

Chapter One

Keeping the Internet Free in the Americas

Dawn Carla Nunziato¹

Introduction

In the workshop “Freedom of Expression and the Internet: Regulatory Aspects in Latin America” organized by Professor Eduardo Bertoni, legal experts from the Western Hemisphere convened to discuss how to facilitate freedom of expression on the Internet. We considered how to balance the harms that may arise from free speech (including harms to privacy, honor, intellectual property, public welfare) against its benefits, as well as the proper role of Internet service providers as intermediaries in protecting and facilitating Internet free speech. We examined the proper role of governments in protecting Internet free speech and in punishing harmful speech -- directly and by regulating intermediaries. We also examined the role of governments in regulating Internet service providers to facilitate the free flow of information on the Internet. In what follows, I offer my introductory observations and recommendations for keeping the Internet free, with an emphasis on the role of Internet service providers and governments in facilitating freedom of expression in the Americas.

Citizens of the Americas today rely on the Internet as a forum for expression and communications to an unprecedented degree. Internet penetration in Latin America is rapidly increasing, as countries realize the importance of the Internet to their economies and to their citizens’ participation in global forums for expression. In this period of rapid development, some countries in Latin America have emerged as leaders in protecting freedom of expression on the Internet. Chile, for example, was the first country in the world to enact net neutrality legislation, ensuring that its ISPs cannot discriminate against content or applications made available to its citizens. In contrast, other countries in Latin America are taking steps in a direction that is decidedly less supportive of Internet free speech. Venezuela, for example, plans to establish an Internet chokepoint at its border to block its citizens from accessing speech that is “aimed at

¹ Professor of Law, The George Washington University Law School. I am very grateful to Eduardo Bertoni, Director of the Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) of the Universidad de Palermo School of Law, for inviting me to participate in the workshop “Freedom of Expression and the Internet: Regulatory Aspects in Latin America,” as well as to all the participants in this workshop, for their excellent work in the area of freedom of expression on the Internet in the Americas.

creating social unrest or disturbing public order.”² In recent years, Brazilian courts have ordered the overly broad blocking of Internet content, and indeed, once ordered *all* access to YouTube to be blocked in that country.³ Developments in filtering technologies have now advanced to the point where it is feasible for governments to censor speech that is disfavored by the government and/or by certain individuals. Given these developments, the time is right to focus on recommendations to governments in Latin America to enable them to preserve the Internet as a forum for free expression and to forgo the temptation to co-opt the Internet as a tool for government control and manipulation. In what follows, I reflect on the efforts of the United States and other countries to navigate these waters, and offer recommendations to protect freedom of expression on the Internet in the Americas.

I. Government Regulation of Internet Service Providers

Internet service providers serve as the gatekeepers for access to the entirety of the Internet’s content and as such, have vast power to control what information is received and communicated by their subscribers. The existence of this power raises the question of under what circumstances ISPs should be required or permitted to exercise this power to prohibit their subscribers from accessing allegedly harmful, illegal, or disfavored content. That is, should governments regulate ISPs to *require* them to restrict access to material that is alleged – by the government or by private parties – to be harmful? Alternatively, governments might enact net neutrality legislation to *prohibit* ISPs from exercising this power to control their subscribers’ access to lawful content. As an example of the first, governments might require their ISPs to prohibit their subscribers from accessing content that the government deems harmful, such as Venezuela is attempting to do. Or governments might require ISPs to block all access to content that an individual alleges to be harmful, as has occurred in Brazil. Or ISPs themselves might choose to block their subscribers’ access to content that the ISP itself determines is undesirable, such as content or applications offered by a competitor or content espousing a social or political viewpoint with which the ISP disagrees. In what follows, I suggest, first, that ISPs generally should be broadly immunized from all liability for hosting harmful content, and second, that ISPs should be legally required to facilitate access to all legal content, without discrimination or censorship.

A. Internet Service Providers Should Be Largely Immune from Liability for Facilitating Access to Harmful Content

Governments face difficult choices regarding whether and how to hold ISPs liable for facilitating access to harmful content, whether by hosting such content, as in the case of

² See Content Filtering in Latin America: Reasons and Impacts on Freedom of Expression, Joana Varon Ferraz, Carlos Affonso Sousa, Bruno Magrani, and Walter Britto, *infra*.

³ *Id.*

YouTube, or providing links to such content, as in the case of Google. The most speech-protective regime would immunize ISPs from any such intermediary liability and would refrain from imposing any obligation on ISPs to remove or disable access to such harmful content – absent a narrowly tailored court order adjudicating such content to be illegal. Conversely, the most speech-restrictive regime would render ISPs directly liable for the harmful third-party content, regardless of whether the ISPs have actual or constructive notice of such content. And there are many possibilities between these two extremes.

The imposition of strict liability on Internet service providers for facilitating allegedly harmful content made available by subscribers has severe consequences for freedom of expression, as it requires ISPs to actively and closely monitor all such content and would incentivize ISPs to remove any content that is even questionably harmful or illegal. Such a system has ultimately been avoided by most countries in the region. Yet, even notice-based liability imposed on service providers has speech-unfriendly consequences. In such a regime, if an affected individual has the right to demand that the ISP take down content that the individual claims is harmful or illegal, the ISP's obligation or incentive to remove such content -- outside of a judicial determination of its illegality -- has deleterious effects on freedom of speech. As one court explained:

[N]otice-based liability for [ISPs] would provide third parties with a no-cost means to create the basis for future lawsuits. Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply "notify" the relevant service provider, claiming the information to be legally defamatory. In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability. [Such a result would dampen] the vigor of Internet speech⁴

The United States has avoided such a speech-unfriendly system in cases where the harm alleged is defamation or privacy violations. Section 230 of the Communications Decency Act⁵ broadly immunizes ISPs from both strict liability and liability upon notice by the affected individual of the allegedly harmful material and immunizes ISPs from any responsibility for facilitating access to allegedly harmful speech. This immunity extends even in cases where ISPs edit, pre-screen, or pay third parties to create or submit, the allegedly harmful content in

⁴ Zeran v. America Online, 129 F.3d 327 (4th Cir. 1997).

⁵ Pub. L. No. 104-104, 110 Stat. 133 (codified as amended at 47 U.S.C. § 223 (2000)). Section 230 provides that “[n]o provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”

question. This immunity, while highly protective, has been extended quite broadly – even to cases where the ISP is an active participant in the creation of the content and the content cannot be fairly said to be provided by “another” information content provider. U.S. courts, in interpreting Section 230, should scrutinize more closely whether the ISP has taken an active role in creating harmful content and should not extend immunity from liability in such cases, in order to strike the proper balance between protecting intermediaries and securing adequate relief to parties harmed by such content.

The United States’s approach with respect to allegations of copyright infringement achieves a result that is much less protective of free speech (and fair use). Under the United States’s Digital Millennium Copyright Act,⁶ a copyright owner essentially has the right to compel ISPs to remove content that he or she claims is infringing, without a judicial determination of the infringing nature of the content. Section 512 of the DMCA grants service providers a safe harbor to limit their liability for direct and indirect copyright infringement if they agree to remove content that a copyright owner *claims* is infringing.⁷ Under the notice and take down provisions of Section 512, a copyright owner may provide notice to a service provider stating that he or she believes that the service provider is hosting or linking to infringing content.⁸ Upon receipt of such notice, the service provider must expeditiously cease hosting or linking to the allegedly infringing content in order to secure the benefits of the statute’s limitations of liability. Although the statute also provides a mechanism for the Internet user who made such content available to defend her use (via a “counter-notification”⁹), this counter-notification mechanism is problematic, rarely invoked, and has had limited effect on the censorship of content enabled under Section 512. Armed with the DMCA, copyright owners today merely need to send a notice to the ISP requesting take down, and ISPs -- having the incentive to secure the limitations of liability provided under Section 512 -- readily comply, by “expeditiously” removing or disabling access to the content.¹⁰ In effect, this provision enables a copyright owner to secure the equivalent of a temporary restraining order – a court order mandating that the allegedly infringing content be removed -- but without benefit of judicial process. Thousands of copyright owners have successfully induced ISPs to censor critical or unflattering uses of their copyrighted content – even in cases where such uses would be considered non-infringing, fair uses under the Copyright Act. Analyses of the thousands of uses of Section 512 reveals a “high incidence of questionable uses of the process ... to create leverage in a competitive marketplace, to protect rights not given by copyright ..., and to stifle

⁶ 17 U.S.C. Sec. 512 (2000).

⁷ 17 U.S.C. Sec. 512 (c)(1)(c).

⁸ 17 U.S.C. Sec. 512 (c) (3).

⁹ 17 U.S.C. Sec. 512 (g) (3) (c).

¹⁰ See Sec. 512 (c)(1)(c).

criticism, commentary and fair use, [resulting in a] continuous and perhaps unquantifiable effect on public discourse.”¹¹

The imposition of notice-based liability upon ISPs for hosting or linking to content that is allegedly infringing leads to speech-unfriendly results. Allowing copyright owners to secure the removal of allegedly infringing content without a judicial determination of the content’s illegality is insufficiently protective of the free speech and fair use rights of internet users and is not a model that should be replicated by other countries in the Americas.

As we have seen, laws incentivizing ISPs to take down allegedly harmful content outside of the judicial process are highly problematic. Yet, even the *judicial* imposition of take-down obligations on ISPs can have speech-unfriendly consequences. In cases in Argentina and Brazil, as will be discussed by other commentators, courts required ISPs to remove links to websites containing famous names like Cicarelli and Maradona. In these cases, courts neglected to narrowly tailor their orders to protect free speech rights and imposed broad take-down orders on ISPs. In such cases, overbroad judicial take-down orders, as well as the ISPs’ overbroad implementation of such orders, have led to severely speech unfriendly consequences.

To avoid such speech-unfriendly results, in regulating the Internet, governments should refrain from passing legislation imposing intermediary liability – whether strict liability or liability upon notice -- on ISPs for facilitating harmful third-party content. And, while courts should have the power to impose take-down obligations in specific cases where ISPs host illegal content, such take-down mandates should be crafted by courts and implemented by ISPs in the most narrowly tailored and precise manner possible so as to avoid overblocking of protected speech.

B. Governments Should Impose Net Neutrality Obligations on Broadband Service Providers

As I set forth in Part I.A., to protect the free flow of information on the Internet, governments should pass legislation broadly immunizing ISPs from liability for hosting harmful or illegal content. Conversely, governments should impose upon broadband service providers the legal obligation to facilitate Internet users’ access to all legal content and should require broadband service providers to serve as neutral conduits for such content, free from discrimination or censorship. Because the Internet has become the most important medium for individuals to express themselves and to communicate with others – in the Americas and throughout the world -- it is imperative that Internet users enjoy a guarantee of free flow of information and communication of ideas, free of censorship or discrimination by governments *or* by the ISPs who are charged with facilitating such communications. Just as telephone companies, in the United States and other countries, have long been legally obligated to connect

¹¹ See Jennifer M. Urban and Laura Quilter, Efficient Process or “Chilling Effects”? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act, 22 Santa Clara Computer and High Tech L.J. 621 (2006).

users' calls and to otherwise facilitate communications free of censorship or discrimination, so too should broadband service providers be required to facilitate the communication and exchange of information without discrimination or censorship. This freedom to communicate has long been essential to our liberal democratic way of life and must continue to be protected in the Internet age.¹²

In the United States, the government historically has imposed affirmative obligations on entities engaged in transportation, communications, and other important public service functions to facilitate the free flow of information and commerce, free of censorship or discrimination. Through this "common carriage doctrine," the United States government has imposed affirmative duties on entities that provide important communication and transportation functions for the benefit of the public. Rather than granting conduits for communication the discretion to regulate speech however they see fit, the common carriage doctrine implemented by U.S. courts and legislatures requires that these entities facilitate all legal content on the same terms and conditions.

In regulating broadband providers, governments should be guided by the principle that underlies modern communications law and the common carriage doctrine -- that liberal democracies require a well-informed citizenry, which in turn requires that citizens enjoy the freedom to communicate and to access communications from a broad range of sources. The same principles that justify regulating telephone companies as common carriers subject to nondiscrimination requirements -- in order to "protect ordinary citizens in their right to communicate"¹³ -- are relevant with regard to Internet communications.

Allowing broadband providers to discriminate against whatever content or applications they choose for whatever reasons they choose is inconsistent with the historical progression of according individuals protection in their freedom to communicate. Permitting broadband providers to restrict the free flow of information and ideas enables these gatekeepers of speech to thwart the "public discussion and informed deliberation that ... democratic government presupposes and the First Amendment seeks to achieve."¹⁴ Absent regulation, broadband providers will enjoy the discretion to discriminate against the content or applications of their choosing and citizens will not be guaranteed the access to a multiplicity of uncensored viewpoints from diverse and antagonistic sources that is necessary for them to participate meaningfully in democratic government. Instead, citizens will be increasingly limited to

¹² For further elaboration of the common carriage doctrine and its application to Internet service providers, see Dawn C. Nunziato, *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age* (2009).

¹³ Ithiel de Sola Pool, *Technologies of Freedom* 106 (1983).

¹⁴ *Id.*

expression that is approved (or not disapproved) by the one or two broadband providers who serve as gatekeepers for their Internet communications.

Broadband providers should therefore be subject to net neutrality regulations that require them to assume at least the nondiscrimination obligations that historically have been imposed upon other common carriers of communications – the duty to facilitate and transmit in a nondiscriminatory manner any and all legal content and applications.

Such net neutrality regulations prohibiting broadband providers from blocking legal content or applications should also mandate *transparency* in any such blocking, requiring broadband providers to inform subscribers of any (illegal) content or applications that were blocked and the reasons for such blocking (e.g., the provider claims that the content was illegal because it contained child pornography or some other type of content deemed illegal in that country). Mandating such transparency in blocking will enable users to impose checks on the blocking decisions of broadband providers and ensure that such blocking does not mask the provider's unlawful discrimination on the basis of content. Internet users enjoy the right to transparency in decisions affecting what content they can access and to be informed that content or applications have been blocked and the reasons for such blocking, so that they can impose checks on broadband providers' discriminatory actions.

In summary, governments should pass legislation prohibiting broadband providers from blocking legal content or applications and from engaging in discriminatory prioritization or degradation of such content or applications. Such legislation should also mandate transparency in blocking or degrading, requiring broadband providers meaningfully to inform Internet users of any content or applications that were blocked or degraded and the reasons therefor, so that users will be able to impose meaningful checks on these decisions of broadband providers and ensure that such actions do not mask unlawful discrimination.

Several Latin America countries have led the way on net neutrality. As will be discussed in this volume, Chile passed the world's first net neutrality legislation, providing that its ISPs "may not arbitrarily block, interfere with, discriminate against, hinder or restrict the right of any Internet user to use, send, receive or offer any legal content, application or service on the Internet, or any kind of legal Internet activity or use."¹⁵ This mandate, however, is subject to the exception allowing "Internet Access Providers [to] take any measure or action that may be necessary for purposes of traffic management and network administration. . ." Colombia has enacted a similar net neutrality law, but one that is not subject to this type of network management exception. The Colombian law provides that "Internet Service Providers may not . . . block, interfere with, discriminate against or restrict the right of any Internet user to use, send,

¹⁵ See Content Filtering in Latin America: Reasons and Impacts on Freedom of Expression, Joana Varon Ferraz, Carlos Affonso Sousa, Bruno Magrani, and Walter Britto, *infra*.

receive or offer any lawful content, application or service on the Internet [and] may not make an arbitrary distinction between content, applications or services on the basis of the origin or ownership thereof.” The net neutrality legislation enacted in Chile and Colombia should serve as a model for other countries in the hemisphere for the protection of Internet users’ right to communicate on the Internet, free of discrimination or censorship.¹⁶ To fulfill the Internet’s promise of being “the most participatory marketplace of mass speech that this country -- and indeed the world – has yet seen,”¹⁷ those who serve as powerful gatekeepers for expression on the Internet should be regulated to ensure that they act as good stewards within this marketplace – free of discrimination and censorship, and true to the free speech values that are necessary to facilitate the public discussion and informed deliberation that democratic government presupposes and that the free speech guarantee requires.

II. Governments Should Enact Protections for Anonymous Speech on the Internet

One of the most speech-enhancing features of the Internet is the ability of speakers to speak critically, without fear of reprisal, about all manner of subjects – including their governments and other matters of political and societal importance. Essential to this aspect of freedom of Internet speech is the ability to speak anonymously or pseudonymously. Yet, several countries in the Americas have enacted measures to restrict or prohibit anonymous speech, in real space and in cyberspace. Venezuela’s Constitution, for example, prohibits anonymous speech, everywhere.¹⁸ Brazil’s Constitution contains a similar prohibition on anonymous speech.¹⁹ These types of restrictions on individuals’ ability to speak anonymously (or pseudonymously) – on the Internet and elsewhere -- are inimical to the free speech guarantee and should be revised. Instead, countries should provide meaningful protections for individuals’ right to communicate and express themselves anonymously on the Internet and in real space.

¹⁶ The United States’ Federal Communications Commission, after years of uncertainty and vacillation, has finally published net neutrality rules, which will become effective in November 2011. These net neutrality rules (1) prohibit wireline or fixed broadband service providers from blocking any lawful content, applications, or services, subject to reasonable network management exceptions, and prohibit these providers from unreasonably discriminating in handling traffic; (2) prohibit wireless or mobile broadband service providers from blocking lawful content or applications that compete with these providers’ own voice or video services, subject to reasonable network management exceptions. See *Preserving the Open Internet*, 76 Fed. Reg. 59192 (Sept. 23, 2011) (to be codified at 47 C.F.R. pt. 8). However, these rules are subject to legal challenge and it is uncertain whether or when they will be implemented.

¹⁷ 929 F. Supp. at 844.

¹⁸ See Freedom House, *Freedom on the Internet 2011*, 366 and n.69, available at <http://www.freedomhouse.org/uploads/fotn/2011/FOTN2011.pdf>

¹⁹ Article 5, Section IV of the Constitution of Brazil provides: “All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms . . . the expression of thought is free, anonymity being forbidden.”

The experience of the United States, since its founding, demonstrates the importance of governmental protections for the right to express oneself anonymously. Protections for anonymous speech have been an important component of U.S. free speech jurisprudence since the founding of the country. Throughout the history of the United States -- and indeed critical to its formation and development as a liberal democracy -- the right of publishers and authors to remain anonymous has served as an important component of the First Amendment right to freedom of speech and of the press. As United States Supreme Court Justice Clarence Thomas explained, summarizing relevant aspects of this history:

There is little doubt that the Framers engaged in anonymous political writing. The essays in the Federalist Papers, published under the pseudonym of Publius, are only the most famous example of the outpouring of anonymous political writing that occurred during the ratification of the Constitution. . . . The earliest and most famous American experience with freedom of the press, the 1735 Zenger trial, centered around anonymous political pamphlets. The case involved a printer, John Peter Zenger, who refused to reveal the anonymous authors of published attacks on the Crown governor of New York. . . . The case . . . signified at an early moment the extent to which anonymity and the freedom of the press were intertwined in the early American mind.²⁰

Protecting the anonymity of publishers and authors serves two fundamental purposes: First, protecting speakers' anonymity allows the content of a speaker's message to be evaluated on its merits instead of in the context of the identity or reputation of the author.²¹ Second, protecting speakers' anonymity allows proponents of unpopular positions or causes to express their views without fear of personal reprisal.²² As such, the protection of anonymous speech is critical to fulfilling the countermajoritarian function of the First Amendment by insulating speakers of unpopular messages from the potential threat of reprisal. As the United States Supreme Court explained in *McIntyre v. Ohio Elections Commission*,²³ drawing from the theory of free speech set forth by John Stuart Mill in *On Liberty*²⁴:

²⁰ *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 350 (1995).

²¹ *Id.* at 334 (“Anonymity provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent.”). See also Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and The Internet*, 75 OR. L. REV. 117, 144 (1996).

²² See *McIntyre*, 514 U.S. at 374; *Talley v. California*, 362 U.S. 60, 64 (1960); Tien, *supra*, at 144 (observing that “one obvious cost of regulating anonymity is potential retaliation against the speaker.”)

²³ 514 U.S. 334 (1995).

²⁴ JOHN STUART MILL, *ON LIBERTY* (1859).

Anonymous speech is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent. Anonymity is a shield from 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 – and their ideas from suppression – at the hand of an intolerant society.²⁵

If speakers' anonymity is not protected, advocates of unpopular ideas will often be dissuaded from speaking, thereby impoverishing the marketplace of ideas. As United States Supreme Court Justice Hugo Black explained *Talley v. California*,²⁶ “persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.”²⁷ The protection for anonymous speech is thus a critical component of an expressive public forum in which individuals can share their opinions with others free of personal reprisal, and have their opinions be evaluated on their own merits.

Although these justifications for protecting anonymous speech are strongest with respect to political speech, the First Amendment's protections for anonymous speech extend to other types of speech as well. As the United States Supreme Court explained in *McIntyre*:

Anonymous pamphlets, leaflets, brochures, and even books have played an important role in the progress of mankind. . . . The author's decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, . . . the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.²⁸

Anonymity thus protects an author's prerogative in defining how to present her ideas to the world. As such, anonymity “safeguards the ability independently to define one's identity that is central to any concept of liberty.”²⁹

²⁵ 514 U.S. at 347.

²⁶ 362 U.S. 60 (1960).

²⁷ 362 U.S. at 64. See Tien, *supra*, at 128-29 (explaining that *McIntyre* is about “fear of viewpoint discrimination, because anonymity is historically tied to the ability of the unpopular and persecuted to criticize oppressive practices and laws.”)

²⁸ 514 U.S. at 340.

²⁹ Tien, *supra*, at 123.

Notwithstanding the importance of protecting anonymous expression, governments throughout the Americas have attempted to erode this protection and to compel the disclosure of the speakers' and publishers' identities in the name of various countervailing interests. For example, in *McIntyre*, the legislature sought to justify a prohibition on the anonymous distribution of campaign literature on the grounds, inter alia, that compelling disclosure of speakers' identities was necessary to prevent fraud and libel.³⁰ While recognizing the importance of such state interests, the United States Supreme Court found that the state had sufficient means of *directly* protecting against fraud and libel in the relevant contexts, and that the state's ban on anonymous campaign literature was an indirect and insufficiently narrowly tailored means of advancing these important state interests.³¹ While the state's interest in preventing fraud and libel might justify a more limited disclosure requirement,³² the Supreme Court found that State's total ban on anonymous pamphleteering was unjustified.³³

The First Amendment right to speak anonymously has also been specifically recognized in the context of Internet communications. In a case that involved the right to speak anonymously in the specific context of Internet communications, the State of Georgia was found to have run afoul of the First Amendment in attempting to prohibit all anonymous and pseudonymous Internet communications. In *Zell v. Miller*,³⁴ Georgia made it a crime falsely to identify one's name (and hence to communicate pseudonymously or anonymously) for the purpose of electronically transmitting data, such as via email. Relying upon *McIntyre*, the court struck down this statute, holding that it impermissibly burdened the constitutional "right to

³⁰ 514 U.S. at 342.

³¹ *Id.* at 344.

³² *Id.*

³³ *Id.* See also *Watchtower Bible and Tract Society of New York v. Village of Stratton*, 536 U.S. 150 (2002). In *Watchtower*, the Supreme Court rejected the locality's justification for mandating disclosure of the identity and affiliation of door-to-door canvassers. In *Watchtower*, the Village of Stratton, Ohio, attempted to justify this disclosure requirement, inter alia, on the grounds of preventing fraud and crime. The Supreme Court found that the complete ban on anonymous door-to-door canvassing that the regulation effected – which applied not only to commercial transactions and to the solicitation of funds, but also to religious and political canvassers and others seeking to enlist support for their causes – was insufficiently narrowly tailored to advance the locality's important interests. Accordingly, the locality's total ban on anonymous door-to-door canvassing was found to be unjustified and its mandatory disclosure requirement for door-to-door canvassers was invalidated.

³⁴ See *Zell v. Miller*, 977 F. Supp. 1228 (N. D. Ga. 1997). See also *American Civil Liberties Union v. Reno*, 929 F. Supp. 824, 831 (1996) (recognizing importance of online anonymity to speakers who seek access to sensitive information), *aff'd*, 521 U.S. 844 (1997).

communicate anonymously and pseudonymously over the Internet.”³⁵ While crediting the state’s compelling interest in preventing fraud in Internet communications, the court nevertheless found that the statute’s blanket prohibition on anonymous and pseudonymous Internet communications was not narrowly tailored to advance this compelling state interest.

Of course, there will be instances when a plaintiff will eventually need to discover the identity of a speaker whose content is alleged to be illegal and harmful to plaintiff. Protections for anonymous speech are not absolute and can be lifted, but only in conjunction with requisite judicial procedures that are sensitive to the interests of both plaintiffs in seeking meaningful relief and of defendants in securing continued protection for their free speech rights to the greatest extent possible. Allowing an aggrieved party to proceed initially against an anonymous John Doe defendant, and enabling a judge to determine whether to compel an Internet intermediary to disclose the identity of the anonymous speaker, adequately balances the interests of both sides.

United States courts’ efforts to balance Internet users’ right to communicate anonymously against other individuals’ property, reputational, and privacy rights are instructive in this regard. In a series of recent cases in which plaintiffs alleged that they were defamed by anonymous Internet postings and sought to discover the identities of the individuals responsible for such postings from the relevant Internet Service Providers, courts have imposed stringent requirements on plaintiffs’ efforts to discover the identities of such individuals. For example, in *Doe v. 2TheMart.com*, the plaintiff, who claimed that she was defamed by an anonymous post, sought to discover from the ISP the identity of an alleged defamatory poster. The court imposed stringent standards on plaintiff’s ability to discover the poster’s identity in order to protect the poster’s right to engage in anonymous speech. Holding that “discovery requests seeking to identify anonymous Internet users must be subject to careful scrutiny by the courts,” the court set forth a demanding multifactor test for evaluating whether plaintiff’s need for such information outweighed the poster’s right to speak anonymously.³⁶ Only upon satisfying this heightened showing would plaintiff’s right to access such information in order to prosecute her defamation action be found to outweigh defendant’s right to speak anonymously. Similarly, in the recent decision in *Independent Newspapers, Inc. v. Brodie*,³⁷ that court articulated the following stringent standard for judges to apply in determining whether to compel disclosure of the identity of an anonymous Internet speaker:

When a trial court is confronted with a defamation action in which anonymous

³⁵ *Zell v. Miller*, 977 F. Supp. 1228.

³⁶ See 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001). Under this four part test, the court will inquire into the following factors in considering whether a subpoena for the identity of non-party Internet speakers should be upheld: “(1) Was the subpoena brought in good faith? (2) Does the information relate to a core claim or defense? (3) Is the identifying information directly and materially relevant to that claim or defense? (4) Is the information available from other sources?”

³⁷ 966 A.2d 432 (Md. Ct. App. 2009).

speakers or pseudonyms are involved, it should: (1) require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, . . .; (2) withhold action to afford the anonymous posters a reasonable opportunity to file and serve opposition to the application; (3) require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster, alleged to constitute actionable speech; (4) determine whether the complaint has set forth a prima facie defamation . . . action against the anonymous posters; and (5), if all else is satisfied, balance the anonymous poster's First Amendment right of free speech against the strength of the prima facie case of defamation presented by the plaintiff and the necessity for disclosure of the anonymous defendant's identity, prior to ordering disclosure.

In summary, the United States since its founding has consistently accorded meaningful protections for anonymous speech. Protection for a speaker's anonymity is a fundamental part of the First Amendment right to freedom of expression. This protection has extended to Internet speech as well, and has been carefully guarded by courts in balancing the interests of parties aggrieved by such speech against speakers' interest in anonymity. The United States's approach should serve as a model for other countries in the Americas in extending protection to speakers for their right to speak anonymously or pseudonymously on the Internet.

III. Governments Should Be Restricted in Filtering Internet Content

In addition to ensuring that service providers do not restrict the free flow of information on the Internet, it is imperative that governments themselves are restricted in their ability to censor Internet content – even content that is deemed illegal within a given country. A growing number of countries are filtering speech on the Internet in a variety of ways and this form of censorship has become a powerful tool for many governments – dictatorships and democracies alike – to control what ideas and information their citizens access.³⁸ Venezuela seems poised to join this growing number of countries. Given the extent and effectiveness of efforts to censor Internet speech throughout the world, protectors of free speech can no longer rest comfortably on the assurance issued by Internet pioneer John Gilmore two decades ago that "the Net interprets censorship as damage and routes around it."³⁹ Pervasive Internet censorship has extended well beyond the usual suspects – China, Saudi Arabia, North Korea, etc. – to less likely suspects like the U.K., Canada, and Australia. Although free speech advocates broadly denounce such censorship, it is likely that many countries – having seized upon powerful filtering tools -- will

³⁸ See Dawn C. Nunziato, How (Not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide, [cite]. Some of the material in this section has been reprinted from this Article.

³⁹ Philip Elmer-Dewitt, First Nation in Cyberspace, *Time International*, Dec. 6, 1993.

continue to restrict Internet content to prohibit their citizens from accessing speech that is deemed harmful or illegal within their countries. Two responses to such censorship can be pursued: (1) continuing to broadly denounce all Internet censorship or (2) advocating for countries at the very least to restrain themselves in restricting Internet speech, to do so as narrowly and precisely as possible, consistent with shared notions of due process. In what follows, I pursue the second approach. While it is not surprising that different countries, given their different histories and national experiences, will espouse different substantive values regarding which speech to restrict -- for example, how to define and whether to restrict hate speech, incitement, Holocaust denial, pornography, child pornography etc.⁴⁰ -- in implementing their prohibitions on such categories of speech, I argue that countries should adhere strictly to fundamental requirements of due process to ensure that their citizens who are subject to such speech restrictions (1) have notice of such restrictions, (2) that any prohibited categories of speech are defined with precision and clarity, such that (3) those subject to such speech restrictions have a meaningful opportunity to secure prompt judicial review of any such decisions to restrict speech.

Protections for free speech have not only substantive dimensions of which categories of speech to protect and which to restrict – which differ from country to country -- but such protections also have important procedural dimensions, which mandate – in the words of the United States Supreme Court -- that “sensitive tools” be implemented to distinguish between instances of protected and unprotected speech.⁴¹ Such procedures and sensitive tools for protecting free speech are as important as the substantive protections themselves. In the words of United States Supreme Court Justice Frankfurter, “[t]he history of American freedom is, in no small part, the history of procedure.”⁴² In particular, courts in the United States in advancing our substantive free speech values have applied stringent procedural safeguards in scrutinizing *prior restraints on speech* – restraints on speech that are imposed prior to a judicial determination of the speech’s illegality – and have looked upon such restrictions with great disfavor. This strong presumption against the legality of prior restraints is also shared by the Latin American countries

⁴⁰ The American Convention on Human Rights, for example, which protects “the right to freedom of thought and expression,” provides that this right does not prohibit subsequent imposition of liability to the extent necessary to ensure “*respect for the rights or reputations of others*” or “*the protection of national security, public order, or public health or morals.*” The Convention further provides that “[a]ny propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law.”

⁴¹ *Bantam Books v. Sullivan*, 372 U.S. 58 (1963).

⁴² *Malinski v. New York*, 324 U.S. 401, 414 (1945) (Frankfurter, J., concurring)

that have ratified the American Convention on Human Rights, which provides that “the right to freedom of thought an expression . . . shall not be subject to prior censorship”⁴³

Nationwide filtering systems impose “prior restraints” -- or restraints on speech prior to a judicial determination of the speech’s illegality. Instead of imposing punishment on such speech after it has been published and adjudicated illegal by a court, these systems regulate the speech at issue before a court has made the determination that such speech is illegal. The procedural framework adopted in the United States for assessing the legality of prior restraints provides a helpful starting point for countries seeking to impose meaningful constraints on government blocking or filtering of Internet content. Translated into the context of nationwide filtering or blocking of Internet speech, these safeguards require, first, that any filtering be imposed subject to *clear and precise definitions of the speech to be regulated*; second, that the filtering scheme *operate in an open and transparent manner*, such that affected Internet users and content providers are provided with *notice* that the content was blocked and the reason for such blocking; and third, that the filtering scheme provide Internet users and content providers with the *opportunity to appeal any such blocking decisions, to a judicial body and in an expeditious manner*. These procedures do not themselves dictate what categories of speech are to be restricted or what categories of speech are to be deemed harmful. Rather, they impose meaningful, process-based safeguards on the implementation of restrictions of whatever categories of speech are deemed harmful by any particular government.

⁴³ Article 13 of the American Convention on Human Rights provides, in full:

1. Everyone has the right to freedom of thought and expression. This right includes freedom 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.
2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure:
 - a. respect for the rights or reputations of others; or
 - b. the protection of national security, public order, or public health or morals.
3. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.
4. Notwithstanding the provisions of paragraph 2 above, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence.
5. Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law.

To understand what is at stake in such a system, and how lack of transparency and openness implicates the rights of Internet users, consider the operation of a filtering scheme translated to the real space context. Imagine a vast real space forum for authors and readers in which millions of authors bring their books to be made available for billions of potentially interested readers. The authors place their books on the bookshelves of the forum and then depart. Billions of readers also come to the forum to search for books of potential interest to them. Unbeknownst to either the authors or the readers, before the content of any book is made available to the readers – or at some point after the books are placed on the bookshelves – the books are scrutinized by unseen and unknown censors to determine whether the content is “permissible,” according to some criteria that are unstated and undiscoverable. If these censors determine that a book or some of its content is impermissible, it is placed on a blacklist and removed from circulation. When the readers enter the forum to select books of potential interest to them, they do not know which books have been removed, nor do the authors of the banned books ever learn whether (and why) their book has been removed. This scenario replicates in real space what occurs in cyberspace under filtering systems when websites are placed on blacklists and the country’s Internet users are prohibited from accessing such content.

In terms of the real space censoring scenario outlined above, it is important to understand that whether the restrictions imposed by the licensing scheme occur *ex ante* – before *any* reader has an opportunity to access the books’ contents – or whether the restrictions occur at some point after the initial circulation of the books’ contents, both types of restrictions would constitute presumptively unconstitutional prior restraints. *Ex ante* prior restraints include those imposed by censorship boards responsible for screening content (such as motion pictures) before they are made available to the public,⁴⁴ and filtering schemes that are imposed *ex ante*, such as filters imposed by governments (in China, for example) for specific words or phrases deemed harmful. *Midstream* prior restraints, in contrast, include those restraints on speech that are imposed after initial circulation but sometime before a judicial determination that the speech is illegal has been made. Because midstream prior restraints are imposed prior to a judicial determination of the content’s illegality, they are as constitutionally suspect as *ex ante* prior restraints. Midstream prior restraints include filtering systems that work from evolving blacklists of websites that are maintained in response to tips or complaints from web users.

The United States Supreme Court considered an example of midstream prior restraints in the case of *Bantam Books v. Sullivan*.⁴⁵ In *Bantam Books*, the Rhode Island Commission to Encourage Morality in Youth was charged with investigating and recommending prosecution of booksellers for the distribution of printed works that were obscene or indecent. The Commission reviewed books and magazines after they were already in circulation, and took it upon itself to notify distributors in cases in which a book or magazine had been distributed that the

⁴⁴ See *Freedman v. Maryland* (state film censorship board); I. A. Court H.R., “The Last Temptation of Christ” Case (Olmedo Bustos et al vs. Chile), Judgment of February 5, 2001, Series C, No. 73 (in which the Chilean Cinematographic Classification Council [Consejo Nacional de Calificacion Cinematografica] considered and rejected the showing of the film “The Last Temptation of Christ”).

⁴⁵ 372 U.S. 58 (1963).

Commission deemed objectionable. In reviewing the constitutionality of this scheme, the Supreme Court held that, even though the restrictions on publication were imposed after initial circulation and distribution, the Commission's actions nonetheless effectuated an unconstitutional prior restraint. The Court explained that "the separation of legitimate from illegitimate speech calls for . . . sensitive tools" and reiterated its insistence that regulations of speech "scrupulously embody the most rigorous procedural safeguards."⁴⁶ The Court observed that, under the Rhode Island scheme, "the publisher or distributor is not even entitled to *notice and hearing* before his publications are listed by the Commission as objectionable" and that there was "no provision whatever for *judicial superintendence* before notices issue or even for *judicial review* of the Commission's determinations of objectionableness." Accordingly, the Court concluded that, in the context of this system of midstream prior restraint, the "procedures of the Commission are radically deficient" and unconstitutional.

1. Openness and Transparency within Filtering Systems

Bantam Books, as well as other cases invalidating systems of prior restraints, teach that in order for any system of prior restraint to embody the requisite procedural safeguards, the affected parties must at a minimum be made aware of such a decision to censor so that they can effectively challenge it. This, in turn, presupposes that affected parties have *notice* of any such censorship so that they can be secured a *meaningful opportunity to challenge* the initial decision to censor in a judicial forum. Filtering systems in which the affected parties are not made aware that content has been filtered fail this threshold requirement. Surprisingly, on this score of openness/transparency versus secrecy/opaqueness in the operation of filtering systems, some of the most speech-repressive countries fare better than some liberal democracies. Saudi Arabia, for example, while implementing a very restrictive system of government-mandated Internet filtering consistent with its overall restrictive religious society, nonetheless operates its filtering system in a transparent and open manner, and appears to provide Saudi users with meaningful notice that their Internet access is being restricted in general, as well with notice of specific acts of filtering in particular. Although Saudi Arabia's Internet restrictions are hostile to free speech on a number of metrics,⁴⁷ these restrictions operate in a transparent and open manner, providing citizens with clear notice of what Internet speech is being restricted and the asserted justifications for such restrictions. When content is blocked in Saudi Arabia (as it frequently is), the Saudi government is very clear about the mechanism by which it effectuates this filtering. It explains to Internet users that "KACST [King Abdulaziz City for Science & Technology] maintains a central log and specialized proxy equipment, which processes all page requests from within the

⁴⁶ *Id.* at 66.

⁴⁷ For example, a 2008 Saudi law on the use of technology provides substantial penalties (five years imprisonment and a fine) for the use of the Internet to distribute content such as pornography or other materials that violate public law, religious values, or the social standards of the kingdom. See *Access Controlled*, Saudi Arabia chapter. Web sites relating to alternative religions (such as those discussing conversion from Islam to Christianity), web sites espousing critical views of Islam, web sites relating to minority Shia groups, sites of global free speech advocates, web sites relating to gay and lesbian issues, sex education and family planning, have all been blocked. See *id.* at 566-67.

country and compares them to a black list of banned sites. If the requested page is included in the black list then it is dropped.”⁴⁸ Regarding its justifications for filtering, the government explains on its official filtering webpage that:

God Almighty directed humanity in the Noble Qur’an in the words of His prophet Joseph: He said, My Lord, prison is more beloved to me than that to which they entice me, and were you not to divert their plot away from me I will be drawn towards them and be of the ignorant. So his Lord answered him and diverted their plot away from him, truly, He is the All-Hearer, the All-Knower.” Yusuf (12):33-34.⁴⁹

When a Saudi Internet user seeks to access a website that is on the blacklist, the user receives a notice, in both English and in Arabic, that “access to the requested URL is not allowed.”⁵⁰ Further, any Internet user receiving such a message and seeking to appeal the blocking decision is instructed that he or she can submit an unblocking request “by using the special forms set up for such requests on the ISU web page.”⁵¹

Similarly, in Finland, users seeking to access content that has been blocked by the nationwide Internet filtering system receive the following message, specifically notifying them that the website they are seeking to access has been blocked:

POLICE.

ENTRY DENIED. Your browser has tried to access a site for which the access has been prevented due to the act on preventive measures on distribution of child pornography. The police maintains and updates a list of these child pornography sites.⁵²

In contrast, other countries are far more opaque and secretive in their implementation of filtering systems, and operate in such a manner that their Internet users are not made aware that the website they are requesting has been blocked, nor even that the country is implementing a nationwide Internet filtering system. In the United Kingdom, for example, which generally has meaningful guarantees of freedom of expression, the nation’s ISPs have for the past seven years been implementing a nationwide Internet filtering program that operates in a nontransparent manner. The vast majority of British ISPs implement the “Cleanfeed” system to block access to websites that have been deemed potentially illegal by the Internet Watch Foundation, a private organization that maintains a list of URLs that are suspected of hosting illegal content that falls into one of the (expanding) categories of child sexual abuse, promoting racial hatred, or hosting

⁴⁸ Id.

⁴⁹ Id.

⁵⁰ Id.

⁵¹ Id.

⁵² See EFFI, Finnish Internet Censorship, available at <http://www.ffi.org/blog/kai-2008-02-18.html#how-the-censorship-works>

criminally obscene adult content.⁵³ Apparently, the vast majority of U.K. Internet users are unaware that their Internet search results are being filtered in this manner.⁵⁴ Furthermore, the ISPs' implementation of Cleanfeed does not inform Internet users when the sites they have requested are filtered or blocked. Instead, when a U.K. user attempts to access a website that the IWF has placed on the blacklist, the user (at least some of the time) receives a generic 404/"file not found" Internet error message, which conveys no information to the Internet user that the website has been placed on the blacklist.⁵⁵ In the words of commentator Lilian Edwards, the U.K. Cleanfeed system "could be the most perfectly invisible censorship mechanism ever invented."⁵⁶

The U.K.'s model of silent, opaque filtering has been influential in other European countries and has also been adopted in Canada. In 2006, Canada's largest ISPs launched Project Cleanfeed Canada, which is modeled explicitly on the UK Cleanfeed project, in conjunction with Cybertip.ca, a Canadian police organization. As in the UK, analysts from Cybertip.ca make determinations as to content that is potentially illegal and place suspected URLs on the Cleanfeed distribution list. Canadian ISPs then block URLs that have been placed on the Cleanfeed distribution list.⁵⁷ And, as in the UK, Internet users are not informed that the content they are searching for has been filtered. Rather, Internet users receive a standard Internet error message that the website they are seeking is unavailable.⁵⁸

Countries implementing nationwide filtering systems to restrict their citizens' access to content that they deem harmful should at the very least operate these systems in an open and transparent manner, consistent with fundamental procedural due process requirements. These systems should operate in a manner such that (1) Internet users are made aware of the operation of such filtering systems generally, and (2) affected users are specifically informed of instances

⁵³ See <http://www.iwf.org.uk/about-iwf/remit-and-role>

⁵⁴ See Nikolaos Koumartzis, *BT's Cleanfeed and Online Censorship in the UK: Improvements for a More Secure and Ethically Correct System*.

⁵⁵ See Nikolaos Koumartzis, *BT's Cleanfeed and Online Censorship in the UK: Improvements for a More Secure and Ethically Correct System*, at 34 ("In case a request is made for accessing a URL [on IWF's blacklist,] a "404" response with the message "page unavailable" is returned to the user.)

⁵⁶ Lilian Edwards, *From Child Porn to China*, in *One Cleanfeed*, available at <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-3/editorial.asp>.

⁵⁷ See *Access Controlled*, *supra*.

⁵⁸ As the Cybertip website sets forth on its FAQ page:

Are people able to tell which addresses are filtered under this system? . . .

No. They get a standard message indicating they are unable to access the Internet address.

See <http://www.cybertip.ca/app/en/cleanfeed>

in which the filters operate to block access to a particular website. Only then can affected content providers and users have the meaningful notice necessary to challenge the decision to censor, and subject the decision to judicial review.

2. Any Categories of Prohibited Speech Should Be Clearly Defined and Delineated

Another threshold procedural requirement for any system of filtering Internet content is that the censor's discretion be meaningfully constrained by clearly defined and precise guidelines. Such a requirement serves to cabin and constrain the discretion of the initial censor and require that they adhere to the legal determination of what content is proscribable. While countries may reasonably differ in their determinations of what categories of speech are illegal content – pornography, hate speech, Holocaust denial, etc. – it is important that, within each country, the definitions of illegal speech – and especially definitions of any illegal speech subject to prior restraint -- be carefully and precisely defined so as to constrain the initial censor's discretion. The United States Supreme Court, for example, has strictly scrutinized the discretion of censors in systems of prior restraint and has rejected as unconstitutional any systems that reposit unbounded discretion to determine whether or not speech is protected. For example, in *Shuttlesworth v. Birmingham*,⁵⁹ the Court evaluated the constitutionality of a parade permitting system that vested the City Commission with the broad discretion to deny parade permits in cases where “in [the Commission's] judgment the public welfare, peace, safety, health, decency, good order, morals or convenience require that [the parade permit] be refused.”⁶⁰ In ruling on a challenge to the statute, the Court held that, because the permitting scheme constituted a prior restraint on expression that conferred “virtually unbridled and absolute power” on the Commission, it failed to comport with the essential due process requirement that any law subjecting the exercise of First Amendment freedoms to the prior restraint of a license must embody “narrow, objective, and definite standards to guide the licensing authority.”⁶¹

Requiring that the criteria by which the censoring authority makes the decision to censor be set forth with precision helps to cabin administrative discretion and also helps to limit “mission creep” within the censoring body. Without a precise and detailed specification of the criteria for censorship, the censor can exercise unbridled discretion to restrict speech.

Not surprisingly, countries that filter Internet content the most extensively also have the broadest and vaguest definitions of content subject to censorship. China, for example, imposes mandatory filters on content that “disrupts the solidarity of peoples,” “jeopardizes the integrity of national unity,” or “harms national honor or interests.”⁶² Similarly, as discussed above,

⁵⁹ 394 U.S. 147 (1969).

⁶⁰ *Id.* at 149-50.

⁶¹ *Id.* at 150-51.

⁶² China imposes restrictions on Internet content that falls within any of the following categories:

- violating the basic principles as they are confirmed in the Constitution;

Venezuela intends to establish an Internet chokepoint at its border to block its citizens from accessing speech that is “aimed at creating social unrest or disturbing public order.”⁶³ The examples from China and Venezuela embody precisely the sort of standardless discretion that fails to impose any meaningful constraints on censors and fails to provide affected Internet users with notice of which speech is subject to censorship.

Filtering Schemes Should Provide for Appealability of Filtering Determinations

Due process considerations in the free speech context further require that any initial decision to censor be *subject to prompt judicial review* in an *adversary proceeding*. United States courts have emphasized the importance of the availability of *expeditious judicial review* of censorship determinations in the prior restraint context.⁶⁴ As the United States Supreme Court explained, “because only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final [prior] restraint.”⁶⁵ In order for a filtering system to effectuate a valid prior restraint, such a system needs to provide for notice to the affected

-
- endangering state security, divulging state secrets, subverting the national regime, or jeopardizing the integrity of national unity;
 - harming national honor or interests;
 - inciting hatred against peoples, racism against peoples, or disrupting the solidarity of peoples;
 - disrupting national policies on religion, propagating evil cults and feudal superstitions;
 - spreading rumors, disturbing social order, or disrupting social stability;
 - spreading obscenity, pornography, gambling, violence, terror, or abetting the commission of a crime;
 - insulting or defaming third parties, infringing on legal rights and interests of third parties;
 - other content prohibited by law and administrative regulations;
 - inciting illegal assemblies, associations, marches, demonstrations, or gatherings that disturb social order; and
 - conducting activities in the name of an illegal civil organization. See *Access Controlled*, *supra*, at 478.

⁶³ See *Content Filtering in Latin America: Reasons and Impacts on Freedom of Expression*, Joana Varon Ferraz, Carlos Affonso Sousa, Bruno Magrani, and Walter Britto, *infra*.

⁶⁴ See *Thirty-Seven Photographs*, 402 U.S. at 372-74; *Kingsley Books, Inc. v. Brown*, 354 U.S. 436 (1957); *Interstate Circuit, Inc. v. City of Dallas*, 390 U.S. 676 (1968); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963).

⁶⁵ See *United States v. Pryba*, 502 F.2d 391, 405 (D.C. Cir. 1974).

parties and an opportunity to secure the expeditious judicial review of an initial censorship decision.⁶⁶

Attempts within the U.S. to impose ISP filters on harmful Internet speech have been found to be unconstitutional because they have failed to provide for judicial review (prompt or otherwise) in an adversary proceeding of the decision to censor. In the *Center for Democracy and Technology v. Pappert*, for example, the Commonwealth of Pennsylvania sought to combat online child pornography by enacting the Internet Child Pornography Act, which required ISPs serving Pennsylvanians to block access to websites allegedly associated with child pornography. The Act permitted the Pennsylvania Attorney General or Pennsylvania district attorneys to seek an ex parte court order requiring an ISP to remove or disable access to items accessible through the ISP's service, upon a showing of probable cause that the item constitutes child pornography. The Act did not require an actual, final determination that the material to be removed actually constituted child pornography before it was placed on the blacklist. In consultation with the affected ISPs, the Attorney General's office decided to implement the Act by proceeding without even securing ex parte court orders and instead by providing "Informal Notices of Child Pornography" to ISPs that hosted websites that were reported by an agent or a citizen and that the Office of the Attorney General had identified as suspected child pornography. The Informal Notice directed the ISP to remove or disable Pennsylvania citizens' access to the suspected material within five days of receipt of Notice.

The statute was challenged, inter alia, as an unconstitutional prior restraint lacking the requisite procedural safeguards. In defense of the statute, the attorney general explained that only material that its office had probable cause to believe constituted child pornography was requested to be removed. The court found that the probable cause showing did not save the statute (nor did the fact that the attorney general only issued "Informal Notices" not court orders, and that the process was therefore "voluntary" not coercive⁶⁷). First, the court explained that in

⁶⁶ For the Court's interpretation of the expeditiousness requirement, see *Thirty-Seven Photographs*, 402 U.S. at 372-74 (delays in judicial determination as long as three months could not be sanctioned; accordingly, federal statute imposing prior restraint must be construed to require a judicial decision within 60 days to uphold the constitutionality of the statute); *Kingsley Books, Inc. v. Brown*, 354 U.S. 436 (1957) (requiring a trial one day after the joinder of issues and a resolution within two days after the trial); *Interstate Circuit, Inc. v. City of Dallas*, 390 U.S. 676, 690 n. 22 (1968) (holding prompt judicial review was assured by provision requiring a judicial determination within nine days of the decision of the administrative body); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963) (noting that prior restraint on speech "tolerated . . . only where it . . . assured an almost immediate judicial determination of the validity of the restraint"); *Redner v. Dean*, 29 F.3d 1495, 1501-02 (11th Cir.1994) (holding that prompt judicial review is never available when judicial review may not be sought until exhaustion of administrative remedies under a scheme that fails to provide adequate time restraints for administrative decision), *cert. denied*, 514 U.S. 1066 (1995); *cf.* *East Brooks Books, Inc. v. City of Memphis*, 48 F.3d 220, 225 (6th Cir.1995) (indicating that potential delay of five months from application to judicial hearing is impermissible).

⁶⁷ On this point, the court explained that the informal and technically noncoercive nature of the attorney general's removal requests did not insulate them from constitutional scrutiny. The court

order to comply with the Supreme Court’s exacting requirements, to be constitutional, a valid final prior restraint must be imposed by a judicial determination in an adversary proceeding. The attorney general’s determination that there was probable cause that the material was illegal was insufficient. Further, even an ex parte judicial determination that the material was illegal would not suffice to impose a constitutional final prior restraint because it did not result from an adversarial proceeding. As the United States Supreme Court explained in *Freedman*, “only a judicial determination *in an adversary proceeding* ensures the necessary sensitivity to freedom of expression.”⁶⁸ Ex parte judicial determinations that are made in the absence of notice and an opportunity to be heard on the part of the adversely-affected speaker are constitutionally deficient, and ex parte *nonjudicial* determinations are constitutionally deficient by an even greater measure.

Under many of the filtering systems implemented in other countries, provisions do exist for some sort of appeal of the censorship decision. However, such provisions for appeal generally do not provide for *judicial* determination and instead merely provide for a second look by the administrative body that made the censorship determination in the first place. In the UK, for example, the IWF website indicates that “any party with a legitimate association with the [blacklisted] content . . . who believes they are being prevented from accessing legal content may appeal [broken link] against the accuracy of an assessment.”⁶⁹ The appeal procedure provided by the IWF, however, does not contemplate judicial review. (Further, as discussed above, it is unclear how a party would learn that the content she was seeking, or seeking to make available, was subject to the IWF’s blacklist, since the Cleanfeed system merely provides Internet users with a generic 404/File not found error message when a requested website is on the IWF blacklist.) Rather, the appeal involves a second look by the IWF itself, and following that, a review by a police agency, whose assessment is final.⁷⁰ Similarly, the Canadian Cybertip filtering system allows for an affected content provider to appeal the initial censorship decision, but that appeals process also does not contemplate judicial review. Rather, the Canadian appeals process provides for a second look by Cybertip Canada personnel, and then ultimately to a review by National Child Exploitation Coordination Centre – a branch of the Canadian Police Centre for Missing and Exploited Children⁷¹ -- whose decision is final.⁷² Such provisions for

explained that removal requests issued by law enforcement officials were not interpreted by the recipient ISPs as being voluntary, even if technically they did not have the force of law.

⁶⁸ *Freedman v. Maryland*, 380 U.S. 51 (1965).

⁶⁹ See <http://www.iwf.org.uk/services/blocking/blocking-faqs#WhatisthecriteriaforaURLtobeaddedtothelist>.

⁷⁰ See IWF Content Assessment Appeal Process, at <http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process>

⁷¹ See <http://www.rcmp-grc.gc.ca/ncecc-cncee/index-accueil-eng.htm>

⁷² See http://www.cybertip.ca/app/en/Cleanfeed_p1#anchor_menu

appeal – because they do not provide for a judicial determination of the affected parties’ rights – fail to accord the requisite protections for freedom of expression.

In summary, nationwide filtering systems – the likes of which are now being imposed by over 40 countries worldwide, and whose numbers Venezuela apparently seeks to join – embody prior restraints on speech, which are inconsistent with the commitments articulated in the American Convention on Human Rights and which violate the due process requirements inherent in the free speech guarantee, absent the inclusion of fundamental process-based safeguards. These free speech due process requirements mandate that such prior restraints implemented by filtering systems be imposed subject to *clear and precise definitions of the speech to be regulated*; implemented *in an open and transparent manner*, such that affected Internet users and content providers are provided with information that the content was blocked and the reason for such blocking; and such that the filtering system provide Internet users and content providers with the *opportunity to appeal any such blocking decisions*, to a *judicial body and in an expeditious manner*. Only such “sensitive tools” for distinguishing between protected speech and unprotected speech can adequately protect individuals’ free speech rights.

Conclusion

To preserve and protect the Internet as a forum for the uninhibited, robust, and wide-open⁷³ exchange of ideas and information in the Americas, governments must take active steps to facilitate such free speech values. The relationship between governments and Internet service providers is of pre-eminent importance in this regard, as ISPs are in the position to be the facilitators of the free flow of information and ideas. On the one hand, ISPs should not be shackled with intermediary liability for hosting harmful content. On the other hand, ISPs should not be granted the discretion to restrict communications flowing through their pipes that they disfavor for one reason or another; rather, they should be subject to meaningful net neutrality regulations requiring them to facilitate all communications without discrimination or censorship. To encourage the free flow of information on the Internet, governments should also provide protections to Internet users to speak anonymously or pseudonymously. Such protections are integral to the right to speak critically in the political and civil realms, and should be preserved in the Internet age. Finally, governments themselves should not engage in censorship of Internet speech, consistent with our shared commitment in the Americas to forgo prior restraints on expression. However, if countries *do* engage in any filtering of unlawful Internet content – as many countries throughout the world are now doing – they should ensure that such state-mandated filtering systems adhere to the most speech-protective procedures and “sensitive tools” for distinguishing between protected and unprotected speech.

⁷³ *New York Times v. Sullivan*, 376 U.S. 254, 268 (1964) (describing “profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open”).