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

Jeffrey Li, Harvard Law School

Available at: https://works.bepress.com/jeffrey_li/1/
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 generally refers to unjustified online speech scrutiny and control by the government or government-approved measures for Internet control. The danger of Internet censorship is the chilling effect and the substantial harm on free speech, a cornerstone of democracy, in cyberspace. This paper compares China’s blocking and filtering system, the class license system of Singapore, and the government-private partnership model of the United States to identify the features, and pros and cons of each model on the international human rights. By finding lessons from each of the model, this paper suggests Taiwan should remain its current meager internet control model and remand flaws in its government and private partnership model adopted by the Copyright Act in accordance with the international human right standards.
# Table of Contents

## PART I. INTRODUCTION ..................................................................................1

## PART II. TAIWAN’S CURRENT INTERNET CONTROL: A U.S. MODEL FOLLOWER ................................................................................................................5

## PART III. WHAT IS “INTERNET CENSORSHIP”? ........................................8

### I. The Features of the Internet and Their Constitutional Implications ..........8
  1. Social Norms........................................................................................................9
  2. Market .................................................................................................................10
  3. Architecture ........................................................................................................11
  4. How Should Law in Cyberspace Be Different? ..................................................13
     (1) Free flow of information in cyberspace .........................................................14
     (2) Access to the Internet as a Human Right......................................................20

### II. The Meaning and Danger of Censorship ..............................................23

### III. The ICCPR Standards to Determine Legitimate Internet Control ..........27

## PART IV. THREE INTERNET CONTROL MODELS .....................................31

### I. Wide Blocking and Filtering—China .........................................................31
  1. The Legal Grounds for the Government to Control Internet Speech ................33
  2. China’s Great Firewall and License System ......................................................35

### II. Internet Control Model Based on Licensing System—Singapore ............38

### III. Internet Control Model of Government and Private Partnership: United States ....43
  1. National Security .................................................................................................43
  2. Child Protection ................................................................................................45
  3. Online Copyright Protection ..........................................................................48
     (1) Copyright a Murky Ground to Control the Internet .....................................49
     (2) OSPs Should Be Subject to International Human Rights Restraints ..........51

## PART V. BEST FIT FOR TAIWAIN—INTERNET CONTROL OR
CENSORSHIP?.........................................................................................................................54

I. Different Constraints in Different Models .................................................................54

II. Lessons From the Models Comparison........................................................................56

III. Future of Taiwan’s Internet Control: Remain Meager is not Evil.................................60
Part I. Introduction

In 2005, Telus, a Canadian telephone company and Internet service provider (“ISP”), blocked its subscribers from accessing the website of the Telecommunications Workers Union (“TWU”). The reason for the block, according to Telus, was to stop the TWU site from inciting the workers to jam Telus’s lines. But the TWU called the move an act of censorship. A similar event happened recently in Brazil. Google in Brazil removed links to a video on YouTube criticizing a candidate in the Brazilian municipal elections in order to obey a court order that found the video would "offend the dignity or decorum" of the candidate.

Censorship, or more specifically, Internet censorship is at the heart of those two cases. The concept of censorship, or just the word itself, evokes distaste and anxiety. Whenever a threat that the right to speak and receive information in cyberspace is perceived, the popular opinion is against it.

---

2 Id.
In comparison, *Internet control* is a more innocuous term. While the way China manages the Internet is widely viewed as censorship, democratic Asian territories like Hong Kong and South Korea have *Internet control* rules. Hong Kong’s the Crimes Ordinance and the Telecommunications Ordinance criminalize attempts to suppress information; the Crimes Ordinance in particular punishes a dishonest intent to deceive with a view to obtaining gain for oneself or another, and a dishonest intent to cause loss to another.\(^4\) As to South Korea, the grounds for Internet control include defamation, child protection, obscenity, and subversive communication, which are all legitimate reasons under South Korean laws for ISPs to block access.\(^5\) Christian Oliver of the *Financial Times* has even suggested that South Korea blocks access to North Korean websites.\(^6\)

South Korea’s Internet control is generally considered more pervasive than Hong

---


\(^6\) Christian Oliver, *Sinking underlines South Korean view of state as monster*, FINANCIAL TIMES (April 1, 2010), http://www.ft.com/intl/cms/s/0/d77d855e-3d26-11df-b81b-00144feabdc0.html#axzz20xDYLDr.
Kong's while less rigorous than China’s infamous Great Firewall. Why does the world perceive China’s Internet regulation as censorship, while other countries’ Internet control systems inspire less distaste? Is it simply because China is not a democracy? More specifically, what constitutes Internet censorship and what exactly is there to fear in censorship?

In fact, there is still a lack of general consensus on how the Internet should be patrolled or regulated worldwide. As the Internet has woven itself into the daily lives of many people on the planet, the control model chosen will inevitably affect the free flow of information and spark free speech concerns and debate. At the center of the debate is whether the 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 rethink its own paradigm requires an analysis of the features of several foreign Internet control

---

models. The comparative method will be applied: to compare Internet control models of China, Singapore, and United States to shed the light on the model selection in Taiwan.

China and Singapore are selected for this survey because like Taiwan, their populations are primarily ethnic Chinese, making them culturally similar to Taiwan. As to the selection of the United States, though Taiwan is a civil law country, many Taiwanese laws are patterned after U.S. laws, especially the U.S. Copyright Act. The survey and the comparison that follow will show how constitutional and international human rights drive or clash with the different models of Internet control.

Part II of this paper discusses the current Internet control-related laws in Taiwan. Part III seeks to answer how cyberspace is different from the physical world, why Internet censorship is noxious, and how the laws that govern cyberspace should be different. Part IV examines three different representative Internet control models: China’s blocking and filtering system, Singapore’s class licensing scheme, and the U.S. government-private partnership model. The international human rights standards under the ICCPR will be applied to analyze the legitimacy of the three Internet models. Lastly, Part V discusses how different constraints form different internet
control model, lessons from models comparison, and how to select the internet control model in Taiwan as the conclusion.

**Part II. Taiwan’s Current Internet Control: A U.S. Model Follower**

Like Hong Kong and South Korea, Taiwan is a democracy; but unlike them, it does not have a general Internet control system, nor has it taken any meaningful steps to patrol speech in cyberspace.

Taiwan is a civil law country. Most of its statutes mirror or are patterned after other countries’ legislation, mostly notably that of the U.S., Germany, and Japan. Although the Taiwan Constitutional law has its own provisions and language, the Constitutional Tribunal sometimes refer to the international human rights treaties or conventions to augment their exposition of certain clauses when interpreting the Constitution.⁹

---

While the country's Internet control at this stage is meager, its Protection of Children and Youths Welfare and Rights Act (the “Child Protection Act”) and Copyright Act do provide an online speech monitoring mechanism.

Articles 46 (2) and (3) of the Child Protection Act require Internet platform providers to establish self-disciplinary measures to protect children’s moral development, restrict the users’ ability to receive or browse, and voluntarily take down certain content after failing to establish such self-disciplinary measures or being informed by the government that certain online content corrupts the minds of underage users.10 Article 46 (1) authorizes the administrative agency to develop protective systems to prevent children from accessing immoral Internet content, including building filtering software, tracking minor’ behavior on the Internet, and establishing a content grading system.11 The Internet platform provider is defined by Article 46 (3) as an 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).12

11 Id.
12 Id.
Meanwhile, Chapter VI-1 of the Copyright Act provides that online service providers ("OSPs")\(^{13}\) may suspend the accounts of customers accused of downloading copyrighted material more than three times, and ISPs are responsible for removing or denying access to copyright infringing content and alerting customers to the infringement by e-mail after violations are brought to their attention by copyright holders.\(^{14}\) The author has once discussed whether the type of online regulation is justified or necessary under the R.O.C. Constitutional law.\(^{15}\)

Though there are only two laws having internet control mechanism, Taiwan’s internet control regulations are similar to U.S.’s government and private partnership model,\(^ {16}\) which imposes liability on private online intermediaries to help the government to filter or block minor-harmed or copyright infringed online materials.

There are very few online speech court cases in Taiwan involving the Child Protection Act or the Copyright Act. Some Taiwanese legislators have suggested that a

\(^{13}\) The OSPs under the Copyright Act refer to internet service providers, rapid saving service providers, information saving service providers, and searching service providers. See article 3 (19) of the Copyright Act.

\(^{14}\) See the Copyright Act, THE LEGISLATIVE YUEN’S LAW SYSTEM (in Chinese), http://lis.ly.gov.tw/lgcgi/lglaw?@18:1804289383:f:NO%3DC701176%20OR%20NO%3DC001176%20OR%20NO%3DC101176$$4$$$NO (last visited April 26, 2013).


\(^{16}\) The U.S. model will be introduced and analyzed subsequently in Part IV. III.
law governing online regulation should be enacted.\textsuperscript{17} However, none has presented a concrete proposal explaining how the Internet should be regulated. Right now, Though currently Taiwan is a U.S. model follower, it is still shopping for a better Internet-regulation. Comparison between different models will help Taiwan to find clear and justifiable standards in selecting future internet control measures.

Part III. What Is “Internet Censorship”? 

I. The Features of the Internet and Their Constitutional Implications

Trying to define what the Internet or cyberspace is is not as instructive as one might think.\textsuperscript{18} It is more enlightening to look at the differences between the physical world and cyberspace and how the differences affect the formation of law in cyberspace.\textsuperscript{19}

\begin{flushleft}
\textsuperscript{17} Jhen Huei-Jhen, \textit{The visual world also needs the law in real world}, SINA NEWS (October 2009), http://news.sina.com.tw/magazine/article/3585-2.html.
\textsuperscript{19} But see JULIE E. COHEN, \textit{CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE} 45-46 (2012) (considering cyberspace not that different from real space and only the experience is changed).
\end{flushleft}
Lawrence Lessig named four critical forces in cyberspace in his book *Code 2.0*, namely, the law, social norms, market, and architecture. He treats the sum of these four constraints as the beginnings of cyberspace regulation, and each constraint affects the others. The distinctions between the physical world and cyberspace are thrown into relief against three of Lessig’s constraints: the social norms, market, and architecture.

1. **Social Norms**

Social norms are different in the physical and virtual domains, which can be attributed mainly to anonymity in the virtual world. Social norms are not imposed on people through mandatory regulatory measures like laws, but are followed voluntarily for the sake of maintaining their reputation or out of shame or moral conscience. In the physical world, when an individual expresses an unethical opinion, he or she might suffer moral accusation and reputation harm. Such concern is diminished in cyberspace since the identities of speakers are often hidden. Believing they can speak with impunity, individuals are less inhibited and are easily tempted to...

---

21 Id.
lower their moral standards when speaking in cyberspace.\textsuperscript{23}

In terms of age, the denizens of cyberspace are different from those of the physical world. Those active on the Internet are generally young, while those who are powerful and old-money rich are older and do not go about their daily business online, except when checking e-mails or reading the news. While the social norms in the physical world are largely shaped by the older generation, the people active online have created their own norms, with the effect of polarizing the online speech.\textsuperscript{24}

But while 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 still a price to pay for violation of social norms in cyberspace. Someone who is out of line can be banned from speaking or accessing a certain online forum, a punishment that is rare in the physical world for defying social norms.

2. Market

\textsuperscript{23} See YoChai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom 8-9 (2006) (indicating how the enhanced autonomy in cyberspace change the individual’s relationship with the others).

\textsuperscript{24} See Cass Sunstein, Republic.com 2.0 46-96 (2007).
As Lessig has already pointed out, a different pricing system has emerged in cyberspace. The pricing systems in the physical world and cyberspace are not the same. For example, music is presented as a product that can be bought and sold in the physical world, while users may find much of the same online for free. On the other hand, books and articles can be read for free in the libraries of the physical world, while the same digital content cannot be accessed without paying and registering with online database service providers.

The other difference between the two realms is that the most of the markets in the physical world are local, serving consumers or users within a nation’s territory. On the other hand, there are no borders in cyberspace and thus more service providers aim to serve global users online, and they need not consider the costs of doing business across borders as they would have to in the physical world.

3. Architecture

The architecture of the virtual world comprises both software and hardware.

Just like in the physical world, where the skills to drive or use transportation services need to be acquired to move about freely, proficiency in using hardware and software is necessary to roam cyberspace. We are born to know and learn how to walk and act in the physical world, while to learn how to use hardware and software demands further skill learning.

The virtual architecture is more complex than the one in the physical world. Roughly every five years, a new generation of software or hardware is introduced, keeping users interested or confounding them, depending on each person's adaptability. Furthermore, differences between the various brands of software or hardware may confuse users or force changes in their habits. Microsoft in all likelihood will keep upgrading its Windows operating system, and every upgrade can be expected to alienate some users as new habits will have to be cultivated. And making the jump from Microsoft to Apple products also requires a change in habits. These online architecture barriers constitute a form of regulation in the virtual world, while the architecture of the physical world does not drive similar changes at the same pace.
4. How Should Law in Cyberspace Be Different?

Besides the different appearances of the three constraints in virtual world and physical world, each constraint, like law, is also different in regions in the physical world. The regional differences in different constraints will also reflect on the internet control policy. Take the comparison of social norms between China and United States as an example, the traditional Chinese social norms do not treat intellectual property rights (‘IP rights”) as an important issues and thus do not use IP rights as a basis to regulate internet; on the contrary, IP rights are highly valued and respected in United States and thus serve an important ground in controlling internet activities.

Differences between regions should be born in mind to correctly tell the nature of internet control regulations in different models. This will be further analyzed in Part V.

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 cannot be a good fit for cyberspace. According to Lessig, to change any four of the
constraints would change the whole regulation, so 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.

(1) Free flow of information in cyberspace

The free flow of information is an important interest and a human right. The importance and borderless nature of freely flowing information is recognized by many international human rights treaties. Take the International Covenant on Civil and Political Rights ("ICCPR") article 19.2 as an example, which reads:

Everyone 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.

Free flow of information is partly achieved by the right "to seek, receive, and

impert information” and thus should be considered recognized as the freedom of speech under the ICCPR. And “through any other media” qualifies free flow of information online as a freedom protected by the article. A similar provision can be found in article 19 of the Universal Declaration of Human Rights (“UDHR”).

The United Nation (“UN”) Human Rights Committee interprets article 19.2 as “[embracing] a right of access to information held by public bodies,” which 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.” 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 affairs and 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 (emphasis added).” Clearly, the Committee believes

---

30 Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948) (Article 19 of the UDHR 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.”)
31 General Comment No. 34 on Article 19, ¶ 18, U.N. Doc. CCPR/C/GC/34 (2011),
32 Id., ¶ 19.
33 Id.
34 Human Rights Committee, General Comment 25, The right to participate in public affairs, voting rights and the right of equal access to public service (Art. 25), (Fifty-seventh session, 1996), ¶ 25, U.N. Doc. CCPR/C/21/Rev.1/Add.7 (1996),
35 Human Rights Committee, supra note Error! Bookmark not defined., ¶ 20.
Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan’s Choice: Jeffrey Li

censorship refers directly to an illegitimate government restriction on free speech.

Though Taiwan is not a signatory to the ICCPR, Taiwan's Congress approved the ICCPR and the International Covenant on Economic, Social and Cultural Rights (the “ICSCR”) on March 31, 2009 and 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”) subsequently.36 R.O.C. President Ma Ying-jeou officially signed the ICCPR and the ICSCR on May 14, 2009 and they were given force on December 10, 2009. The ICCPR and its General Comments are recognized in Taiwan as a domestic law sand may guide the interpretation of the Constitution.37

The U.S. Supreme Court has expounded on free flow of information in many cases, underscoring the importance of protecting free speech.38 Jonathan Penney, Achal Mehra, and Marci Hamilton and Clemens Kohnen have discussed the free flow

37 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 NEW VOICES ABOUT CAPITAL PUNISHMENT (forthcoming June. 2013).
38 See, e.g., Associated Press v. U.S., 326 U.S. 1, 20 (1945) (free flow of information is a fundamental public welfare elements under the First Amendment); Pell v. Procunier, 417 U.S. 817, 832 (1974) (the freedom of express includes the free flow of information of public figure as the most important public interest); 44 Liquomart, Inc. v. Rhode Island, 517 U.S. 484, 512 (1996) (the text and free flow of information under the First Amendment shows that to regulate speech is more dangerous to regulate conduct).
of information as an independent right.\textsuperscript{39}

Though the U.S. Supreme Court has not yet directly recognized the interest of the free flow of information in cyberspace, the Taiwan Constitutional Tribunal (the “TCT”) has weighed in on the subject tentatively in two interpretations. In the reasoning for Interpretation No. 613, the TCT stated:\textsuperscript{40}

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

\textsuperscript{39} 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 166-167 (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).

\textsuperscript{40} No. 613 reasoning, Taiwan Judicial Yuen Constitutional Tribunal Interpretation (July 21, 2006), http://www.judicial.gov.tw/constitutioyncourt/EN/p03_01.asp?expno=613.
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.

The TCT opined in Interpretation No. 613 that the freedom of communication required the government to prevent the impingement of such freedom but did not give the standards for judicial review. The TCT reiterated its position in Interpretation No. 678.41

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 guidelines whose application depend on

---

41 No. 678 reasoning, Taiwan Judicial Yuen Constitutional Tribunal Interpretation (July 2, 2010), http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=678.
the content of the speech at issue should be created.

The TCT further referred to the necessity test under the R.O.C. Constitution article 23 for reviewing whether the restriction on freedom of communication is justified.\(^{42}\) Though the TCT did not discuss the considerations in weighing and balancing free flow of information with the other interests, it recognized the free flow of information cyberspace as a part of the constitutional freedom of speech in Taiwan.

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.\(^{43}\) 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.\(^{44}\) When any local government desires to impose restrictions on

---

\(^{42}\) Id.

\(^{43}\) See Jeffrey Li, COPYRIGHT V. FREE FLOW OF INFORMATION IN CYBERSPACE 198-200 (2011) (in Chinese).

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 tread necessarily.

The UN General Assembly (“GA”) 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.

(2) **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. The architecture of the virtual world creates barriers for users and thus affects the online community differently, shaping the social norms differently. Meanwhile, the pricing system online is built on the power to control access.

Whether access to the Internet should be recognized as a human right is still highly controversial. Vinton Cerf, one of the opponents on this issue, argues that “technology is an enabler of rights, not a right itself.”46 He believes that technology has failed to meet the “high bar” of being considered as a human right, since the right to make a living, access information, or speak freely is not necessarily coupled to technology.47 On the other hand, advocates for recognizing Internet access as a human right suggest that articles 19 and 27 of the UDHR already provide the basis for treating access to the Internet as a human right, and that such access should not be an isolated right, but inseparable from the right to association and expression.48 One such advocate, Sherif Elsayed-Ali, disagrees with Cerf, arguing that access to the

47 Id.
Internet would become “an essential component of the rights to freedom of expression and access to information” in the foreseeable future and should be available to everyone, just like education.\footnote{Sherif Elsayed-Ali, Internet access is integral to human rights, EGYPT INDEPENDENT LIVE BLOG (January 15, 2012), http://www.egyptindependent.com/opinion/internet-access-integral-human-rights.}

In the physical world, everyone is born into the world and the only exit is death. In cyberspace, whoever controls access reigns over cyberspace. Access to the Internet thus should be an equal human right to be granted to everyone in order to preclude arbitrary and tyrannical control of the online gateway. Moreover, since 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. Cyberspace is therefore as important as education, and equal access to the Internet should be protected just as equal access to education should be.

As discussed above, under Article 19 of the ICCPR and the UN Human Rights Committee's General Comment No. 34, the right for people to access public information is a basic and important human right. Since the ability to access the Internet will gradually be 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 UN Human Rights 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. The resolution first confirms that the rights people have offline should also be protected online notwithstanding frontiers, especially the freedom of expression under the ICCPR article 19. The resolution thus “calls 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”.

II. 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. And the first step toward defining

---


52 Id. ¶ 3.
censorship is determining whether it is a negative or neutral term.

Eli Pariser has described censorship as “a process by which government alters facts and content,” and thinks such concept is inherently negative. P.G. Ingram, meanwhile, suggests that censorship denotes the restrictive policy governing publication, public performance, or exhibition, and holds that “censorship is only one limitation of liberty,” which does not necessarily constitute repression.

The U.S. Supreme Court seems to treat censorship as a negative term rather than neutral. In Near v. Minnesota (1931), the Court deemed that a statute allowing the public authority to sue a newspaper owner or publisher because the paper contained scandalous and defamatory news against public officers had an “essence of censorship” and should be unconstitutional, unless the owner or publisher could prove the news are true and the motive is just. The Court further concluded that the freedom of the press had historically been treated by the U.S. Constitution to mean


54 P.G. INGRAM, CENSORSHIP AND FREE SPEECH: SOME PHILOSOPHICAL BEARINGS 1-4 (2000); See Salman Rushdie & Jonathan Rauch, Censorship can be Beneficial, in CENSORSHIP: OPPOSING VIEWPOINTS 17, 18 (David Bender & Bruno Leone eds., 1997) (defining censorship as “the restriction, absolutely or merely to some part of the population…by the proper political authorities, of intellectual, literacy, or artistic material in any format”).


56 Id. at 713.
“immunity from previous restraints or censorship.” The Court appeared to treat restraints as a type of censorship muffling the press and found censorship against the freedom of the press undesirable under the U.S. Constitution.

Censorship, then, is an effort of the government to prohibit or suppress certain contents of speech or publications that do not have an actual negative effect on others or the public. The risk of censorship, as indicated by the U.S. Supreme Court in Cohen v. California (1971), is that “governments might soon seize upon the censorship of particular words as a convenient guise for banning the expression of unpopular views.” The governmental censorship against a specific speaker may inevitably require self-censorship, and self-censorship may create a chilling effect inducing mass censorship.

If the government could arbitrarily examine the contents of a speech and prohibit publication or expression, self-censorship and its chilling effect may become a reality and the goal that “[d]ebate on public issues should be uninhibited, robust, and wide-open” will be out of reach, which is a real threat to democracy. Censorship

---

57 Id. at 716.
60 Id. at 270.
or self-censorship therefore should be averted.62

The Supreme Court has made it clear that censorship means illegitimate prohibition against speech content that begets a chilling effect. In the physical world, when the government prohibits certain contents of speech, the law is enforced by the government and people will refrain from disseminating such contents for fear of being penalized. But in cyberspace, mere criminalization of dissemination of forbidden information is not enough to stop certain speech owing to the pervasive anonymity, and measures like 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.63

What constitutes illegitimate control or censorship, is another critical question here. In the United States, whether a measure to prohibit expression is legitimate should depend on the legal grounds and the appropriateness of the measure, that is,

whether it passes the necessity test.\textsuperscript{64} But when discussing the censorship issue in the context of international human rights, should the test remain the same?

III. The ICCPR Standards to Determine Legitimate Internet Control

To determine what constitutes a legitimate ground to restrict the freedom of expression, the UN Human Rights 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 “[p]aragraph 3 may never be invoked as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights.”\textsuperscript{65} The position of the Committee 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 ruling in \textit{Brandenburg v. Ohio (1969)}, which indicated that the State cannot forbid “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.”\textsuperscript{66}

\textsuperscript{65} General Comment No. 34 on Article 19, ¶ 22, U.N. Doc. CCPR/C/GC/34 (2011).
There are three legitimate grounds to regulate speech in article 19.3 of the ICCPR, which are protecting others’ rights and reputations, national security or public order, and public health or morals. The list of grounds is limited. What protection of others’ rights and reputations or public health encompasses is clear, but not the protection of public order, public morals, and national security. The Committee thus further defined national security, public morals, and public order 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

---

68 Id. ¶ 30-2.
public order (ordre 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 “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.

Even if the reason in article 19.1 of the ICCPR can be cited to limit the freedom

of expression, the means adopted by the government must be necessary. The UN

Human Rights Committee interprets the necessity test under article 19.3 of the ICCPR

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.”69 When reviewing the necessity test, the form and means of expression

must be taken into account, that “the value placed by the Covenant upon uninhibited

expression is particularly high in the circumstances of public debate in a democratic

---

69 Human Rights Committee, General Comment 27, Freedom of movement (Art.12), (Sixty-seventh
society concerning figures in the public and political domain." 70

The UN Human Rights Committee believed 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.” 71 The Committee further pointed out that any restrictions on the Internet-based information dissemination system and the systems to support such 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.” 72 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 of the ICCPR.

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

71 Id. ¶ 42.
72 Id. ¶ 43.
Part IV. Three Internet Control Models

In this section, the Internet control models of China, Singapore, and the United States will be examined to see whether they constitute legitimate restriction on the freedom of speech under international human rights law or whether they should be deemed Internet censorship, with an eye toward their applicability to Taiwan.

I. Wide Blocking and Filtering—China

In the eyes of the world, China is arguably conducting Internet censorship, 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

---

73 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 Fallow, China’s Internet Censorship is Effective, in CENSORSHIP: OPPOSING VIEWPOINTS 113, 113 (Scott Barbour ed., 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 having the “world’s most advanced and sophisticated system of censorship”);
“Decision”) to require Internet users to provide their real names to ISPs before using their online pseudonyms. 74 Besides paragraph 6 of the Decision, which requires ISPs to collect the real names of Internet users, paragraph 7 makes ISPs responsible for filtering and censoring illegal online speech. 75 Some reports have concluded that the Decision is the Chinese government’s attempt to further tighten its grip on the Internet, suggesting that the Decision was a reaction to the cooperation among Chinese Internet users to expose a string of financial and sexual scandals that have caused at least 10 local officials to resign or be dismissed. 76

The Decision is intended to pull back the veil of anonymity in cyberspace so the government can identify the online speakers and stamp out “undesirable” online speech or information dissemination. The consequence of this measure is a dampening of the active Chinese blogosphere that forces speakers to censor themselves. The Decision may not pass the necessity test under article 19.3 of ICCPR.


since it could be challenged as not a less restrictive means.\textsuperscript{77} It is not legitimate in the context of international human rights and thus constitutes Internet censorship.

The Decision is obviously 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. The Internet control system in China can be understood by the legal basis for it and how it is carried out.

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

The legal grounds for the government to forbid private Internet information service providers (“IISPs) to produce, reproduce, release, or disseminate online information under the Measures for Managing Internet Information Services (“MMIIS”), issued by the State Council on September 25, 2000, effective October 1, 2000, include national security, state interest and honor, national unity or ethnic discrimination, state policy towards religious, social order, the regulation of pornography, gambling, violence, homicide, terrorism, and human dignity and rights.

\textsuperscript{77} Article 19.3 of ICCPR reads: “The exercise of the 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 protection of national security or of public order (ordre public), or of public health or morals.”
infringement. These grounds seem to be derived from the grounds for prohibiting dissemination of verboten information 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, 1997.79

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 MMISI.80 According to article 23, failure of commercial IISPs to censor dubious online speech will cost them their licenses, and for noncommercial IISPs, their websites may be shut down.81

China is not the only country that requires private IISPs or online service providers to help patrol and regulate Internet speech; democratic countries like the United States also use many different measures to compel ISPs to censor online speech in some situations.82 The critical difference between China and U.S.’s models is the legal basis for controlling interne is vague a general, instead of specific.

80 Id.
81 Id.
82 The U.S. model will be introduced and analyzed subsequently in Part Iv. III.
The Chinese government’s grounds for assigning private IISPs responsibility to censor Internet speech are national security, state interest and honor, national unity or ethnic discrimination, state policy towards religious, social order, the regulation of pornography, gambling, violence, homicide, terrorism, human dignity, and rights infringement. Of all these reasons, national unity, state honor, and social order are relatively abstract and overbroad, which unjustifiably expand the grounds recognized by the ICCPR. Also, invoking state policy on religion to justify suppression of online speech is not justifiable under article 18.1 of the ICCPR, which protects the freedom of religion.  

For the above reasons, China is commonly perceived as practicing 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 their operating licenses and assigning IISPs the

---

83 The ICCPR article 18.1 reads: “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.”
responsibility to report “aberrant” online speech or behavior, the Chinese government forces the IISPs to do the government’s bidding to control the Internet.\textsuperscript{84} Operating without a license would mean forced website closures and fines for the IISPs.\textsuperscript{85}

As to the Great Firewall of China, it consists of blocking and content filtering techniques.\textsuperscript{86} The blocking system comprises Domain Name System (“DNS”) block and Uniform Resource Location (“URL”) keyword block. 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 the request of the users to access the IP address and the users will see the message “site not found error” on their screens.\textsuperscript{87} As to the URL keyword block, the government not only blocks certain IP addresses but also monitors forbidden words in URLs and blocks the prohibited links.\textsuperscript{88}


\textsuperscript{88} \textit{Id.}. 
The content filtering system is nothing related to DNS but to establish a blacklist of words and conduct Internet monitoring. If a webpage contains words from the blacklist, the page will be off limits to the general public.\textsuperscript{89}

Basically, the Great Firewall is a powerful apparatus erected by the Chinese government that selectively blocks website operators and Internet users to regulate the Internet. While it is established 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 the ICCPR article 19.3?

The licensing, blocking and filtering system in China are unnecessary and perceived as Internet censorship simply because it is not designed to be “content-specific” as required by the ICCPR article 19.3, but rather a general and arbitrary clamp on online activities to maintain the Chinese authoritarian scheme and to squash any criticism against the Community Party or the government.

But what if the grounds were content-specific and recognized by the ICCPR

\textsuperscript{89} Id.
article 19.1, e.g., to eradicate online child pornography? Would the filtering and blocking, as well as the licensing scheme, pass the necessity test in that case?  

II. Internet Control Model Based on Licensing System—Singapore

Unlike China’s Internet control through blocking and content filtering, Singapore established a “class license” scheme to indirectly control the Internet.  

Under the Broadcasting Class License Notification of Broadcasting Act of Singapore (the “Act”), both the Internet content providers (“ICPs”) (who provide programs on the World Wide Web through the Internet) and ISPs are subject to the class license scheme. Most of the ICPs and ISPs are automatically class licensed upon their establishment, while some groups are required to register within 14 days of the commencement of their operations, or when notified by the government (e.g., religious groups, political groups, news groups, Internet cafes, schools, and public

The class licensed ICPs and ISPs are obligated to comply with the Singaporean Internet Code of Practice (the “Code”) but failure of compliance will trigger no sanctions from the government. Both ICPS and ISPs are required to deny access to sites containing materials banned by the Code. 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. ICPs should make sure that there is no Code-prohibited material on their programs and deny access to materials prohibited by the government authorities.

The definition of “prohibited material” as provided in paragraph 4(1) of the Code is “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.” To flesh out the abstract grounds, the Code also lists factors that should be considered in determining whether a certain material is

94 The Schedule of the Act: Internet Code of Practice, supra note Error! Bookmark not defined., ¶ 1(2).
95 Id. ¶ 3(1) & (2).
96 Id. ¶ 3(3) & (4).
97 Id. ¶ 4(1).
prohibited, including nudity, sexual violence, explicit sexual activity, child
pornography, homosexuality, extreme violence, and ethnic, racial, and religious
hatred. 98

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. Most of the considerations listed in paragraph 4(3) of the Code concern
obscenity, violence, child pornography, or hate speech, which are restricted and
content-specific under the ICCPR standard. So whether the Singaporean online
control constitutes censorship is down to the class license scheme and the power
vested in ICPs and ISPs to block access to cyberspace.

The UN Human Rights 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.”99 It further explained the conditions for subjecting the broadcast
media to the licensing system:100

98 Id. ¶ 4(2).
100 Id.
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 licence fees should be
reasonable and objective, clear, transparent, nondiscriminatory and
otherwise in compliance with the Covenant.

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 a tenuous 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; i.e., the criteria for the license should be reasonable and objective, clear,
transparent, and nondiscriminatory.

As Lewis S. Malokoff has 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. 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. The Singaporean practice is toothless because 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; also, there are not enough government personnel on hand to monitor the compliance of the ICPs or the ISPs. If the Singaporean government declares that it owns or controls the Internet, it does so only nominally. On the other hand, if the Singaporean government threatens to revoke the class license, the system will produce better result.

However, it is illegitimate for a government to declare, whether de facto or de jure, that the Internet resources belong to it and people need to secure its permission before using the Internet. The scheme of “inalienable” class licenses is married by such unjustifiable implications. Furthermore, if the Singaporean government used license 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 regime could be considered as

102 Sarah B. Hogan, To Net or Not to Net: Singapore’s Regulation of the Internet, 51 FED. COMM. L.J. 429, 446 (1999).
103 See id. at 446-7.
not a less restrictive mean compared with fines or suspension of the license.

III. Internet Control Model of Government and Private Partnership: United States

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. The U.S. system requires private ISPs or ICPs to cooperate with the government to either monitor the Internet or block access. Each of the grounds and measures designed to control the Internet are analyzed and compared with the international human rights (i.e., the ICCPR) and the U.S. 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”) on October 26, 2001 to grant the

---

104 See CHRISTINE ZUCHORA-WALSKE, INTERNET CENSORSHIP: PROTECTING CITIZENS OR TRAMPLING FREEDOM 43-59 (2010).
government more power to search private communication data.\textsuperscript{105} Particularly, the Patriot Act authorizes government agents to intercept e-mail and monitor online activities.\textsuperscript{106} The Stored Communication Act ("SCA") further gives the government power to require online communication service providers to disclose subscribers’ private information with a court warrant in accordance with the criminal procedure rules.\textsuperscript{107}

National security is an explicitly given and justifiable ground under article 19.3 of the ICCPR to restrict the online free flow of information. Maybe 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 the courts.\textsuperscript{108} The remaining issue is whether the means chosen by the United States is necessary to achieve the goal.

However, the means adopted by the U.S. government are monitoring and intercepting, which are equivalent to online surveillance. Even if the ground is an acceptable objective, it has to be asked whether monitoring every online

\textsuperscript{105} See Doe v. Gonzales, 449 F. 3d 415, 418 (2d. Cir. 2006).
\textsuperscript{106} See 18 U.S.C. § 2516.
\textsuperscript{107} See 18 U.S.C. § 2703.
\textsuperscript{108} See ZUCHORA-WALSKY, supra note Error! Bookmark not defined., at 100.
communication is necessary and whether it stifles the online free flow of information unnecessarily, especially when the interest of free flow of information is more important in cyberspace.\textsuperscript{109}

2. Child Protection

The U.S. Congress first enacted the Communication Decency Act of 1996 ("CDA") to criminalize the deliberate delivery or display to a person under 18 any message that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."\textsuperscript{110} Thought the act was to protect minors from harmful materials online, it was invalidated by the U.S. Supreme Court in \textit{Reno v. American Civil Liberties Union} (1997).\textsuperscript{111} The Court applied strict scrutiny to deem that "indecent" and "patently offensive" are too vague and broad, which would cause a chilling effect, and the CDA as a criminal statute is not allowed by the First Amendment.\textsuperscript{112}

The other effort of the Congress to control Internet content in 1996 was the Child


\textsuperscript{110} \textit{See 47 U.S.C § 223.}

\textsuperscript{111} \textit{Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).}

\textsuperscript{112} \textit{See id. at 870-2.}
Pornography Prevention Act ("CPPA"), which expanded the federal prohibition on child pornography to include pornographic images on computers. In Ashcroft v. Free Speech Coalition (2002), the Supreme Court also found the CPPA unconstitutional on the grounds that by community standards the CPPA is overly vague in determining child pornography and broad, and it was not a necessary means.

The Congress did not cease its effort to create online child protection measures after losing the battles in the Supreme Court. In 1998 it enacted the Child Online Protection Act ("COPA") to require 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. Failure to comply with the COPA carries criminal liabilities. The Supreme Court in Ashcroft v. American Civil Liberties Union (2004) held that the Third Circuit was correct to affirm the District Court's ruling that enforcement of the COPA should be prohibited because the statute likely violates the First Amendment. The Supreme Court deemed that blocking and filtering software is a less restrictive and likely a more effective alternative, since the

---

113 18 U.S.C. § 2256(8).
filters “impose selective restrictions on speech at the receiving end, not universal restrictions at the source.” There are two other less restrictive alternatives to the COPA the Congress passed after the district court trial: a ban on misleading domain names and a statute for the creation of a “Dot Kids” domain.

Meanwhile, the 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. The Supreme Court upheld the CIPA because it “help[s] public libraries fulfill their traditional role of obtaining material of requisite and appropriate quality for educational and informational purposes” and “[e]specially because public libraries have traditionally excluded pornographic material from their other collections.”

It thus seems that combating child pornography with a selective blocking and filtering system is more likely to be accepted under the U.S. Constitution than a general denial of access. Child protection, especially when it comes to child pornography, can be considered an important public moral under the ICCPR article

117 Id. at 666-667.
118 Id. at 672.
19.3. The question, however, is whether there are alternatives to the filtering scheme that the U.S. Supreme Court will find even less restrictive.

3. **Online Copyright Protection**

Using licenses, criminal sanctions, or subsidies to require online service providers or ISPs to filter or block is a means of indirect government Internet control and should be subject to international human right and constitutional review. Even if such means passes the necessity test, the legitimacy of indirect government Internet control still depends on whether the ground for restriction is specific, like national security or child protection, and not overbroad or general, as in China’s case.

Is copyright protection a specific ground for the U.S. government to adopt a government-private partnership scheme to control the Internet? The Digital Millennium Copyright Act of 1998 (the “DMCA”) Section 512(a)-(d) prescribes safe harbor guidelines for Online Service Providers (“OSPs”) to minimize their copyright infringement liability. 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.\textsuperscript{121}

OSP\textsuperscript{s} are required to adopt a policy to terminate the accounts of copyright infringers.\textsuperscript{122} If the service providers receive a notice from copyright holders or assignees, they must remove or block access to the allegedly infringing materials.\textsuperscript{123} The notification must specifically identify the infringing elements of the materials.\textsuperscript{124}

However, copyright is too broad a reason to filter or block online speech and should not automatically exempt private OSP\textsuperscript{s} from the international human rights restraints.

\textbf{(1) Copyright a Murky Ground to Control the Internet}

Copyright protection may be considered a part of public morals and thus a legitimate ground to restrict the online free flow of information. Nonetheless, since copyright systems do not adopt a registration scheme, it is difficult to learn whether a subject is protected by someone’s copyright and so whether copyright is infringed is

\textsuperscript{121} 17 U.S.C. § 512 (a)-(d).
\textsuperscript{122} 17 U.S.C. § 512 (i)(1).
\textsuperscript{123} 17 U.S.C. § 512 (c).
seldom a black-and-white issue.\textsuperscript{125} It is also difficult to anticipate whether the defendant can successfully invoke the fair use exception.\textsuperscript{126}

Under the DMCA, the OSPs are authorized and required to take down online copyright infringing materials after receiving a notice from the right holder, while the private copyright holders or “claimers” are empowered, in the place of the court, to determine whether their copyright is infringed, which makes this system susceptible to abuse of power.\textsuperscript{127} The system neutralizes the fair use protection so that fair use cannot be a counterweight to OSPs’ removal of materials prompted by right claimers.\textsuperscript{128} Once the ground is discretionary and nonspecific, it cannot serve as justification to restrict the online free flow of information and defies international human rights. The DMCA is therefore in essence similar to the Chinese licensing and filtering censorship system.\textsuperscript{129}

\begin{thebibliography}{99}
\bibitem{125} See \textsc{Lawrence Lessig}, \textit{Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity} 288 (2004).
\bibitem{126} See id. at 107.
\bibitem{128} See Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 529, 559-560 (1985) (to see idea and expression dichotomy and fair use as an important mechanism to balance the freedom of speech and copyright); \textit{See also} 17 U.S.C. § 107.
\bibitem{129} See \textsc{Dawn C. Nunziato}, \textit{Virtual Freedom-Net Neutrality and Free Speech in the Internet Age} 17 (2009) (characterizing the DMCA as ISP censorship scheme).
\end{thebibliography}
(2) OSPs Should Be Subject to International Human Rights Restraints

The U.S. government could argue that in the government-private partnership scheme, it is the OSP that takes down and terminates the accounts and not the government and there are no international human rights or constitutional issues in a strictly private relationship between private parties. But the general principle underlying most of the constitutions worldwide is that human rights protection is the responsibility of the government of a State, and not a private person. Though there is not yet an international human rights exception theory, there is a state action exception in the United States that when there is a “close sufficient nexus” between the government and the private person’s action, the action should be deemed a state action and subjected to the constitutional restraints. The private use of government property, supervised and investigated by the government, and assumption of public function have been considered by the Supreme Court to constitute such

---


132 See Burton v. Wilmington Parking Authority, 365 U.S. 715 (1961) (deeming that the lessee of the state property should be bound by the Fourteenth Amendment if the lease furthers and forms an integral part of a state operation).


close sufficient nexus.

The state action theory is not only a U.S. local theory but has also been recognized by U.N. General Assembly in Responsibility of States for Internationally Wrongful Acts 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.\textsuperscript{135}

Dawn C. Nunziato has argued that the state action theory should apply in the virtual world, that Internet intermediaries, i.e., OSPs, are serving traditional government functions and are in close association with the government, which wishes to evade its responsibility by delegating its power to Internet intermediaries.\textsuperscript{136} In fact, the Internet intermediaries in online forums are just like the company town in Marsh v.

Alabama and play the role of the government of a State.\textsuperscript{137} In cyberspace, the operator or host of a discussion forum enjoys the power to shape the rules and order on that forum. It is a space with a government-and-private person relationship and thus the human right restraints should be applied to prevent the government from dodging the constitutional restrictions.

Furthermore, the notice and takedown scheme was devised by the U.S. legislature in order to relieve OSPs of their burden of secondary copyright liability and reduce copyright holders’ expenses on proving the infringement.\textsuperscript{138} 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 the government’s authorization. From such perspective, the DMCA’s immunity scheme is just like the license system of China and Singapore’s Internet control system, and imprisonment and the subsidy under U.S. online child protection legislation are manifestations of indirect government Internet control.

The question to be asked about the DMCA is whether Internet intermediaries


should be assigned secondary liability, especially vicarious infringement liability.\textsuperscript{139}

The government should not transfer its burden and the consequences of the failure to monitor and stop online copyright infringement to private Internet intermediaries by imposing vicarious liability. Perhaps realizing vicarious liability would put too much burden on OSPs, the Congress further designed the DMCA immunity scheme to alleviate the burden. However, owing to the unclear criteria for determining copyright infringement, the scheme remains cause for concern.

Part V. Best Fit for Taiwan—Internet Control or Censorship?

I. Different Constraints in Different Models

Social norms, market, and architecture are not only different between visual world and physical world. The comparison of three models shows that even in physical world, the three constraints may also be different. The differences between regional constraints also affect the development of internet control models.

\textsuperscript{139} The vicarious infringement was established and illustrated by MGM Studios v. Grokster, 545 US 913, 930-31 (2005) (if the defendant has the ability to supervise the infringing conduct and has a direct financial interest from the infringing activity, he should be vicarious liable to the infringement).
In China, the social norms are created and formed by the government. Democratic may be demanded by the people but not available, and order supersedes all values and become the most important. The restriction grounds for internet control thus include general and vague national unity, state honor, and etc. and become internet censorship scheme.

The creation of class license scheme without threatening to repeal the license to force the ISPs and ICPs to censor the internet by Singaporean government creates a special architecture different from the other internet architecture in the other real world regions. The Singaporean internet architecture also to certain extent reflects the social norms of Singapore.

Finally, the U.S. government and private partnership internet control model put the whole regulation power to the internet market managers, i.e., the online intermediaries. The 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 deciders.

What are the three constraints in Taiwan? Many Taiwan’s social norms are
similar to China. For instance, the Chinese culture does not emphasize copyright protection, on the other hand, it encourages the artists to intimate the other’s masterpieces. However, Taiwan is affected by U.S. IP protection pressure and policies and thus amended its Copyright Act to fulfill the U.S. expectation.\(^\text{140}\) Taiwan’s Copyright Act is constructed by market force from United States, and the law itself eventually changes the social norms for protecting copyright.\(^\text{141}\)

### II. Lessons From the Models Comparison

The comparative analysis of Singapore’s, China’s, and the United States’ models show that the grounds matter the most in determining whether the model constitutes censorship or control under the ICCPR article 19. The grounds for the government to restrict the free flow of information in cyberspace should not be general and vague, but must be specific enough and achieve the objectives listed in article 19.1 of the ICCPR.\(^\text{142}\)

As to the means adopted by the government to achieve the objectives, the

---


necessity test under article 19.3 is applied to determine their legitimacy. The free flow of information is a greater interest in cyberspace than in the physical world, and the interests of worldwide Internet users should be no less important than the interests of local users. Therefore, greater consideration should be given to the free flow of information online.

Systems like the Chinese firewall creating a blocking list and utilizing general filtering are not necessary means to protect critical interests. The licensing systems of both China and Singapore are not less restrictive means mostly because the government has no justification to claim ownership of the resources of the Internet.

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 like the one used by the United States for child protection is a necessary means is disputable, but is more justified 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 the OSPs to monitor and block access to infringing materials do not
pass the necessity test because copyright infringement cannot be clearly defined. The only suitable organ to decide whether copyright is infringed is the court, after hearing both sides’ arguments and considering both the copyright infringement and fair use. To confer the power of judging copyright issues on OSPs or right holders will render the government-private partnership supernumerary under article 19.3 of the ICCPR.

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 its constitutional or international human rights obligations. The U.S. state action theory therefore needs to be adopted to prevent this kind of risk.

A critical lesson we may learn from efforts to apply the state action doctrine on internet is not 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. ¹⁴³ One commentator rightly pointed out that there are at least four dangers for granting private proxy internet control power: “danger of error,” danger of “self-censorship that blocks any content that could precipitate the threat of sanctions”, the danger of

¹⁴³ See, e.g., Lawrence Soley, Private Censorship, Corporate Power, in CENSORING CULTURE: CONTEMPORARY THREATS TO FREE EXPRESSION 15-28 (Robert Atkins & Sevtlana Mincheva eds. 2006) (discussing the expansion of corporate power and its relationship to censorship); EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM 101-3 (2011) (suggesting that it is the private companies are conducting today’s censorship).
adopting over restrictive measures, and the danger of lees likelihood to challenge the proxy’s action in the court.\textsuperscript{144} Any of the above dangers is highly possible to cause chilling effect and equals to censorship.

Just as Tim Wu noted that “[p]ower is power, wherever it is found,” and “private sector power over speech can be nearly as terrifying as public power.”\textsuperscript{145} As long as the private ICPs or ISPs holds the power to control internet having danger of causing chilling effect, the international human right restraints must not be relieved simply because ICP or ISP is not a government. We must carefully use stat action theory to conduct a case by case examination and leave the internet users a chance to be protected by free flow of information right against the private online services operators.

Article 19 of the ICCPR requires the State to only protect free flow of information in cyberspace; the State \textit{may} but is not required to restrict the online free flow of information on the grounds of certain important government interests. A State


will always encounter challenge in circumscribing the right of worldwide online users when doing so in the name of a local interest, no matter how trivial it is. As a result, only worldwide interests could constitute a good reason under article 19.1 of the ICCPR to limit free flow of information. Child protection, an issue that continues to gain attention globally, may be a justifiable ground. National security, copyright, defamation, and other interests, are still more local and the State is and should always be cautious in choosing whether to regulate the Internet on the basis of such local interests and the means to protect such interests.

III. Future of Taiwan’s Internet Control: Remain Meager is not Evil

Juxtaposing Taiwan’s current meager Internet controls, i.e., the Child Protection Act and Copyright Act, with those of China, Singapore, and the United States, it becomes evident that Taiwan’s paradigm is a borderline censorship model like the U.S. government and private partnership. The Child Protection Act adopts a selective program demanding self-discipline and access denial from Internet service platform providers at the request of the government to shield minors from online pornographic materials. The ground is a specific one that is recognized by the ICCPR article 19.1 and the selective blocking and filtering is arguably a necessary means. On the other
hand, the immunity afforded to OSPs under Taiwan’s Copyright Act, similar to the U.S. DMCA, is tainted by possible unconstitutionality too and susceptible to criticism. Both the U.S. DMCA and Taiwan’s Copyright Act immunity schemes, for compelling OSPs to monitor and block access in cyberspace, are unjustifiable under article 19 of the ICCPR.

In the final analysis, Taiwan’s current Copyright Act paradigm is problematic and a lightning rod for controversy. Taiwan has a choice of 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 U.S. stringent and expanding online copyright protection model and remain the status quo, i.e., the meager online regulation paradigm. Meager interne control model does not violate the requirements of international human right and Taiwan could form its “let the internet free” paradigm as the fourth model.  

147 In 1984, Stewart Brand proposed that information wants to be free, which was cited by John Perry Barlow in the early 90s who argued “Information Replicates into the Cracks of Possibility.” See John Perry Barlow, The Economy of Ideas, WIRED, http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html (last visited April 26, 2013).