by a user on the Google video service. Even though the video was taken down within hours of notification by Italian law enforcers,[17] the judge found the Google executives guilty.[18] This decision has been much criticized both inside and outside Italy, and it remains to be seen whether the extension of liability to content hosts such as Google will be widely adopted in Europe. However, leaving aside the question of Google's liability as an intermediary, the case illustrates how the violation of privacy rights may be a source of liability.[19]

---

13. See Reporters Without Borders, "Countries Under Surveillance – Thailand," "Internet Enemies Report," 2009, available at http://en.rsf.org/surveillance-thailand,36673.html; U.S. State Department, "2009 Human Rights Report: Thailand," 11 March 2010, available at http://www.state.gov/g/drl/rls/hrrpt/2009/eap/136010.htm (hereafter U.S. State Department, "2009 Human Rights Report: Thailand") (accessed 15 November 2010).

14. For example, many politically focused bulletin boards and forums in Thailand have self-censored their content to avoid being blocked under the CCA. See U.S. State Department, "2009 Human Rights Report: Thailand." For a discussion of how China has privatized censorship, see section two.

15. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT (accessed 15 November 2010).

16. The DPD does provide for some exceptions, for example, processing of personal data by a natural person for a "purely personal or household activity:" Directive 95/46/EC, art. 4(2).

17. "Google bosses convicted in Italy," BBC News, 24 February 2010, available at http://news.bbc.co.uk/2/hi/8533695.stm. See also L. Harris, "Deep Impact: Italy's Conviction of Google Execs Threatens Global Internet Freedom," *Huffington Post*, 24 February 2010, available at http://www.huffingtonpost.com/leslie-harris/deep-impact-italys-convic_b_474648.html (accessed 15 November 2010); A. Bright, "Will Italy's Conviction of Google Execs Stick?," Citizen Media Law Project, 2 March 2010, available at http://www.citmedialaw.org/blog/2010/will-italys-conviction-google-execs-stick (accessed 15 November 2010).

18. G. Sartor and M. Viola de Azevedo Cunha, "The Italian Google Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents," 2010, available at http://ssrn.com/abstract=1604411 (accessed 15 November 2010).

19. As discussed in section two, the EU E-Commerce Directive (ECD), 2000/31/EC limits the liability of specific internet intermediaries for content authored or disseminated by third-party users. However, in an ambiguous provision, art. 1.5 of the ECD states that the "Directive shall not apply to … questions relating to information society services covered by Directives 95/46/EC [the DPD] and 97/66/EC [a related privacy directive]." The meaning of art. 1.5 is a source of uncertainty, and different EU Member States may interpret the relationship between the two Directives differently where it comes to intermediary liability for the data protection violations committed by users of an online service.

2. Existing Laws Applied to Online Content

2.1 Existing Laws that Regulate Speech Can be Applied to Online Content

In some cases, governments simply apply existing laws to online content. Under its hate speech laws, France prohibits the sale of Nazi memorabilia. A French court penalized Yahoo! in 2000 for providing access to such material online, arguing that existing French law applies to internet speech.[20] In Turkey, it is a crime to insult the founder of the Republic, Mustafa Kemal Atatürk, or to "disparage Turkishness," and authorities have applied this law to videos hosted on YouTube.[21]

However, applying offline rules to the internet poses special problems and may yield rules with harsh consequences. The UK has applied its "multiple publication rule" in deciding online defamation cases. Stemming from longstanding common law, the rule provides that each individual sale or distribution of defamatory content can be considered a separate publication and can thus give rise to a separate cause of action. Applying this rule to online content raises serious problems, particularly because content can be widely disseminated almost instantaneously and is often mirrored, archived, and made available years after initial publication. Nevertheless, UK courts have applied this rule to online content, treating "each viewing of a defamatory posting" as a new publication that can give rise to damages.[22] This creates the possibility that a litigious plaintiff could bring an endless string of lawsuits for a single piece of content as it is archived, mirrored, and redistributed online. The enormous threat of liability this would pose to media organizations and other content authors online can have a grave chilling effect on online expression.[23]

---

20. *UEJF et Licra v. Yahoo! Inc. et Yahoo France*, Tribunal de Grande Instance de Paris, 22 May 2000, translation available at http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (accessed 15 November 2010). Yahoo! successfully sought a declaratory judgment in the U.S. district court that the French judgment was unenforceable under the First Amendment to the Constitution. However, an appellate court reversed the lower court's decision on procedural grounds, leaving the status of the French order unsettled. *Yahoo! Inc. v. LICRA and UEJF*, 433 F.3d 1199 (9th Cir. 2006), available at http://cases.justia.com/us-court-of-appeals/F3/433/1199/546158/ (accessed 15 November 2010).

21. Akdeniz and Altiparmak, *Internet: Restricted Access*. The provision on "Turkishness" was amended in 2008 to limit its application and lower penalties. See also S. Tavernise, "Turkey to Alter Speech Law," *New York Times*, 25 January 2008, available at http://www.nytimes.com/2008/01/25/world/europe/25turkey.html (accessed 15 November 2010). Nevertheless, concerns remain about its application, including in the internet context. See Jeffrey Rosen, "Google's Gatekeepers," *New York Times*, 28 November 2008, available at http://www.nytimes.com/2008/11/30/magazine/30google-t.html (discussing the struggle between Google and Turkey over YouTube videos) (accessed 15 November 2010). In addition, Turkey has also passed a law specifically dealing with regulation of expression on the internet: see OSCE Turkey Report.

22. C. Davidson, "U.K. Internet Publication Rule Upheld; Internet Viewings Constitute Republication," Proskauer Privacy Law Blog, 13 March 2009, available at http://privacylaw.proskauer.com/2009/03/articles/international/uk-internet-publication-rule-upheld-internet-viewings-constitute-republication/ (accessed 15 November 2010). The UK rule was upheld by the European Court of Human Rights. A. Hirsch, "Times Fails to Overturn 'Internet Publication Rule' in Court Case," *The Guardian*, 10 March 2009, available at http://www.guardian.co.uk/media/2009/mar/10/times-european-court-single-publication (accessed 15 November 2010).

23. In contrast, the United States applies a single publication rule, where any one edition of a newspaper or any one radio broadcast is considered a single publication, and only one action can be brought by a plaintiff for that publication. U.S. courts have upheld the single publication rule for online content. For further background, see I. Maytal, "Libel Lessons from Across the Pond: What British Courts Can Learn from the United States' Chilling Experience with the 'Multiple Publication Rule' in Traditional Media and the Internet," 3 *Journal of International Media & Entertainment Law* 121 (2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1655046 (accessed 15 November 2010).

2.2 Application of Broadcast Media Regulations to Online Content

In applying offline rules to the internet, the question arises of what is the appropriate subset of offline rules to use. Some countries are extending to the internet rules developed for traditional broadcast media (radio and television), even though these rules are not particularly well suited to the unique attributes of the internet as an abundant, borderless, user-controlled medium.

Within the European Union, the Audiovisual Media Services Directive (AVMS), which once only regulated broadcast television, has been revised to apply to content available through "on-demand" audiovisual media services. This includes internet content that consists of commercial mass media that is "television-like" and whose function is to "inform, entertain and educate the general public."[24] It is unclear whether EU Member States will interpret and apply these terms to cover novel online video services, including those that support user-generated content (UGC). But the mere fact that the internet is being subsumed at all under the AVMS is troubling, because broadcast media were traditionally subject to more restrictions than other kinds of media.

Many of the historic rationales for strictly regulating broadcast media do not apply to the internet. Traditionally, broadcast media were characterized by scarcity and limited user control. At a technical level, the ability to exploit the electromagnetic spectrum was limited. Content was pushed out over a limited number of channels, and viewers or listeners had little control over what information they might receive. Moreover, concentrated ownership was (and remains) an issue with traditional media, in part because of the high costs of producing and disseminating content. Together, these factors were cited in the past to justify licensing requirements and stricter rules for content on broadcast media.[25]

In contrast, the internet is uniquely user-controlled. Individuals can exercise choice over what information to access, and parents can employ a variety of tools to screen their children from unwanted content.[26] Unlike newspapers or television stations, which exercise direct editorial control over content, the content host—that is, the web host or the provider of a platform for UGC—often has no editorial control over the content itself. The capacity of the internet's networked architecture is essentially unlimited; new outlets for expression can be added by any user at very little cost. The model of platforms that allow users to post content at no charge does not have precedent in the broadcast world. Also, the internet provides a virtually instantaneous right of reply. These unique attributes suggest that online content is entitled to stronger free expression protections than any other media.[27]

---

24. Directive 2010/13/EU of the European Parliament and of the Council on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (codified version), Recitals 22 and 24, 10 March 2010 (stating that "television-like" means "they compete for the same audience as television broadcasts, and the nature and the means of access to the service would lead the user reasonably to expect regulatory protection within the scope of this Directive"), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:095:0001:0024:EN:PDF (accessed 15 November 2010).

25. See, e.g., *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978); *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 380 (1969); Benton Foundation, "Advisory Committee on Public Interest Obligations of Digital Television Broadcasters," available at http://www.benton.org/initiatives/obligations/charting_the_digital_broadcasting_future/sec2 (accessed 15 November 2010).

26. J.B. Morris, Jr and C.M. Wong, "Revisiting User Control: The Emergence and Success of a First Amendment Theory for the Internet Age", 8 First Amend. L. Rev. 109 (2009), available at http://www.cdt.org/files/pdfs/morris_wong_user_control.pdf (accessed 15 November 2010).

27. If anything, television and radio are becoming more like the internet, suggesting that, rather than extending traditional restrictions to the internet, such restrictions are now less justifiable even for traditional media.

Applying traditional broadcast media laws to online platforms would cripple the innovation, growth, and diversity of information that the internet has enabled. Licensing requirements for content or websites would create a severe bottleneck, reducing the current abundance of UGC to amounts comparable with what we find on television. Licensing costs would meanwhile destroy the internet as a low-barrier-to-entry medium. License requirements would additionally provide governments with one more lever to control content. This is a lesson already apparent to China's internet users; China only allows local ISPs to deliver licensed websites and uses the license approval and renewal process as a means of censoring content and enforcing requirements for websites to self-censor.[28]

There is, however, one important qualification to our warning about the danger of extending traditional broadcasting laws to the internet. This exception concerns the subset of regulations that sustain public service broadcasting. In many parts of the world, public service broadcast laws are specifically intended to increase the diversity and independence of views heard over the airwaves. In the digital age, if public service broadcasters are unable to offer online services such as websites, on-demand services, and a range of innovative online applications, then their relevance, their viability, and the longer-term future of a dual (public and private) broadcasting system will be cast into doubt. This, in turn, would have a negative impact on the provision of quality output in key program strands, including news, in countries around the world, from Japan and Thailand to Canada, Germany, and the UK. Thus, rather than ignoring the internet in public service broadcasting laws, free expression and independent media might be best served by making it clear in those laws that public broadcasting entities can also disseminate content through the internet.

28. Websites hosted on Chinese servers are required to navigate multiple layers of bureaucracy and, sometimes, political as well as legal roadblocks to obtain what is known as an Internet Content Provider (ICP) license. John Bishop and Chris Myrack, "FOCUS: Google License Issue Seized by China to Make Political Statement," AFX News Limited, 23 February 2006, available at http://www.forbes.com/feeds/afx/2006/02/23/afx2547661.html (accessed 15 November 2010). Once the license is granted, the grantee is responsible for monitoring site content and engaging in self-censorship; the national telecommunications law prohibits websites from hosting or facilitating distribution of a wide range of content, including material that "harms the national interest" or "undermines social stability." PRC Telecommunications Regulations, [2000] State Council Order no. 291, available at http://www.isc.org.cn/20020417/ca38931.htm (accessed 15 November 2010). Those who fail to comply with the self-censorship requirements risk losing their ICP license, their website, and their business license: "*China's Information Control Practices and the Implications for the United States, Testimony Before the United States-China Economic and Security Review Commission,* 30 June 2010 (testimony of Rebecca MacKinnon, Visiting Fellow, Center for Information Technology Policy, Princeton University), available at http://www.uscc.gov/hearings/2010hearings/written_testimonies/10_06_30_wrt/10_06_30_mackinnon_statement.php (accessed 15 November 2010). Most famously, Google battled to maintain its ICP license after it redirected all users who visited its google.cn website to its uncensored Hong Kong site, google.hk. D. Drummond, "An Update on China," Google Blog, 28 June 2010, available at http://googleblog.blogspot.com/2010/06/update-on-china.html (accessed 15 November 2010). See ge2nerally R. MacKinnon, "Studying Chinese Blog Censorship," RConversation, 29 November 2008, available at http://rconversation.blogs.com/rconversation/2008/11/studying-chines.html (accessed 15 November 2010).

III. Liable Parties

Once it has been determined that particular content is unlawful under applicable law, a second question arises of who is to be held liable. The answer varies from country to country. In the online world, as offline, the original author or creator of unlawful content is almost always liable. However, under some national laws, and with respect to certain content, persons or entities that distribute or possess unlawful content that they did not create can also be held liable. For example, it is unlawful in many countries to knowingly possess child abuse images.[29] With many forms of traditional media, both the author of content and the publisher (for example, the newspaper or television station) can be held liable, based in part on the premise that publishers exercise editorial control over the content.[30] To some extent, these principles extend online: a newspaper remains liable for the online content that it selects and edits.

A critical question is whether to impose liability on internet intermediaries for content hosted or disseminated on their services but created by users. Internet intermediaries are the technological entities that provide the platforms and conduits for digital communications, including internet service providers, web hosting companies, search engines, platforms for UGC (blog hosting sites, video hosting sites, social networking sites, etc.), and a range of other online service providers.[31] In fact, any site that enables user comments could be considered an intermediary with respect to that user content.

It is important to understand that the role of these intermediaries is quite different from that of the traditional publisher: While technologies and business models may vary, for the most part internet intermediaries simply transmit content requested by the user or, in the case of UGC platforms, disseminate or host at zero or low monetary cost to the user content that has been created and uploaded by users, usually without any

29. M.A. Healy, "Child pornography: an international perspective," 2 August 2004, available at http://www.crime-research.org/articles/536/5 (accessed 15 November 2010).

30. See, e.g., Citizen Media Law Project, "Immunity for Online Publishers Under the Communications Decency Act: Background on Publisher and Distributor Liability," April 2009, available at http://www.citmedialaw.org/legal-guide/immunity-online-publishers-under-communications-decency-act (accessed 15 November 2010).

31. OECD, "The Economic and Social Role of Internet Intermediaries," April 2010, DSTI/ICCP(2009)9/FINAL, available at http://www.oecd.org/dataoecd/49/4/44949023.pdf (accessed 15 November 2010).

prior review. This is very different from the control exercised by newspapers with respect to the articles they publish, or by radio stations with respect to the content they broadcast.

For many online services, the sheer volume of content makes it impossible or economically unviable for a hosting platform to screen all UGC. To illustrate: users post over 24 hours of video to YouTube every minute,[32] and an average of 750 tweets are posted to Twitter every second.[33] To pre-screen such a volume of content for potentially unlawful expression would require enormous staff and resources, making many open forums for user content prohibitively expensive, forcing some to shut down and making others too expensive for speakers of limited means. In contrast, a newspaper selects and authors a limited number of articles per issue.

In recognition of these differences between traditional media and the internet, a number of countries, including the United States and EU Member States, have laws that generally protect internet intermediaries from liability.[34] Such policies have been critical to the growth of the internet as an open platform for economic innovation and human development; their continuation is key to preserving the medium as a platform for free expression and democratic participation.[35] However, this policy framework protecting intermediaries from liability for the acts of their users is under pressure. Some governments see internet intermediaries as a convenient point of control. Because the internet enables relatively anonymous or pseudonymous activity online, it is often difficult to identify the actual author of offensive content. Even if identifiable, the wrongdoer may be outside a government's jurisdictional reach. Accordingly, some governments turn to ISPs and other intermediaries: by holding intermediaries liable for illegal content if they do not block or remove it, governments can compel them to monitor and police user content more actively.[36]

The United States has an especially strong form of protection for internet intermediaries: Except for copyright infringement (see discussion below), intermediaries in the United States are not liable for the content that is created by third parties and hosted on or transmitted over the services of those intermediaries.[37] To complicate matters, however, some platforms may combine both traditional and UGC models: for example, a newspaper's website may enable users to comment on traditional news articles without prior review by editors. In both the United States and the UK, under the laws protecting content hosts, courts have found newspapers that

---

32. "YouTube has 24 hours of video uploaded every minute," Reuters MediaFile, 17 March 2010, available at http://blogs.reuters.com/mediafile/2010/03/17/youtube-has-24-hours-of-video-uploaded-every-minute/ (accessed 15 November 2010); YouTube Fact Sheet, available at http://www.youtube.com/t/fact_sheet (accessed 15 November 2010).

33. Over 3,000 tweets were posted each second during the last 15 minutes of the 2010 World Cup final. "The 2010 World Cup, a Global Conversation," Twitter Blog, 15 July 2010, available at http://blog.twitter.com/2010/07/2010-world-cup-global-conversation.html (accessed 15 November 2010); "Big Goals, Big Game, Big Records," Twitter Blog, 18 June 2010, available at http://blog.twitter.com/2010/06/big-goals-big-game-big-records.html (accessed 15 November 2010).

34. Two separate laws provide protections for internet intermediaries under U.S. law: section 512 of the Copyright Act, 17 U.S.C. 512 (for copyright infringement) and section 230 of the Communications Act, 47 U.S.C. 230 (for a range of other kinds of claims). The EU provides protections for intermediaries in the E-Commerce Directive, 2000/31/EC.

35. Center for Democracy & Technology, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," April 2010, available at http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf (hereafter CDT, "Intermediary Liability") (accessed 15 November 2010).

36. CDT, "Intermediary Liability."

37. 47 U.S.C. § 230, http://www.law.cornell.edu/uscode/47/230.html (accessed 15 November 2010).

provide such interactive features are not liable for the comments that readers post.[38] Under U.S. law, content hosts enjoy liability protections even where they voluntarily moderate or restrict access to objectionable user comments.[39] In many other countries, however, the status of the liability risk for newspapers that also host user content is uncertain.

A number of other countries protect intermediaries by variations on what is known as a notice-and-takedown regime. Under such a framework, certain intermediaries are protected from liability provided that they take down unlawful material when made aware of its existence. For example, under the EU-wide E-Commerce Directive, a provider of hosting services for user-submitted content can avoid liability for such content if it does not have actual knowledge of illegal activity and if it "expeditiously" removes the unlawful content when made aware of it.[40] This Directive was enacted before the advent of the Web 2.0 UGC era, and the scope of liability protection in the EU is in flux. For example, the interpretation of key terms, including what constitutes "knowledge" or "expeditious," varies greatly between countries and even within the same country.[41]

U.S. copyright law also has a notice-and-takedown system, under which service providers may be liable for the infringing conduct of their customers unless they meet the criteria for the "safe harbor" outlined by section 512 of the Digital Millennium Copyright Act (DMCA).[42] Criteria vary depending on the type of provider.[43] For example, hosts must take down infringing material when notified by the copyright owner of its presence on the provider's service (among other requirements).[44]

---

38. See, e.g., *Karim v. Newsquest Media Group, Ltd* [2009] EWHC 3205 (QB), 27 October 2009, available at http://www.bailii.org/ew/cases/EWHC/QB/2009/3205.html (finding that a newspaper was eligible for the defense provided by the E-Commerce Directive regulations as hosts of user commentary) (accessed 15 November 2010); "Court Ruling Clarifies Law on User-Generated Content," HoldtheFrontPage, 29 October 2009, available at http://www.holdthefrontpage.co.uk/law/091029karim.shtml (accessed 15 November 2010). See also *Collins v. Purdue University*, 2010 WL 1250916 (N.D. Ind. 24 March 2010); E. Goldman, "230 Protects Newspaper from Liability for Reader Comments—Collins v. Purdue," Technology & Marketing Law Blog, 5 April 2010, available at http://blog.ericgoldman.org/archives/2010/04/230_protects_ne.htm (accessed 15 November 2010).

39. Section 230(c)(2)(A) of the Communications Act, 47 U.S.C. 230. It is less clear whether the law in the UK or other EU Member States would allow websites that moderate user comments to benefit from protection as hosts.

40. Art. 14, E-Commerce Directive, 2000/31/EC, available at http://ec.europa.eu/internal_market/e-commerce/index_en.htm (accessed 15 November 2010). See also OpenNet Initiative, Europe – Regional Overview, 2009, available at http://opennet.net/research/regions/europe (accessed 15 November 2010). The Directive expressly encouraged self-regulation by industry (rather than imposing a mandate) in creating appropriate notice and takedown procedures. Recital 40, E-Commerce Directive, 2000/31/EC. See also "First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce," pp. 14–16, available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF (hereafter "First Report on the Application of Directive 2000/31/EC") (accessed 15 November 2010).

41. The Directive also does not extend immunity to search engines or portals that provide links to content. However, many EU Member States have extended immunity to such service providers in recognition of their importance to the functioning of the internet: "First Report on the application of Directive 2000/31/EC," p. 13.

42. 17 U.S.C. 512, available at http://www4.law.cornell.edu/uscode/17/512.html (accessed 15 November 2010). For a good overview of the DMCA, see Frequently Asked Questions (and Answers) about DMCA Safe Harbor, available at http://www.chillingeffects.org/dmca512/faq.cgi (accessed 15 November 2010). For example, a content hosting provider must, among other things, take down infringing material when notified of its presence on the provider's network by the copyright owner; must not have known about the infringement (or must take down the content if it becomes aware of the activity); and must not receive direct financial benefit from the infringing activity where the provider is able to control the activity: 17 U.S.C. 512(c).

43. 17 U.S.C. 512(c).

44. If a service provider meets the relevant requirements, only the individual infringing customer may be subject to liability; if the provider doesn't satisfy the requirements, it loses its safe harbor. The DMCA also provides that this safe harbor is not conditioned on providers' monitoring or affirmatively investigating unlawful activity on their networks: 17 U.S.C. 512(m).

Requiring intermediaries to implement a notice-and-takedown system is one way to ensure that intermediaries are not actively engaging in or encouraging the unlawful behavior occurring on their services. However, notice-and-takedown systems are vulnerable to abuse by both governmental and private actors.[45] Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown.[46] Intermediaries typically have little or no incentive to challenge a takedown request, even if they suspect the notice-and-takedown system is being abused.[47] Advocates have documented how these drawbacks can chill free expression.[48] Efforts to encourage more countries to impose liability on intermediaries in the name of copyright, especially when those countries do not have counterbalancing protections, thus raise concerns that intermediary liability frameworks could lead to increased monitoring by ISPs or other limitations on expression.[49]

Chile and Brazil have sought to ameliorate some of the problems with notice-and-takedown regimes. Chile recently passed a bill limiting the liability of ISPs for copyright infringements by their customers. On its surface, the Chilean law appears similar to the United States' DMCA. However, unlike in the United States, Chilean content hosts are not required to remove access to infringing material until notified by a court order.[50] In requiring a court order, rather than simply a privately issued notification, to initiate a takedown, Chile's law is designed to prevent the types of abuses that are possible under more traditional notice-and-takedown

45. While U.S. copyright law provides some penalty for misuse of the notice and takedown process, the high costs of challenging a notice in court may prevent many users from doing so, diminishing any deterrent effect these penalties might have against abuse: 17 U.S.C. 512(f). See E. Goldman, "Rare Ruling on Damages for Sending Bogus Copyright Takedown Notice – Lenz v. Universal," Technology & Marketing Law Blog, 26 February 2010, available at http://blog.ericgoldman.org/archives/2010/02/standards_for_5.htm (accessed 15 November 2010).

46. N. Villeneuve, "Evasion Tactics: Global Online Censorship is Growing, but so are the Means to Challenge it and Protect Privacy," *Index on Censorship* 36(4) November 2007, available at http://www.nartv.org/mirror/evasiontactics-indexoncensorship.pdf (accessed 15 November 2010). U.S. copyright law gives users an opportunity to object to the takedown action by filing a "counter-notice." This process requires disclosure of user information and consent to court jurisdiction: 17 U.S.C. 512(g). See also Center for Democracy & Technology, "Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech," September 2010, available at http://www.cdt.org/files/pdfs/copyright_takedowns.pdf (accessed 15 November 2010).

47. The question of whether particular content is actually illegal may involve a factual inquiry, careful balancing of competing interests, and consideration of defenses. Rather than make these judgments, intermediaries will normally not risk liability, they will simply take down the material as soon as they receive the request to do so.

48. See Electronic Frontier Foundation, "Takedown Hall of Shame," available at http://www.eff.org/takedowns (documenting abuses of U.S. trademark and copyright law to silence critics or political opponents); and Chilling Effects Clearinghouse, available at http://www.chillingeffects.org/index.cgi (both sites accessed 15 November 2010).

49. Several countries (including the United States and members of the EU) are currently negotiating the Anti-Counterfeiting Trade Agreement (ACTA), a multilateral trade agreement that could potentially encourage more countries to impose liability on intermediaries in the name of copyright protection. Negotiating parties released a pre-decisional draft of ACTA in April 2010. For analysis of this draft, see D. Sohn, "Cloak of Secrecy Lifted as ACTA Text Goes Public," Policy Beta, 21 April 2010, available at http://www.cdt.org/blogs/david-sohn/cloak-secrecy-lifted-acta-text-goes-public (accessed 15 November 2010). See also M. Geist, "ACTA Draft Text Released: (Nearly) Same as it Ever Was," Michael Geist Blog, 21 April 2010, available at http://www.michaelgeist.ca/content/view/4972/125/ (accessed 15 November 2010); and "EU Data Protection Supervisor Warns Against ACTA, Calls 3 Strikes Disproportionate," Michael Geist Blog, 22 February 2010, available at http://www.michaelgeist.ca/content/view/4809/125/ (accessed 15 November 2010).

50. Chapter III, art. 85-L to 85-U, Ley N° 20435, Modifica La Ley N° 17.336 Sobre Propiedad Intelectual (4 May 2010), available at http://www.leychile.cl/Navegar?idNorma=1012827&idParte=&idVersion=2010-05-04 (Texto no Oficial). See also V. Sreeharsha, "No Safe Harbors in Argentina," NYTimes Bits Blog, 20 August 2010, available at http://bits.blogs.nytimes.com/2010/08/20/no-safe-harbors-in-argentina/; "Chile Breaks New Ground in Regulating IP Liability," WIPO Magazine, June 2010, available at http://www.wipo.int/wipo_magazine/en/2010/03/article_0009.html. For a detailed legislative history of the law, from the perspective of intellectual property advocates, see International Intellectual Property Alliance, "Chile: International Intellectual Property Alliance 2010 Special 301 Report on Copyright Protection and Enforcement" 18 February 2010, available at www.iipa.com/rbc/2010/2010SPEC301CHILE.pdf (sites accessed 15 November 2010).

regimes. Meanwhile, as of this writing, Brazil is debating a law that would provide general protections for intermediaries provided they comply with all court-issued takedown orders.[51]

India revised its intermediary liability regime to strengthen protections for intermediaries, but the law may still pose considerable risks for free expression and create uncertainty over the scope of liability risk. Under the Information Technology Act (ITA) (2008), intermediaries are protected from liability for third-party content if they remove or disable access to illegal content in response to state-issued notifications or if they have "actual knowledge" that they are transmitting or hosting such content.[52] Intermediaries must also "observe due diligence while discharging" requirements of the law, as provided by rules which the government will promulgate.[53]

This compromise regime, implemented in 2009, arose from recognition that a 2000 law which made most intermediaries liable for all third-party content would likely freeze innovation and growth.[54] The safe harbor does not, however, appear to extend to the transmission and hosting of child pornography, [55] leaving open questions about how intermediaries can avoid liability under this provision without considerable monitoring and self-censorship.[56] In the past, ISPs in India blocked large numbers of non-infringing sites out of fear of taking on liability.[57] Although protections for intermediaries are strengthened with respect to UGC, the ITA also empowers the government to order intermediaries to block content and to assist in a wide range of surveillance activities under threat of fines or imprisonment.[58]

Finally, some countries have rejected notice-and-takedown frameworks and instead have adopted strict liability regimes. China presents a stark example of how intermediary liability is used to stifle expression and

---

51. See "New Draft Bill Proposition: Available for Download," Marco Civil da Internet, 21 May 2010, available at http://culturadigital.br/marco-civil/2010/05/21/new-draft-bill-proposition-available-for-download. The drafting process has been remarkable for its level of netizen input. See "Sobre," Marco Civil da Internet, available at http://culturadigital.br/marcocivil/sobre/ (accessed 15 November 2010).

52. Information Technology Act, Section (Amendment) 79 (2008) (In.).

53. Information Technology Act, Section 79 (2008) (In.). Concerns have been raised that these requirements may still place too high a burden on intermediaries. Freedom House, "Freedom on the Net: A Global Assessment of Internet and Digital Media," 1 April 2009, available at http://www.freedomhouse.org/template.cfm?page=383&report=79 (hereafter Freedom House, "Net"). See also "Short Note on IT Amendment Act, 2008," Center for Internet & Society, February 2009, available at http://www.cis-india.org/advocacy/igov/it-act/short-note-on-amendment-act-2008 (hereafter Center for Internet & Society, "Short Note") (sites accessed 15 November 2010).

54 A. Anchayil and A. Mattamana, "Intermediary Liability and Child Pornography: A Comparative Analysis," *Journal of International Commercial Law and Technology* Vol. 5, Issue 1 (2010) (hereafter Anchavil and Mattamana, "Child"). The new law expanded the definition of intermediaries to include a wider range of entities and modeled a new safe harbor provision for intermediaries after the one in the EU's E-Commerce Directive: Information Technology Act, section 2(1)(W) (2008) (In.), available at http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf (accessed 15 November 2010); see also Anchavil and Mattamana, "Child," p. 54.

55. The law imposes strict, criminal liability on "whoever publishes or transmits or causes to be published or transmitted material in any electronic form" depicting child pornography, Information Technology Act, section 67B (2008) (In.), available at http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf (accessed 15 November 2010).

56. Rules that explain enforcement of this provision have yet to be promulgated. Anchavil and Mattamana, "Child," p. 55; Center for Internet & Society, "Short Note."

57. Freedom House, "Net," pp. 64–65.

58 See generally M. Mitta, "Govt can't ban porn websites for obscenity," *Times of India*, 11 February 2010, available at http://timesofindia.indiatimes.com/india/Govt-cant-ban-porn-websites-for-obscenity/articleshow/5558110.cms#ixzz10EZEjQfp. See also P. Prakash, "Primer on the New IT Act," Internet Governance Blog, 29 July 2009, available at http://www.cis-india.org/advocacy/igov/blog/primer-it-act (sites accessed 15 November 2010).

to control online behavior. Chinese law imposes liability on multiple layers of internet intermediaries for any unlawful content that is transmitted or hosted on their service, including ISPs, websites, host companies, blog platforms, and other online service providers.[59] If any of these intermediaries allows users to post or send unlawful content, then the intermediary can face fines, criminal liability, or revocation of its operating license. In this way, the government has effectively delegated a portion of its information control system to the private sector. Furthermore, the impact on free expression is made worse because the categories of prohibited expression are broadly and vaguely defined. For example, content that "harms the interests of the nation" is illegal.[60] To protect themselves from liability, intermediaries have an incentive to stay well back from the line, censoring even lawful content.[61]

The Thai CCA, discussed above, also creates liability for intermediaries: if the service provider "supports or consents to commit" offenses defined in section 14 of the Act, then section 15 imposes on service providers the same punishment as it imposes on individual users who violate the CCA.[62] The CCA provides little guidance as to what constitutes "support" or "consent to commit." Free expression advocates have voiced concern over how broadly Thai officials have interpreted this provision so far: for example, in 2009, law enforcement officials charged the executive director of news website, Prachathai.com, with a violation of section 15 for allowing to remain on the site user comments that allegedly violated *lèse majesté* laws.[63]

In short, while pursuing intermediaries may seem like good policy in the short term, such approaches can adversely affect freedom of expression and access to information online and reduce the opportunities for innovation and the creation of local content. In the face of national laws that hold intermediaries liable for content created or sent by their users, intermediaries have tended to overreact, limiting even the lawful content that users post on or disseminate through their services.

59. OpenNet Initiative, "China Country Profile," 2009, available at http://opennet.net/research/profiles/china (accessed 15 November 2010).

60. Congressional Executive Commission on China, "Freedom of Expression – Laws and Regulations," available at http://www.cecc.gov/pages/virtualAcad/exp/explaws.php#vaguelaws (accessed 15 November 2010).

61. R. MacKinnon, "Studying Chinese Blog Censorship," RConversation, 29 November 2008, available at http://rconversation.blogs.com/rconversation/2008/11/studying-chines.html (accessed 15 November 2010).

62. Computer Crimes Act, section 15.

63. OpenNet Initiative, "Regional Overviews – Asia" [n.d.], available at http://opennet.net/research/regions/asia (accessed 15 November 2010).

IV. Cross-Border Issues

In the past, it was assumed that governments could control what kind of content came across their borders, and a nation's content liability laws were imposed almost entirely on content that was physically produced in or brought into that country. Even television and most radio broadcasts had geographic limitations. On the internet, where content produced in one country can be accessed globally, content creators and consumers may face great uncertainty about which country's laws apply. The U.S. and Canadian governments have declined to assert blanket jurisdiction against foreign defendants for illegal content posted on the internet abroad but accessible inside their respective countries. In the United States (where most content liability laws are enacted at the state level), jurisdictional principles tend to examine whether a content creator purposefully directed his activities towards a given state. However, other governments have extended their jurisdictional reach to impose national laws upon foreign defendants merely because content was made available on the internet.[64]

One of the earliest cases taking a broad view of internet jurisdiction arose in Australia, where the High Court held that the Dow Jones company was subject to the jurisdiction of Australian courts (and to the standards of Australian law) for allegedly defamatory material that appeared in an online version of one of its publications, despite the fact that the website was produced and hosted in the United States and was available by subscription to only a handful of subscribers in Australia.[65]

A number of countries have tried to insist that intermediaries take down content hosted abroad. In one well-known example, mentioned above, Turkish officials demanded that Google remove from its YouTube service certain videos that insulted Atatürk, under the theory that such videos harmed Turks outside Turkey. When Google agreed only to block access to the videos to users located in Turkey, the authorities responded by blocking YouTube entirely.[66]

---

64. K. Wimmer and E.R. Pogoriler, "International Jurisdiction and the Internet," Covington & Burling LLP, 2006, available at http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/InternationalJurisdiction.pdf (hereafter Wimmer and Pogoriler). See also S. Davidson, "International Considerations in Libel Jurisdiction," Forum on Public Policy, spring 2008, available at http://forumonpublicpolicy.com/archivespring08/davidson.pdf (sites accessed 15 November 2010).

65. Wimmer and Pogoriler.

66. See J. Rosen, "Google's Gatekeepers", *New York Times*, 28 November 2008, available at http://www.nytimes.com/2008/11/30/magazine/30google-t.html (accessed 15 November 2010); OSCE Turkey Report, p. 16.

Another well-known case, also discussed briefly above, arose in France, where Yahoo! was accused of selling Nazi memorabilia in violation of France's hate speech laws. Yahoo! argued that its servers were located in the United States, the auctions were transacted in the United States, and Yahoo!'s business primarily targeted U.S. residents, and thus it should not be subject to French jurisdiction. The case is often seen as an exercise of expansive jurisdiction, but in fact fits within more limited concepts of jurisdiction. For Yahoo! had established a French subsidiary, it was consciously shipping physical items into France, and it displayed advertisements in French alongside the forbidden pages.[67]

A particularly troubling practice has come to be known as "libel tourism." [68] When someone believes his reputation has been falsely besmirched, he can sue the speaker. But the speaker and offended party may reside in a country where it is difficult to prove defamation or libel, for example, because of rules placing the burden of proof on the plaintiff or other rules protecting free expression. "Libel tourism" is the practice where the plaintiff files suit in another country such as the UK, where it is relatively easy for a defamation plaintiff to prevail and where the courts are willing to exert jurisdiction over foreign defendants, as long as the material was obtainable in the UK.[69] However, in the internet age, when content created in one jurisdiction is accessible in virtually any other, libel tourism can be a "mechanism for enforcing global censorship."[70]

In response to the "danger that one country's unduly restrictive libel laws will affect freedom of expression worldwide on matters of valid public interest," the United States recently enacted a law that makes nearly all libel rulings in nations with weaker protections for speech unenforceable in the United States.[71] In another

---

67. Y. Akdeniz, "Case Analysis of *League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v. Yahoo! Inc. (USA), Yahoo France,* Tribunal de Grande Instance de Paris (County Court of Paris), Interim Court Order, 20 November 2000," Electronic Business Law Reports, 2001, available at http://www.cyber-rights.org/documents/yahoo_ya.pdf; R. Salis, "A Look at how U.S.-Based Yahoo! was Condemned by French Law," available at http://www.juriscom.net/txt/jurisfr/cti/yauctions.htm. Yahoo! sued in U.S. court to have the judgment declared unconstitutional under the First Amendment to the Constitution, but an appellate court decided on procedural grounds that the case could not be considered. *Yahoo! Inc. v. La Ligue Contre Le Racisme (LICRA)*, 433 F.3d 1199 (9th Cir. 2006), *cert. denied*, 547 U.S. 1163 (2006), available at http://caselaw.findlaw.com/us-9th-circuit/1144098.html.

68. See, e.g., Editorial, "Bringing an End to 'Libel Tourism,'" *New York Times*, 30 September 2008, p. A26, available at http://www.nytimes.com/2008/09/30/opinion/30tue3.html; A. Cohen, "'Libel Tourism' – When Freedom of Speech Takes a Holiday," *New York Times*, 15 September 2008, p. A24, available at http://www.nytimes.com/2008/09/15/opinion/15mon4.html (sites accessed 15 November 2010).

69. For example, in 2004, Rachel Ehrenfeld, the American author of the book *Funding Evil: How Terrorism is Financed – and How to Stop It*, was sued for defamation in a UK court by a man she named as a possible financier of terrorism, Khalid Salim Bin Mahfouz. Even though the book had not yet been published in the UK, the court determined it had jurisdiction to hear the case because 23 copies of the book had been purchased online in the UK and because a portion of the book was also available on the web. This was not the first, nor the last, time that UK courts claimed jurisdiction because the alleged offending material was available online. See T.W. Moore, "Untying Our Hands: The Case for Uniform Jurisdiction Over 'Libel Tourists,'" 77 Fordham L. Rev. 3243 (2009), available at law.fordham.edu/assets/LawReview/500flspub18464.pdf. See also R. Chepesiuk, "Libel tourism," Global Journalist, 1 July 2004, available at http://www.globaljournalist.org/stories/2004/07/01/libel-tourism/ (sites accessed 15 November 2010).

70. C. Walker, "Libel Tourism: The Globalization of Censorship", *International Herald Tribune*, 16 March 2009, available at http://www.freedomhouse.org/template.cfm?page=72&release=788. See also IFEX, "Capsule Report: 'Libel Tourism' a Growing Threat to Free Speech, Say ARTICLE 19 and Freedom House," 22 May 2008, available at http://www.ifex.org/united_kingdom/2008/05/22/capsule_report_libel_tourism_a/. Moreover, the effects of these adverse decisions are magnified by the UK's internet publication rule, mentioned in section 1. Though UK libel laws may be the most infamous, Brazilian law also provides remedies for questionable affronts. Committee to Protect Journalists, "U.S. Reporter Faces 'Insult' Suit in Brazil Air Crash Aftermath," 29 September 2009, available at http://cpj.org/2009/09/us-reporter-faces-insult-suit-in-brazil-air-crash.php (sites accessed 15 November 2010).

71. SPEECH Act, 28 U.S.C. §§ 4101-4105, available at http://www.govtrack.us/congress/bill.xpd?bill=h111-2765 (accessed 15 November 2010).

positive development, the incoming UK government pledged in May 2010 to review the country's famously plaintiff-friendly libel laws.[72]

72. HM Government, "The Coalition: Our Programme for Government," p. 11 (May 2010) (laying out policy priorities of newly formed UK coalition government), available at http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_187876.pdf. See also D. Greek, "Changes to UK Libel Laws Proposed," ComputerActive, 24 June 2010, available at http://www.computeractive.co.uk/computeractive/news/2264200/bill-proposes-changes-uk-libel (sites accessed 15 November 2010).

V. Policy Reforms

The internet has become a vibrant platform for journalism, UGC, and all other manner of expression. However, the original policy framework that enabled the internet as we know it is threatening to fray. Media and free expression advocates have a role to play in promoting policy reforms in key areas:

- **Promote protections for internet intermediaries**. Advocate for laws that protect internet intermediaries from liability for UGC. Intermediaries are key enablers of expression online because they provide the conduits and platforms for a robust variety of content. Laws that impose liability on intermediaries for the third-party content they host or transmit will force intermediaries to scrutinize and limit the use of their services by all users.
- **Advocate for a country-of-origin principle for expression**. Many EU Directives (for example, the E-Commerce Directive and the AVMS) include a provision that service providers are only subject to the laws of their home country, even when doing business in another EU Member State.[73] The purpose is to facilitate the EU single market by simplifying the rules for cross-border business, requiring compliance with one national law instead of many. Extending this principle more broadly to content liability would permit authors and publishers to place their content online without fear of unexpectedly violating an obscure regulation in a distant land solely through a presence on the internet.
- **Oppose extension of broadcast regulation to the internet**. The internet's unique technical attributes support the argument that digital content is entitled to stronger free expression protections than traditional media. Individuals control what they see and access online, and the internet enables users to publish and disseminate content at little to no cost. Factors that justified the restrictive regulation of broadcasting, including concerns about scarcity, cost, or intrusive unwanted content, do not apply to the internet; it follows that those traditional broadcast regulations should not be extended to the internet. (Regulation that protects quality programming by public service broadcasters is another matter.)

73. Frequently Asked Questions on the proposed Directive on Services in the internal market, "6.3 What Does the Country of Origin Principle Mean?," available at http://ec.europa.eu/internal_market/services/services-dir/faq/200410-faq-point06_en.htm (accessed 15 November 2010). This rule is subject to various limitations including, in the case of the cited Directive, that if a service provider has a physical establishment in another EU Member State, it is also subject to that Member State's laws.

The MDM Reference Series papers published so far, and available on **www.mediapolicy.org** and **www.soros.org**, are:

1. *Online Media and Defamation*—Toby Mendel
2. *Digital Media and Investigative Reporting*—Mark Lee Hunter
3. *Mobile TV: Challenges and Opportunities Beyond 2011*—Ronan de Renesse
4. *Citizen Journalism and the Internet*—Nadine Jurrat
5. *Digitization and Media Business Models*—Robert Picard
6. *Freedom of Expression Rights in the Digital Age*—Andrew Puddephatt
7. *Net Neutrality and the Media*—Stefaan Verhulst
8. *Gatekeeping in the Digital Age*—Peter Looms
9. *Technical Standards in Terrestrial Television*—David Wood
10. *The Digital Dividend*—Gérard Pogorel
11. *How television went digital in the Netherlands*—Nico van Eijk and Bart van der Sloot

Mapping Digital Media is a project of the **Open Society Media Program** and the **Open Society Information Program.**

Open Society Media Program

The Media Program works globally to support independent and professional media as crucial players for informing citizens and allowing for their democratic participation in debate. The program provides operational and developmental support to independent media outlets and networks around the world, proposes engaging media policies, and engages in efforts towards improving media laws and creating an enabling legal environment for good, brave and enterprising journalism to flourish. In order to promote transparency and accountability, and tackle issues of organized crime and corruption the Program also fosters quality investigative journalism.

Open Society Information Program

The Open Society Information Program works to increase public access to knowledge, facilitate civil society communication, and protect civil liberties and the freedom to communicate in the digital environment. The Program pays particular attention to the information needs of disadvantaged groups and people in less developed parts of the world. The Program also uses new tools and techniques to empower civil society groups in their various international, national, and local efforts to promote open society.

Open Society Foundations

The Open Society Foundations work to build vibrant and tolerant democracies whose governments are accountable to their citizens. Working with local communities in more than 70 countries, the Open Society Foundations support justice and human rights, freedom of expression, and access to public health and education.

For more information:

Open Society Media Program
Open Society Foundation

4th Floor Cambridge House, 100 Cambridge Grove
London, W6 0LE, United Kingdom

mappingdigitalmedia@osf-eu.org
www.mappingdigitalmedia.org
www.soros.org/initiatives/media

Cover Design: Ahlgrim Design Group
Design and Layout: Judit Kovács | Createch Ltd.

OPEN SOCIETY FOUNDATIONS