

# Developing Internet Policy in Latin America: A Global Perspective

by Cynthia Wong, James X. Dempsey and Ellery Roberts Biddle<sup>1</sup>

## 1. Introduction

The chapters of this book describe some of the pressing Internet policy issues that nations all over the world are facing today.

As the authors in this volume recognize, the uniquely open and decentralized nature of the Internet can empower individuals to seek, receive and impart information and ideas on an unprecedented scale. The Internet can be a powerful platform for innovation, access to knowledge, civic participation, and economic growth.

However, the Internet's openness and freedom are not guaranteed by the technology itself. The Internet has developed so rapidly because of very specific choices made by policymakers and the technology industry who created a framework based on the principles of open access, competition, innovation, and human rights.

Now, however, that policy framework is being challenged. Governments in Latin America, as elsewhere in the world, want to find ways to prevent crime, terrorism, and breaches of cybersecurity; at the same time, they seek to protect children, safeguard reputation and privacy, and enforce intellectual property rights online. As they address these challenges, policymakers throughout Latin America are grappling with fundamental questions: What kind of Internet do they want for their country? How can the government protect human rights while addressing legitimate policy concerns? And what role should Internet intermediaries—ISPs, search engines, and other online service providers—play in achieving policy aims?

In this chapter, we aim to contextualize Latin American Internet policy within the global debate about Internet freedom and regulation in the twenty-first century.

## 2. Building the Internet Policy Framework on the Foundation of Human Rights

The Internet has certain fundamental attributes that distinguish it from communications technologies of the past: To an unprecedented extent, it is global, abundant, and (relatively) inexpensive. The Internet accommodates an unlimited number of speakers and its barriers to entry are relatively low. The network does not need editors or gatekeepers at its center in order to function. Instead, the Internet's design places power in the hands of users at the edges of the network. Every user can be a publisher, while at the same time every user can control the content he or she accesses.<sup>2</sup>

---

<sup>1</sup> The Center for Democracy & Technology is a non-profit organization based in Washington, D.C. that is dedicated to keeping the Internet open, innovative, and free. We thank Eduardo Bertoni for the opportunity to contribute to this volume.

<sup>2</sup> James X. Dempsey, "The Internet at Risk: The Need for Higher Education Advocacy," *EDUCAUSE Review*, vol. 42, no. 6 (2007) <http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume42/TheInternetatRiskTheNeedforHig/162066>.

The goal of preserving these attributes should guide Internet policymaking. Moreover, these essential Internet attributes – openness, user control, accessibility – are directly linked to human rights principles. The right of free expression not only serves democratic interests; it also promotes innovation. The right to privacy is not only fundamental to autonomy and personal development; it is also necessary for e-commerce to flourish. Both at the national and international levels, an approach to Internet policy that is based on human rights principles will generate the legal and regulatory framework that will maximize the potential of the Internet.

Thus, policymakers should look to international and regional human rights instruments—namely the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the American Convention on Human Rights—as a guide in this process. The Inter-American Court and other regional and international human rights institutions may be important sources of Internet policy, along with national processes.

Article 19 of the Universal Declaration states that everyone has the right “to seek, receive and impart information and ideas through any media and regardless of frontiers.” In similar terms, Article 13 of the American Convention protects the right “to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.”

These words seem to have special relevance to the Internet. The concept of a right to “impart” information and ideas takes on new meaning in the era of “Web 2.0,” where online entities ranging from social networking sites to blogging platforms support user-generated content free-of-charge and allow anyone with access to an Internet-connected computer to disseminate ideas, opinions, and cultural expression. Similarly, the rights to “seek” and “receive” information seem to anticipate search engines, Twitter feeds, and other Internet services. And when Internet censorship in one country may infringe on the right of persons in other countries to “impart” or “receive” information “regardless of frontiers,” the traditional deference given to local laws and norms may need to be reconsidered. Moreover, the American Convention has provisions that go beyond the Universal Declaration, prohibiting restrictions on the right of expression “by indirect methods or means, such as the abuse of ... private controls over ... equipment used in the dissemination of information.”

Yet international human rights instruments also recognize that the right to freedom of expression can be restricted in order to serve other legitimate interests, including respect for the rights or reputation of others. The chapters in this book explore the tensions between freedom of expression and other rights and interests.

The unique attributes of the Internet are relevant in reconciling these tensions and developing balanced solutions to the problems faced online. Human rights institutions have made it clear that, in assessing any government policy affecting free expression, it is important to consider the medium. Regulation that would be appropriate for broadcast TV, where the spectrum is limited, may not be appropriate for cable, and less so for the Internet. Some courts have held that the ability of Internet users to circumvent certain restrictions makes it harder to justify those restrictions. Similarly, the availability of user-controlled filtering tools for parents and schools means that ISP filtering mandated by the government is less necessary to protect children from harmful material online, and therefore less justified as a policy.

In a similar vein, given the essentially unlimited capacity of the Internet to accommodate contrasting views, there may be less need for government intervention to ensure fairness or

balance or to protect reputation. Mistakes can be corrected and the right of reply can be effectuated instantaneously.

As the chapters in this book show, by understanding the Internet's unique characteristics and grounding our efforts in human rights principles, we can address the difficult questions regarding policy for the digital age.

### **3. Chapter comments**

#### **3.1. Intermediary liability**

Every day, millions of journalists, educators, students, business people, scientists, government officials, politicians, and ordinary citizens go online to speak, access information, and participate in countless aspects of public and private life. All of this expressive, social, political, and economic activity is made possible because Internet service providers (ISPs), telecommunications carriers, websites, online services, and a range of other technological intermediaries serve as conduits and platforms for expression and communication. Over the past decade, these services have innovated extensively and expanded rapidly. They have grown to support new uses, including the remarkable development of platforms that support user-generated content. Many of these services are free of charge to users, greatly expanding opportunities for speech and enterprise.

Early in the history of the Internet, a key question arose: Should these intermediaries be held liable for harmful or illegal content created or posted by their users? In looking at various national and regional approaches, we can observe a general trend: Those governments that have sought to maximize growth of the Internet and online services have tended to limit civil and criminal liability for Internet intermediaries. In contrast, governments in the most Internet-restrictive countries often hold intermediaries responsible for illegal content posted by users, or impose other duties on intermediaries to police user expression. This practice forces intermediaries to become content gatekeepers. Imposition of liability on intermediaries not only reduces the space for free expression, it also hinders innovation and limits expansion of Internet access.<sup>3</sup>

As Claudio Ruiz and Juan Lara explain, many of the Latin American countries surveyed in their chapter do not have clear legislative frameworks for the responsibility of intermediaries for unlawful content created or disseminated by users, especially outside of copyright infringement. Court cases have produced a muddled jurisprudence, providing little guidance to companies that might want to offer services in Latin America and giving citizens little indication of how their acts of expression (and personal privacy) will be protected online. The principles outlined by Ruiz and Lara offer a roadmap for the development of policy on this subject in Latin America.

Laws addressing intermediary liability in the U.S. and the EU are worth highlighting. Two separate laws embody U.S. policy on intermediary liability: Section 230 of the Communications Act and Section 512 of the Copyright Act.<sup>4</sup> Section 230 states that Internet intermediaries

---

<sup>3</sup> CDT, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation" (April 2010) [http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability\\_%282010%29.pdf](http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf).

<sup>4</sup> 47 U.S.C. § 230, <http://www.law.cornell.edu/uscode/47/230.html>; 17 U.S.C. 512, <http://www.law.cornell.edu/uscode/17/512.html>.

cannot be held liable for content created, transmitted, or uploaded by their users. The protection against liability applies without condition to a variety of claims (except for copyright and federal criminal law).

With respect to copyright, Section 512 provides protection to certain service providers if they take down copyrighted content in response to private notices from the copyright holders. This approach is often called a “notice and takedown safe harbor.”

The European Union also provides significant protections against liability under its E-Commerce Directive.<sup>5</sup> The EU rules distinguish between conduits (such as ISPs), caching services, and intermediaries that host third party content. Host intermediaries must comply with a notice and takedown system to qualify for liability protection. This notice and takedown system applies not just to claims of copyright infringement but to all types of content.

In our view, these legal protections have been as important to freedom of expression online as constitutional and human rights protections. These protections have enabled the dramatic growth of social networking services and other interactive sites for user-generated content. Without these legal protections, the cost of developing new Internet services and applications would be much higher, potentially limiting innovation and opportunities for individual expression.

To promote innovation and growth in domestic Internet industries and to protect fundamental rights, Latin American governments should seek to enact laws protecting intermediaries against liability for the unlawful behavior of users. If duties are imposed on intermediaries to qualify for legal protection, these duties must be clearly defined and must take into account the technical role and function of the specific type of intermediary.

Ruiz and Lara show how “notice-and-takedown” requirements can be vulnerable to abuse, especially if the takedown obligation can be triggered by the mere issuance of a notice, without a judicial determination of the illegality of the content. This would allow a government official, a corporation, or an individual to silence the expression of others simply by issuing a takedown notice. Chilean copyright law requires that notice<sup>6</sup> of infringing content be in the form of a judicial order; this is an important protection against abuse, as it places the work of deciding whether particular content infringes a copyright properly in the judiciary’s hand, rather than obligating intermediaries to make determinations that they are not equipped to make.

Of course, as discussed in the section on Argentina, the effectiveness of this approach in preserving free expression depends on the quality of the judicial process that produces the takedown orders. The process must include delivery of notice to the user who uploaded the content, adequate judicial consideration of the rightsholder’s copyright claim, and an opportunity to appeal the decision. Under U.S. copyright law, host intermediaries seeking the safe harbor will take down content in response to a notice issued by the copyright holder. Yet the law provides that the person who posted the contested content has the power to claim that the infringement notice was erroneous, in which case the intermediary can put the challenged

---

<sup>5</sup> E-Commerce Directive, 2000/31/EC, [http://ec.europa.eu/internal\\_market/e-commerce/index\\_en.htm](http://ec.europa.eu/internal_market/e-commerce/index_en.htm). See also OpenNet Initiative, Europe - Regional Overview (2009), <http://opennet.net/research/regions/europe>.

<sup>6</sup> Under the statute, notice means how the platform acquires “effective knowledge,” which triggers obligations to take down content.

content back up without risking liability.<sup>7</sup> Individual EU member states may also provide similar protections in their national law.

On the other hand, the process also must be streamlined to keep up with the speed and volume of infringement online. As in other contexts, viewing intermediary responsibility measures through a human rights lens may help in crafting coherent policies that protect fundamental rights and promote ICT growth. As Ruiz and Lara point out, any law detailing intermediary responsibility must be evaluated against standards of necessity (including the measure's effectiveness) and proportionality, as well as for its impact on free expression and innovation.

Certain kinds of unlawful expression or activity may not be suitable for the notice and takedown approach, especially where notices are issued without judicial review. For example, intermediaries are not well-suited to determine whether a piece of content is defamatory. Imagine a case where a blogger accuses a public official of embezzling money from the town treasury. If the allegation is true, then the blogger is serving an important public function by drawing attention to local corruption. If the allegation is false, the statement may be defamatory. However, upon receiving a takedown request, the company that hosts the blog online has no way of assessing the veracity of the statement. The process of determining whether a statement is defamatory is very difficult because defamation cases by nature require careful factual discovery and analysis. Intermediaries are not at all equipped to make these kinds of adjudications and should not be enlisted to take down content without court oversight.

We raise a note of caution with respect to one suggestion by Ruiz and Lara. They recommend that ISPs maintain records on their users so that a user can be contacted in the event of an illegal infraction. Anonymous online activity raises a lot of controversy, but anonymous speech is an important component of free expression, especially with regards to matters of public concern where persons might hesitate to speak out if they fear being identified.

In the U.S., the Supreme Court has upheld the right to anonymous speech.<sup>8</sup> International human rights mechanisms have also urged that national laws preserve the opportunity for anonymous speech.<sup>9</sup> At public Internet centers and in places where WiFi access is available, a requirement for access providers to identify each user could discourage some customers from using the Internet. Moreover, the work of collecting names of all users would be costly and could raise the cost of offering public access. This obligation could prompt these entities to stop offering service, thereby diminishing access.

As Ruiz and Lara note, requiring service providers to collect and retain data about their users' online activity merits further discussion. At CDT, we believe that data retention mandates of this nature are often disproportionate because such mandates intrude on the privacy of all users to

---

<sup>7</sup> The infringement notice could be erroneous because, for example, the use of the content was "fair use," a doctrine under U.S. law that allows for some limited uses of a copyrighted work without permission of the copyright owner.

<sup>8</sup> *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995) (noting that "Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.")

<sup>9</sup> Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and the OAS Special Rapporteur on Freedom of Expression, Dec. 21, 2005, [http://www.osce.org/documents/rfm/2005/10/26809\\_en.pdf](http://www.osce.org/documents/rfm/2005/10/26809_en.pdf).

address the illegal activity of only a few users. As we note below, an alternative is to require “data preservation,” which targets specific users that are the subject of a lawsuit or law enforcement investigation.

U.S. law offers Internet intermediaries another important protection. Under Section 230, intermediaries are not only protected from liability when they host user content, they are also immune from liability when they remove user content or disable user activity that they consider inappropriate. This protection supports, for example, the anti-spam and cybersecurity efforts of ISPs, allowing them to block traffic that they believe is spam or contains harmful code, so long as they act in good faith. It also supports the ability of social media services to remove material that is sexually explicit, violent, or harmful and to write and enforce their own terms of service. This freedom to remove content or ban users is not one that service providers should take lightly, though, and service providers must be transparent and consistent in their practices.<sup>10</sup> In addition, service providers must resist government pressure to turn voluntary standards into a mandate.

### **3.2. Privacy and data protection**

Data protection is one of the key components of the framework supporting e-commerce and Internet development, as it allows users to trust that their personal data will be protected when they make online transactions. In his chapter, Lorenzo Villegas draws some of the critical distinctions necessary to understanding this topic, and he identifies some of the current tensions around the right to privacy.

The right to privacy has three major aspects: First, there is the right of privacy, or data protection, as it concerns the relationship between a corporation and its customers. In the U.S., we call this consumer privacy. Second, there is the right of privacy that the citizen has with respect to the government in its administrative and social welfare capacities. This branch of privacy concerns data the government collects about its citizens in the course of providing education, health services or other social programs, in the course of administering its tax system, and in carrying out other civil functions. The third major branch of privacy concerns the right to be protected against coercive data collection by the government in the course of criminal or national security investigations.

As to the first branch of privacy, the principles for data protection in the consumer context received early articulation in 1980 when the Organisation for Economic Cooperation and Development (OECD) issued a set of Privacy Guidelines that contained definitions, eight Privacy Principles, and enforcement approaches.<sup>11</sup> The eight OECD principles are often called the Fair Information Practice Principles (FIPPs or FIPs). The OECD Guidelines and the FIPs have had enormous global influence and have been adapted in a variety of legislative and self-regulatory measures.

---

<sup>10</sup> Erica Newland, Caroline Nolan, Cynthia Wong and Jillian York, “Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users” (September 2011) [http://www.cdt.org/files/pdfs/Report\\_on\\_Account\\_Deactivation\\_and\\_Content\\_Removal.pdf](http://www.cdt.org/files/pdfs/Report_on_Account_Deactivation_and_Content_Removal.pdf).

<sup>11</sup> “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” [http://www.oecd.org/document/20/0,2340,en\\_2649\\_34255\\_15589524\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html).

In 1995, the European Union adopted its Data Protection Directive, based on the OECD FIPs, that established a detailed privacy regulatory structure for adoption into national law by EU member states.<sup>12</sup> As Villegas notes, the EU directive has had an influence in Latin America, particularly in Argentina. The United States has not comprehensively adopted the FIPs, but the U.S. has a series of sector-specific data protection laws – one for financial information, one for medical records, one for telecommunications data, and so on – which incorporate the FIPs to varying degrees while leaving significant areas without express regulation. Nevertheless, the U.S. Federal Trade Commission has recognized the FIPs as the best available framework for consumer privacy,<sup>13</sup> and the Obama Administration has called for adoption of comprehensive federal privacy legislation.<sup>14</sup>

Also relevant to Latin America is the privacy framework adopted in November 2004 by the twenty-one member economies of the Asia-Pacific Economic Cooperation forum (APEC).<sup>15</sup> Recently, APEC has addressed the issue that Villegas identifies as one of the most difficult: the application of inconsistent national laws to data moving across borders. In September 2011, the Electronic Commerce Steering Group of APEC formally approved the Cross Border Privacy Rules (CBPR) initiative as an effort to facilitate data flows while ensuring meaningful privacy protection within the region. The CBPR system seeks to balance the competing values of privacy, commerce, and national sovereignty.<sup>16</sup>

The rules for the second branch of privacy, concerning the relationship between the citizen and the government in its administrative capacity, are also based on the Fair Information Practices. The EU Data Protection Directive covers both commercial entities and governmental entities (although it exempts governmental operations concerning public security, defense, State security and criminal justice). With regard to this branch of privacy, the United States was actually ahead of Europe. The U.S. Congress adopted the Privacy Act in 1974, applying many of the FIPs to governmental records collected and maintained by the federal government in its administrative capacity. (The US Privacy Act does not completely exclude law enforcement and national security records, but those records are exempt from many of the Act's provisions.)

Finally, the third branch of privacy concerns the power of the government to forcefully interfere with private life, including in the home, and the confidentiality of communications. In the U.S., this aspect of privacy is governed by the federal Constitution, where the Fourth Amendment protects the people against “unreasonable searches and seizures.”

---

<sup>12</sup> Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML>.

<sup>13</sup> Federal Trade Commission (Bureau of Consumer Protection), A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, (Dec. 1, 2010) available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

<sup>14</sup> U. S. Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 2010), [http://www.ntia.doc.gov/reports/2010/IPTF\\_Privacy\\_GreenPaper\\_12162010.pdf](http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf).

<sup>15</sup> The APEC Framework (2005) [http://publications.apec.org/publication-detail.php?pub\\_id=390](http://publications.apec.org/publication-detail.php?pub_id=390).

<sup>16</sup> Justin Brookman, “Can Cross-Border Privacy Rules Trump Divergent Data Protection Laws” (October 4, 2011) <http://www.cdt.org/blogs/justin-brookman/410can-%E2%80%9Ccross-border-privacy-rules%E2%80%9D-trump-divergent-data-protection-laws>.

For Latin America, all three branches of privacy have their foundations in Article 11 of the American Convention and in most national constitutions, including in the traditional right of habeas data. However, it is probably fair to say that no country in the Americas (the U.S. included) has a legal framework that comprehensively protects the right of privacy in all three of its branches. And to complicate the situation, as Villegas explains, the Internet introduces new concerns. It also heightens tensions between rights. Special care must be taken to ensure that the right of privacy is not used to undermine other democratic principles.

For example, the Internet offers huge potential to increase governmental transparency and accountability, by making government information available online. At the same time, however, to the extent that government information pertains to individuals, caution must be exercised. Consider, for example, court records. In the pre-digital age, much data was technically public, in the form of legal pleadings and other documents introduced in the course of judicial proceedings. However, this data, while “public,” was hard to access. Now, as courts move their records online, that data may be readily searchable. The U.S. Supreme Court has noted that there is a “vast difference between the public records that might be found after diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.”<sup>17</sup> Government agencies should not use privacy as an excuse for avoiding transparency, but they must be careful in putting court records online, making sure that sensitive financial or medical information is protected.<sup>18</sup>

Villegas raises what is perhaps the most fundamental question regarding privacy: What data should be protected? In the U.S. and Europe, this question is often posed in terms of what is “personally identifiable information” (PII). In the U.S., for example, many argue that Internet Protocol addresses (“IP addresses”) are not PII, while in Europe the Article 29 Working Party has held that IP addresses are PII.<sup>19</sup> It is important to recognize that changes in technology are making the distinction between PII and non-PII less pertinent, because it is increasingly possible to re-identify data that is supposedly anonymous.<sup>20</sup> The U.S. Federal Trade Commission has warned companies that they should not rely on outdated notions of what is and what is not PII. The Commission has suggested that it may extend its authority to data previously deemed to be non-PII.<sup>21</sup>

---

<sup>17</sup> Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989) <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=489&invol=749>.

<sup>18</sup> CDT, “A Quiet Revolution in the Courts: Electronic Access to State Court Records, A CDT Survey of State Activity and Comments on Privacy, Cost, Equity and Accountability” (August 2002) <http://cdt.org/publications/020821courtrecords.shtml>.

<sup>19</sup> “Opinion 4/2007 on the concept of personal data,” [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf).

<sup>20</sup> CDT, “Encouraging the Use of, and Rethinking Protections for De-Identified (and “Anonymized”) Health Data” (June 2009) [http://cdt.org/healthprivacy/20090625\\_deidentify.pdf](http://cdt.org/healthprivacy/20090625_deidentify.pdf).

<sup>21</sup> Federal Trade Commission (Bureau of Consumer Protection), A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, (Dec. 1, 2010) available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>

The question of intermediary liability also presents itself in the context of privacy. The tendency to hold Internet intermediaries (such as search engines and hosts) liable for privacy intrusions instigated by others is a dangerous trend that threatens the openness of the Internet.<sup>22</sup>

Villegas examines the recent controversy over “data retention,” which we mention in brief above. As we know, the providers of telecommunications and Internet services collect and store a wealth of data about their customers. In recent years, however, some governments have been dissatisfied with the amount of information that service providers collect and retain in the ordinary course of business. These governments have imposed or considered imposing legal mandates requiring service providers to retain certain data about all their users for specified periods of time, even when that data no longer is needed for a business purpose. Generally, under these mandates, the data must be collected and stored in a manner such that it is linked to users’ names or other identification information. Government officials may then request access to this data, pursuant to the laws of their respective countries, for criminal investigations and often for national security investigations as well. The laws that require ICT companies to store data about their users are typically referred to as data retention laws.<sup>23</sup>

Data retention, by creating records that link highly detailed descriptions of users’ Internet activity to identifying information, violates not only the right to privacy but also the right to freedom of expression, and the right to be presumed innocent. The cost of complying with data retention mandates imposes huge costs on companies and poses significant risks to privacy and security. Data compiled in pursuit of legitimate goals can be abused by the government. It is also vulnerable to identity theft.

The Council of Europe’s Convention on Cybercrime<sup>24</sup> takes a different approach. Countries signing the COE Convention must adopt laws authorizing government officials to demand that a communications service provider *begin, upon receipt of a specific request*, to store – “preserve” – data about a specific user or device relevant to a specific criminal investigation or proceeding. Typically, the service provider is required to continue preserving this data for up to a maximum period of time, such as 90 days, while the government agents obtain the necessary authorization to compel its disclosure. This process is known as *data preservation* and offers an alternative means of satisfying many of the government’s needs that is preferable to data retention.

### 3.3. Filtering

In their article, Varon, Affonso, Magrani, and Britto do well to illustrate how Internet filtering can have a significant impact on freedom of expression. Any Internet filtering proposal should be assessed under the human rights criteria of necessity, effectiveness, proportionality and less restrictive alternatives. An assessment of filtering should consider four key questions: (1)

---

<sup>22</sup> CDT, “Intermediary Liability: Protecting Internet Platforms for Expression and Innovation” (April 2010) [http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability\\_%282010%29.pdf](http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf).

<sup>23</sup> CDT, “Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development” (October 2011) [http://cdt.org/files/pdfs/CDT\\_Data\\_Retention\\_Paper.pdf](http://cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf).

<sup>24</sup> Council of Europe: Convention on Cybercrime, Apr. 16, 2011, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

Where in the network is filtering occurring? (2) What kind of content is being filtered? (3) Is the filtering voluntary or is it being conducted under government mandate? (4) What is the broader context for access and user choice?

In addition, in assessing filtering proposals, policymakers and advocates must pay careful attention to the particular means of filtering and the risks of mistakes and overbreadth. Too often in debates over Internet content, Internet filtering proponents focus only on the societal interest that they believe would be served by filtering. They assume that the proposed filtering will work perfectly and that only illegal content will be affected, ignoring the risk of collateral damage that filtering mechanisms can impose on lawful content.<sup>25</sup> As the authors suggest, the goals of filtering may be legitimate, but it is critical that policymakers fully consider the unintended side effects.

As Varon and her colleagues explain, filtering can occur at all of the network, from online applications, to the domain name system, to the routers of the ISPs, to the desktop of the end user.<sup>26</sup> Identifying the point in the network at which filtering takes place is key to measuring its proportionality and impact. While filtering by ISPs can be very troubling, filtering by the operators of social networking sites and platforms for user-generated content poses very different considerations. Websites are free to craft and enforce terms of service and community guidelines that govern what they will and will not allow. Consider, for example, a social networking site such as Facebook or Orkut. These sites set terms of use that prohibit certain kinds of content and they voluntarily police their networks to remove this content. Likewise, a site such as YouTube sets rules for the type of content it will host.<sup>27</sup>

Transparency and due process are critically important when online service providers limit what their users can post. While the operators of sites are free to accept or not accept certain types of content on their sites, users should be informed how such decisions will be made and given the opportunity to contest the host's decisions.<sup>28</sup> In the case of automated filtering, service

---

<sup>25</sup> There is extensive evidence that filters are overbroad. *Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 651 (E.D. Pa. 2004) (noting the overbreadth of IP address- and domain name-based ISP filtering); Thomas Claburn, "ICE Confirms Inadvertent Web Site Seizures," *Information Week* (February 18, 2011), [http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=229218959&cid=RSSfeed\\_IWK\\_All](http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=229218959&cid=RSSfeed_IWK_All) (describing unintended blocking of over 84,000 web hosts in a law-enforcement action); Marina Kameny, "First, China. Next: the Great Firewall of... Australia?" *Time* (June 16, 2010), [http://www.time.com/time/world/article/0,8599,1995615,00.html?xid=rss-world&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+time/world+%28TIME:+Top+World+Stories%29](http://www.time.com/time/world/article/0,8599,1995615,00.html?xid=rss-world&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+time/world+%28TIME:+Top+World+Stories%29) (citing the fact that a dentist's website and that of a pet-care facility ended up on an Australian blacklist proposed to form the basis of a mandatory ISP filtering system).

<sup>26</sup> For more information about the technical aspects of Internet filtering, see Jonathan Zittrain and John Palfrey, "Internet Filtering: The Politics and Mechanisms of Control," Chapter 3 in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press) 2008, <http://opennet.net/accessdenied>.

<sup>27</sup> YouTube's "Community Guidelines" prohibit a wide range of content, including pornography, videos showing animal abuse, drug abuse, under-age drinking and smoking, or bomb making, hate speech, and harassment or intimidation. [http://www.youtube.com/t/community\\_guidelines](http://www.youtube.com/t/community_guidelines). In addition, YouTube has implemented its "Content ID" filtering system to prevent the uploading of copyright-infringing videos. <http://www.youtube.com/t/contentid>.

<sup>28</sup> CDT, "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users" (September 21 2011), [http://cdt.org/files/pdfs/Report\\_on\\_Account\\_Deactivation\\_and\\_Content\\_Removal.pdf](http://cdt.org/files/pdfs/Report_on_Account_Deactivation_and_Content_Removal.pdf).

providers should be sensitive to the risk of overbreadth and take steps to safeguard against it, perhaps even erring on the side of letting some borderline content through.<sup>29</sup> So long as these practices are truly voluntary on the part of the online service providers and are transparent and are fairly and consistently applied, and so long as there are alternative avenues for individuals to disseminate their content, these voluntary forms of filtering or control are probably not objectionable. Any burden that such editorial decisions place on free expression can be mitigated (in many cases) by the availability of other competing platforms and websites that have different policies.

ISPs are in a much different position. They are the one service provider through which all content must flow; if an ISP were to block particular content, subscribers would be prevented from accessing that content at *any* online source. Moreover, in many countries, users have a limited choice of ISPs, so filtering at the ISP level may leave users with no alternative path to access blocked information. In addition, when faced with filtering mandates, ISPs may have to resort to technical means that are grossly overbroad – or excessively intrusive. As the authors point out with respect to the overturned Brazilian order to block YouTube in response to a claim regarding one video, filtering by ISPs can affect much more expression than is intended.<sup>30</sup> The level of inspection of traffic required for ISPs to block particular sites or content would involve substantial privacy intrusion and might also degrade network performance. These risks do not apply, however, when ISPs offer truly user-controlled filtering options, such as end-user parental control software, that allow individual subscribers to limit what content they can access.

The unique position of ISPs is a principal reason why the U.S. Internet neutrality rules to which the authors refer apply only to ISPs, and not to social networks, search engines, or hosts for user-generated content such as YouTube. Because of the unique position of ISPs, it is appropriate to impose on them rules that prevent arbitrary or anticompetitive behavior with respect to content.

In recent years, there have been efforts to impose filtering mandates through the domain name system. Using the DNS to control content poses an especially high risk of suppressing lawful expression and can also exacerbate cybersecurity risks. In addition, using the DNS to take action against foreign sites will generate cross-jurisdictional disputes in which each country tries to use the domain name system to assert domestic jurisdiction over foreign websites.<sup>31</sup>

It is also important to consider the nature of the content being filtered. Filtering to protect network security or to protect users from unwanted security threats may raise fewer free-expression concerns than filtering to address third-party interests or broader social policy issues. For example, it is generally considered permissible for ISPs to filter spam, phishing emails and other malware. Nonetheless, the filtering standards must be transparent and consistently applied, and ISPs must have a mechanism of due process for those whose communications are

---

<sup>29</sup> Such a safeguard could be, in the context of filters for copyrighted content, a policy to allow short segments of recognized works – clips likely to fall within limitations and exception to copyright – to pass through the filter.

<sup>30</sup> *Center for Democracy & Technology v. Pappert*.

<sup>31</sup> CDT, “The Perils of Using the Domain name System to Address Unlawful Internet Content” (September 2011) <http://www.cdt.org/files/pdfs/Perils-DNS-blocking.pdf>.

blocked. If they adhere to these principles, ISPs should have the ability to protect their services and their users from spam, fraud and attempts to disrupt service.

As a technical matter, it is also important to consider the extent to which the targeted content is identifiable by a filter. A filter can be designed to recognize a specific piece of copyrighted content, such as a song or movie. As the authors point out, technology cannot weigh all factors relevant to legality, but it can at least recognize the nature of the content. A site like YouTube has the ability to screen content as it is being uploaded for anything that matches a known copyrighted file.<sup>32</sup> However, in the case of defamatory content, this approach is not technologically possible, since an infinite range of unpredictable content could be defamatory.

A third dimension to consider is whether the filtering is voluntary or mandated by government. A legal obligation to filter is very problematic for freedom of expression, whether applied to ISPs or online application providers. As noted by Varon and her colleagues, service providers that face a penalty for failing to filter will likely err on the side of caution, which would result in overbroad blocking. Imposing mandatory filtering obligations on intermediaries, even with regard to highly specific content, may impose such risks and costs that those intermediaries decide not to offer service at all or curtail their free services, thus diminishing the venues available for expression and even reducing access to lawful content.<sup>33</sup>

The Council of Europe has warned that, if filtering is to be applied to the Internet, it must be done carefully and in accordance with Article 10, the free expression provision of the European Convention on Human Rights, which is similar to Article 13 in the American Convention. The COE urges that governmental blocking or filtering only occur where the conditions of Article 10(2) are met: filtering must concern “specific and clearly identifiable content, a competent national authority [must make] a decision [based] on its illegality and the decision [must be open for review] by an independent and impartial tribunal or regulatory body.”<sup>34</sup> In addition, national law should include protections against abuse of filters and overblocking, and provisions for redress. Even with regard to children’s exposure to “harmful content,” the Council recognizes that “every action to restrict access to content is potentially in conflict with the right to freedom of expression and information” and thus cautions that any system should be developed in full compliance with those principles.<sup>35</sup>

Several of the Special Rapporteurs have also issued a joint statement condemning

---

<sup>32</sup> See <http://www.youtube.com/t/contentid>. See also Elinor Mills, “Google unveils YouTube antipiracy tool” (October 15, 2007) [http://news.cnet.com/8301-10784\\_3-9797622-7.html](http://news.cnet.com/8301-10784_3-9797622-7.html).

<sup>33</sup> CDT, “Intermediary Liability: Protecting Internet Platforms for Expression and Innovation” (April 2010), [http://cdt.org/files/pdfs/CDT-Intermediary%20Liability\\_\(2010\).pdf](http://cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf).

<sup>34</sup> Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters (Adopted Mar. 26, 2008), [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2008\)6](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6).

<sup>35</sup> Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment (Adopted July 8, 2009), <https://wcd.coe.int/ViewDoc.jsp?id=1470045&Site=CM>. The Council concluded that “it is not possible to eliminate entirely the danger of children being exposed to content or behaviour carrying a risk of harm, and that consequently media (information) literacy for children, parents and educators remains a key element in providing coherent protection for children against such risks.”

governmentally mandated filtering: “Filtering systems which are not end-user controlled – whether imposed by a government or commercial service provider – are a form of prior censorship and cannot be justified.”<sup>36</sup>

Finally, filtering must be examined in light of the broader context for access and user choice. Varon and her colleagues describe the lack of a competitive market for ISPs in many countries in Latin America (which is also true in the United States). If there is no competition, even voluntary filtering may be too restrictive of the rights of free expression and access to information. In this context, even voluntary filtering may violate the provision of the American Convention prohibiting restrictions on the right to free expression by indirect and private means.

### **3.4. Defamation and jurisdiction**

Human rights principles do not prohibit defamation laws. To the contrary, many international human rights instruments, including the American Convention, recognize and protect the right to reputation.<sup>37</sup> However, defamation laws can discourage speech, interfering with both the right of free expression and the right to access information. The use of defamation law to silence critics poses a danger both online and offline and requires a sensitive balancing of interests.

The European Court of Human Rights has developed a body of law that balances the right to free expression with the obligation to protect the reputation or rights of others. When the Court examines whether an imposition of liability for defamation is “necessary in a democratic society,” in general it will consider several factors: the subject matter of the publication, the position of the author, the position of the person against whom the criticism was directed, the characterization of the contested statements by the domestic courts, the wording used by the author, and the penalty imposed by the domestic courts. When assessing the right to reputation, the Court accords governments the least amount of protection (and therefore is least likely to permit an infringement on free expression when the speech involves criticism of governments), followed by public officials acting in their official capacity or other instances where matters of “public interest” are concerned.

Private individuals and the private aspects of a public official’s life receive the most protection. In general, it appears that the European Court gives more deference to privacy and reputation than do courts in the United States. However, to ensure that a balance is maintained, the Court in several cases has upheld a judgment of defamation while overturning heavy financial or penal sanctions for defamatory acts.<sup>38</sup>

Eduardo Bertoni’s chapter on determining jurisdiction in defamation cases describes one of the most difficult, unresolved challenges facing the Internet: how to resolve conflicts of law and

---

<sup>36</sup> “International Mechanisms for Promoting Freedom of Expression,” Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and the OAS Special Rapporteur on Freedom of Expression, Dec. 21, 2005, <http://www.osce.org/fom/27455>.

<sup>37</sup> Convención Americana sobre Derechos Humanos, Artículo 11, 22 de noviembre, 1969: <http://www.oas.org/juridico/spanish/tratados/b-32.html>

<sup>38</sup> CDT, “Regardless of Frontiers: Human Rights Norms in the Digital Age,” April 21, 2011, p51. <http://www.cdt.org/policy/regardless-frontiers-human-rights-norms-digital-age>

divergent theories of jurisdiction in the context of a medium whose architecture does not conform to traditional geographical boundaries. Jurisdictional issues arise not only in the defamation context, but also with respect to data protection, prohibitions on speech (for example, laws prohibiting hate speech), and law enforcement access to stored data. In all of these areas, two or more countries with different legal standards may claim jurisdiction over the same data or content. Nations around the world are grappling with the question of when a private litigant, a government regulator, or a law enforcement officer may legitimately assert jurisdiction over digital data or online expression stored or hosted outside of the country of the person or entity asserting jurisdiction.

No coherent theory of jurisdiction has yet emerged, either globally or regionally, but the issue implicates constitutional and human rights, due process, and the rule of law. A joint statement by UN, OSCE and OAS Special Rapporteurs for free expression provides some initial guidance: “Jurisdiction in legal cases relating to Internet content should be restricted to States in which the author is established or to which the content is specifically directed; jurisdiction should not be established simply because the content has been downloaded in a certain State.”<sup>39</sup> Even within this guideline, the question of how to determine whether or not content was “specifically directed” into a jurisdiction remains complex.

As Bertoni points out, overbroad assertions of jurisdiction in defamation cases can have an especially restrictive effect on freedom of expression. Those who express themselves online typically have little control over who accesses the content that they create, if it is posted on the open Internet. If individuals fear being held liable by a foreign court for defamation or are unsure of whether their online speech will be regulated under the law of another state, they will be less likely to exercise their right to free expression. The impact would fall especially heavily on the speakers of modest means who would otherwise be empowered by the Internet; without the ability to hire lawyers to advise them on their global exposure to liability, or to appear in courts around the world to defend them, they may either “self-censor” their speech or face crushing penalties.

In other areas where conflicting laws and divergent claims of jurisdiction are creating similar tensions – most notably in the area of data protection – governments, industry, and civil society stakeholders are seeking to achieve greater harmonization of the substantive legal standards in order to minimize the conflicts and the jurisdictional tension. Harmonization alone, however, is not enough: since freedom of expression is at issue, it is critical that the harmonized standard be based on human rights principles. Accordingly, Bertoni recommends harmonization under human rights standards articulated in the ACHR. This approach could prove fruitful: regional harmonization would decrease jurisdictional tensions while taking into account strong regional norms that acknowledge both freedom of expression and the right to honor.

As part of this effort at harmonization, attention should be given to the decriminalization of defamation. Human rights institutions have urged states to decriminalize defamation, allowing only for civil action.<sup>40</sup> If leading Latin American policymakers were to move forward on decriminalizing defamation, they could provide a powerful example for the global community.

---

<sup>39</sup> “International Mechanisms for Promoting Freedom of Expression,” Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression (2005), <http://www.osce.org/fom/27455>.

<sup>40</sup> “Tenth Anniversary Joint Declaration: Ten Key Challenges to Freedom of Expression in the Next Decade,” UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS

This chapter also raises specific issues about the role of intermediaries. As we mention in our discussion of the chapter written by Ruiz and Lara, any rule holding intermediaries liable for the defamatory content created by their users generates additional freedom of expression concerns. Service providers faced with the risk of liability may be quick to take down content whenever they receive an allegation that it is defamatory since they are not well positioned to judge defamation.<sup>41</sup>

Court injunctions also present another critical intermediary issue: When courts rule in favor of defamation plaintiffs, too often they issue overbroad orders to Internet intermediaries to implement the ruling, thereby generating additional freedom of expression concerns. For example, Ruiz and Lara document cases in Argentina where courts have issued overbroad injunctions requiring Internet intermediaries to prevent access or links to future defamatory speech about a victim.<sup>42</sup> When issued against Internet intermediaries, such injunctions can lead to overblocking, restricting lawful and non-defamatory speech. While human rights standards allow limitations on freedom of expression to protect the reputational rights of others, such measures must meet standards of proportionality and necessity. One area for further research may be an exploration of how court injunctions could be crafted to be more proportionate in addressing defamation – that is, how to narrow injunctions issued by a court to target the defamatory speech and to minimize the impact on lawful and non-defamatory speech.

#### 4. Conclusion

The Internet will become increasingly essential to nearly all aspects of our political, social, and economic lives over time. Millions of citizens in Latin America are joining the global community of users online each year. To date, the Internet has demonstrated its potential as a powerful engine for human rights, civic participation, and economic growth. Yet as the chapters of this book illustrate, the Internet's open and free nature is not guaranteed by technology. To ensure the fullest benefit to economic development and human rights, the Internet must be supported by a policy framework that protects privacy, promotes the free flow of information, discourages intermediary liability, and encourages innovation and competition.

Still, the Internet's unique characteristics present novel policy challenges that governments and civil society must address: How do we promote freedom of expression, privacy, and access to knowledge online while also protecting children, safeguarding security, tackling crime, and enforcing intellectual property rights? How Latin American states answer the policy questions described in this book will have long-lasting impact.

Latin America is well-positioned to lead the world in enacting laws that support the open Internet. The American Convention on Human Rights articulates robust norms that uphold freedom of expression and privacy. Though open questions remain about how to apply existing

---

Special Rapporteur on Freedom of Expression & ACHPR Special Rapporteur on Freedom of Expression and Access to Information (2010), <http://www.cidh.org/relatoria/showarticle.asp?artID=784&IID=1>.

<sup>41</sup> CDT, “Intermediary Liability: Protecting Internet Platforms for Expression and Innovation” (April 2010) [http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability\\_%282010%29.pdf](http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf).

<sup>42</sup> See Vinod Sreeharsha, “No Safe Harbors in Argentina,” *New York Times*, August 20, 2010, <http://bits.blogs.nytimes.com/2010/08/20/no-safe-harbors-in-argentina/>.

standards to new Internet technologies, an approach to Internet policy that is based on strong human rights norms can generate the legal framework that can maximize the potential of the Internet throughout the region.