Journal of Technology Law & Policy

Volume XIV – Fall 2013

ISSN 2164-800X (online)

DOI 10.5195/tlp.2013.131

http://tlp.law.pitt.edu

Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice

Jeffrey (Chien-Fei) Li

Abstract

Internet censorship refers to a government's unjustified scrutiny and control of online speech or government-approved control measures. The danger of Internet censorship is its chilling effect and substantial harm on free speech, a cornerstone of democracy, in cyberspace. This article compares China's blocking and filtering system, Singapore's class license system, and the United States' government-private partnership model and identifies the features of each model. This article also explores the pros and cons of each model under international human rights standards. By finding lessons from each of the models, this article contends that Taiwan should retain its current minimal Internet control model. Further, Taiwan should fix flaws in its current Internet control system, including the private partnership model adopted by the Copyright Act, to be consistent with Article19.3 of the ICCPR.

Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice

Jeffrey (Chien-Fei) Li*

INTRODUCTION

In 2005, Telus, a Canadian telephone company and Internet Service Provider ("ISP"), blocked subscribers from accessing the Telecommunications Workers Union ("TWU") website.[1] The reason for the block, according to Telus, was to stop the TWU site from inciting workers to jam Telus's lines.[2] The TWU argued that the move was an act of censorship.[3]

A similar event occurred recently in Brazil. To comply with a court order, Google Brazil removed links to a video on YouTube that criticized a candidate in the Brazilian municipal elections.[4] The court order found that the video would "offend the dignity or decorum" of the candidate.[5]

Censorship, more specifically, Internet censorship is at the heart of the two cases. The concept of censorship, and just the word itself, evokes distaste and anxiety. Popular opinion opposes threats to the right to free speech and access to information in cyberspace.[6] In comparison, *Internet control* is a more innocuous term. China's regulation of the Internet is widely viewed as censorship, whereas the regulation by democratic Asian territories, such as Hong Kong and South Korea, is

* Harvard LL.M., 2013.

[1] *Telus cuts subscriber access to pro-union website*, CBC NEWS (July 24, 2005, 10:45 PM), http://www.cbc.ca/news/canada/story/2005/07/24/telus-sites050724.html.

[2] *Id.*

[3] *Id.*

[4] *Brazil: Google blocks YouTube video*, NEWS 24 (Sept. 28, 2012, 11:00 AM), http://www.news24.com/World/News/Brazil-Google-blocks-YouTube-video-20120928.

[5] *Id.*

[6] *See* LAWRENCE LESSIG, CODE VERSION 2.0, at 275 (2006) (concluding that the constitutional value of protecting freedom of speech should also be informed and used to constrain the state in architecting cyberspace).

Journal of Technology Law & Policy

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

viewed as Internet control.[7] For instance, Hong Kong's Crimes Ordinance and Telecommunications Ordinance, criminalize attempts to suppress information.[8] The Crimes Ordinance also punishes both a dishonest intent to deceive with a view of obtaining gain for oneself or another and a dishonest intent to cause loss to another.[9] In South Korea, the grounds for Internet control include defamation, child protection, obscenity, and subversive communication.[10] These are all legitimate reasons under South Korean laws for ISPs to block access to the Internet.[11] Christian Oliver of the *Financial Times* also reports that South Korea blocks access to North Korean websites.[12]

While South Korea's Internet control is generally considered more pervasive than Hong Kong's, it is not as rigorous as China's infamous Great Firewall.[13] Why does the world label China's Internet control as censorship, while other countries' Internet control systems do not incur such characterization? Is it simply because China is not a democracy? More specifically, at what point would we view the Internet control as censorship?

---

[7] For instance, the OpenNet Initiative after conducting research made the conclusion to China's Internet regulation as "lack of transparency, which has long been a hallmark of the government's management and suppression of information." In comparison, the conclusion on Hong Kong is that there is "no evidence of filtering," and only some blockings exist. As to South Korea, though the OpenNet Initiative concluded that "its citizen do not have access to a free and unfiltered Internet," it still considered the South Korea "imposes a substantial level of filtering for a free and democratic society." RONALD DELBERT ET AL., ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 268, 372 (2008).

[8] *See* The Crimes Ordinance, Cap. 200, § 161 (H.K.) (1997), http://www.legislation.gov.hk/eng/home.htm?SearchTerm=Criminal%20Jurisdiction%20Ordinance%20%28Amendment%20of%20Section%202%282%29%29%20Order%202002; *see also* The Telecommunications Ordinance, Cap. 106, § 27A (H.K.) (2012), http://www.legislation.gov.hk/eng/home.htm?SearchTerm=Criminal%20Jurisdiction%20Ordinance%20%28Amendment%20of%20Section%202%282%29%29%20Order%202002.

[9] *See* The Crimes Ordinance, Cap. 200, § 161 (H.K.) (1997), http://www.legislation.gov.hk/eng/home.htm?SearchTerm=Criminal%20Jurisdiction%20Ordinance%20%28Amendment%20of%20Section%202%282%29%29%20Order%202002.

[10] *See South Korea*, OPENNET INITIATIVE (Aug. 6, 2012), https://opennet.net/research/profiles/south-korea#footnoteref30_tx3m2uh; *see also* Jongpil Chung, *Comparing Online Activities in China and South Korea: The Internet and the Political Regime*, 48 ASIAN SURVEY 5, 727–51 (2008).

[11] *See id.*

[12] Christian Oliver, *Sinking underlines South Korean view of state as monster*, FINANCIAL TIMES (Apr. 1, 2010, 3:00 AM), http://www.ft.com/intl/cms/s/0/d77d855e-3d26-11df-b81b-00144feabdc0.html#axzz2OxDYLDkr.

[13] *Compare Internet Censorship in Hong Kong*, WIKIPEDIA, http://en.wikipedia.org/wiki/Internet_censorship_in_Hong_Kong (last modified Aug. 19, 2013) (describing Internet censorship in Hong Kong as "very little"), *with Internet Censorship in South Korea*, WIKIPEDIA, http://en.wikipedia.org/wiki/Internet_censorship_in_South_Korea (last modified Sept. 8, 2013) (describing Internet censorship in South Korea as "pervasive").

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

There is still a lack of general consensus on how the Internet should be patrolled or regulated worldwide.[14] As the Internet has woven itself into the daily lives of people across the planet, the control model a government chooses inevitably affects the flow of information, sparks free speech concerns, and gives rise to debate. At the center of the debate is whether constitutional or international human rights constraints on the freedom of speech in the physical world should be relaxed in cyberspace.

To answer all those questions, as well as how Taiwan should create its own paradigm, requires an analysis of different existing Internet control models. This article will apply a comparative method to analyze Internet control models of China, Singapore, and United States and find the features of each model. The comparison between models will help in drawing a line between Internet control and censorship under the international human rights standard. With the features and distinctions of each model in mind, this article then recommends how Taiwan should choose its own Internet control model.

China and Singapore were selected for this survey because, like Taiwan, their populations are primarily ethnic Chinese, making them culturally similar to Taiwan. The United States was selected because even though Taiwan is a civil law country, many Taiwanese laws are patterned after United States' laws.[15] The survey and the comparison that follows illustrate how constitutional and international human rights drive or clash with the different models of Internet control.

Part I of this article concerns the current Internet control-related laws in Taiwan. Part II investigates how cyberspace is different from the physical world, and explores why Internet censorship is noxious. This part also discusses how the laws governing cyberspace should be different than those governing the physical world. Part III examines three different representative Internet control models: China's blocking and filtering system, Singapore's class licensing scheme, and the United States' government-private partnership model. Additionally, this part applies international human rights standards under the International Covenant on Civil and Political Rights ("ICCPR") to determine the legitimacy of the three

[14] *See, e.g.*, REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 203–19 (2012) (introducing the internet governance issues); INTERNET GOVERNANCE: INFRASTRUCTURE AND INSTITUTIONS (Lee A. Bygrave & Jon Bing eds., 2009) (pointing out five possible models for regulating the internet).

[15] *Compare*, for example, the U.S. Copyright Act, 17 U.S.C. §§ 101–1332 (2006), *with The Copyright Act* (Taiwan), THE LEGISLATIVE YUEN'S LAW SYSTEM (in Chinese), *available at* http://lis.ly.gov.tw/lgcgi/lglaw?@18:1804289383:f:NO%3DC701176*%20OR%20NO%3DC001176%20OR%20NO%3DC101176$$4$$$NO (last visited Apr. 26, 2013).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

models. Part IV addresses how different constraints form different Internet control models and lessons drawn from the models comparison, and concludes by recommending an Internet control model to Taiwan.

I. TAIWAN'S CURRENT INTERNET CONTROL: A U.S. MODEL FOLLOWER

Taiwan is comparable to both Hong Kong and South Korea in that Taiwan is a democracy. Unlike Hong Kong and South Korea, however, Taiwan does not have a general Internet control system and has not taken any meaningful steps to patrol speech in cyberspace.[16]

Taiwan is a civil law country. Most of its statutes are patterned after other countries' legislation, mostly notably that of the United States, Germany, and Japan.[17] Taiwan often borrows the reasoning of United States' cases or its ordinances to guide patterns of the laws. For instance, the Constitutional Tribunal has cited United States laws as guidance in many of its interpretations.[18] Additionally, although the Taiwan Constitution has its own provisions and language, the Constitutional Tribunal often refers to international human rights treaties or conventions.[19] These references are used to augment exposition of certain clauses when interpreting the Constitution.[20]

---

[16] *See* discussion *infra* regarding Taiwan's current meager Internet control scheme.

[17] *See, e.g.*, HUNGDAH CHIU & JYH-PIN FA, TAIWAN'S LEGAL SYSTEM AND LEGAL PROFESSION 1 (1994) ("Chinese law as implemented and practiced in Taiwan today . . . it contains remnants of imperial Chinese law . . . while also borrowing heavily and adopting principles and concepts from civil law jurisdiction (such as German and Japan) as well as the United States"); BAKER & MCKENZIE, TAIWAN: A LEGAL BRIEF 12 (2002) ("Taiwan has a codified system of law . . . . The contents of the Codes were drawn from the laws of other countries with similar codified systems (e.g. Germany and Japan) and from traditional Chinese laws.").

[18] *See, e.g.*, *J.Y. Interpretation No. 342*, JUSTICES OF THE CONSTITUTIONAL COURT, JUDICIAL YUAN, R.O.C., http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=342 (last visited Oct. 31, 2013) (citing the United States' Federal Supreme Court's case *Field v. Clark*, 143 U.S. 649 (1890), as well as German and Japan's court's judgment to present the concept of parliamentary autonomy of the state council, which also demonstrates that Taiwan's law are impacted by these three jurisdiction); *J.Y. Interpretation No. 601*, JUSTICES OF THE CONSTITUTIONAL COURT, JUDICIAL YUAN, R.O.C., http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=601 (last visited Oct. 31, 2013).

[19] *See, e.g.*, *J.Y. Interpretation No. 587 & 623*, JUSTICES OF THE CONSTITUTIONAL COURT, JUDICIAL YUAN, R.O.C. (both referring to the Convention on the Right of the Child); *J.Y. Interpretation No. 582*, JUSTICES OF THE CONSTITUTIONAL COURT, JUDICIAL YUAN, R.O.C. (referring to the European Convention for Protection of Human Rights and Fundamental Freedoms and the International Covenant on Civil and Political Right), http://www.judicial.gov.tw/constitutionalcourt/p03.asp (last visited Apr. 20, 2013).

[20] *See, e.g., id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

While Taiwan's Internet control at this stage is minimal, it does control some aspects of online speech through the Protection of Children and Youths Welfare and Rights Act (the "Child Protection Act") and Copyright Act.[21] Article 46(1) of the Child Protection Act authorizes the administrative agency to develop protective systems to prevent children from accessing immoral Internet content.[22] This includes: building filtering software, tracking minor' behavior on the Internet, and establishing a content grading system.[23] Articles 46(2) and (3) require Internet platform providers[24] to establish self-disciplinary measures to protect children's moral development and restrict the user's ability to receive or browse the Internet.[25] The Child Protection Act also requires Internet platform providers to remove certain content after failing to establish such self-disciplinary measures or if informed by the government that certain online content corrupts the minds of underage users.[26]

Meanwhile, Chapter VI-1 of the Copyright Act provides that online service providers ("OSPs")[27] may suspend the accounts of customers; accused of downloading copyrighted material more than three times.[28] ISPs are responsible for removing or denying access to copyright infringing content and alerting customers to the infringement by e-mail after copyright holders bring violations to their attention.[29]

Even though there are only two sources of law that have Internet control mechanisms, Taiwan's Internet control regulations are similar to the United States'

---

[21] *See Child and Youth Welfare Protection Act* (Taiwan), promulgated on Aug. 8, 2010, *available at* http://lis.ly.gov.tw/lgcgi/lglaw?@18:1804289383:f:NO%3DC705125*%20OR%20NO%3DC005125%20OR%20NO%3DC105125$$4$$$NO (last visited Apr. 20, 2013); *The Copyright Act* (Taiwan), *supra* note 15.

[22] *Child and Youth Welfare Protection Act* (Taiwan), *supra* note 21.

[23] *Id.*

[24] *Id.* (stating internet platform providers are defined as entity providing any platform services accessible online [e.g., online storage space, online information for building websites, smart card value-adding service, and web page linkage services]).

[25] *Id.*

[26] *Id.*

[27] *See The Copyright Act* (Taiwan), *supra* note 15, at art. 3(19) (stating the OSPs under the Copyright Act refer to internet service providers, rapid saving service providers, information saving service providers, and searching service providers).

[28] *See The Copyright Act* (Taiwan), *supra* note 15.

[29] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

government-private partnership model.[30] As will be discussed later, this partnership model imposes liability on private online intermediaries to help the government to filter or block minor-harmed or copyright infringed materials online.

Only a few Internet speech cases in Taiwan involve the Child Protection Act and Copyright Act. Some Taiwanese legislators have suggested that a law governing online regulation should be enacted.[31] However, no legislation put forth has presented a concrete proposal explaining how the Internet should be regulated. As Taiwan shops for enhanced Internet regulation, a comparison between different Internet control models will help Taiwan find clear and justifiable standards in selecting future control measures.

II. WHAT IS "INTERNET CENSORSHIP"?

A. The Features of the Internet and Their Constitutional Implications

Trying to define "Internet" or "cyberspace" is not as instructive as one might think.[32] It is more enlightening to look at the differences between the physical world and cyberspace and determine how the differences affect the formation of law in cyberspace.[33]

Lawrence Lessig named four critical forces in cyberspace in his book *Code 2.0*: the law, social norms, market, and architecture.[34] Lessig treats the sum of these four constraints as the beginnings of cyberspace regulation, and explores how each constraint affects the others.[35] The distinctions between the physical world and cyberspace are reflected in three of Lessig's constraints: the social norms, market, and architecture.

[30] *See* the U.S. model introduced and analyzed *infra* Part IV(III).

[31] Jhen Huei-Jhen, *The visual world also needs the law in real world*, SINA NEWS (Oct. 2009), http://news.sina.com.tw/magazine/article/3585-2.html.

[32] *See, e.g.*, Reno v. ACLU, 521 U.S. 844, 849–53 (1997) (introducing the history and development of Internet and how it functions).

[33] *But see* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 45–46 (2012) (considering cyberspace is not that different from real space and only the experience is changed).

[34] *See* LESSIG, *supra* note 6, at 123.

[35] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

1. Social Norms

Social norms are different in the physical and virtual domains, which can be attributed mainly to anonymity in the virtual world.[36] For example, in the virtual domain, social norms are not imposed on people through mandatory regulatory measures like laws; they are instead followed voluntarily for the sake of maintaining reputation or out of shame or moral conscience.[37] Alternatively, in the physical world, when an individual expresses an unethical opinion, that individual might suffer moral accusation and reputational harm. Such concerns are diminished in cyberspace because the identities of speakers are often hidden.[38] Believing they can speak with impunity, individuals are less inhibited and are easily tempted to lower their moral standards when speaking in cyberspace.[39]

In terms of age, the denizens of cyberspace are different from those of the physical world. Active Internet users are generally younger, while less frequent users tend to be older, poorer, and do not go about their daily business online.[40] While social norms in the physical world are largely shaped by the older generation, cyberworld norms are shaped by active online users, often with the effect of polarizing online speech.[41]

The comparatively lax social norms in the virtual world give the speakers greater freedom to exchange their ideas with less regard for self-censorship. There is, however, still a price to pay for violation of social norms in cyberspace. Violators can be banned from speaking or accessing a certain online forum, a punishment that is rare in the physical world for defying social norms.[42]

---

[36] *See* Albert Z. Kovacs, *Quieting the Virtual Prison Riot: Why the Internet's Spirit of "Sharing" Must Be Broken*, 51 DUKE L.J. 753, 757–58 (2001) (illustrates the feature of anonymity in cyberspace).

[37] *See* Daniel B. Levin, *Building Social Norms on the Internet*, 4 YALE SYMP. ON L. & TECH. 97, 102–11 (2001–2002) (discussing different theories of norm development).

[38] *See id.* at 117.

[39] *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 8–9 (2006), *available at* http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf (indicating how the enhanced autonomy in cyberspace change the individual's relationship with the others).

[40] *See Demographics of Internet Users*, PEW INTERNET (Apr. 17–May 29), http://pewinternet.org/Static-Pages/Trend-Data-(Adults)/Whos-Online.aspx (according to the tracking survey done in 2013 by Pew Research Center, between 18–29 adults, 98% in the group uses internet, while to whom over 65 years old, only 56% of them uses internet).

[41] *See* CASS SUNSTEIN, REPUBLIC.COM 2.0, at 46–96 (2007) (discussing polarization effect of online speech).

[42] See *infra* Part III discussing the selected Internet control models for instances when persons are banned from speaking/accessing certain online forum.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

2. Market

As Lessig has already pointed out, a different pricing system has emerged in cyberspace.[43] For example, music is presented as a product that can be bought and sold in the physical world, but the same music can be listened to online for free. Conversely, books and articles can be read for free in the libraries of the physical world, but the same digital content typically cannot be accessed without first paying and registering with online database service providers.

Another difference between the two realms is that most markets in the physical world are local, serving consumers or users within a nation's territory.[44] The lack of borders in cyberspace, and consequently the absence of transboundary business costs, means that more service providers aim to serve global users online.[45]

3. Architecture

In physical world, architecture regulates behavior automatically without the need of enforcement.[46] As Lessig has pointed out, there are not many available forums for people to make public addresses due to the restriction caused by architecture in the physical world.[47] Also, in real space, we may erect barriers to exclude certain groups' participation in activities.[48] Further, the architecture makes it difficult for one to hide in real space.[49]

On the other hand, the architecture of the virtual world comprises both software and hardware.[50] This architecture makes the Internet decentralized, have multiple access points, and transcend geographical boundaries—features that led Lessig to refer to cyberspace architecture as "First Amendment in cyberspace."[51] These features eliminate restrictions under the physical world architecture,

---

[43] LESSIG, *supra* note 6, at 124.

[44] *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET, ILLUSIONS OF A BORDERLESS WORLD? (2008) [hereinafter GOLDSMITH & WU].

[45] *See id.*

[46] Levin, *supra* note 37, at 101.

[47] LESSIG, *supra* note 6, at 235.

[48] *Id.* at 86.

[49] *Id.* at 45.

[50] *Id.* at 124.

[51] *Id.* at 237.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

including the impossibility of being invisible and inability to participate.[52] Since the architecture in cyberspace changes the power structure and serves so importantly in protecting freedom of speech, the issue of how to regulate cyberspace is therefore one that cannot be overlooked.[53]

4. How Should Law in Cyberspace Be Different?

Besides their different appearances in the virtual and physical worlds, the three constraints (social norms, market, architecture) also operate differently in various regions of the world. These regional differences—including culture, market, and government structure—impact Internet control policy. Take the comparison of social norms between China and United States as an example. Traditional Chinese social norms do not treat intellectual property rights ("IP rights") as an important issue;[54] therefore, China does not use IP rights as a basis to regulate the Internet.[55] By contrast, United States social norms highly value and respect IP rights; consequently, IP rights and serve an important ground in controlling Internet activities in the United States.[56] Regional differences should be borne in mind when judging the nature of Internet control regulations in different models.[57]

If cyberspace and the physical world are different in terms of social norms, market, and architecture, it follows that the laws that bind the physical world may not be a good fit for cyberspace. According to Lawrence Lessig, to change any four

---

[52] *Id.* at 45–46, 86–87.

[53] *See id.* at 237.

[54] *See* WILLIAM P. ALFORD, *Don't Stop Thinking About . . . Yesterday: Why There Was no Indigenous Counterpart to Intellectual Property Law in Imperial China*, *in* TO STEAL A BOOK IS AN ELEGANT OFFENCE: INTELLECTUAL PROPERTY LAW IN CHINESE CIVILIZATION 9, 16–17 (1995) (suggesting that efforts done by tradition Chinese government before 20th century is merely for the secure of national power).

[55] Though China does have laws protecting intellectual property rights, the notoriously poor implementation of which is often subject to criticism, *see, e.g.*, Martha Magadalena Kleyn, *The Role of culture in Business Transactions and Protection of Intellectual Property Rights within Asian Countries such as China and Japan*, 47 LES NOUVELLES 37, 42–43 (2012); Lael S., *Ghost Shifts and IP Rights in China*, INTERNET AND INTELLECTUAL PROPERTY JUSTICE CLINIC OF UNIVERSITY OF SAN FRANCISCO LAW SCHOOL (May 2011), http://lawblog.usfca.edu/internetjustice/2011/ghost-shifts-and-ip-rights-in-china/.

[56] Western culture treats property rights, including IP rights, as natural ones. One of the origin of IP rights is considered to be from John Locke's theories, *See, e.g.*, Justin Hughes, *The Philosophy of Intellectual Property*, 77 GEO. L.J. 287, 297–300 (1988); Linda J. Lacey, *Of Bread and Roses and Copyrights*, 1989 DUKE. L.J. 1532, 1540 (1989).

[57] *See infra* Part IV for further discussion of this point.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

of the constraints would change the whole regulation.[58] Therefore the law governing the virtual world should be different. Examining the free flow of information online and access to the Internet as a human right will help determine whether to expand or limit the scope of the law of the physical world when applying it to cyberspace.

a. Free flow of information in cyberspace

The free flow of information is an important interest and human right. Many international human rights treaties recognize the importance and borderless nature of freely flowing information.[59] Article 19.2 of the International Covenant on Civil and Political Rights ("ICCPR") reads: "[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[60]

Free flow of information is partly achieved by Article 19.2's language, "to seek, receive, and impart information[,]" and thus should be recognized as freedom of speech under the ICCPR. Additionally, the language "through any other media" qualifies free flow of information online as a freedom protected by Article 19.2.

In General Comment 34, the United Nations ("UN") Human Rights Committee (the "Committee") interprets Article 19.2 as "[embracing] a right of access to information held by public bodies[.]"[61] This requires the government to "proactively put in the public domain Government information of public interest" and "make every effort to ensure easy, prompt, effective and practical access to such information."[62] Besides the right to access online information of the government, the Committee also stressed in General Comment No. 25 that it is essential for citizens to exchange information and ideas about public and political

---

[58] LESSIG, *supra* note 6, at 123.

[59] *See, e.g.*, International Covenant on Civil and Political Rights art. 19, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. GAOR, 3d Session, at 71, U.N. Doc. A/810 (1948).

[60] ICCPR, *supra* note 59. A similar provision can be found in Article 19 of the Universal Declaration of Human Rights ("UDHR"), which reads: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Universal Declaration of Human Rights, *supra* note 59.

[61] U.N. GAOR Human Rights Committee, 102d Sess., ¶ 18, U.N. Doc. CCPR/C/GC/34 (2011).

[62] *Id.* ¶ 19.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

affairs.[63] Such free communication "implies a free press and other media able to comment on public issues and to inform public opinion *without censorship or restraint*."[64] The foregoing suggests that the Committee believes censorship refers directly to an illegitimate government restriction on free speech.

Though Taiwan is not a signatory to the ICCPR, Taiwan's Congress approved both the ICCPR and the International Covenant on Economic, Social and Cultural Rights (the "ICSCR") on March 31, 2009.[65] Taiwan subsequently passed and promulgated the Act to Implement the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights (the "Act").[66] Republic of China (R.O.C.) President Ma Ying-jeou officially signed the ICCPR and the ICSCR on May 14, 2009, and the acts were given force on December 10, 2009.[67] The ICCPR and its General Comments are recognized in Taiwan as domestic law and may guide the interpretation of the Constitution.[68]

In the United States, the Supreme Court has expanded on the free flow of information in many cases, underscoring the importance of protecting free speech.[69] Scholars Jonathan Penney, Achal Mehra, Marci Hamilton and Clemens Kohnen have discussed the free flow of information as an independent right.[70] The

---

[63] Human Rights Comm., General Comment 25, *The right to participate in public affairs, voting rights and the right of equal access to public service*, 57th Sess., ¶ 25, U.N. Doc. CCPR/C/21/Rev.1/Add.7 (July 12, 1996).

[64] *Id.* (emphasis added).

[65] MA YING-JOEU, *Foreword by the ROC President*, *in* CORE DOCUMENT FORMING PART OF THE REPORTS REPUBLIC OF CHINA (TAIWAN) I–II (Sept. 2012), retrieved from *Initial State Reports on ICCPR & ICESCR*, RESPECT, PROTECT & FULFILL HUMAN RIGHTS (Oct. 24, 2012), http://www.humanrights.moj.gov.tw/ct.asp?xItem=285670&ctNode=33254&mp=205.

[66] *The Act to Implement the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights* (Taiwan), promulgated on Apr. 22, 2009, *available at* http://www.humanrights.moj.gov.tw/lp.asp?ctNode=32913&CtUnit=12352&BaseDSD=7&mp=200 (last visited Nov. 3, 2013) [hereinafter The Act].

[67] *Id.*

[68] *See* Nigel N. T. Li, Joyce W. J. Chen & Jeffrey Li, *Cutting the Gordian Knot: Applying Article 16 of the ICCPR to End Capital Punishment*, *in* CAPITAL PUNISHMENT: NEW PERSPECTIVES (Peter Hodgkinson ed., forthcoming Dec. 2013).

[69] *See, e.g.*, Associated Press v. U.S., 326 U.S. 1, 20 (1945) (free flow of information is fundamental public welfare element under First Amendment); Pell v. Procunier, 417 U.S. 817, 832 (1974) (freedom of express includes free flow of information of public figure as most important public interest); 44 Liquomart, Inc. v. Rhode Island, 517 U.S. 484, 512 (1996) (text and free flow of information under First Amendment shows that regulating speech is more dangerous than regulating conduct).

[70] *See, e.g.*, Jonathon W. Penney, *Internet Access Rights: A Brief History and Intellectual Origins*, 38 WM. MITCHELL L. REV. 1 (2011) (suggesting that the free flow of information should be treated as an independent paradigm); ACHAL MEHRA, FREE FLOW OF INFORMATION: A NEW PARADIGM 166–67

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

U.S. Supreme Court has not yet directly recognized the interest of the free flow of information in cyberspace. However, the Taiwan Constitutional Tribunal (the "TCT") has tentatively weighed in on the subject in two interpretations. In the reasoning for Interpretation No. 613, the TCT stated:

> The freedom of speech as guaranteed by Article 11 of the Constitution embodies the freedom of communication, namely, the freedom to operate or utilize broadcasting, television and other communications and mass media networks to obtain information and publish speeches. Communications and mass media are the means and platforms by which public opinions are formed. . . . In light of the said functions of mass media, the freedom of communication not only signifies the passive prevention of infringement by the state's public authority, but also imposes on the legislators the duty to actively devise various organizations, procedures and substantive norms so as to prevent information monopoly and ensure that pluralistic views and opinions of society can be expressed and distributed via the platforms of communications and mass media, thus creating a free forum for public discussion.[71]

The TCT opined in Interpretation No. 613 that the freedom of communication required the government to prevent the infringement of such freedom but did not give standards for judicial review.[72] The TCT reiterated its position in Interpretation No. 678:

> The safeguard of freedom of speech as such also includes the protection of the freedom of communication and broadcasting, that is, the people's freedom to access information and express opinions through radio broadcasting, television or other means of communication or networks (*see* J.Y. Interpretation No. 613). However, the constitutional safeguard over the freedom of speech and the methods of communication is not absolute; varying protection mechanisms and

(1986) (proposing the notion of international free flow of information and suggesting that the U.S. should abolish the distinction between domestic and international communications); Marci A. Hamilton & Clemens G. Kohnen, *The Jurisprudence of Information Flow: How the Constitution Constructs the Pathways of Information*, 25 CARDOZO L. REV. 267 (2003) (proposing three types of free flow of information from people to government, government to people, and between private parties).

[71] No. 613 Interpretation, Taiwan Judicial Yuen Constitutional Tribunal Interpretation (July 21, 2006), http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=613.

[72] *Id.* (lacking standards for judicial review).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

guidelines whose application depend on the content of the speech at issue should be created.[73]

The TCT also referenced R.O.C. Constitution Article 23[74] for reviewing whether the restriction on freedom of communication is justified.[75] Though the TCT did not discuss the considerations in weighing and balancing the free flow of information with the other interests, it recognized the free flow of information in cyberspace as a part of the constitutional freedom of speech in Taiwan.[76]

In the physical world, the need to treat the free flow of information as an independent interest different from the freedom of speech may not be apparent. However, in cyberspace, information can traverse far greater distances and at far greater speed.[77] By the very nature of the Internet, Internet users can receive and disseminate more information and do it nearly instantly. The interest of the people in the free flow of information online is thus enhanced. Moreover, everyone online can enjoy free flow of information, not just certain groups of a country's citizens, unless the country has imposed harsh Internet censorship measures.[78] When any local government desires to impose restrictions on the free flow of information in cyberspace in the name of local interests, it should remember that it is interfering with world interests and rights and therefore should design the measures necessarily.

---

[73] No. 678 Interpretation, Taiwan Judicial Yuen Constitutional Tribunal Interpretation (July 2, 2010), http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=678.

[74] Article 23 of R.O.C. Constitution reads: "All the freedoms and rights enumerated in the preceding Articles shall not be restricted by law except such as may be necessary to prevent infringement upon the freedoms of other persons, to avert an imminent crisis, to maintain social order or to advance public welfare." JUSTICES OF THE CONSTITUTIONAL COURT, JUDICIAL YUAN, R.O.C., http://www.judicial.gov.tw/constitutionalcourt/en/p07_2.asp?lawno=36 (last visited: Nov. 3, 2013).

[75] No. 678 Interpretation, Taiwan Judicial Yuen Constitutional Tribunal Interpretation (July 2, 2010), http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=678.

[76] *Id.*

[77] *See, e.g.*, April Mara Major, *Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution*, 78 WASH. U. L.Q. 59, 97–103 (2000); Patrick O'Neil, *Optimizing and Retricting the Flow of Information: Remodeling the first Amendment for a Convergent World*, 55 U. PITT. L. REV. 1057, 1070–72 (1994); Levin, *supra* note 37, at 115–21.

[78] *See* Ingrid Volmer, *Universalism and Particularism: The Problem of Cultural Sovereignty and Global information Flow*, *in* BORDERS IN CYBERSPACE: INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE 78–79 (Brian Kahin & Charles Nesson eds., 1997) (pointing out the special interest of global communication).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

The United Nations General Assembly ("UNGA") also pointed out the special consideration and interest in preserving the flow of information online in one of its reports on May 16, 2011:

> The Special Rapporteur emphasizes that there should be as little restriction as possible to the flow of information via the Internet, except in few, exceptional, and limited circumstances prescribed by international human rights law. He also stresses that the full guarantee of the right to freedom of expression must be the norm, and any limitation considered an exception, and that this principle should never be reversed.[79]

b. Access to the Internet as a Human Right

The differences between the physical world and cyberspace in terms of the social norms, market, and architecture show that access to space or gate control matters more in cyberspace rather than in the physical world.[80] The architecture of the virtual world creates barriers for users, thereby affecting the online community differently, and shaping the social norms differently.[81] At the same time, the online pricing system functions on the power to control access.[82]

Whether access to the Internet should be designated as a human right is still controversial. Vinton Cerf, an opponent to the Internet being recognized as a human right, argues, "technology is an enabler of rights, not a right itself."[83] He believes that technology has failed to meet the "high bar" of being considered as a human right because the right to make a living, access information, or speak freely is not necessarily coupled to technology.[84] Conversely, advocates for recognizing Internet access as a human right argue that Articles 19 and 27 of the UDHR[85]

---

[79] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on Key Trends and Challenges to the Right of all Individuals to Seek, Receive and Impart Information and Ideas of all Kinds Through the Internet*, Human Rights Council, ¶ 68, U.N. Doc. A/HRC/17/27 (May 16, 2011).

[80] *See supra* Part II discussing differences between physical world and cyberspace in terms of societal norms, market, and architecture.

[81] LESSIG, *supra* note 6, at 124.

[82] *Id.*

[83] Vinton G. Cerf, *Internet Access Is Not a Human Right*, N.Y. TIMES (Jan. 4, 2012), http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=2&ref=opinion&.

[84] *Id.* (stating that even if the Internet is necessary to realize human rights, and thus should be guaranteed now, it should be viewed as a means, not as an end, or a "right," in itself).

[85] *See* Universal Declaration of Human Rights, *supra* note 59, at art. 19, 27.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

already provide the basis for treating access to the Internet as a human right. Specifically advocates argue such access should not be an isolated right, but rather inseparable from the right to association and expression.[86] One such advocate, Sherif Elsayed-Ali, disagrees with Cerf, arguing that access to the Internet has become and will continue to be "an essential component of the rights to freedom of expression and access to information" in the foreseeable future and should be available to everyone, similar to education.[87]

In the physical world, everyone is born into the world and the only exit is death. In cyberspace, whoever controls Internet access reigns supreme. Thus, access to the Internet should be a human right granted to everyone. Doing so would preclude arbitrary and tyrannical control of the online gateway. Furthermore, as more and more information in the physical world is digitized and uploaded, the ability to access the Internet will gradually reflect the ability to acquire basic information or knowledge about the world. Access to cyberspace is therefore as important as education, and equal access to the Internet should be protected just the same.[88]

As discussed above, Article 19 of the ICCPR and the Committee's General Comment No. 34 recognize the right for people to access public information as a basic and important human right.[89] Because the ability to access the Internet will gradually become a measure of the ability to access information, it should rightly be deemed an independent human right under Article 19 of the ICCPR.

Article 19 of the ICCPR and the Committee's General Comment No. 34 may also be the reason why, in July 2012, the UN Human Rights Council passed a resolution widely considered to recognize access to the Internet as a human right.[90] The resolution first confirms that the rights people have offline should also be protected online notwithstanding frontiers, especially the freedom of expression

---

[86] Cerf, *supra* note 83.

[87] Sherif Elsayed-Ali, *Internet Access Is Integral to Human Rights*, EGYPT INDEP. LIVE BLOG (Jan. 15, 2012, 1:19 PM), http://www.egyptindependent.com/opinion/internet-access-integral-human-rights.

[88] *See id.*

[89] *See infra* Part II–I (4)(1) (discussing Article 19 of the ICCPR and General Comment No. 34).

[90] *See, e.g.*, Somini Sengupta, *U.N. Affirms Internet Freedom as a Basic Right*, N.Y. TIMES (July 6, 2012), http://bits.blogs.nytimes.com/2012/07/06/so-the-united-nations-affirms-internet-freedom-as-a-basic-right-now-what/; *see also* Alex Fitzpatrick, *Internet Access Is a Human Right, Says United Nations*, MASHABLE (July 6, 2012), http://mashable.com/2012/07/06/internet-human-right/; Talia Ralph, *UN deems Internet access a basic human right*, GLOBALPOST (July 6, 2012, 20:01), http://www.globalpost.com/dispatch/news/politics/diplomacy/120706/un-deems-internet-access-basic-human-right-0.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

under the ICCPR Article 19.[91] The resolution thereby "[c]alls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries."[92]

Due to the free flow of information interest in cyberspace and recognition of access to the Internet as a human right, the restriction on Internet activities would have to be subject to cautious constitutional examination in order to acquire justifiability. Avoiding Internet censorship is therefore the priority concern of governmental measures controlling the Internet. The danger and meaning of censorship is analyzed in the next section.

B. The Meaning and Danger of Censorship

Before exploring issues of Internet censorship, it is necessary to understand what *censorship* means in the context of this discourse. The first step toward defining censorship is determining whether it is a negative or neutral term.[93]

Eli Pariser describes censorship as "a process by which government alters facts and content," and thinks such a concept is inherently negative.[94] P.G. Ingram, meanwhile, suggests that censorship denotes the restrictive policy governing publication, public performance, and exhibition.[95] As is such, "censorship is only one limitation of liberty," which does not necessarily constitute repression, and is therefore merely a neutral term.[96]

---

[91] Human Rights Council Res. 20/8, Rep. of the Human Rights Council, 20th Sess., June 18–July 6, 2012, U.N. Doc. A/HRC/20/8/ at ¶ 1 (June 29, 2012).

[92] *Id.* at ¶ 3.

[93] *See* BLACK'S LAW DICTIONARY 1031, 1042 (6th ed. 1991), which defines the word "negative" as "a denial; a proposition by which something is denied, a statement in the form of denial." "Neutral" is defined as "indifferent, unbiased, impartial; not engaged on either side; not taking an active part with either of the contending sides." If censorship is a negative term, it means censorship is not acceptable and denial. By contrast, if censorship is a neutral term, then it means it is simply an unbiased description of restrictive measure of the government.

[94] ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK 140–41 (2011); *see* Salman Rushdie & Jonathan Rauch, *Censorship is Harmful*, *in* CENSORSHIP: OPPOSING VIEWPOINTS 26 (David Bender & Bruno Leone eds., 1997) (referring censorship as eroding First Amendment's value).

[95] P.G. INGRAM, CENSORSHIP AND FREE SPEECH: SOME PHILOSOPHICAL BEARINGS 1–4 (2000); *see also* Thomas Storck, *Censorship can be Beneficial*, *in* CENSORSHIP: OPPOSING VIEWPOINTS 17, 18 (David Bender & Bruno Leone eds., 1997) (defining censorship as "the restriction, absolute[ly] or merely to some part of the population . . . by the proper political authorities, of intellectual, literacy, or artistic material in any format").

[96] *See* INGRAM, *supra* note 95.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

The U.S. Supreme Court seems to treat censorship as a negative term rather than a neutral one. In *Near v. Minnesota* (1931), the statute at issue prohibited a newspaper owner or publisher from publishing scandalous and defamatory material.[97] The Court determined that prohibiting the activity without providing the publisher an opportunity to verify the content as true had an "essence of censorship."[98] The Court held that the statute was an unconstitutional restraint upon liberty of the press as guaranteed by the Fourteenth Amendment.[99] The Court also noted that the freedom of the press had historically been treated by the Constitution to mean "immunity from previous restraints or censorship."[100] The Court appeared to treat censorship as synonymous to illegitimate restraints that muffle the press and publication and found censorship undesirable under the United States Constitution.

Censorship, then, is a governmental effort to suppress certain contents of speech or publications, regardless of whether they have an actual negative effect on individuals or the public. The risk of censorship, as indicated by the U.S. Supreme Court in *Cohen v. California* (1971), is that the "governments might soon seize upon the censorship of particular words as a convenient guise for banning the expression of unpopular views."[101] Governmental censorship against a specific speaker may inevitably create self-censorship, and self-censorship may create a chilling effect, inducing mass censorship.[102]

If the government could arbitrarily examine the contents of speech and prohibit publication or expression, combined with self-censorship, the chilling effect may become a reality. This undesirable reality would diminish the goal that "[d]ebate on public issues should be uninhibited, robust, and wide-open[,]"[103]and create a real threat to the democratic value of freedom of expression.[104] Censorship or self-censorship should therefore be averted.[105]

---

[97] Near v. Minnesota, 283 U.S. 697 (1931).

[98] *Id.* at 713.

[99] *Id.* at 723.

[100] *Id.* at 716.

[101] Cohen v. California, 403 U.S. 15, 26 (1971). *See also* New York v. Ferber, 458 U.S. 747, 756 (1982).

[102] *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 278–79 (1964) (quoting Smith v. California, 361 U.S. 147, 153–54 (1959)).

[103] *Id.* at 270.

[104] *See* Svetlana Mintcheva, *The Censor Within*, *in* CENSORING CULTURE: CONTEMPORARY THREATS TO FREE EXPRESSION 299, 302–03 (Robert Atkins & Svetlana Mintcheva eds., 2006) (stating

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

In the physical world, when the government prohibits certain contents of speech, the government's enforcement of the prohibition causes people to refrain from disseminating such contents for fear of being penalized.[106] In cyberspace, the pervasive anonymity of the Internet means that mere criminalization of dissemination of forbidden information is not enough to stop certain speech.[107] Measures such as blocking or filtering must be applied to enforce the law, which may explain why *Internet censorship* is often seen as a synonym of *Internet filtering*, when access to information online is controlled or denied.[108]

What constitutes illegitimate control or censorship is another critical question. In the United States, whether a measure to prohibit expression is legitimate depends on the legal grounds and the appropriateness of the measure; that is, whether it passes the *necessity test*[109] under Article 19.3 of ICCPR, which requires the measure to be appropriately achieving the goals, to be the least restrictive mean, and to be proportionate.[110] When discussing Internet censorship issues in the context of international human rights, should the standard remain the same? The next section explores international grounds and limitations for Internet control, and attempts to carve out clear guidance.

C. The ICCPR Standards to Determine Legitimate Internet Control

Article 19.3 of the ICCPR provides three legitimate grounds for regulating freedom of expression.

> The exercise of the [freedom of expression] rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (1) For respect of the rights or reputations of others; (2) For

---

the idea that censorship, including self-censorship, threatens freedom of expression. "Self-repression often derives from fear . . . This fear threatens creative activity . . . .").

[105] *See* Storck, *supra* note 95, at 17–18.

[106] *See id. See also* INGRAM, *supra* note 95.

[107] LACEY ALFORD, THE GREAT FIREWALL OF CHINA: AN EVALUATION OF INTERNET CENSORSHIP IN CHINA 5 (2010); *see* Robert Faris et al., *Censorship 2.0*, 3 INNOVATIONS 165–87 (2008).

[108] ALFORD, *supra* note 107; Faris, et al., *supra* note 107.

[109] *See* E. THOMAS SULLIVAN & RICHARD S. FRASE, PROPORTIONALITY PRINCIPLES IN AMERICAN LAW: CONTROLLING EXCESSIVE GOVERNMENT ACTIONS 53–66 (2009).

[110] *Id. See also* Section III *supra* discussing the ICCPR standards to determine legitimate Internet control.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

> the protection of national security or of public order (order public), or of public health or morals.[111]

To determine what constitutes a legitimate ground to restrict freedom of expression, the Committee clarifies that "[s]tates parties should put in place effective measures to protect against attacks aimed at silencing those exercising their right to freedom of expression" and Article 19.3 "may never be invoked as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights."[112] The Committee's position that mere advocacy of an idea or thoughts may not constitute a justification for the government to regulate speech coincides with the U.S. Supreme Court's holding in *Brandenburg v. Ohio* (1969).[113] This holding reflects the principle that the State cannot "forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[114]

Article 19.3's three legitimate grounds for regulating speech are themselves limited restrictions.[115] What the respect of others' rights and reputations or public health encompasses is clearer than the protection of national security, public order, and public morals. In General Comment 34 the Committee defined national security, public order, and public morals under Article 19.3 of the ICCPR as narrow and limited authorizations:

> 30. Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information . . . . 31. On the basis of maintenance of public order (order public) it may, for instance, be permissible in certain circumstances to regulate speech-making in a particular public place . . . . 32. The Committee observed in general comment No. 22, that

---

[111] ICCPR, *supra* note 59, at art. 19, ¶ 3.

[112] *Id.* at art. 19 general cmt. 34, ¶ 22.

[113] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

[114] *Id.*

[115] ICCPR, *supra* note 59, at art. 19, ¶ 23.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

> "the concept of morals derives from many social, philosophical and religious traditions; consequently, limitations . . . for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition." Any such limitations must be understood in the light of universality of human rights and the principle of non-discrimination.[116]

Even if the reason emphasized in Article 19.3 of the ICCPR[117] can be cited to limit the freedom of expression, the means adopted by the government to restrict the rights guaranteed by Article 19.1 and 19.2 must pass Article 19.3's necessity test:[118] the restrictions "shall only be such as are provided by law and are *necessary*."[119] The Committee interprets the necessity test as requiring the restrictive measures to "be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected."[120] When reviewing the necessity test, the form and means of expression must be taken into account and "the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain."[121]

The Committee stated that "[t]he penalization of a media outlet, publishers or journalist solely for being critical of the government or the political social system espoused by the government can never be considered to be a necessary restriction of freedom of expression."[122] The Committee further pointed out that any restrictions on the Internet-based information dissemination system and the systems to support such a system should be compatible with Article 19.3, according to which the "[p]ermissible restrictions generally should be content-specific" and "generic bans on the operation of certain sites and systems are not allowed."[123]

---

[116] *Id.* at ¶¶ 30, 32.

[117] Article 19.1 reads: "Everyone shall have the right to hold opinions without interference." ICCPR, *supra* note 59, at art. 19.1.

[118] *Id.* at art. 19, ¶ 22 ("Paragraph 3 lays down specific conditions and it is only subject to these conditions that restrictions may be imposed: the restrictions must be "provided by law"; they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3; and they must conform to the strict tests of necessity and proportionality.").

[119] *Id.* at art. 19.3 (emphasis added).

[120] *Id.* at art. 12 general cmt. 27, ¶ 14, Sept. 12, 2011.

[121] *Id.* at art. 12, ¶ 34.

[122] *Id.* at ¶ 42.

[123] *Id.* at ¶ 43.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

Furthermore, "to prohibit a site or information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government" is also not permissible under Article 19.3.[124]

With an understanding of the international human rights standards on restricting the free flow of information in cyberspace, a comparison and analysis of the different Internet control models is now possible and will be explored in Part III.

III. THREE INTERNET CONTROL MODELS

In this section, the Internet control models of China, Singapore, and the United States will be examined to determine whether the models constitute legitimate restrictions on the freedom of speech under international human rights law or whether they should be deemed Internet censorship. The examination of these models will also provide guidance to Taiwan for its Internet control model selection.

A. China—Internet Control Through Wide Blocking and Filtering

To the rest of the world, China conducts Internet censorship.[125] But is this perception of China justified?

On December 28, 2012, the Standing Committee of the National People's Congress of China issued the Decision on Strengthening the Protection of Online Information (the "Decision") to require Internet users to provide their real names to ISPs before using their online pseudonyms.[126] Besides paragraph 6 of the Decision, which requires ISPs to collect the real names of Internet users, paragraph 5 makes

[124] *Id.*

[125] *See, e.g.*, Christopher Stevenson, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*, 30 B.C. INT'L & COMP. L. REV. 531, 534 (2007) (considering China is by no means the only country censoring internet content); James Fallows, *China's Internet Censorship is Effective*, *in* CENSORSHIP: OPPOSING VIEWPOINTS 113 (Scott Barbour 2010) (considering China as the most censorious country in the world); Jessica E. Bauml, *It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship*, 63 FED. COMM. L.J. 607, 704 (deeming China to have the "world's most advanced and sophisticated system of censorship").

[126] *See, e.g.*, Keith Bradsher, *China Toughens Its Restrictions on Use of the Internet*, N.Y. TIMES (Dec. 28, 2012), http://www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html?hp&_r=2&; Will Morrow, *Chinese government imposes new Internet censorship law*, WORLD SOCIALIST WEB SITE (Jan. 7, 2013), http://www.wsws.org/en/articles/2013/01/07/chin-j07.html.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

ISPs responsible for filtering and censoring illegal online speech.[127] Some reports have concluded that the Decision represents the Chinese government's attempt to further tighten its grip on the Internet following the attempt by Chinese Internet users to expose a string of financial and sexual scandals that have caused at least ten local officials to resign or be dismissed.[128]

The Decision undoubtedly is intended to pull back the veil of anonymity in cyberspace so the government can identify the online speakers and stomp out "undesirable" online speech or information dissemination.[129] The consequence of this measure is a dampening of the active Chinese blogosphere because it forces speakers to censor themselves.[130] Moreover, the Decision likely does not pass Article 19.3's necessity test since it could be challenged as not using the least restrictive means.[131] For this reason, the Decision is not legitimate in the context of international human rights and thus constitutes Internet censorship.

---

[127] *The Decision on Strengthening the Protection of Online Information*, XINHUA NEWS (Dec. 28, 2012, 15:42:04), http://news.xinhuanet.com/politics/2012-12/28/c_114195221.htm.

[128] Bradsher, *supra* note 126; *see also The online real name system built by China draws attention*, BBC CHINESE WEB SITE (Dec. 28, 2012), http://www.bbc.co.uk/zhongwen/simp/chinese_news/2012/12/121228_china_internet_control.shtml.

[129] *See, e.g.*, King-wa Fu, Chung-hong Chan & Michael Chau, *Assessing Censorship on Microblogs in China: Discriminatory Keyword Analysis and the Real-Name Registration Policy*, 17 IEEE INTERNET COMPUTING 42, 46 (2013) ("There has been widespread concern that the true identity disclosure policy would have created a chilling effect on online comments, especially on political criticism and sensitive topics."); Margot Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815, 878–79 (2013) ("China's policy is an example of a real-name policy targeting dissidents, but not civility."); *China: Renewed Restrictions Send Online Chill*, HUMAN RIGHTS WATCH (Jan. 4, 2013), http:// www.hrw.org/news/2013/01/04/china-renewed-restrictions-send-online-chill (Considering the decision having "a chilling message to China's netizens," and "[t]he government's decision is an effort to silence critics and curb anonymity online by further conscripting internet companies to monitor and censor users.")

[130] *See* Part II(2) *supra* discussing self-censorship.

[131] *See supra* Part II discussing the ICCPR standards to determine legitimate Internet control. South Korean had a similar online real name system like China, the identity verification scheme, which is held unconstitutional by the Constitutional Court of Korea. One of main reasons adopted by the Constitutional Court is that the identity verification scheme is not a less-restrictive mean: " . . . identity verification of the penetrator uploading that illegal information can be substantially conducted by tracing or confirming internet addresses. In addition, remedy for victims can also be fully obtained by blocking distribution or diffusion of illegal information—deletion or taking temporary measures in terms of illegal information by service provider (Article 44-2 Section 1 and 2 of the Information Communications Network Act) or denial, suspension or making temporary restriction on handling illegal information against message board manager or operator (Article 44-7 Section 2 and 3 of the Information Communications Network Act)—or post-crime compensation or criminal punishment." Identity Verification System on Internet, 2010 Hun-Ma 47, 252 (2012), *available at* http:// english.ccourt.go.kr/.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

The Decision is not the first time the Chinese government has tried to regulate online speech and order, nor is it the only Internet censorship measure the government has ever adopted.[132] The Internet control system in China can be understood both by the legal basis it invokes and by how the legal basis is carried out.

1. The Legal Grounds for the Government to Control Internet Speech

The Measures for Managing Internet Information Services ("MMIIS") provides extensive legal grounds for the Chinese government to forbid private Internet Information Service Providers ("IISPs) to produce, reproduce, release, or disseminate online information.[133] They include: national security, state interest and honor, national unity or ethnic discrimination, state policy towards religion, social order, the regulation of pornography, gambling, violence, homicide, terrorism, human dignity, and rights infringement.[134] These grounds seem to be derived from the grounds for prohibiting dissemination of verboten information, which can be found in Article 5 of the Rules of Managing and Protecting Security for Computer Information Network and Internet, promulgated by the Chinese Ministry of Public Security on December 30, 1997.[135]

The IISPs are obliged to censor the content of dubious online speech to stop the transmission of illegal online information and immediately record and report as required by Article 16 of the MMIIS.[136] According to Article 23, failure of commercial IISPs to censor dubious online speech will cost them their license; for noncommercial IISPs, their websites may be shut down.[137]

China is not the only country that requires private IISPs or online service providers to help patrol and regulate Internet speech.[138] Democratic countries like

---

[132] *See* Bradsher, *supra* note 126 (stating besides the following internet censorship measures of China the article is going to introduce and analyze, there are other many censorship efforts done by the Chinese government. For instance, the government purposefully begins their blocking of the foreign famous media websites (e.g., The New York Times and BBC) in 2008 based on the reason that the government may not have sufficient techniques to review the contents on those websites).

[133] *See Measures for Managing Internet Information Services*, CHINA CULTURE, http://www.chinaculture.org/gb/en_aboutchina/2003-09/24/content_23369.htm (last visited Apr. 26, 2013).

[134] *Id.*

[135] *See The Rules of Managing and Protecting Security for Computer Information Network and Internet*, THE MINISTRY OF PUBLIC SECURITY OF THE PEOPLE'S REPUBLIC OF CHINA (Dec. 30, 1997) (in Chinese), http://www.mps.gov.cn/n16/n1282/n3493/n3823/n442104/452202.html.

[136] *Measures for Managing Internet Information Services*, *supra* note 133.

[137] *Id.*

[138] *See* the U.S. model introduced and analyzed *infra* Part III (III).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

the United States also use many different measures to compel ISPs to censor online speech in various situations.[139] The critical difference between the Chinese model and the United States model is this: the Chinese legal basis for controlling the Internet is vague and general, while the United States' is specific and narrow.[140]

Of the Chinese government's grounds for assigning private IISPs responsibility to censor Internet speech,[141] national unity, state honor, and social order are relatively abstract and overbroad. This unjustifiably expands the restrictive grounds recognized by Article 19.3 of the ICCPR.[142] For instance, invoking state policy towards religion to justify suppression of online speech contradicts Article 18.1 of the ICCPR, which protects the freedom of religion.[143]

For the above reasons, China's Internet control is appropriately perceived as Internet censorship, and it reinforces its system with the so-called Great Firewall of China.

2. China's Great Firewall and License System

By threatening to take away operating licenses and assigning IISPs the responsibility to report "aberrant" online speech or behavior, the Chinese government forces the IISPs to do the government's bidding to control the Internet.[144] The government is able to enforce this because of the consequences of operating without a license, which would mean forced website closures and fines for the IISPs.[145]

The Great Firewall of China consists of blocking and content filtering techniques.[146] The blocking system comprises Domain Name System ("DNS")

---

[139] *Id.*

[140] *See* accompanying text and *infra* Part III (III) discussing the U.S. model.

[141] *See* discussion *infra* for complete list of grounds.

[142] *See infra* Part II.

[143] ICCPR, *supra* note 59, at art. 18, ¶ 1 (providing that "Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching.").

[144] *See China*, OPENNET INITIATIVE (Aug. 9, 2012), https://opennet.net/research/profiles/china-including-hong-kong#footnoteref77_ukdt84a; Bauml, *supra* note 125, at 705.

[145] Cynthia Liu, *Internet Censorship as a Trade Barrier: A Look at the WTO Consistency of the Great Firewall in the Wake of the China-Google Dispute*, 42 GEO. J. INT'L L. 1199, 1210–11 (2011).

[146] *See, e.g.*, MACKINNON, *supra* note 14, at 34–40; GOLDSMITH & WU, *supra* note 44, at 87–104; DELBERT ET AL., *supra* note 2, at 263–71; JOSEPH HOUSE, INTERNET CENSORSHIP IN CHINA (2011).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

blocking and Uniform Resource Location ("URL") keyword block.[147] With regards to the blocking system, China's government creates a list of IP addresses to block and if a webpage's domain name is on the list, the DNS will turn down a user's request to access the IP address.[148] Users attempting to access the IP address will see the message "site not found error" on their screens.[149] As to the URL keyword block, the government monitors forbidden words in URLs and blocks the prohibited links.[150] DNS establishes a blacklist of words and conducts Internet monitoring.[151] If a webpage contains words from the blacklist, the page will be off limits to the general public.[152]

Basically, the Great Firewall is a powerful Internet regulation apparatus erected by the Chinese government that selectively blocks website operators and Internet users. While the preceding discussion establishes that the basis for the Chinese's Internet control is illegitimate, does the blocking system, which forces ISPs to report "questionable" online behavior by threatening to take away their operating licenses, pass the necessity test under Article 19.3 of the ICCPR?

China's licensing, blocking and filtering system fails the necessity test, and is aptly perceived as Internet censorship, simply because it is not designed to be "content-specific" as required by the ICCPR Article 19.3. Instead, it provides a general clamp on online activities that works to maintain the Chinese authoritarian regime by "clipping social ties whenever any collective movements are in evidence or expected."[153]

However, what if the measures were content-specific and recognized by the ICCPR Article 19.3, such as to eradicate online child pornography? Would the filtering, blocking and licensing scheme pass the test under Article 19.3 of ICCPR

---

[147] *See* MACKINNON, *supra* note 14; *see also* GOLDSMITH & WU, *supra* note 44; DELBERT ET. AL., *supra* note 2.

[148] James Fallows, *The Connection Has Been Reset*, THE ATLANTIC (Mar. 1, 2008, 12:00 PM), http://www.theatlantic.com/magazine/archive/2008/03/-the-connection-has-been-reset/306650/; *China: The Art of Censorship*, INDEX ON CENSORSHIP, http://www.indexoncensorship.org/2010/10/china-the-art-of-censorship/ (last visited Sept. 17, 2013).

[149] *Id.*

[150] *Id.*

[151] *See id.*

[152] *Id.*

[153] Gary King, Jennifer Pan & Margaret E. Roberts, *How Censorship in China Allows Government Criticism but Silences Collective Expression*, 107 AMERICAN POLITICAL SCIENCE REVIEW 1, 1 (2013). It shall be noted, however, that the authors also point out that "the purpose of the censorship program is not to suppress criticism of the state or the Communist Party."

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

in that case?[154] An investigation into the Singapore and United States models shows how governmental measures pass or fail Article 19.3's test.

B. Singapore—Internet Control Model Based on Licensing System

Unlike China's direct Internet control through blocking and content filtering, Singapore's "class license" scheme indirectly controls the Internet.[155] Under the Broadcasting Class License Notification of Broadcasting Act of Singapore (the "Act"), both Internet content providers ("ICPs"), who provide programs on the World Wide Web through the Internet, and ISPs are subject to the class license scheme.[156] Most of the ICPs and ISPs are automatically class licensed upon their establishment.[157] However, some groups are required to register within fourteen days of the commencement of their operations, or when notified by the government.[158] These groups include: religious groups, political groups, news groups, Internet cafes, schools, and public libraries.[159]

The class licensed ICPs and ISPs are obligated to comply with the Singaporean Internet Code of Practice (the "Code"), though failure to comply will trigger no sanctions from the government.[160] Both ICPS and ISPs are required to deny access to sites containing materials banned by the Code.[161] ISPs should refrain from subscribing to any newsgroup if they believe the newsgroup contains prohibited materials and unsubscribe from any newsgroup by the orders of the authorities.[162] ICPs should ensure that there is no Code-prohibited material on their programs and deny access to materials prohibited by the government authorities.[163]

---

[154] DELBERT ET AL., *supra* note 147.

[155] *See, e.g.*, Lewis S. Malakoff, *Are You My Mommy, or My Big Brother? Comparing Internet Censorship in Singapore and the U.S.*, 8 PAC. RIM L. & POL'Y J. 423, 427–33 (1999); Sarah B. Hogan, Note, *To Net or Not to Net: Singapore's Regulation of the Internet*, 51 FED. COMM. L.J. 429, 446 (1999).

[156] Paragraph 2 and 3 of the Broadcasting Class License Notification of Broadcasting Act, Chapter 28 Section 9, N 1 G.N. No. S 306/1996 REVISED EDITION 2004 (Feb. 29, 2004) [hereinafter The Broadcasting Act].

[157] *Id.* at ¶ 4. *See also Internet Service & Content Provider Class License*, MEDIA DEVELOPMENT AUTHORITY, http://www.mda.gov.sg/Licences/Pages/IntSCPCLicence.aspx (last visited Apr. 20, 2013).

[158] The Broadcasting Act, *supra* note 156, at ¶ 4.

[159] *Id.*

[160] The Schedule of the Broadcasting Act: Internet Code of Practice, ¶ 1(2) (listing the various penalties for violating the code).

[161] *Id.* at ¶ 3(1) & 4.

[162] *Id.* at ¶ 3(1) & (2).

[163] *Id.* at ¶ 3(3) & (4).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

Paragraph 4(1) of the Code defines "prohibited material" as "material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws."[164] To flesh out the abstract grounds, the Code also lists factors that should be considered in determining whether certain material is prohibited, including nudity, sexual violence, explicit sexual activity, child pornography, homosexuality, extreme violence, and ethnic, racial, and religious hatred.[165]

The grounds for the Singaporean government to ask the ICPs or ISPs to regulate Internet speech content are consistent with the grounds under Article 19.3 of the ICCPR.[166] Most of the considerations listed in paragraph 4(3) of the Code concern obscenity, violence, child pornography, or hate speech.[167] These areas are similarly restricted and content-specific under the ICCPR standard. Therefore, whether the Singaporean online control constitutes censorship comes down to the class license scheme and the power vested in ICPs and ISPs to block access to cyberspace.

The Committee indicated in General Comment No. 34 that "[r]egulatory systems should take into account the differences between the print and broadcast sectors and the Internet, while also noting the manner in which various media converge."[168] Comment 34 further explained the conditions for subjecting the broadcast media to the licensing system: "States parties must avoid imposing onerous licensing conditions and fees on the broadcast media, including on community and commercial stations. The criteria for the application of such conditions and license fees should be reasonable and objective, clear, transparent, nondiscriminatory and otherwise in compliance with the Covenant."[169]

Based on these statements, the Committee seems to recognize that the Internet is different from the traditional print and broadcast media, and that it facilitates the convergence of various media. As a result, to claim that bandwidth is limited to justify regulation of the Internet through the license system is not a potentially possible argument. Even if the license system for the Internet is considered legitimate under the ICCPR Article 19, it must at least comply with the limitations imposed by the Committee on the broadcast media license system—that is, the

[164] *Id.* at ¶ 4(1).

[165] *Id.* at ¶ 4(2).

[166] *See Initial State Reports on ICCPR & ICESCR*, *supra* note 65.

[167] *See* The Schedule of the Broadcasting Act: Internet Code of Practice, *supra* note 160, at ¶ 4(3).

[168] ICCPR, *supra* note 59, at art. 19, general cmt. 34, ¶ 39.

[169] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

criteria for the license should be reasonable, objective, clear, transparent, and nondiscriminatory.[170]

As Lewis S. Malokoff observed, the enforcement of the Code is lagging because the class license scheme does not include any ban or sanctions, and thus serves merely as a symbolic regulation.[171] Although the government keeps a blacklist of operators, those on the blacklist can easily evade detection by changing their addresses and go on to operate similar websites.[172] The Singaporean practice is toothless. The operators' class licenses are like birthrights; they are mostly given upon establishment or are easily obtained by a rubberstamping registration authority and cannot be revoked.[173] Further, there are not enough government personnel on hand to monitor the compliance of the ICPs or the ISPs.[174] If the Singaporean government declares that it owns or controls the Internet, it does so only nominally. If the Singaporean government threatened to revoke the class license, the system would produce better results.

However, it is illegitimate for a government to declare, whether *de facto* or *de jure*, that the Internet resources are exclusive and that citizens need to secure the governments permission before using the it. The scheme of "inalienable" class licenses is married by such unjustifiable implications. Furthermore, if the Singaporean government used licensing as a condition (i.e., to repeal the license or shut down the websites) to force the ICPs or ISPs to censor certain online speech, such a regime could be considered as not applying the least restrictive means as compared with fines or suspension of the license.

C. United States—Internet Control Through Government-Private Partnership

The grounds for the United States to specifically design a set of means or system to control Internet speech may be summarized to include national security, child protection, and copyright.[175] The United States' government-private partnership system requires private ISPs or ICPs to cooperate with the government

[170] *Id.*

[171] Malakoff, *supra* note 155, at 443–46.

[172] Hogan, *supra* note 155, at 446.

[173] *See id.* at 446–47.

[174] *Id.*

[175] *See* CHRISTINE ZUCHORA-WALSKE, INTERNET CENSORSHIP: PROTECTING CITIZENS OR TRAMPLING FREEDOM 43–59 (2010).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

to either monitor the Internet or block access.[176] In the following discussion, each of the grounds permitting Internet control are analyzed and compared with international human rights standards under the ICCPR and United States constitutional standards.

1. National Security

In response to the terrorist attack of September 11, 2011, the United States passed the USA PATRIOT Act ("Patriot Act")[177] on October 26, 2001 to provide the government with greater authority to search private communication data.[178] Particularly, the Patriot Act authorizes government agents to intercept e-mail communications and monitor online activities.[179] The Stored Communication Act ("SCA") gives the government further power to require online communication service providers to disclose subscribers' private information with a court warrant, in accordance with criminal procedure rules.[180]

National security is an explicitly given and justifiable ground under Article 19.3 of the ICCPR to restrict the free flow of information online.[181] Perhaps because the ground is highly justifiable, the constitutionality of controlling the Internet for the sake of national security is less likely to be controversial or challenged by courts.[182] The remaining issue is whether the means chosen by the United States is necessary to achieve that goal. The principle of proportionality would play a critical role here.[183]

The means adopted by the United States government include monitoring and intercepting, which are equivalent to online surveillance.[184] Surveillance would

---

[176] *See* Julie Adler, Note, *The Public's Burden in a Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship*, 20 J.L. & POL'Y 231, 233–34 (2011).

[177] Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001), *available at* http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

[178] *See* Doe v. Gonzales, 449 F.3d 415, 418 (2d Cir. 2006).

[179] *See* 18 U.S.C. § 2516 (2012).

[180] *See id.* at § 2703.

[181] *See* ICCPR, *supra* note 59.

[182] *See* ZUCHORA-WALSKE, *supra* note 175, at 100.

[183] *See* U.N. GAOR Human Rights Committee, 102d Sess., ¶ 34, U.N. Doc. CCPR/C/GC/34 (2011).

[184] *See* ZUCHORA-WALSKE, *supra* note 175, at 100.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

inevitably invade one's privacy as protected by ICCPR Article 17,[185] and the Committee has already declared that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[186] In light of the interests involved (i.e., online privacy and free flow of information) and the degree of interference that would be caused, these measures should not be deemed proportional under Article 19.3 of the ICCPR. Further, is monitoring every online communication necessary? Or, given the increased interest of the free flow of information in cyberspace, do the measures stifle the online free flow of information unnecessarily?[187] These are questions that the government would need to answer under the necessity test of Article 19.3. National security is definitely not an absolute authorization by the ICCPR; the measures adopted by the government under such ground should still observe the necessity and proportionality principle under Article 19.3 of ICCPR.

2. Child Protection

The United States Congress first enacted the Communication Decency Act of 1996 ("CDA") to criminalize deliberate delivery or display of any message that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs" to persons under the age of eighteen.[188] Although, the act was intended to protect minors from harmful materials online, the U.S. Supreme Court invalidated it in *Reno v. American Civil Liberties Union* (1997).[189] In holding the statute unconstitutional under the First Amendment, the Court applied a strict scrutiny analysis to conclude that the terms "indecent" and "patently offensive" were vague and broad.[190] "The vagueness of such a regulation[,]" the Court explained, "raises special First Amendment concerns because of its obvious chilling effect on free speech."[191]

---

[185] Article 17 of ICCPR reads: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." ICCPR, *supra* note 59, at art. 17.

[186] U.N. GAOR Human Rights Committee, 32d Sess., ¶ 8, U.N. Doc. CCPR/C/GC/16 (1988).

[187] *See* DELBERT ET AL., *supra* note 7, at 45–51 (illustrating the overbroad problem of online filtering).

[188] 47 U.S.C. § 223(d) (1996), *declared unconstitutional by* Reno v. ACLU, 521 U.S. 844 (1997).

[189] Reno v. ACLU, 521 U.S. 844 (1997).

[190] *See id.* at 870–72.

[191] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

Congress' other effort to control Internet content in 1996 was the Child Pornography Prevention Act ("CPPA"), which redefined the federal prohibition on child pornography to include pornographic images on computers.[192] In *Ashcroft v. Free Speech Coalition* (2002), the Supreme Court found the CPPA unconstitutional on the grounds that the community standards of the CPPA are overly vague and broad in determining child pornography, and it was not a necessary means.[193]

Congress did not cease efforts to create online child protection measures after losing the two battles in the Supreme Court. In 1998, Congress enacted the Child Online Protection Act ("COPA").[194] COPA required online commercial providers of "material harmful to minors" defined by contemporary community standards, to restrict minors' access to their sites by requiring a credit card number.[195] Failure to comply with COPA carried criminal liabilities.[196]

The Supreme Court in *Ashcroft v. American Civil Liberties Union* (2004) held that the U.S. Court of Appeals for the Third Circuit correctly affirmed the district court's ruling that enforcement of COPA should be prohibited because the statute violates the First Amendment.[197] In its analysis, the Court considered whether less restrictive, but just as effective, measures existed than those employed by COPA.[198] The Supreme Court reasoned that blocking and filtering software is a less restrictive and likely a more effective alternative, since the filters "impose selective restrictions on speech at the receiving end, not universal restrictions at the source."[199] However, there are two other potentially less restrictive alternatives to COPA that Congress passed after the district court trial: a ban on misleading domain names and a statute for the creation of a "Dot Kids" domain.[200] The Court remanded the case, in part, to "allow the District Court to take into account those additional potential alternatives."[201]

---

[192] 18 U.S.C. § 2256(8) (2012).

[193] Ashcroft v. Free Speech Coalition, 535 U.S. 234, 258 (2002).

[194] 47 U.S.C. § 231 (2006), *declared unconstitutional by* ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. Pa. 2007).

[195] *Id.*

[196] *Id.*

[197] Ashcroft v. ACLU, 542 U.S. 656 (2004).

[198] *Id.* at 660–67.

[199] *Id.* at 666–67.

[200] *Id.* at 672.

[201] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

Additionally, Congress passed the Children's Internet Protection Act of 1999 ("CIPA") to grant federal funds to public libraries that install software to block obscene and pornographic information.[202] The Supreme Court upheld CIPA and out of six concurring justices, four justices reasoned that CIPA "help[s] public libraries fulfill their traditional role of obtaining material of requisite and appropriate quality for educational and informational purposes . . . [e]specially because public libraries have traditionally excluded pornographic material from their other collections."[203]

Based on the foregoing, combating child pornography with a selective blocking and filtering system is more likely to be held constitutional than a general denial of access. With regards to international human rights standards, child protection, especially when it comes to child pornography, can be considered an important public moral that is content-specific under Article 19.3 of the ICCPR.[204] In this respect, the online child protection makes the United States' Internet control model distinct from China's general access denied Internet control model. Selective blocking and filtering system is appropriate to achieve the goal of protecting children and also proportionate under the necessity test of Article 19.3. The question left for future discussion, however, is whether there are alternatives to the filtering scheme that the international community or U.S. Supreme Court will find less restrictive.

3. Online Copyright Protection

Using licenses, criminal sanctions, or subsidies to require online service providers or ISPs to filter or block content is a means of indirect governmental Internet control and should be subject to international human right standards and constitutional review. Even if a government's use of such means passes ICCPR Article 19.3's necessity test,[205] the legitimacy of indirect governmental Internet control still depends on whether the grounds for restriction are specific, like national security or child protection, and not overbroad or general, as in China's case.[206]

---

[202] Children's Internet Protection Act, Pub. L. No. 106-554, 114 Stat. 2763 (2000) (codified as amended in scattered titles and sections of U.S.C.).

[203] United States v. Am. Library Ass'n, 539 U.S. 194, 211–12 (2003).

[204] *See* ICCPR, *supra* note 59; *see also supra* Part II-(III) regarding ICCPR standards to determine legitimate internet control.

[205] Part II *supra* discusses the necessity test.

[206] *Compare* Part III(I) discussing China's Internet control model with Part III(III)(1)–(2) concerning the United States' Internet control model with regards to national security and child protection.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

Is copyright protection a specific enough ground for the U.S. government to justify its government-private partnership scheme to control the Internet? The Digital Millennium Copyright Act of 1998 ("DMCA") Section 512(a)–(d) prescribes safe harbor guidelines for Online Service Providers ("OSPs") to minimize their copyright infringement liability.[207] OSPs are not liable for: (1) transitory digital network communications; (2) system caching; (3) information residing on systems or networks at the direction of users; and (4) information location tools.[208]

OSPs are required to adopt a policy to terminate the accounts of copyright infringers.[209] If the service providers receive a notice from copyright holders or assignees, they must remove or block access to the alleged infringing materials.[210] The notification must specifically identify the infringing elements of the materials.[211]

As will be highlighted in the following analysis, copyright is too broad a reason to filter or block online speech and should not automatically exempt private OSPs from the international human rights restraints.

a. Copyright a Murky Ground to Control the Internet

Copyright protection could be considered a part of public morals under ICCPR Article 19.3 and thus a legitimate ground to restrict the free flow of information online.[212] Nonetheless, since copyright systems do not adopt a registration scheme, it is difficult to learn whether a subject is protected by someone's copyright.[213] Consequently, copyright infringement is seldom a black-and-white issue.[214] It is also difficult to anticipate whether the defendant can successfully invoke the fair use exception.[215]

---

[207] 17 U.S.C. § 512 (a)–(d) (2012).

[208] *Id.*

[209] *Id.* at § 512(i)(1).

[210] *Id.* at § 512(c)(1)(C).

[211] *Id.* at § 512(c)(3)(iii); *see* Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

[212] *See* ICCPR, *supra* note 59.

[213] *See* Darrin Keith, *Copyright's Deus Ex Machina: Reverse Registration as Economic Fostering of Orphan Works*, 55 J. COPYRIGHT SOC'Y U.S.A. 201, 206–09 (2008).

[214] *See* LESSIG, *supra* note 6, at 99, 288.

[215] Fair use is deemed as an important mechanism to balance the conflict between freedom of speech and copyright by the U.S. Federal Supreme Court. *See generally* Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 529, 559–60 (1985); Eldred v. Ashcroft, 537 U.S. 186, 218–20 (2003).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

Under the DMCA, OSPs are required to take down online copyright infringing materials after receiving a notice from the right holder.[216] This empowers private copyright holders, or "claimers," in lieu of the court, to determine whether their copyright is infringed.[217] This makes the system susceptible to abuse of power.[218] Further, the system neutralizes the fair use exception because fair use is barely possible to be invoked by the claimed infringer against an OSP's removal of materials prompted by copyright claimers.[219] In essence, the DMCA is discretionary and nonspecific and therefore cannot serve as a legitimate justification to restrict the free flow of information online.[220] For this same reason, DMCA also resembles the Chinese licensing and filtering censorship model.[221] Accordingly, the DMCA, as it currently stands, defies the international human rights guaranteed by Article 19 of the ICCPR.[222]

b. OSPs Should Be Subject to International Human Rights Restraints

The U.S. government could argue that in its government-private partnership scheme, the OSP is the entity that takes down and terminates the accounts, not the government. As such there are no international human rights or constitutional

---

According to Section 107 of the Copyright Act of 1976, 17 U.S.C. § 107, "the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright." The factors for determining fair use include

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

[216] *See* Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 683–84 (2006) (finding that the take-down procedure sometimes involved misled copyright holders' notices and created problematic requests not provided by the DMCA).

[217] *Id.*

[218] *Id.*

[219] *Id.* at 666. *See generally* Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 559–60 (1985) (to see idea and expression dichotomy and fair use as an important mechanism to balance the freedom of speech and copyright); *see also* 17 U.S.C. § 107 (2012).

[220] *See supra* Part II discussing ICCPR standards to determine legitimate internet control.

[221] *See supra* Part III(I) discussing China's internet control model; *see also* DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE 17–19 (2009) (characterizing the DMCA as ISP censorship scheme).

[222] *See supra* Part II.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

issues in the strictly private relationship between private parties. However, the general principle underlying most worldwide constitutions is that human rights protections are the responsibility of the State, and not a private person.[223] In the United States, there is the state action exception, which holds that when there is a "sufficiently close nexus" between the government and a private person's action, the action should be deemed a state action and subjected to constitutional restraints.[224] Private activities on government property, services supervised and investigated by the government, and private assumption of public functions have been considered by the Supreme Court to constitute a sufficiently close nexus.[225]

The state action theory is not limited to the United States, but has been recognized by the UNGA in Responsibility of States for Internationally Wrongful Acts in Article 6, which reads:

> The conduct of an organ placed at the disposal of a State by another State shall be considered an act of the former State under international law if the organ is acting in the exercise of elements of the governmental authority of the State at whose disposal it is placed.[226]

Dawn C. Nunziato argues that the state action theory should apply in the virtual world; that Internet intermediaries, such as OSPs, are serving traditional government functions and are in close association with the government; and that the government evades responsibility by delegating its power to Internet intermediaries.[227] In fact, Internet intermediaries in online forums is precisely the

---

[223] *See generally* G.A. Res. 2200A (XXI), U.N. GAOR, Supp. No. 16, U.N. Doc. A/2890 (Mar. 23, 1976) (the Preamble of the ICCPR reads: "[c]onsidering the obligation of States under the Charter of the United Nations to promote universal respect for, and observance of, human rights and freedoms, ..."); *The Civil Rights Cases*, 109 U.S. 3, 11 (1883) (stating that Fourteenth Amendment of the United States Constitution does not cover individual invasion of the individual rights).

[224] *See, e.g.*, Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U.L. REV. 503, 504 (1985); Fernando A. Bohorquez Jr., Note, *The Price of PICS: The Privatization of Internet Censorship*, 43 N.Y.L. SCH. L. REV. 523, 539–40 (1999).

[225] *See* Burton v. Wilmington Parking Auth., 365 U.S. 715 (1961) (private use of government property) (deeming that lessee of state property should be bound by the Fourteenth Amendment if lease furthers and forms integral part of state operation). *See* Pub. Utilities Comm'n v. Pollak, 343 U.S. 451 (1952) (service supervised and investigated by government). *See* Marsh v. Alabama, 326 U.S. 501 (1946) (considering town corporation owner should be subject to First Amendment constraints).

[226] U.N. G.A. Res. 56/83, art. 6, U.N. Doc. A/RES/56/83 (Dec. 12, 2001).

[227] NUNZIATO, *supra* note 221, at 97–100. *See also* Dawn C. Nunziato, *How (not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide*, 42 GEO. J. INT'L L. 1123, 1141 (2011) (claiming that the state action doctrine should apply to ISP in cyberspace).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

private assumption of public functions that the Supreme Court held to be state action, such as the private management of a company town in *Marsh v. Alabama*.[228] In cyberspace, the operator or host of a discussion forum enjoys the power to shape the rules and order on that forum.[229] It is a space involving a government-and-private person relationship. Thus, the ICCPR's human rights standards should be applied to prevent the government from dodging constitutional responsibilities.

Furthermore, the notice and takedown scheme was devised by the United States legislature in order to relieve OSPs of their burden of secondary copyright liability and reduce copyright holders' expenses for proving infringement.[230] The safe harbor offered to OSPs for taking down dubious online speech and the power of private copyright claimants to call out an infringement both come from government authorization.[231] From this perspective, the DMCA's immunity scheme is just like China's and Singapore's license system of Internet control.[232]

The question to be asked about the DMCA is whether Internet intermediaries should be assigned secondary liability, especially vicarious infringement liability.[233] Perhaps realizing vicarious liability would put too much burden on OSPs; Congress designed the DMCA immunity scheme to alleviate the burden.[234] However, due to the unclear criteria for the copyright holders in determining copyright infringement, the scheme remains cause for concern.[235]

---

[228] *Marsh*, 326 U.S. at 501. *See* Adler, *supra* note 176, at 253–54.

[229] *See* Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, *in* BORDERS IN CYBERSPACE: INFORMATION POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE 90–91 (Brian Kahin & Charles Nesson eds., 1997).

[230] *See* Urban & Quilter, *supra* note 216, at 636.

[231] *See* 17 U.S.C. § 512(a)–(d) (2012).

[232] *See supra* Part III(I)–(2) discussing China's and Singapore's Internet control system.

[233] Vicarious infringement was established and illustrated by MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930–31 (2005) (holding that if the defendant has the ability to supervise the infringing conduct and has a direct financial interest from the infringing activity, he should be vicariously liable for the infringement).

[234] *See* 17 U.S.C. § 512(a)–(d) (2012).

[235] The DMCA only requires the claimed copyright holder to fulfill certain forms of notification, and a statement that "the complaining party has a good faith belief that use of the material in the manner complained of is not authorized" by it. There is no actual criteria for the OSPs to determine whether the copyright is indeed infringed. 17 U.S.C. § 512(c)(3)(a)(v).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

IV. BEST FIT FOR TAIWAN—INTERNET CONTROL OR CENSORSHIP?

A. Different Constraints in Different Models

Social norms, market, and architecture are different between the virtual world and physical world. But the comparison of three models shows that even in just the physical world, the three constraints operate differently. Regional differences, including culture, market, and government structure, affect the constraints which, in turn, impacts the development of Internet control models.

In China, the social norms are created and formed by the government.[236] Democracy may be demanded by the people but not available; order is more important, superseding all values.[237] The restrictive measures for Internet control, particularly general and vague terms such as national unity and state honor, make China's Internet control model one of censorship.

In Singapore, the government's class license scheme, which lacks governmental threats to repeal licenses to force ISPs and ICPs to censor the Internet, constitutes a unique architecture, different from the other Internet control models across the globe. The Singaporean Internet control architecture reflects, to a certain extent, the social norms of Singapore.[238]

Finally, the United States' government-private partnership mode of Internet control gives exclusive regulatory power to the online intermediaries.[239] This model recognizes that the real dominant force in the online market is not the government in physical world, but the online intermediaries as internet access gatekeepers.

---

[236] *See* Miron Mushkat & Roda Mushkat, *Economic Growth, Democracy, the Rule of Law, and China's Future*, 29 FORDHAM INT'L L.J. 229, 256 (2005) (claiming China as "the ruling elite maintains a firm grip on society," and "the measure of benevolence and self-restraint" are "displayed by the power holders.").

[237] *See id.* at 256 (arguing that there are "two key aspects to the "anti-political" orientation. One is the rejection of a pluralism of interests and viewpoints in favor of a putative and exigent unity of purpose. Differences are denied rather than reconciled. Consequently the second is the search for an imposition of a singular form of rationality or a unitary principle onto political debate," and citing Bruce Gilley's argument that "these two aspects of the end-of-politics syndrome—an emphasis on the unity of interests and a unitarian principle—are playing a pivotal role in shaping policy in early Twenty-First Century China in the concrete form of the doctrine of economyism and the doctrine of proceduralism.").

[238] *See* Joseph C. Rodriguez, *A Comparative Study of Internet Content Regulation in the United States and Singapore: The Invincibility of Cyberporn*, 1 ASIAN-PAC. L. & POL'Y J. 9, 39 (2000) ("The differences between the U.S. and Singapore Internet content regulations demonstrate that the individual plays a more subordinate role in Singapore society than in U.S. society. That is, individual rights are more subordinate to government interests in Singapore than in the U.S.").

[239] *See supra* Part III(III).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

How do the social norm, market, and architecture constraints operate in Taiwan? Many of Taiwan's social norms are similar to China. For instance, stemming from Confucianism, China's tradition, culture, and thought do not emphasize IP rights protection.[240] Similarly, as observed by Jean Lin, due to the fact that "Taiwan's lack of protection of intellectual property has cultural roots" and is impacted by traditional Confucian thoughts, copyright enforcement faces difficulties.[241] At the same time, however, Taiwan is affected by United States intellectual property protection pressure and policies.[242] For example, Taiwan amended its Copyright Act to fulfill the U.S. government's expectations.[243] Taiwan's Copyright Act is constructed by market force from United States, and the law itself eventually changes the social norms for protecting copyright.[244]

B. Lessons From the Internet Models Comparison

The comparative analysis of China's, Singapore's, and the United States' model shows that the grounds for regulation matter the most in determining whether the model constitutes illegitimate censorship or legitimate control under Article 19 of the ICCPR. The grounds for the government to restrict the free flow of information in cyberspace should not be general and vague, but specific and targeted enough to achieve the objectives listed in Article 19.1 and 19.2 of the ICCPR.[245]

To be legitimate, the means adopted by the government to achieve its control objectives must survive Article 19.3's necessity test.[246] The free flow of

---

[240] Heidi Hansen Kalscheur, *About "Face": Using Moral Rights to Increase Copyright Enforcement in China*, 39 HASTINGS CONST. L.Q. 513, 515–16 (2012).

[241] Jean Lin, *The U.S.—Taiwan Copyright Agreement: Cooperation or Coercion?*, 11 UCLA PAC. BASIN L.J. 155, 166–67 (1992).

[242] *See, e.g.*, Trade Act of 1974 § 301, 19 U.S.C. § 2411 (2012).

[243] *Id.*; *see also* Lin, *supra* note 241; Laura W. Young, *IP Protection in China and Taiwan*, THE LAW OFFICE OF WANG & WANG, http://www.wangandwang.com/news-articles/articles/ip-protection/ (last visited Nov. 11, 2013) (stating "By early 1992 losses due to copyright piracy were estimated at U.S. $669 million. The U.S. designated Taiwan as a Priority Foreign Country and initiated an investigation into its trade practices, a process that can end with trade sanctions against the listed trade partner. Under this pressure, Taiwan's Legislative Yuan passed the new copyright law within two months, and the investigation was terminated. Taiwan executed a bilateral Memorandum of Understanding ("MOU") with the U.S. in 1989, in which Taiwan agreed among other things, to promulgate a new Copyright Law."),

[244] Lin, *supra* note 241 (stating Section 301 of the Trade Act of 1974 leverages the benefits of trading with the U.S. market to achieve compliance with international trade norms).

[245] *See supra* Part II. *See also* ICCPR, *supra* note 59, at Art. 19, general cmt., ¶ 34.

[246] *See* Part II *supra* discussing the necessity test.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

information is a greater interest in cyberspace than in the physical world.[247] The interests of Internet users worldwide should be more important than those of local users. Therefore, greater consideration should be given to the free flow of information online.

Systems like the Chinese Great Firewall that create a blocking list and utilize general filtering to protect generic and abstract interests are not necessary, as there is a lack of "direct and immediate connection between the expression and the threat."[248] The licensing systems of both China and Singapore are not the least restrictive means,[249] mostly because the government has no justification to claim ownership over the Internet, and there are other available means (e.g., fines or suspension of the license).

Under the government-private partnership scheme, such as the one adopted by the United States, whether a case-by-case filtering and blocking system or a selective system for child protection is a necessary means is disputable.[250] At the very least, these measures are more justifiable under Article 19.3 of the ICCPR when used to control the online activities of underage users.

As to online copyright protection, the immunity scheme adopted by the United States to force OSPs to monitor and block access to infringing materials does not pass the necessity test because copyright infringement cannot be clearly defined.[251] The judiciary remains the only suitable authority to decide whether a copyright has been infringed, after hearing both sides' arguments and considering both the copyright infringement and fair use exception. Conferring the power of judging copyright issues on OSPs or right holders render the government-private

---

[247] See Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. DAYTON L. REV. 179, 183 (2001).

[248] U.N. GAOR Human Rights Committee, 102d Sess., ¶ 35, U.N. Doc. CCPR/C/GC/34 (2011).

[249] *See id.* at ¶ 34.

[250] The blocking and filtering software could be argued as not a less-restrictive mean. *See, e.g.*, Emily Vander Wilt, *Considering COPA: A Look at Congress's Second Attempt to Regulate Indecency on the Internet*, 11 VA. J. SOC. POL'Y & L. 373, 422–23 (2004) (stating "Blocking and filtering software is not a satisfactory alternative to COPA's regulation of Web producers because it puts the whole onus of protecting children on the potential victims of harmful material and their parents, and removes the government from any involvement whatsoever."); Amitai Etzioni, *On Protecting Children from Speech*, 79 CHI.-KENT L. REV. 3, 33 (2004) (stating "However, when it comes to the protection of children from harmful cultural materials, voluntary protections are highly ineffectual. Most parents and educators do not activate the V-chips in their televisions; movie theaters, and most assuredly CD shops and video rental stores, often do not enforce the rating and labeling systems in place; and only a minority of parents purchase protective filtering software for their home computers.").

[251] *See supra* Part III-(III)-(3).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

partnership scheme suspicious under Article 19.3 of the ICCPR, as protecting copyright determined by private parties may not serve as a justifiable ground.

The real risk of the government-private partnership model is that the government could delegate its duty and function to private online service providers to evade constitutional or international human rights obligations.[252] The United States state action theory should therefore be adopted to prevent this kind of risk.[253]

A critical lesson drawn from efforts to apply the state action doctrine on the Internet is not that there is a State behind the private online service operators, but that in cyberspace, the private service operators are the real controllers or power holders.[254] One commentator rightly points out that there are at least four dangers in granting Internet control power to private proxies: the danger of error, the danger of self-censorship blocking any content that could precipitate the threat of sanctions, the danger of adopting over restrictive measures, and the danger of a lesser likelihood to challenge the proxy's action in the court.[255] Each of these dangers carries with it a high possibility of causing a chilling effect, thus equating to censorship.[256]

Tim Wu noted, "[p]ower is power, wherever it is found," and "private sector power over speech can be nearly as terrifying as public power."[257] As long as private ICPs or ISPs hold the power to control the Internet there is a danger of a chilling effect. International human rights cannot be ignored simply because the ICP or ISP is not a government entity. The state action theory must be carefully used on a case-by-case basis to ensure that Internet users' right to the free flow of information is protected from private online services operators.

---

[252] *See supra* Part III-(III) discussing adoption of state action theory.

[253] *Id.*

[254] *See, e.g.*, EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 101–03 (2011) (suggesting that it is the private companies that are conducting today's censorship); Lawrence Soley, *Private Censorship, Corporate Power*, *in* CENSORING CULTURE: CONTEMPORARY THREATS TO FREE EXPRESSION 15, 15–28 (Robert Atkins & Sevtlana Mintcheva eds., 2006) (discussing the expansion of corporate power in relationship to censorship).

[255] Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 27–32 (2006). *See also* Jay Wahlquist, *The World Summit of the Information Society: Making the Case for Private Industry Filtering to Control Extraterritorial Jurisdiction and Transnational Internet Censorship Conflict*, 1 INT'L. & MGMT. REV. 283, 300–02 (2005).

[256] Kreimer, *supra* note 255 (discussing dangers of censorship by proxy).

[257] Tim Wu, *Is Filtering Censorship? The Second Free Speech Tradition*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 83, 97 (Jeffrey Rosen & Benjamin Wittes eds., 2011).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

Article 19 of the ICCPR only requires a state to protect the free flow of information in cyberspace; the State *may* but is not required to restrict the online free flow of information on the grounds of certain important government interests.[258] A State will always encounter challenges in circumscribing the right of worldwide online users when doing so in the name of a local interest, no matter how trivial.[259] Child protection, an issue that continues to gain attention globally, may be a justifiable ground. However, with regards to vague interests like national security, copyright infringement, defamation, and other interests that are still more local, the State should always be cautious in choosing whether to regulate the Internet on the basis of such local interests and the type of means used to regulate.

C. Future of Taiwan's Internet Control: Remaining Meager is Not Evil

Juxtaposing Taiwan's current meager Internet controls[260] with those of China, Singapore, and the United States, makes evident that Taiwan's paradigm is a borderline censorship model similar to the United States' government-private partnership scheme. The Child Protection Act adopts a selective program demanding self-discipline and access denial from ISPPs at the request of the government to shield minors from online pornographic materials.[261] This measure is specific and likely sufficiently necessary to survive Article 19.3's necessity test.

On the other hand, Taiwan's current Copyright Act paradigm is problematic and a lightning rod for controversy. The immunity afforded to OSPs under Taiwan's Copyright Act, which is similar to the United States' DMCA, is potentially unconstitutional and certainly susceptible to criticism.[262] Furthermore, by compelling OSPs to monitor and block access in cyberspace, Taiwan's Copyright Act is unjustifiable restriction under Article 19.3 of the ICCPR.

---

[258] *See supra* Part II discussing legitimate grounds to restrict freedom of expression under ICCPR.

[259] *See* David R. Johnson, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370–74 (1996).

[260] *See, e.g.*, Taiwan's Child Protection Act and Copyright Act. *See Child and Youth Welfare Protection Act* (Taiwan), promulgated on Aug. 8, 2010, *available at* http://lis.ly.gov.tw/lgcgi/lglaw?@18:1804289383:f:NO%3DC705125*%20OR%20NO%3DC005125%20OR%20NO%3DC105125$$4$$$NO (last visited Apr. 20, 2013); *The Copyright Act*, *supra* note 15.

[261] *See* art. 46 of the *Child and Youth Welfare Protection Act*, *supra* note 260 (last visited Nov. 9, 2013).

[262] *See* Fa-Chang Cheng, *The Reflection of DMCA Safe Harbor Rule in Thinking of General Liability for the ISP Through its Users' Violation of Law within Cyberspace*, 1 INT'L J. SOUND, MUSIC & TECH. 5, 9 (2011), *available at* http://www.3kbioxml.com/3k/index.php/IJSMT/article/viewFile/88/50 (stating "To embody the "notice and take down" policy into the law protecting other interests may run the risk of directly conflicting with the freedom of speech by its nature and may be invalid because the law cannot pass the constitutional strict scrutiny.").

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

Taiwan currently faces calls for legislation that implements a more intricate Internet control model. In June of 2013, the Intellectual Property Office proposed an amendment to copyright law to establish a blacklist for foreign websites that infringe copyright and require the ISPs to block those websites.[263] Under the pressure from Internet groups' advocacy and public criticism, the Intellectual Property Office finally withdrew such attempt.[264] As this issue continues to develop, one thing is certain: Taiwan has a choice between fully endorsing and practicing Internet censorship or protecting the free flow of information online with a moderate but necessary control system.

How should Taiwan Internet control legislation evolve to comply with international human rights? Stop following the United States' stringent and expanding online copyright protection model would be the first step. Furthermore, in designing any further Internet control mechanism, as lessoned from the models comparison, the protected interest must be specific and concrete, and the measures adopted for protecting such interest must be necessarily designed under Article 19.3 of ICCPR. Keeping in place the current meager online regulation paradigm is not an evil. After all, the Internet control models of China, Singapore, or United States, no matter how different they are, represent only one type of Internet governance—the model of regulating Internet by national government and law.[265] Opposite of this internal government and law model are self-regulating and market and economic models for Taiwan to select. A mixture of both does not violate the

[263] Maira Sutton, *Taiwanese Users Thwart Government Plans to Introduce Internet Blacklist Law*, ELECTRONIC FRONTIER FOUND. (June 3, 2013), https://www.eff.org/deeplinks/2013/06/taiwanese-users-thwart-government-plans-introduce-internet-blacklist-law.

[264] *See* Sharone Tobias, *Internet and Press Freedom in Taiwan*, THE DIPLOMAT (June 28, 2013), http://thediplomat.com/the-editor/2013/06/28/internet-and-press-freedom-in-taiwan/.

[265] Lawrence B. Solum observed and categorized into five Internet governance models as following: 1. The model of cyberspace and spontaneous, which refers to the Internet self-autonomous right. This model can be understood as that the Internet community should govern by itself. 2. The model of transnational institutions quasi-private cooperative and international organizations based on the treaty agreement between nations, which refers the Internet governance to build a structure like national borders in the cyberspace as a whole. 3. The model of code and Internet architecture, which to certain extent barrows the concept of Lawrence Lessig the code is the law in cyberspace. Internet governance then refers to the protocols or software that decides the Internet orders. 4. The model of national governments and law, which relies the Internet governance on the internal regulations of each states with the traditional notion of borders. 5. The model of market regulation and economics which assumes that market forces drive the fundamental decisions about the nature of the Internet. *See* Lawrence, *Models of Internet Governance*, *in* INTERNET GOVERNANCE: INFRASTRUCTURE AND INSTITUTIONS 48–91 (B. Solum Lee A. Bygrave & Jon Bing eds., 2009).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu

requirements of international human rights and Taiwan could form its "let the internet free"[266] paradigm as the fourth Internet control model.

[266] *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html (last visited Nov. 9, 2013) (stating "We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.").

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.131 ● http://tlp.law.pitt.edu