Washington Journal of Law, Technology & Arts

Volume 7 | Issue 3 Article 6

1-1-2012

Internet as a Human Right: A Practical Legal Framework to Address the Unique Nature of the Medium and to Promote Development

Young Joon Lim

Sarah E. Sexton

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 3 WINTER 2012

ESSAY

INTERNET AS A HUMAN RIGHT: A PRACTICAL LEGAL FRAMEWORK TO ADDRESS THE UNIQUE NATURE OF THE MEDIUM AND TO PROMOTE DEVELOPMENT

Young Joon Lim and Sarah E. Sexton[*]

Cite as: 7 Wash J.L. Tech. & Arts 295 (2012)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1114

ABSTRACT

A Taiwanese court sentenced a blogger to 30 days of detention for her comments that a restaurant's food was too salty and that the locale was unsanitary. In Indonesia, a woman was sentenced to six months in jail for libel after an e-mail she sent to friends about poor treatment she received in a hospital was posted on Facebook. These are not isolated cases of persecution, but part of a broad pattern of challenges facing individuals around the world. The United Nations recently released a report on legal trends involving restriction of expression on the Internet, declaring that freedom of expression on the Internet is a human right. If Internet freedom is a human right, what are the limits of that entitlement? This Essay explores existing legal models and restrictions on online communication through case studies, including discussion of restrictions in countries affected by the Arab Spring of 2011. This Essay suggests six basic elements for a legal framework that can support the unique challenges presented by the Internet as it becomes a primary mode of communication.

---

[*] Sarah E. Sexton, UC Berkeley, School of Law (Boalt Hall), Class of 2010. Young Joon Lim, Ohio University, E.W. Scripps School of Journalism, Ph.D. Candidate 2013. Thank you to our families, Dr. Michael Sweeney, and Alicia Hoffer for her assistance with this publication.

TABLE OF CONTENTS

INTRODUCTION

The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, recently released a report on the trends and challenges facing

freedom of expression, with particular concentration on the Internet.[1] The report received a great deal of press attention and was greeted with headlines such as, "The U.N. Declares Internet Access a Human Right."[2] Some articles have questioned the notion of Internet access as a human right, and the headlines raise the question of whether access to and freedom of expression on the Internet are deserving of the same respect as other human rights. What is the place of such rights in existing legal systems? What legal framework can be used to protect such rights on the Internet, a milieu that is often thought of as wild, borderless, and anonymous?

The Internet and other new telecommunications technologies affect many facets of society, and bring with them the opportunity to generate disagreements and discord. As such, societies need a way to resolve these disputes while protecting the interests of the parties involved. A legal framework can help maintain order and bring resolution to conflicts. It is necessary for such a legal framework to address the unique challenges presented by the Internet as it becomes a primary mode of communication.

Across the globe, different approaches are emerging. Certain regimes have adopted approaches that infringe on their citizens' basic human rights. Restrictions on Internet access and online expression limit many of the freedoms considered to be basic human rights, as recognized by international bodies such as the United Nations. To bring greater legitimacy to the rights of citizens to access the Internet and freely post online, a legal framework recognizing access to the Internet and freedom of expression online as human rights should be adopted.

This Essay explores the treatment of Internet freedom as a human right and considers the limits to that entitlement. It considers existing legal models and restrictions on online communication and access.

---

[1] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, delivered to General Assembly*, U.N. Doc. A/HRC/17/27 (May 16, 2011) [hereinafter *Report of the Special Reporter*].

[2] Adam Clark Estes, *The U.N. Declares Internet Access as a Human Right*, ATLANTIC WIRE (June 6, 2011), http://www.theatlanticwire.com/technology/2011/06/united-nations-wikileaks-internet-human-rights/38526.

The analysis focuses on protecting freedoms.

I. WHY DOES INTERNET FREEDOM MATTER?

To some, the Internet may seem like a modern luxury, and the suggestion that Internet access should be considered a human right may seem exaggerated. This criticism might ring true if the right were an entitlement—if Internet access as a human right meant that governments should issue laptops to citizens and provide wireless connections. More realistically, access to the Internet and freedom of expression, opinion, and speech online are simply contemporary technological manifestations of the existing human right of freedom of expression, opinion, and speech as recognized by the International Covenant on Civil and Political Rights.[3] As technology adapts and presents new modes of communication, new forums for expression flourish. Because these rights are inherently tied to human and economic development, freedom of expression online and access to the Internet deserve international attention and global, cooperative enforcement.

It is important to recognize that rights and development are intertwined in a way that is simultaneous and codependent. Here, whether recognition of expression rights fosters development, or whether development is itself exertion of rights, is beyond the scope of this analysis. The Internet has proven an effective tool for the promotion and protection of human rights by disseminating information.[4] It is an enabler of other economic, social and cultural, as well as civil and political, rights.[5]

The Internet's speed also facilitates rapid action to respond to human rights violations and may supply accurate, real-time information. Human rights organizations are able to use the Internet in their operations in innovative ways. Also, the Internet serves as a

---

[3] International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), 21 U.N. GAOR, 21st Sess., Supp. No. 16 at 52, U.N. Doc. A/6316 (Dec. 16, 1966), *available at* http://www2.ohchr.org/english/law/ccpr.htm [hereinafter Covenant on Civil and Political Rights].

[4] HUMAN RIGHTS AND THE INTERNET 7 (Steven Hick, Edward F. Halpin, & Eric Hoskins eds., 2000).

[5] *See Report of the Special Reporter*, *supra* note 1, at 7.

means to educate, organize and track information about human rights violations.[6] An example of the Internet's ability to quickly disseminate on-the-ground information is the way postings from Tunisians' Facebook pages during the revolution of 2011 were collected, translated, and reposted on the website Nawaat, an independent blog produced by Tunisians in exile.[7] The information then passed via Twitter to mainstream journalists.[8]

Furthermore, access to information and a free press increase transparency, reduce corruption, stir debate, and keep pressure on governments. The Internet is a means of gaining broader political participation, and it sparks dialog to influence government and the democratic process.[9] As a medium, the Internet is unique in making it easier for a broader range of voices to access information without the influence of institutions or entrenched power-holders. Citizen journalists spread their messages and their realities through the eyes of those on the ground. Bloggers and online forums offer alternative sources of information. Governments are less able to control the flow of information than through traditional media.[10]

The borderless nature of the Internet is an international exchange point. Movements can be trans-nationalized and build support from and solidarity with individuals across the globe.[11] During the Arab Spring uprisings in early 2011, for example, the governments of China and Iran attempted to block the flow of images and information of the uprisings on their news networks and Internet.[12] In China, the reaction was strong because the government feared a "Jasmine

---

[6] Lloyd Axworthy, *The Mouse is Mightier than the Sword*, *in* HUMAN RIGHTS AND THE INTERNET 16, 19 (Steven Hick, Edward F. Halpin, & Eric Hoskins eds., 2000).

[7] JEFFREY GHANNAM, SOCIAL MEDIA IN THE ARAB WORLD: LEADING UP TO THE UPRISINGS OF 2011 16 (2011), *available at* http://cima.ned.org/sites/default/files/CIMA-Arab_Social_Media-Report%20-%2010-25-11.pdf.

[8] *Id.*

[9] Bruce Etling, Robert Faris & John Palfrey, *Political Change in the Digital Age: The Fragility and Promise of Online Organizing*, 30 SAIS REV. 37 (Summer-Fall 2010), *available at* http://dash.harvard.edu/handle/1/4609956.

[10] *Id.*

[11] Simon Cottle, *Media and the Arab Uprisings of 2011: Research Notes*, 12 JOURNALISM 647, 654 (2011), *available at* http://www.contexting.me/files/CottleMediaandtheArabUprising.pdf.

[12] *Id.* at 655.

Revolution" modeled on the pro-democracy protests that were spreading across the Arab world.[13]

The decentralized associations and loose networks formed through the Internet just described enable change in authoritarian regimes.[14] Yet such regimes are simultaneously becoming more sophisticated in blocking, tracking, and limiting Internet access and online expression. States have begun to monitor and filter online content and posters, including through cyber-attacks, threats, and intimidation. Governments also have employed the law as a means to control online speech.[15] China and Iran stand out as the most egregious in their control of online information. Still, several dozen countries filter the Internet, such as Burma, Tunisia, Uzbekistan, and Vietnam.[16]

II. EXISTING FRAMEWORK

A. Legitimate Restrictions

While the freedoms of speech, expression, and opinion are well-recognized among the international community, even absolutists recognize that there are appropriate boundaries to these freedoms. For example, certain types of expression are restricted to promote public safety and the interests of society. Examples of restricted speech include child pornography; hate speech; direct and public incitement to commit genocide; and advocacy of national, racial, or religious hatred that constitutes incitement to discrimination or violence.[17] While some restrictions are absolute and serve to protect the rights of individuals, such as the right to life,[18] a gray area emerges surrounding legal concepts such as defamation. Different cultures take varying approaches as to how to distinguish between legitimate and restricted expression. The following sections describe some of the existing structures.

---

[13] *Id.*
[14] Etling, Faris & Palfrey, *supra* note 9.
[15] *Id.*
[16] *Id.*
[17] *See Report of the Special Reporter*, *supra* note 1, at 8.
[18] *Id.*

B. Article 19

Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, as adopted by the General Assembly of the United Nations, provides that everyone has the right to express his or herself through any media.[19] Article 19 guarantees that every person has the right to hold opinions without interference and to freedom of expression, including freedom to seek, receive, and impart information and ideas of all kinds. Notwithstanding, Article 19 includes limits aimed at protecting national security, public order, public health, morals, and the rights and reputations of others.[20]

The U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression interprets Article 19 to be so inclusive as to adapt to any modern technological development. The broad language of the article was drafted with the foresight to accommodate the Internet and the burst of new modes of media.[21]

C. Comment 34

In July 2011, the United Nations Human Rights Committee adopted General Comment 34 to Article 19, suggesting that freedom of opinion and of expression are "indispensable conditions for the full development of the person."[22] The comment further states that these freedoms are essential for any society. Freedom of expression is necessary for government transparency and accountability, two elements essential for the promotion and protection of human rights. General Comment 34 specifically states that means of expression include the Internet and all forms of audio-visual and electronic and

---

[19] Covenant on Civil and Political Rights, *supra* note 3.

[20] Mark Erik Hecht & Rodney Neufeld, *The Internet and International Children's Rights*, *in* HUMAN RIGHTS AND THE INTERNET 153-54 (Steven Hick, Edward F. Halpin, & Eric Hoskins eds., 2000).

[21] *See Report of the Special Reporter*, *supra* note 1.

[22] Human Rights Committee, *General Comment No. 34, Article 19: Freedoms of Opinion and Expression*, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011).

Internet-based modes of expression.[23] The comment emphasizes that states should take into account developments in technologies and how communications have changed as a result. Comment 34 encourages states to foster the independence of new media and to ensure access to them.

Comment 34 does not advocate unfettered discretion for the restriction of freedom of expression; it suggests that laws must guide authorities as to what type of expression may be properly restricted. Specifically, Comment 34 supports the restriction of freedom of expression in order to protect other rights. Restrictions "on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines" are only permissible to the extent that they are compatible with promoting human rights, transparency, and accountability. Comment 34 also condemns prohibiting the publication of material solely on the basis that it may be critical of a government or political system.

Comment 34 also addresses defamation, the treatment of which has been a point of contention in regulation of speech. The comment advocates for the precise tailoring of defamation laws to ensure that they comply with the principles of transparency and accountability, suggesting the decriminalization of defamation. Laws that criminalize defamation should leave room for defenses of truth and not be applied to "those forms of expressions that are not, of their nature, subject to verification."[24] Comment 34 also suggests a greater amount of leeway with respect to public figures when the published statements are untrue but published without malice. The Comment states that imprisonment is never an appropriate punishment for defamation.

III. EXISTING EXAMPLES OF GOVERNMENT TREATMENT OF THE INTERNET

National governments allow varying degrees of Internet freedom

---

[23] *Id.*
[24] *Id.*

and take different approaches to policing online expression. Section A discusses restrictions on Internet expression imposed by authoritarian regimes in the Middle East. Section B discusses criminalization of Internet speech in various countries. Section C describes attempts to regulate online expression through private intermediaries. Section D discusses attempts in the U.S. to restrict online speech.

A. Restrictions on Access and Criminalization of Content

Governments have used blocking or filtering technologies to limit access to specific websites or to completely halt access to the Internet in order to quash undesired communications. These restrictive actions may legitimately be used to target undesired information, yet there is danger that blocking can be administered in arbitrary, secretive, and excessive ways.[25] This impedes the freedom of expression as set out in Article 19, paragraph 3 of the International Covenant on Civil and Political Rights.[26] As blocking stops more than the targeted information, its broad application is over-inclusive. Lastly, blocking is often done without the possibility for judicial review or independent monitoring.[27]

Blocking garnered international attention during the Arab Spring, during which challenged governments shut down Internet access in attempts to stop organizers and other protestors from spreading their message, rallying support, and planning their strategy online. While it is too early to comment on the effect these uprisings have wrought on domestic Internet policies, we can reflect on the systems that were in place in these countries at the time of the uprisings.

The governments, challenged by the uprisings, tried to censor and contain the dispersal of images and information by cutting the cord on the Internet, in addition to monitoring telecommunications and limiting the entry and mobility of foreign journalists. Repressive regimes deploy sophisticated digital censorship and monitoring capabilities, and they sometimes engage in cyber attacks against

---

[25] *See Report of the Special Reporter*, *supra* note 1, at 10.
[26] Covenant on Civil and Political Rights, *supra* note 3.
[27] *See Report of the Special Reporter*, *supra* note 1, at 10.

dissidents.[28] For example, in April 2008 the Egyptian government quashed a group of online organizers attempting to carry out a strike against the government by tracking them down via their digital footprints. A video of one such organizer's tearful release was widely-viewed on YouTube, and served as a powerful tool of repression.[29]

1. Egypt

In Egypt, prior to the overthrow of Mubarak in 2011, politically sensitive websites were blocked. While no law specifically gave the government power to filter such websites, the Penal Code and the Emergency Law provided the government with the authority to restrict and monitor communications.[30] Egypt's Emergency Law allowed authorities to detain individuals for long periods of time without a hearing. Egypt also relied on extralegal enforcement. It allowed censorship, indiscriminate confiscation, and forced closures as the Ministry of Interior saw fit.[31] Freedom of the press and freedom of expression faced severe limits. Egypt's Press Law criminalized criticizing the president or the leaders of foreign countries and spreading false news.[32] This law also applied to online communications. Online writers and bloggers were harassed and detained for their online and offline activities.[33] For example, in 2003 state officials detained activist Ashraf Ibrahin on charges of "spreading false news" for e-mailing stories and photographs of police violence at anti-war demonstrations to international human rights organizations.[34]

While the Mubarak government did not support unlimited access to content, it recognized the importance of access to the Internet. The Egyptian government implemented programs to expand Web access.

---

[28] *See* EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM (2011).

[29] Etling, Faris & Palfrey, *supra* note 9, at 37-49.

[30] ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 276 (Ronald Deibert et al., eds. 2008) [hereafter ACCESS DENIED].

[31] *Id*.

[32] *Id*.

[33] *Id*. at 278.

[34] *Id*.

The government started the Free Internet Program, which allowed users to access the Internet for the price of a local telephone call. This program served as a model for other developing countries. Egypt grew to have the largest fixed-line communications network in the Arab world.[35] Many Egyptian Internet users do not have personal computers but rely on Internet cafés. Internet café owners were required to obtain a license from the Ministry of Telecommunications to operate. Internet café owners also reported that security officials instructed them to keep lists of their customers and the customers' identification numbers. With four licensed Internet carriers, eight data service providers, and hundreds of Internet service providers, it is ironic that the same government which promoted this access was the same government brought down by the many people who expressed their opinions and organized online.

It is not clear what has changed following the end of the Mubarak government. The same week Mubarak was arrested, blogger Maikel Nabil was sentenced to three years in prison for "insulting the military."[36] Also, the Supreme Council issued a letter to Egyptian editors ordering them not to report on the armed forces without advanced permission. The head of the Armed Forces Morale Affairs Department, General Ismail Etman, stated at a news conference, "Freedom of expression is guaranteed as long as it is respectful and doesn't question the armed forces."[37]

The bloggers and online writers in Egypt still straddle the line between political activists and citizen journalists, speaking to topics that mainstream journalists cannot touch. These writers serve as an alternative source for information to audiences that distrust the mainstream media because of the legacy of governmental control.

2. Libya

The Libyan government systematically blocked and restricted access to the Internet. In particular, the government targeted political opposition, content critical of the government, and websites that

---

[35] *Id.* at 277.

[36] Lawrence Pintak, *Breathing Room: Toward a New Arab Media*, COLUM. JOURNALISM REV., May/June 2011, at 23.

[37] *Id.*

advocate the rights of the minority group Amazigh (Berbers).[38] The country's press laws established many restrictions, punishable by large fines and imprisonment, and made private media illegal. The laws have also been applied to expression on the Internet. Anyone convicted of disseminating information that conflicted with the constitution or "fundamental social structures," or that tarnished Libya's image abroad, could be punished with life imprisonment or even death under Libya's penal code.[39] Also, in order to obtain a ".ly" domain name, Libya's top-level domain, a website "must not contain obscene, scandalous, indecent, or contrary to Libyan law or Islamic morality words, phrases or abbreviations."[40]

3. Syria

The Syrian government has relied on vague and overly broad laws to attack various types of information. The government blocks pornographic websites and censors websites with "pro-Israel or hyper-Islamist" bents and those calling for autonomy for Syrian Kurds.[41] Syria's government maintains regulatory control over Internet service providers ("ISPs"). Internet café owners must obtain a license from the Telecommunications Department's local office and must follow the Conditions Manual, which includes specifications on the spacing between computers.

Syria's constitution protects "the right to freely and openly express his views in words, in writing, and through all other means of expression" and "the freedom of the press, of printing, and publication in accordance with the law." However, other legislative provisions allow the government to restrict these rights. For example, Article 4(b) of the 1963 Emergency Law authorizes the government to monitor all publications and communications and to arrest anyone whose crimes constitute "an overall hazard."[42] Moreover, the Press Law of 2001 gives the government control and censorship of all print media. This same law penalizes the printing of falsehoods or

[38] ACCESS DENIED, *supra* note 30, at 276.
[39] *Id.* at 321.
[40] *Id*. at 323.
[41] *Id*. at 380.
[42] *Id*. at 382.

fabricated reports and writing on topics relevant to "national security or national unity" is forbidden. The government applies these laws to online publications as well.[43] The government has prosecuted individuals for e-mailing photos or articles produced by another political party, posting information exposing police crackdowns, and voicing opposition to the government. These actions have created fear, which also leads to self-censorship.

4. Tunisia

The Tunisian government deployed a system of laws, regulations, and surveillance to keep tight control over the Internet. ISPs were required to send the Ministry of Telecommunications a list of their subscribers each month.[44] Also, ISPs, Web page owners, and Web server owners were responsible for policing the content of the pages and servers they hosted.[45] They had to ensure that content adhered to the Press Code's rules. In particular, the content could not upset public order.[46] All fixed-line Internet traffic passed through facilities controlled by the Tunisian Internet Agency, an entity established by the Ministry of Telecommunications charged with regulating the Internet and domain name system.[47] The government loads SmartFilter software onto the agency's servers and may filter content across the country's ISPs.[48]

B. Criminalization of Online Expression and Defamation

Some states have gone so far as to criminalize online expression even when it is legitimate (*i.e.*, not falling into the protected categories discussed above in Section II(A)). Some governments have applied existing criminal laws to online expression, while others have enacted new laws designed for online expression.[49] These laws are

---

[43] *Id.* at 382.
[44] *Id.* at 397.
[45] *Id.*
[46] *Id.* at 398.
[47] *Id.* at 395.
[48] *Id.* at 397.
[49] *See Report of the Special Reporter*, *supra* note 1, at 10.

premised on the basis of protecting reputation and national security and on countering terrorism. In practice, they allow governments to censor and stifle dissent.[50]

Reporters Without Borders reported that in early 2012, 153 people were imprisoned on charges related to the content of their online postings.[51] The countries with the most imprisoned bloggers were China (68 prisoners), Iran (20), and Vietnam (18).[52]

The Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression disapproves of imprisonment as a punishment, arguing it is a disproportionate response to imparting information. Instead, it advocates for the decriminalization of defamation. Defamation is a communication that tends to damage another's reputation. It includes any publication that exposes a person to distrust, hatred, contempt, ridicule, or anything that may impute incompetence, incapacity, or unfitness in the performance of an individual's trade, occupation, or profession.[53] The report further instructs that criminal protections in the name of national security or counter-terrorism should be limited to situations in which the government can demonstrate that: "(a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence."[54]

As forums to express one's opinion about businesses, services, and government are becoming increasingly prevalent on the Internet, people describe their unfortunate experiences or post harsh reviews of poor customer service. But there are more opportunities for the recipients of reviews to react.

For example, a simple statement ("The beef noodles were too salty") posted on a review website may have been an honest reaction

---

[50] *Id.*

[51] Reporters Without Borders, *Press Freedom Barometer 2012*, http://en.rsf.org/press-freedom-barometer-netizens-imprisoned.html?annee=2012 (last visited Feb. 11, 2012).

[52] *Id*.

[53] GEORGE L. BLUM, CRITICISM OR DISPARAGEMENT OF DENTIST'S CHARACTER, COMPETENCE, OR CONDUCT AS DEFAMATION, 120 A.L.R. 5TH 512 (2004).

[54] *See Report of the Special Reporter*, *supra* note 1, at 11.

to a less-than-stellar meal, but it also amounted to an arrestable offense in Taiwan. In June of 2011, The Taichung branch of the Taiwan High Court sentenced Taiwanese blogger Liu to 30 days in detention, suspension for two years, and a fine of 200,000 New Taiwan Dollars payable to the restaurant that received the below-average review. Liu wrote that the restaurant's food was too salty and that the locale was unsanitary and infested with cockroaches. She also criticized the way the owner let customers park their cars. The restaurant owner filed charges against her and accused her of defamation. The Taichung District Court ruled that the blog post exceeded reasonable bounds. While the court found that her comment about the cockroaches was narration of facts and not intentional slander, it found that the comments about unsanitary conditions were untrue based on health inspector reports.[55]

In Indonesia, Prita Mulyasari was sentenced to six months in jail for libel after she emailed her friends about the poor treatment she received at the Omni International Hospital. When the hospital misdiagnosed her with dengue fever, she e-mailed 20 of her friends about her experience. The friends then posted her criticism of the hospital on their Facebook pages without her knowledge. The hospital pursued criminal and civil cases against Mulyasari. Initially, the courts rejected both cases, but prosecutors appealed. The Supreme Court convicted Mulyasari of libel under the Electronic Information and Transactions Law. While the law allows for six years in jail as punishment, Mulyasari received a suspended six-month jail term.[56]

These are not isolated cases, but part of a broader challenge facing individuals around the world. Criminalization of defamation remains a hotly contested topic at the international level.

C. Intermediary Enforcement

Because the Internet depends largely on private companies to provide access, connectivity, hosting, and online forums, ensuring

---

[55] Lin Liang-che, *Blogger Given Suspended Prison Sentence Over Critical Restaurant Review*, TAIPEI TIMES (Jun. 23, 2011), http://www.taipeitimes.com/News/taiwan/archives/2011/06/23/2003506487.

[56] *Indonesia Woman Gets Suspended Term for Facebook Libel*, BBC NEWS (Jul. 11, 2011), http://www.bbc.co.uk/news/world-asia-pacific-14104471.

freedom of online expression poses additional challenges. ISPs and online platforms have enjoyed relative immunity from liability for third-party content communicated via their services. However, some governments have begun to recognize these intermediaries as a more easily-reached link in controlling communications. As a result, legal protections for these intermediaries are eroding.[57] Countries may call upon ISPs to cut service to individuals or larger populations. They may also try to hold companies accountable for content posted by third-parties on their websites. For example, the European Union has a policy of notice and takedown that protects the intermediary.[58] The process is not transparent, and it is executed by the private company.

Intermediary enforcement is inherently problematic in a capitalist marketplace. A neutral body is needed to enforce the rules and ensure a level playing field. The U.N. Special Rapporteur suggests that intermediaries should: only enforce restrictions after judicial intervention; be transparent to users or the wider public about the measures they take; and, if possible, warn users before the implementation of restrictive measures.[59] Most importantly, La Rue suggests intermediaries limit their enforcement to the content at issue. As a parallel, users should have a means of appealing any enforcement action.[60]

The public-forum doctrine has emerged in response to these concerns. This doctrine recognizes that speech should be protected online but that not all online speech is the same. The case law creates three categories: (1) traditional public forums, (2) designated public forums, and (3) nonpublic forums. Regulation of speech within nonpublic forums is not subject to the same level of scrutiny as speech in public forums.[61] As mentioned above, the vast majority of online forums rely on a privately owned company. The private company regulates content. This creates an Internet with virtually no public spaces.[62] Thus, the level of scrutiny applied to restrictions of

---

[57] *See Report of the Special Reporter*, *supra* note 1, at 11.

[58] *Id*.

[59] *Id.* at 14.

[60] *Id*. at 21.

[61] DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE 71 (2009).

[62] *Id*. at 77.

Internet speech is low.

In the United States, the law generally protects ISPs and websites from liability for content passed through their services. Section 230 of the Communication Decency Act (CDA) of 1996 provides immunity from liability to ISP's that publish information offered by third parties.[63] Under Section 230, it is usually difficult to hold ISPs accountable, but this norm is not without exception. Recent cases involving MySpace and Craigslist indicate courts may be amenable to the idea of holding websites accountable for actions resulting from information they transmit.[64] In *Doe v. MySpace*, the Fifth Circuit affirmed the district court's ruling that Section 230's "Good Samaritan" provision barred the plaintiff's negligence action against MySpace for failure to protect her underage daughter from a predator she met on the social networking site.[65]

In *Doe IX v. MySpace*, the district court in Texas granted a motion to dismiss a suit brought by the parent of a child who was assaulted by a sexual predator the child met on MySpace.[66] There, the court, unlike the Fifth Circuit, considered and found that MySpace was partially responsible for creating information exchanged.

In *Chicago Lawyers' Committee For Civil Rights Under Law, Inc. v. Craigslist, Inc.*, the Seventh Circuit held that Craigslist had not violated the Fair Housing Act by allowing rental advertisements that stated preference with respect to race, religion, sex, or family status.[67] While the court ruled in favor of Craigslist yet again under the protections of Section 230, it noted that Section 230 immunity does not apply to online service providers when they "materially contribute" to the unlawfulness of the content.[68] As the Ninth Circuit explained in *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, "the Communications Decency Act was not meant to create a lawless no-man's-land on the Internet."[69]

---

[63] 47 U.S.C. § 230 (2006).

[64] *See* Shahrzad Radbod, *Craigslist—A Case for Criminal Liability for Online Service Providers?*, 25 BERKELEY TECH. L.J. 1 (2010).

[65] Doe v. MySpace, 528 F.3d 413 (5th Cir. 2008).

[66] Doe IX v. MySpace, 629 F.Supp. 2d 663 (E.D. Tex. 2009).

[67] Chicago Lawyers' Comm. For Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008).

[68] *Id*.

[69] Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521

Most recently, in August of 2011, the Internet company Google entered into a settlement agreement in which it forfeited $500 million to the United States Department of Justice after it was targeted for content advertised through its online AdWords program. Google sold ads through AdWords to Canadian pharmacies advertising drugs to U.S. audiences. Google agreed to pay a $500 million settlement.[70] This amount represents the estimated revenue the Canadian pharmacies received from their sales to the United States consumers. Google was aware that the Canadian pharmacies were illegally shipping prescription drugs into the United States. Google blocked other countries' pharmacies from doing the same but continued to sell advertisements to the Canadian pharmacies. In 2009, Google stopped these sales when it became aware of the government's investigation.[71] In the agreement, Google acknowledges improperly assisting Canadian online pharmacy advertisers in running advertisements that targeted a U.S. audience.[72] The government stated that it would hold companies accountable for violating "federal law and put[ting] at risk the health and safety of American consumers."[73] At this point, it is unclear how far this reach will extend to Internet companies.

The lesson gleaned from the above cases involving Craigslist, MySpace, and Google is that even in the United States the government puts pressure on private Internet companies to police third-party content communicated via their websites. This responsibility places an added burden on companies and serves as a hurdle to emerging Web-based businesses.

F.3d 1157, 1164 (9th Cir. 2008).

[70] Press Release, Department of Justice, Google Forfeits $500 Million Generated by Online Ads & Prescription Drug Sales by Canadian Online Pharmacies (Aug. 24, 2011), http://www.justice.gov/opa/pr/2011/August/11-dag-1078.html.

[71] David Goldman, *Google pays $500 Million to Settle DOJ Case Over Illegal Drug Ads*, CNN MONEY (Aug. 24, 2011), http://money.cnn.com/2011/08/24/technology/google_settlement.

[72] Department of Justice, *supra* note 70.

[73] *Id*.

D. Attempts to Regulate Online Speech in the U.S.

In the United States, case law suggests that the Internet enjoys broad First Amendment rights like those afforded to print media.[74] However, Congress has considered the idea of applying broadcast-like indecency standards to the Internet as part of telecommunications legislation. Congress attempted this through the Communications Decency Act (CDA). The purpose of the broader act was to reduce regulation and encourage "the rapid deployment of new telecommunications technologies."[75] However, the United States Supreme Court held that the anti-indecency provisions of the CDA violated the First Amendment because the regulations were a blanket, content-based restriction on the freedom of speech.[76] The challenged provisions of the CDA sought to protect minors from harmful material on the Internet. The CDA did not limit itself to particular times or individuals. Nor did it recognize the unique nature of Internet communications. Further the CDA did not define "indecent" communications.[77] Courts interpreting the First Amendment distinguish between "indecent" and "obscene" sexual expressions, protecting only those that are indecent.[78]

Advocates of free speech and freedom of information have lobbied legislatures for federal and state net neutrality legislation that would prohibit ISPs from discriminating against any legal content they transmit.[79] In 2007, members of Congress introduced the Internet Freedom Preservation Act of 2007, which would have amended the Communications Act of 1934, making it unlawful for any ISP to "block, interfere with, discriminate against, impair, or degrade the ability of any person to use a broadband service to access, use, send, post, receive, or offer any lawful content, application, or service made available via the internet" or to change on the basis of the type of content the applications or services made

---

[74] KENNETH CREECH, ELECTRONIC MEDIA LAW AND REGULATION 373 (2003).
[75] Reno v. Am. Civil Liberties Union, 521 U.S. 844, 857 (1997).
[76] *Id.* at 868.
[77] *Id.* at 865.
[78] Sable Communications v. FCC, 492 U.S. 115, 126 (1989).
[79] NUNZIATO, *supra* note 61, at 131.

available.[80] Acts by the same name were proposed in 2008 and 2009, yet all have died in Congress. The proposed Blogger Protection Act of 2008 also failed to make it out of committee.[81] This bill would have amended the Federal Election Campaign Act of 1971 to protect uncompensated Internet activity from being treated as a contribution.[82]

The push for net neutrality continues in the United States, despite opposition by interested parties. However, Internet expression has flourished within the U.S. because of laws that provided the Internet industry great protections.[83] Without a law like Section 230 of the CDA, service providers would, at the very least, confront a multitude of lawsuits.[84]

IV. ESTABLISHING A LEGAL FRAMEWORK FOR PROTECTING INTERNET AS A HUMAN RIGHT

A. Essential Elements for a Legal Framework

Information on the Internet is not confined to the same geographical boundaries as states. Thus, if a state passes laws to control material in its own jurisdiction, this does not stop its citizens from accessing or distributing illegal material through other countries.[85] To be truly effective in blocking all prohibited material, jurisdiction and enforcement would have to be situated at the international level. Governments have come to understand that independent censorship is not as effective as international cooperation.[86] At the international level, the Internet is governed by voluntary codes of practice, public awareness campaigns, education, and other morally persuasive solutions.[87]

---

[80] S. 215, 110th Cong. (2007).

[81] *H.R. 5699 (110th): Blogger Protection Act of 2008*, GOVTRACK.US, http://www.govtrack.us/congress/bills/110/hr5699 (last visited April 8, 2012).

[82] *Id.*

[83] Daithí Mac Síthigh, *The Right to Communicate*, PUBLIUS PROJECT (Nov. 29, 2008), *available at* http://publius.cc/right_communicate.

[84] *Id.*

[85] HUMAN RIGHTS AND THE INTERNET, *supra* note 4, at 160.

[86] *Id.*

[87] *Id.*

A legal framework is not only important out of respect for the rule of law, but it would have a practical impact on the lives of people and on the development of economies. The Internet allows individuals who once had no forum for expression or ability to compete with wealthy, dominant powers to communicate, advertise, and be heard with relatively little cost and fewer barriers than other modes of communication.

We suggest that an international legal framework be adopted to protect the rights of individuals, specifically their freedom of speech and access to the Internet. After review of the existing models, the following factors emerge as essential elements of a legal structure that is successful in protecting freedoms and fostering development. We suggest six factors that all legal systems should incorporate to protect and promote access to the Internet as a human right.

1. Proportionate Response

Any response to online expression should target the objectionable content and not block more information than is necessary, nor should access be denied entirely without just cause. The response should be precisely targeted at the particular matter of concern. Blocking access to the Internet in general should almost never be a response. A government's decision to restrict access to the Internet or content should only target legitimately threatening content that could incite violence or cause a threat to public safety. Also, legal systems should clearly define what activity would be regulated under criminal statutes and what activity should be enforced under a civil system. Criminal punishments for undesirable online content should be limited only to child pornography, hate speech, direct and public incitement to commit genocide, and advocacy of national, racial or religious hatred that incites discrimination or violence.[88] Governments should work to decriminalize defamation and move to a civil legal mechanism.

[88] *See Report of the Special Reporter*, *supra* note 1, at 8-9.

2. Constitutional Protections or Detailed Legislative Regulations

Criteria for which material a government may block and acceptable responses to offending information should be contained in published law. The regulations should be accessible to the public. As was observed above, many of the crackdowns on the Internet under Egypt's prior regime occurred outside the scope of defined law. This cannot be tolerated in a system where rule of law governs and people are able to dispute and challenge the regulations if enforced against them. Freedom of speech and expression online should be adopted as Constitutional protections. States should consider adopting specific laws to ensure that freedom of expression is protected online. States should also adopt programs to help improve access to the Internet, so that it does not become a tool controlled by a powerful few.

3. Neutral Body, Non-corporate Enforcement

A neutral enforcement body should be established to ensure that enforcement does not burden corporations or unequally empower them. The U.N. Special Rapporteur suggests that, to safeguard against abuse, such a body must have no commercial or political affiliations.[89] This body would also serve to protect the growth of Internet companies, because the companies would not be responsible for policing online activity as they would be in a system where they themselves were charged with enforcement.

As the Internet increasingly moves into position as the world's dominant mode of communication, it is a vehicle to spread truth, encourage transparency, hold governments accountable, and uncover corruption. Such a powerful tool should be open, free and accessible. Legal systems should be established to protect it and prevent it from being abused. An independent body charged with the ability to hear evidence and apply clear, nationally established regulations would be best equipped to uphold these ideals. The independent body could operate like an administrative court to weigh evidence for and against writers and posters of online content. This "Internet Court" could then issue decisions about whether online content should be blocked,

[89] *Id.* at 19.

removed, or edited.

4. Judicial Review

The decisions of the "Internet Court" should be appealable to a higher court within the state's existing legal system. A user whose rights have been infringed should have the ability to seek redress in a court of law.

5. Transparency

The criteria for deciding when to enforce restrictions on access and content should be established ex ante and publicized. The process undertaken to decide enforcement actions should also be documented and accessible to the public upon request. The proceedings of any "Internet Court" should be transparent and open to the public. The media should have access to this information in order to inform the public and hold the body accountable.

6. International Approach

In order for any legal system to enforce its regulations on such an international phenomenon as the Internet, it must be cognizant of its place in a broader context. It is just one player in a global web of authorities. Cooperation and partnership between jurisdictions may be the best way to address issues posed by online content. This element of international cooperation also arises because of the space for international conflict over treatment of the Internet.

International Cooperation may take the shape of joint education products or campaigns. It may also involve sharing of evidence and resources between enforcement bodies. As cyberlaw scholar Lawrence Lessig suggests, in order to protect fundamental values, social and legal power is structured and constrained not only by a legal text or constitution but also by a way of life—which he calls an "architecture."[90] He explains:

---

[90] LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 4 (2006).

> To regulate well, you need to know (1) who someone is, (2) where they are, and (3) what they're doing. But because of the way the Internet was originally designed . . . there was no simple way to know (1) who someone is, (2) where they are, and (3) what they're doing. Thus, as life moved onto (this version of) the Internet, the regulability of that life decreased. The architecture of the space—at least as it was—rendered life in this space less regulable.[91]

International enforcement is challenged with creating an Internet culture that is local and personalized, where societal norms apply.

CONCLUSION

Legal systems should incorporate these six factors in order to elevate as a protected human right a person's freedom to the Internet. This is particularly important as the medium becomes the dominant mode of communication, exchange of thought, and commerce. Internet as a human right serves as a tool, an instrument with which people can work and fight to achieve their other economic, social, cultural, civil, and political rights. It deserves the respect accorded to other human rights and other media.

---

[91] *Id.* at 23.