ERROR: ESSAY NOT FOUND
COMPARING CENSORSHIP IN CHINA AND SOUTH KOREA

Quynh-Dan Nguyen
Law School, Faculty of Laws, Humanity and Arts University of Wollongong
E-mail: qdn994@uowmail.edu.au

Abstract

Increasing use of Internet all over the world has made world's communication borderless. While such condition might benefited most people, however, it invites greater risks of misinformation and opportunities for detrimental self-expression. State's control has various degree of manners in controlling a massive flow of information. This paper will examine the current methods of internet control utilized by the governments of China and Korea, and analyze the extent to which these respective regimes impinge on the human right to freedom of opinion and expression. It begins with an overview on the international standards for freedom of expression, and the limited permissible restrictions upon the right. Furthermore, the examination of the existing legislation and regimes implemented in China and Korea, respectively, and a comparison of features such as legal grounds and practical effectiveness will be undertaken. Finally, it will discuss whether the censorship regimes implemented in China and Korea constitute legitimate restrictions upon, or impermissibly violate, the right to freedom of expression.

Keywords*: Censorship, human rights, freedom of opinion, freedom of expression*

I. INTRODUCTION

The rapid proliferation of Internet throughout the world has facilitated an unprecedented level of communication. Increased dissemination of information, however, invites greater risks of misinformation and opportunities for detrimental self-expression. Today, almost every state controls online access to information in some way,[1] though in varying manners and degrees.[2]

The People's Republic of China, which comprises the largest number of Internet users in the world,[3] and the

[1] Kristen Farrell, 'The Big Mamas Are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression' (2007) 15 *Michigan State Journal of International Law* 577, 577.

[2] Farrell, above n 1, 577; Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697, 714.

[3] OpenNet Initiative, *China: Country Profile* (9 August 2012) OpenNet Initiative <http://access.opennet.net/wp-

Republic of Korea (South Korea, hereafter referred to simply as 'Korea'), the world leader in internet penetration,[4] both enact considerable restrictions upon internet activity through various filtering, surveillance and legislative methods. Although Korea today enjoys one of the most successful democracies in East Asia,[5] the controls it exerts to regulate online activity are not as dissimilar to those of authoritarian China as may be expected. Despite the guarantees of freedom of expression in each of their respective Constitutions,[6] the restrictions placed upon online use by these two regimes may pose serious risks to citizens' rights freedom of expression.

This essay will examine the current methods of internet control utilised by the governments of China and Korea, and analyse the extent to which these respective regimes impinge on the human right to freedom of opinion and expression. Part I will provide an overview on the international standards for freedom of expression, and the limited permissible restrictions upon the right. Part II will examine the existing legislation and regimes implemented in China and Korea, respectively, and a comparison of features such as legal grounds and practical effectiveness will be undertaken in Part III. Finally, Part IV will discuss whether the censorship regimes implemented in China and Korea constitute legitimate restrictions upon, or impermissibly violate, the right to freedom of expression.

II. METHODOLOGY

Since the paper will examine the current methods of internet control utilized by the governments of China and Korea, and analyze the extent to which these respective regimes impinge on the human right to freedom of opinion and expression, normative-juridical research-method is applied.

content/uploads/2011/12/accesscontested-china.pdf> 276; citing International Telecommunication Union, *Internet Indicators: Subscribers, Users and Broadband Subscribers* (2009) <http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False>.

[4] Eric Fish, 'Is Internet Censorship Compatible With Democracy? Legal Restrictions of Online Speech in South Korea' (2009) 2 *Asia-Pacific Journal on Human Rights and the Law* 43, 50.

[5] Yun-han Chu et al., *How East Asians View Democracy* (Columbia University Press, 2008) 28, cited in Fish, above n 4, 50.

[6] See «中华人民共和国宪法» [Constitution of the People's Republic of China] art 35; «대한민국 헌법» [Constitution of the Republic of Korea] art 21.

The approach of this paper is the statute and comparative approach. This research will explore the comparison of state control on freedom of opinion and expression between China and Soth-Korea.

III. RESULT AND DISCUSSION

FREEDOM OF OPINION AND EXPRESSION

It is appropriate to begin with a look at the nature of the right to freedom of opinion and expression. This right, also described as 'freedom of speech', is preserved in international law, both in the United Nation (UN)'s *Universal Declaration of Human Rights*[7] ("*UDHR*") and the *International Covenant on Civil and Political Rights*[8] ("*ICCPR*"). Article 19 of the *UDHR* provides for the right to freedom of expression, which includes "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers […] through any […] media of his choice".[9] Article 19 of the *ICCPR* provides substantially the same right.[10]

The UN's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression ("Special Rapporteur") has recognised that the wording of Article 19 of the *UDHR* includes and accommodates future technological developments, [11] and as such, it is accepted that the Internet (and other new communication technologies) is equally applicable under the existing framework of international human rights law.[12] It must also be recognised that freedom of expression is not an absolute right. Article 19.3 provides that legitimate restrictions may be made, only 'for the respect of the rights or reputations of others, the protection of

[7] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948).

[8] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976).

[9] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) art 19.

[10] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976) art 19.

[11] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (16 May 2011) 7 [21].

[12] Ibid.

national security, public order, public health, or morals'.[13]

Legitimacy based on the purposes set out in the article 19.3 is the second of three elements set out in the three-part, cumulative test framed by the Special Rapporteur. The first requirement is predictability and transparency (restrictions must be provided by law, which must be formulated with sufficient precision and made accessible to the public[14]), and the final element is necessity and proportionality (restrictions must be proven as necessary and the least restrictive means required to achieve the purported aim). [15] Variations of this three-part test have been used by international courts to examine limitations on freedom of expression,[16] and in Part III of this essay, these three elements will be used as means to assess the respective internet censorship regimes of China and Korea.

INTERNET CENSORSHIP IN CHINA AND SOUTH KOREA

A. China

China's legal and regulatory framework for internet control is considered to be the most advanced, complex and sophisticated regime of internet censorship in the world.[17]

A number of laws and administrative regulations, in conjunction with a sophisticated technological framework, operate to control internet use in China using two main strategies: directly controlling internet activity through blocking and filtering methods, and inducing self-censorship by internet users through surveillance and punitive sanctions. The 'Great Firewall of China' is a highly sophisticated system of blocking and filtering techniques.[18] In China, internet

[13] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976) art 19.3.

[14] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (16 May 2011) 8 [24].

[15] Ibid.

[16] Philip Chwee, 'Bringing in a New Scale: Proposing a Global Metric of Internet Censorship' (2015) 38 *Fordham International Law Journal* 825, 836.

[17] Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697, 702, citing Jan Bruck, *Reporters Without Borders Warns Against Internet Censorship* (3 December 2010) <http://www.dw-world.de/dw/article/0,,5349061,00.html>; Reporters without Borders, *List of the 13 Internet Enemies* (7 Nov 2006) <http://en.rsf.org/list-of-the-13-internet-enemies-07-11-2006,19603>.

[18] Jeffrey Chien-Fei Li, 'Internet Control or Internet Censorship? Comparing the

services are based on interconnecting networks, which all must pass through the Ministry of Information Industry's international gateway. [19] As Internet Service Providers (ISPs) can only access global networks through one of the interconnecting networks, all internet access through Chinese ISPs is effectively captured by the government's filter.[20]

The state is also able to regulate internet activity through Internet Information Service Providers (IISPs) and ISPs, by enforcing legislation which allocates liability to these bodies for the misconduct of their users. The *Measures for Managing Internet Information Services*[21] ("the Measures") adopted in 2000 create a number of legal obligations for IISPs and ICPs, which compel them to conduct their own censorship practices, in order to avoid various sanctions.

The Measures make IIS providers directly responsible for content published on their servers. [22] They are prohibited by Article 15 from producing, reproducing, releasing or disseminating information that falls under the categories forbidden by the state, [23] and are further obliged by Article 16 to censor, record and report forbidden information. [24] Violation of these measures can make ICPs liable for fines, shutdown, criminal liability and licence revocation. [25] ISPs are also

Control Models of China, Singapore, and the United States to Guide Taiwan's Choice' (2013) 14 *Pittsburgh Journal of Technology Law & Policy* 1, 24.

[19] Jongpil Chung, 'Comparing Online Activities in China and South Korea: The Internet and the Political Regime' (2008) 48(5) *Asian Survey* 727, 734-735.

[20] Ibid.

[21] «互联网信息服务管理办法» [Measures for Managing Internet Information Services] (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000.

[22] OpenNet Initiative, *China: Country Profile* (9 August 2012) OpenNet Initiative <http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf> 276, 280; citing «互联网信息服务管理办法» [Measures for Managing Internet Information Services] (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000, art 20.

[23] «互联网信息服务管理办法» [Measures for Managing Internet Information Services] (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000, art 15.

[24] «互联网信息服务管理办法» [Measures for Managing Internet Information Services] (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000, art 16.

[25] OpenNet Initiative, *China: Country Profile* (9 August 2012) OpenNet Initiative <http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf> 276, 280; citing «互联网信息服务管理办法» [Measures for Managing Internet Information Services] (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000, art 20.

required by the Measures to record information relating to subscriber activity, and keep these records for 60 days for supply upon demand by relevant state authorities.[26]

Consequently, much of the implementation of internet censorship (such as keyword blocking and removal of search results[27]) is carried out by IISPs and ISPs, who are controlled by the government through legal responsibilities. Additionally, a "virtual police" system employs around 30,000 "cyber cops" to monitor online content, and selectively terminate domestic sites or block foreign sites that are found to disseminate 'sensitive' information.[28]

A wide range of topics are considered sensitive by the Chinese government.[29] Blocked online content includes information relating to independence for Taiwan or Tibet, the Dalai Lama, Falun Gong, police brutality, Tiananmen Square, human rights in China, democracy, as well as pornography and obscene content.[30]

Aside from controlling what content is accessible by blocking and filtering, the state also controls internet use by inducing self-censorship by netizens. End users are subject to controls such as those issued by the *Decision of the NPC Standing Committee on Safeguarding Internet Security* ("the Decision"),[31] which prescribe sanctions including fines, content removal and criminal liability for violations.[32] Numerous arrests have been made, not only of journalists, bloggers and activists, but even of 'ordinary' users of social media.[33] For example, in 2010, a Twitter user was arrested for retweeting a sarcastic comment about anti-Japanese protests in China.[34] 77 imprisonments of netizens were reported in 2009,[35] and Amnesty

[26] «互联网信息服务管理办法» [Measures for Managing Internet Information Services] (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000, art 14.

[27] Farrell, above n 1, 586.

[28] Chung, above n 19, 735.

[29] Farrell, above n 1, 587.

[30] See Chung, above n 19, 735; Farrell, above n 1, 587.

[31] «全国人大常委会关于加强网络信息保护的决定» [Decision of the NPC Standing Committee on Safeguarding Internet Security] (People's Republic of China) National People's Congress Standing Committee, 28 December 2000.

[32] OpenNet Initiative, *China: Country Profile* (9 August 2012) OpenNet Initiative <http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf> 276, 281.

[33] See Chung, above n 19, 737.

[34] OpenNet Initiative, above n 32.

[35] Ibid.

International has reported China to have the largest number of imprisoned journalists and cyber-dissidents in the world.[36]

The threat of these sanctions pose even greater concern to netizens since the enactment in recent years of 'real-name registration laws', which require internet users to register their real name and personal information when signing up with ISPs or on websites such as microblogs and message boards. Users may use nicknames or pseudonyms online but their identities are still discoverable by the microblog companies and the government.[37]

This scheme was first introduced on a national level in 2012 by the Decision, [38] which had the effect of creating the legal obligation of real-name registration not only for blog providers, but those who allow "website access" or "post[ing] information via the network".[39] The law has since been further expanded to instant messaging applications and mobile phone SIM card purchasers.[40]

A draft "Cybersecurity Law" released in 2015 by the National People's Congress in China also reiterates the current rules associated with real-name registration, [41] and imposes legal liability for violations by service providers, which include fines ranging between RMB 50,000 to 500,000 ($10,000 to $100,000 AUD) and licence suspension. [42] It is speculated that the draft will be passed into law with very few changes, based on past legislative behaviour.[43]

The combination of real-name registration, which removes anonymity

[36] Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697, 704, citing Amnesty International, *Background Information on Freedom of Expression in China* (2011) <http://www.amnestyusa.org/individuals-at-risk/priority-cases/background-information-on-shi-tao/page.do?id=1361025>.

[37] Jyh-An Lee and Ching-Yi Liu, 'Real-Name Registration Rules and the Fading Digital Anonymity in China' (2015) 25 *Washington International Law Journal* 1, 12.

[38] [Decision of the NPC Standing Committee on Safeguarding Internet Security] (People's Republic of China) National People's Congress Standing Committee, 28 December 2000.

[39] «全国人大常委会关于加强网络信息保护的决定» [Decision of the NPC Standing Committee on Safeguarding Internet Security] (People's Republic of China) National People's Congress Standing Committee, 28 December 2000, art 6; cited in Lee and Liu, above n 37, 13.

[40] Lee and Liu, above n 37, 13.

[41] [Cybersecurity Law (Draft)] (People's Republic of China) National People's Congress Standing Committee, 7 July 2015, art 20 [unofficial English translation found here: <http://chinalawtranslate.com/cybersecuritydraft/?lang=en>].

[42] [Cybersecurity Law (Draft)] (People's Republic of China) National People's Congress Standing Committee, 7 July 2015, art 53.

[43] Lee and Liu, above n 37, 15.

from internet use, as well as the threat of punitive action, creates a chilling effect upon internet speech, by encouraging self-censorship for fear of punishment by the state. Research has even found that self-censorship caused by the suspicion and perception that one is being surveilled has been more effective than the Great Firewall at controlling internet use.[44]

B. Republic of Korea

The regulation of online content in Korea is largely enacted through the use of 'takedown orders' and defamation laws. The primary regulatory body is the Korea Communications Standard Commission (KCSC), which is empowered [45] to determine what content constitutes "unlawful information" on the internet, [46] and also make orders to intermediaries such as ICPs and website owners to block or shut down websites, delete messages, and/or suspend users,[47] pursuant to the *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.* ("the *Network Act*").[48]

Under Article 44-7 of the *Network Act*, which prohibits the circulation of 'unlawful' information, the KCSC can order a provider of information communications services or a message board operator to reject, suspend or restrict such information.[49] Failure by a person responsible for an online provider or message board to comply with such a request is punishable by a fine of up to ten million won or imprisonment for up to two years.[50]

This legislation creates liability for information communications service providers in respect to their users'

[44] Davis, 'China's Eye on the Internet' *ScienceDaily* (online), 12 September 2007 <https://www.sciencedaily.com/releases/2007/09/070911202441.htm>

[45] [Framework Act on Telecommunications] (Republic of Korea) 24 January 2011, art 3.

[46] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (21 March 2011) addendum 2 ('Mission to the Republic of Korea') 9 [32].

[47] OpenNet Initiative, *South Korea: Country Profile* (6 August 2012) OpenNet Initiative <http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-south-korea.pdf> 355.

[48] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012.

[49] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 44-7.

[50] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 73(5); *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 12 [44].

actions. Internet portals have been found liable by the Supreme Court for failing to delete defamatory and malicious comments posted on their news services websites, and have been ordered to pay compensation of up to KRW 30 million ($30,000 AUD) in damages to victims of defamation.[51] The threat of these significant sanctions act to equip the KCSC with a considerable amount of authority over intermediaries in regulating online content.[52]

Internet intermediaries are also required to play a role in online censorship through operation of Article 44-2 of the *Network Act*. This provision allows victims of defaming or otherwise personally harmful information to request the relevant provider of information and communications services to delete the information.[53] Upon receipt of such a request, the provider, or intermediaries, must take action to delete or block access to the information for up to 30 days.[54] During such a suspension, the KCSC will determine whether the information is to be allowed or deleted. However, the operation of Article 44-2 means that information claimed to be fraudulent or scandalous can be blocked immediately, before an actual determination is made about the legitimacy of the complaints.

Although the problem of cyber-bullying was cited as the main justification for introduction of this law in 2008,[55] many have perceived the measures as a method of controlling online discussion for the KCSC.[56] Critics have pointed to cases that appear to suggest that this power has been exercised in relation to political discussion or policy-based criticism of government officials.[57]

Moreover, Article 44-3 encourages intermediaries to monitor and take temporary measures at their own discretion, even without complaints.[58] Article 44-2(6) further provides that if a provider takes necessary measures, it may have its

[51] Park Sungwoo and Kim Miju, 'Court says Web portals are responsible for comments' *Korea JoongAng Daily* (online), 18 April 2009 <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2903746>.

[52] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 12 [44].

[53] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 44-2.

[54] OpenNet Initiative, above n 47, 355.

[55] Ibid.

[56] See Fish, above n 4, 86.

[57] Ibid 86-88.

[58] See [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 44-3.

liability for damages mitigated or discharged.[59] The combination of these two provisions create a concern that intermediaries may be inclined to 'err on the side of safety' by overusing their vague scope of discretion in Article 44-3 to avoid liability.[60]

Regulation of online content in Korea is generally directed at 'socially harmful content' and content relating to national security, in particular content relating to North Korea. [61] Content containing North Korea propaganda falls under the classification of "illegal content" due to operation of the *National Security Act*,[62] which prohibits content which "praises, promotes, and glorifies North Korea".[63] Blocking of 27 foreign sites, 338 social networking accounts and 132 online communities, and deletion of 15,168 items of propaganda for jeopardising national security were reported by police in 2013.[64]

Individuals have also been arrested for discussing North Korea online. In 2002, a Democratic Labor Party activist, Kim Kangpil, was accused of committing "an act advantageous to the enemy" under Article 7 of the *National Security Act* and sentenced to one year's imprisonment for posting articles about North Korea on the party's website.[65]

Another of the central priorities of Korea's online filtering policy is protection of the youth from "harmful" internet content, described as "immoral, violent, obscene, speculative and antisocial information". [66] Article 42-2 of the *Network Act* provides that those who transmit "unwholesome media" as defined by the *Juvenile Protection Act* must take measures to restrict access to juveniles,[67] and Article 42 requires that websites containing adult content must

[59] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 44-2(6).

[60] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 11.

[61] OpenNet Initiative, above n 47, 360.

[62] «국가보안법» [National Security Act] (Republic of Korea) 1948.

[63] Freedom House, *Freedom on the Net: South Korea* (2014) Freedom House <https://freedomhouse.org/sites/default/files/resources/South%20Korea.pdf> 5.

[64] Ibid; citing Hongdu Park [In Park's first year, the number of violators of the National Security Act has leaped] 경량 신문 (online), 19 February 2014 <http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201402190924151&code=940202>.

[65] Chung, above n 19, 739.

[66] OpenNet Initiative, above n 47, 354.

[67] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 42-2.

warn visitors and require identification verification for access.[68]

Homosexual content was classified as "obscenity and perversion" in the 2001 "Internet Content Rating Service", [69] designed to protect adolescents from viewing content deemed by officials as "illegal and harmful materials" online.[70] Gay and lesbian websites were classified as "harmful" to minors and youth, and <www.exzone.com>, a website about gay and lesbian issues, was shut down as a result.[71] However, this practice was reversed by 2003 due to international backlash,[72] influence from Seoul High Court dicta stating that preventing youths from viewing homosexual content might be unconstitutional, as well as a recommendation by the National Human Rights Commission.[73]

Another important method of controlling online speech is through the penalties for "cyber defamation", which are specifically provided in the *Network Act*.[74] A person who defames another through an information and communications network is punishable by imprisonment for up to three years or by fine not exceeding 20 million won for *facts*, or imprisonment up to ten years or by fine not exceeding 50 million won for *false facts*.[75]

The penalties for cyber defamation are noticeably stronger than those prescribed for defamation in the criminal law. Under Article 307 of the Criminal Act, defamation is punishable by imprisonment for up to two years or by fine not exceeding five million won for *facts*, or imprisonment up to ten years or by fine not exceeding ten million won for *false facts*.[76] The higher speed and wider audience reach of online communication have been cited as reasons for the harsher penalties.[77]

The Network Act's stated purpose includes an aim of "developing an environment in which people can utilize information and communications

[68] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 42; OpenNet Initiative, above n 47, 354.

[69] Chung, above n 19, 739.

[70] Ibid.

[71] Ibid.

[72] Fish, above n 4, 77, 94.

[73] Ibid 78.

[74] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 70.

[75] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 70.

[76] «형법» [Criminal Act] (Republic of Korea) 3 October 1953, art 307.

[77] Freedom House, above n 63, 11.

networks in a sounder and safer way."[78] However, concern has been expressed that the cyber defamation laws have been used to target statements that are true and in the public interest and penalise individuals who express criticisms of the government.[79]

COMPARISON

A. Regulated Content

The legal grounds for internet censorship in China are found in Article 15 of the Measures, and include: national security and national unity, state interest and honour, ethnic discrimination, state policy towards religion, social order and stability, the regulation of pornography, gambling, violence, homicide or terrorism, human dignity, and rights infringement.[80]

Research indicates that China's internet blocking is primarily focused on content that has the potential to undermine the authority of the Communist government and its control over social stability,[81] as well as content that relates to politically sensitive issues.[82] Chinese filtering also targets 'socially harmful' content, primarily websites related to pornography and online gambling.[83] The legal grounds for blocking online content in Korea are found in the nine categories of forbidden information provided by Article 44-7 of the Network Act. These grounds include obscenity, defamation, creating fear, protection for juveniles against "unwholesome" material, state secrets, activity prohibited by the National Security Act, and criminal activity.[84]

Testing conducted by OpenNet Initiative consistently finds that filtering in Korea primarily targets content related to conflict and security, particularly regarding North Korea.[85] Besides protection of national security, however, online regulation in Korea also has a significant emphasis on protection against defamation and abusive behaviour, and protection against 'harmful material' including

[78] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 1.

[79] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 8 [25].

[80] [Measures for Managing Internet Information Services] (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000, art 15.

[81] OpenNet Initiative, above n 47, 287.

[82] Ibid.

[83] Ibid.

[84] [Act on Promotion of Information and Communications Network Utilization and Information Protection, etc] (Republic of Korea) 18 August 2012, art 44-7.

[85] OpenNet Initiative, above n 47, 360.

gambling, pornography, nudity and sexual violence.[86]

A comparison of the categories of content subject to online regulation in these two countries reveal a number of similarities. Although Korea does not engage in the same level of filtering as China,[87] both countries primarily focus on content that each respective state considers a threat to its political stability. China blocks content relating to issues such as Taiwan and Tibet, while Korea blocks content relating to North Korea. Both countries also engage in online censorship for the purposes of protecting society from perceived moral or social harms such as gambling and pornography. This paternalistic approach is markedly Asian in nature, and reveals the Confucian ideology that both countries share.[88]

B. Methods of censorship

While both countries use some similar methods to regulate online activity, they rely more heavily on different strategies. In China, the focus is on the extensive filtering capabilities of the Great Firewall. In Korea, on the other hand, the level of filtering is "generally low" [89], and the state's approach is more dependent on other measures such as takedown orders and defamation laws.[90]

Both countries use strategies to induce self-censorship in addition to directly controlling accessibility of online content. China's surveillance of internet users and arrests of cyber-dissidents creates a chilling effect in respect to political speech, while a degree of self-censorship in relation to abusive speech is encouraged by the threat of cyber defamation laws in Korea.

C. Cyber defamation

While China has criminal laws applying to defamatory statements alleging false facts, [91] Korea's law is even stricter in that it also punishes true facts. Korean law also distinguishes Cyber Defamation as a distinct offence, unlike China, whose legislation specifies that online expression falls under the basic criminal laws for

[86] See ibid.

[87] See ibid; OpenNet Initiative, above n 32.

[88] See Jong-Sung You, 'The Cheonan Dilemmas and the Declining Freedom of Expression in South Korea' (Paper presented at the 2014 International Studies Association annual convention, Toronto, Canada, 28 March 2014) 23.

[89] See OpenNet Initiative, above n 47, 360.

[90] Ibid.

[91] John M. Leitner, 'To Post or Not to Post: Korean Criminal Sanctions for Online Expression' (2010) 25 *Temple International and Comparative Law Journal* 43, 66.

defamation.[92] China applies the same punishment for defamation, regardless of medium of expression, while the cyber defamation laws in Korea are prescribed higher maximum penalties than defamation expressed in other mediums.

This difference may be explained by the unique socio-cultural context of Korean society, and events that have led to a stronger drive for protection against defamatory speech. The primarily cited motivation for Korea's online restriction relating to defamatory comments and online speech stems from the problem of 'cyber-bullying' in Korean society.[93] Societal factors which contribute to the high numbers of suicides triggered by online speech include the high penetration of Internet use in Korean society, a small number of universally used discussion sites, and a cultural emphasis on 'keeping face'.[94] The suicide of the "Nation's Actress", Choi Jinsil, in 2008 due to false rumours, among a number of other high-profile celebrity suicides linked to online rumours, have prompted public support for increased governmental control of online communication.[95] This social issue, although not unique, bears a heavier impact in Korean society, and has motivated the introduction of measures such as cyber defamation laws in Korea.[96]

D. Real name registration

China and Korea are the only two countries in the world to have adopted systems of online real-name registration.[97] Although only China currently has this scheme in place, it was first introduced in Korean law.[98]

The real-name system was introduced in Korea in 2009 as a response to the 'cyber-bullying' suicide events discussed above.[99] Article 44-5 of the Network Act required real identity verification of online users of websites with more than 100,000 visitors a day.[100] The scheme, however, was

[92] Ibid.
[93] See Fish, above n 4, 84-85.
[94] Fish, above n 4, 84.
[95] Fish, above n 4, 84-85.
[96] See Fish, above n 4.
[97] Fish, above n 4, 84.
[98] David A. Caragliano, 'Real Names and Responsible Speech: The Cases of South Korea, China, and Facebook' (Paper presented at The Right to Information & Transparency in the Digital Age, Stanford University, 11-12 March 2013); Lee and Liu, above n 37; John Leitner, 'Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals' (2009) 9 *Journal of Korean Law* 83.
[99] John Leitner, 'Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals' (2009) 9 *Journal of Korean Law* 83, 86-94.
[100] Ibid 90.

abandoned after a unanimous ruling by the Constitutional Court of Korea that Article 44-5 was unconstitutional in 2012.[101] The Court found that 'the public gains achieved had not been substantial enough to justify restrictions on individuals' rights to free speech'.[102] Although China originally introduced the system based on the Korean model,[103] it has declined to follow Korea's abandonment of the scheme, and continues to advocate the real-name registration system in its new 2015 draft law.

E. Practical effectiveness

The methods employed by China and Korea to censor online content face some challenges in respect to practical application. Blocking of content, by both countries, can be circumvented by methods including proxy servers or Virtual Private Networks (VPNs).[104] The "Network Authoritarian Model"[105] used by the Chinese government to take advantage of the business sector's profit-driven motives and corporate resources relies upon compliance by private ISPs. This presents a challenge when ISPs do not have incentive or ability to cooperate, which is beginning to surface with the introduction of real-name registration rules which create overwhelming compliance costs,[106] resulting in inconsistencies and uncertainties in enforcement.[107] Uneven application of the law has undermined the effectiveness of the real-name registration system in Korean experience.[108]

Korea's methods are unable to control foreign websites.[109] While the Chinese filtering system requires access to all foreign sites to pass through the government-controlled networks, and threatens to kick out foreign websites that fail to comply,[110] Korea's limited internet filtering prevents access to only a limited number of websites, and the Korean government has thus far been unwilling to kick out major websites

[101] Freedom House, above n 63, 12.

[102] 'South Korea's real-name net law is rejected by court' , *BBC* (online), 23 August 2012 < http://www.bbc.com/news/technology-19357160>.

[103] Lee and Liu, above n 37, 16.

[104] Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697, 729.

[105] Lee and Liu, above n 37, 3.

[106] Ibid 23-26.

[107] Ibid.

[108] David A. Caragliano, 'Real Names and Responsible Speech: The Cases of South Korea, China, and Facebook' (Paper presented at The Right to Information & Transparency in the Digital Age, Stanford University, 11-12 March 2013) 6.

[109] Fish, above n 4, 92.

[110] Ibid.

(such as Youtube and Google) for failing to comply with its laws.[111] Another obstacle for Korea's regime is the inability of the KCSC to handle the number of complaints it receives.[112] It is estimated that to deal with the hundreds and thousands of articles and comments for which it receives complaints, the Commission would need to hire thousands more employees.[113] In comparison to these weaknesses in the Korean model, the Chinese regime of online censorship and its highly advanced Great Firewall filtering system is much more effective at controlling online content.

LEGITIMATE RESTRICTIONS TO FREEDOM OF EXPRESSION?

A. Legal grounds

Pursuant to Article 19.3 of the ICCPR, restrictions upon the right to expression are only permissible 'for the respect of the rights or reputations of others, the protection of national security, public order, public health, or morals'.[114] In respect to protection of morals, it is emphasised by the UN Human Rights Committee ("the Committee") that "the concept of morals derives from many social, philosophical and religious traditions" and that "limitations must be understood in the light of universality of human rights".[115] As such, China and Korea's relatively paternalistic approaches to online regulation in regards to content such as pornography and gambling should be accepted, as they are informed by cultural conceptions of morals which are legitimate for the contexts in which they operate.

However, while some of the legal grounds provided in the Chinese and Korean legislation authorising blocking/deletion of online information do fall under the permissible grounds (such as child protection), a number of grounds have been criticised for being too broad and vague.

Legal grounds provided in Article 15 of China's Measures, such as national unity, state honour and social order, are found to be 'relatively abstract and overbroad'[116] and

[111] Ibid.
[112] Ibid.
[113] Ibid.
[114] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976) art 19.3.
[115] International Covenant on Civil and Political Rights, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976) art 19, General Comment 23, quoted in Li, above n 18, 19.
[116] Li, above n 24.

'needlessly vague'.[117] The prohibited categories of information in Article 44-7(1) of Korea's Network Act similarly lack clarity. The prohibition on "content that attempts, aids or abets to commit a crime" has been identified as too broad by the Special Rapporteur,[118] especially considering the wording of some crimes such as "obstruction of business".[119] The vagueness of these broad grounds for censorship is problematic, as they create too much ambiguity to operate as the precise restrictions allowed by Article 19.3.

B. Proportionality

Even where restrictions are based on acceptable legal grounds, they are also required by Article 19.3 of the ICCPR to be necessary and the least restrictive means required to achieve the purported aim.[120] The Committee has 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".[121] Many of the arrests of individuals in China and Korea for online speech have been disproportionate, as they have related to speech considered obscene or scandalous, or political without posing any threat to national security.[122] As filtering can provide less restrictive means of dealing with subversive speech, the criminal punishment of imprisonment is clearly disproportionate in these cases, and constitutes impermissible restrictions of freedom of expression.

The Committee has further stated that Article 19.3 requires permissible restrictions to be "content-specific"[123] and "generic bans on the operation of certain sites and systems are not allowed."[124] A system that utilises general filtering and a blocking list, like China's Great Firewall, is not necessary, as there is no "direct and immediate connection between the

[117] Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697, 705.

[118] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 12 [45].

[119] Ibid.

[120] Ibid.

[121] International Covenant on Civil and Political Rights, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976) art 12, General Comment 27, [42], quoted in Li, above n 18, 20.

[122] See OpenNet Initiative, above n 32.

[123] International Covenant on Civil and Political Rights, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976) art 12, General Comment 27, [43], quoted in Li, above n 18, 21.

[124] Ibid.

expression and the threat".[125] Although Korea's system of takedown orders blocks content reactively rather than proactively, there are still concerns about the Network Act's delegation of responsibility to intermediaries rather than an independent body, especially considering provisions that give intermediaries a vague discretion to block information that is likely to be over-applied to avoid liability.[126] The excessive authority given to intermediaries to regulate online content may indicate that this system also fails the necessity test.

Korea's cyber defamation laws also fail on proportionality, as their 'inherently harsh' sanctions of up to ten years imprisonment or up to 50 million won ($50,000) impose disproportionate penalties.[127] They are even more disproportionate in respect to defamation for true facts. The real-name registration scheme currently implemented in China is also disproportionate to its purported aim of addressing online malicious speech, pornography and "unfounded rumours"[128]. Korea's experience with this scheme has highlighted numerous problems, including privacy violations, cyber security, and practical enforcement issues.[129] Considering these factors, the Constitutional Court of Korea has found that the scheme's benefits were not sufficient to justify the significant restrictions it imposed on citizens' right to free speech.[130] Additionally, there exist other less restrictive methods to trace online users[131] or to remedy harm done by a person's expression.[132]

C. Predictability and transparency

The criterion of predictability and transparency requires that restrictions must be formulated with sufficient precision and made accessible to the public.[133]

China's regime of internet filtering fails to meet the transparency requirements

[125] Li, above n 18, 39.

[126] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 11 [41].

[127] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 8 [28].

[128] Lee and Liu, above n 37, 16.

[129] See Lee and Liu, above n 37.

[130] *Identity Verification System on the Internet* 47, 252(consolidated), August 23, 2012] <http://search.ccourt.go.kr/>.

[131] Ibid 23-30.

[132] Caragliano, above n 108, 7.

[133] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (16 May 2011) 8 [24].

of Article 19.3, with results from OpenNet Initiative testing reporting a low level of transparency, due to the lack of a publicly available list of banned sites, as well as no available mechanisms for users to request review of blocked sites.[134] It is also not obvious when a website has been blocked, as blocked sites will redirect users to a network timeout error page, which can be attributed to network errors.[135]

It is also important that legislation restricting the right to freedom of expression is applied by a body which is independent of any political, commercial, or other unwarranted influences, in a manner that is neither arbitrary nor discriminatory, with adequate safeguards against abuse.[136]

The constitution and procedures of the KCSC have raised serious concerns that there are insufficient safeguards to ensure that it does not operate as a de facto post-publication censorship body to delete information critical of the Government or powerful corporations.[137] Although the KCSC is a nominally independent statutory organisation, its nine members are appointed by the President,[138] which raises questions about its independence, given the degree of influence that can be exerted by the President and dominant political party.[139]

Concerns have also have been expressed about the lack of transparency, accountability and scrutiny of the KCSC.[140] The procedures of removing illegal online content do not notify authors of blocked or deleted content nor allow them to provide their opinion before the KCSC's decision.[141] While authors can challenge the commission directly about a ruling, they have no independent avenue for appeal.[142] This raises concerns that judgements made by the KCSC may be arbitrary and politically,

[134] OpenNet Initiative, above n 32, 287.

[135] Ibid.

[136] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (16 May 2011) 8 [24].

[137] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 12 [47].

[138] Freedom House, above n 63, 6, citing Jeong-hwan Lee, 'A private organization under the president? The KCSC's structural irony' (in Korean), *Media Today* (online), 14 September 2011, <http://bit.ly/1aYr0GA>.

[139] See *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 9 [32].

[140] See *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 12.

[141] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 12 [47]; Freedom House, above n 63, 4.

[142] Freedom House, above n 63, 6.

socially or culturally motivated, lacking legal grounds.[143] It has been reported that the KCSC in many cases has blocked entire blogs even where only a small portion of posts are deemed problematic.[144]

The National Human Rights Commission of Korea's recommendation that the authority and functions of the KCSC be transferred to an independent self-regulatory body with higher transparency and accountability[145] would be appropriate to ensure that online regulation which amounts to restriction of the freedom of expression is carried out in a more legitimate manner.

IV. CONCLUSION

Freedom of expression is a fundamental human right, and the importance in its preservation is reflected by the extremely limited nature of the acceptable grounds for restriction in ICCPR Article 19.3. By failing to comply with the requirements of Article 19.3, the internet censorship regimes of China and South Korea constitute violations of the rights provided by Article 19 and guaranteed by their own Constitutions.

Even more problematic than direct methods of censorship, are the measures that have been taken to conduct surveillance upon citizens, or punish individuals for their online speech. Governmental censorship against a specific speaker, along with paranoia and fear of sanctions, create a culture of self-censorship.[146] Self-censorship may create a chilling effect, which, in turn, can effect mass censorship.[147]

While the internet regulatory regimes in China and Korea share some similarities, however, their impacts are not the same. Although they both regulate online content on relatively similar grounds, and censor directly as well as inducing self-censorship, the major difference lies in the degree to which they exert control over political speech. While internet users are prohibited from raising anti-government issues in China, netizens in Korea are free to discuss or even criticise government policies and political

[143] *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 12; Freedom House, above n 63, 6.

[144] Freedom House, above n 63, 6.

[145] See *Mission to the Republic of Korea*, UN Doc A/HRC/17/27/Add.2, addendum 2, 12.

[146] Li, above n 18, 17.

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

leaders, provided the speech does not endanger 'national security' or constitute 'cyber defamation'. [148] This key difference preserves the distinction between China's authoritarian state, and Korea's democracy, for which freedom of expression and political critique is essential. However, there is a still a need for redress of both regimes, in order to protect the rights to self-expression of citizens in China and Korea. Both states must find a balance, to regulate online activity for the benefit of their citizens, but only through restrictions to the right to freedom of expression for reasons and in ways that are legitimately permissible by international law.

REFERENCES

JOURNAL

Eric Fish, 'Is Internet Censorship Compatible With Democracy? Legal Restrictions of Online Speech in South Korea' (2009) 2 *Asia-Pacific Journal on Human Rights and the Law* 43, 50.

South Korea's real-name net law is rejected by court , *BBC* (online), 23 August 2012 < http://www.bbc.com/news/technology-19357160>.

David A. Caragliano, 'Real Names and Responsible Speech: The Cases of South Korea, China, and Facebook' (Paper presented at The Right to Information & Transparency in the Digital Age, Stanford University, 11-12 March 2013); Lee and Liu, above n 37; John Leitner, 'Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals' (2009) 9 *Journal of Korean Law* 83.

David A. Caragliano, 'Real Names and Responsible Speech: The Cases of South Korea, China, and Facebook' (Paper presented at The Right to Information & Transparency in the Digital Age, Stanford University, 11-12 March 2013) 6.

Davis, 'China's Eye on the Internet' *ScienceDaily* (online), 12 September 2007 <https://www.sciencedaily.com/releases/2007/09/070911202441.htm>

Decision of the NPC Standing Committee on Safeguarding Internet Security] (People's Republic of China) National People's Congress Standing Committee, 28 December 2000.

Freedom House, *Freedom on the Net: South Korea* (2014) Freedom House <https://freedomhouse.org/sites/default/files/resources/South%20Korea.pdf>

Hongdu Park, '박근혜 정부 1 년 '국가보안법 위반 사범' 대폭

[148] Chung, above n 19, 740.

증가' [In Park's first year, the number of violators of the National Security Act has leaped] 경량 신문 (online), 19 February 2014 <http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201402190924151&code=940202>.

*Identity Verification System on the Internet (*인터넷 실명제*)* [24-2(A) KCCR 590, 2010 헌마 47, 252(consolidated), August 23, 2012] <http://search.ccourt.go.kr/>.

Jeffrey Chien-Fei Li, 'Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice' (2013) 14 *Pittsburgh Journal of Technology Law & Policy* 1.

Jeong-hwan Lee, 'A private organization under the president? The KCSC's structural irony' (in Korean), *Media Today* (online), 14 September 2011, <http://bit.ly/1aYr0GA>.

Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697.

Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697, 702, citing Jan Bruck, *Reporters Without Borders Warns Against Internet Censorship* (3 December 2010) <http://www.dw-world.de/dw/article/0,,5349061,00.html>; Reporters without Borders, *List of the 13 Internet Enemies* (7 Nov 2006) <http://en.rsf.org/list-of-the-13-internet-enemies-07-11-2006,19603>.

Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697, 704, citing Amnesty International, *Background Information on Freedom of Expression in China* (2011) <http://www.amnestyusa.org/individuals-at-risk/priority-cases/background-information-on- shi-tao/page.do?id=1361025>.

Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697.

Jessica E. Bauml, 'It's a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship' (2010) 63 *Federal Communications Law Journal* 697.

John Leitner, 'Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals' (2009) 9 *Journal of Korean Law* 83.

John M. Leitner, 'To Post or Not to Post: Korean Criminal Sanctions for Online Expression' (2010) 25 *Temple International and Comparative Law Journal* 43.

Jongpil Chung, 'Comparing Online Activities in China and South Korea: The Internet and the Political Regime' (2008) 48(5) *Asian Survey* 727.

Jong-Sung You, 'The Cheonan Dilemmas and the Declining Freedom of Expression in South Korea' (Paper presented at the 2014 International Studies Association annual convention, Toronto, Canada, 28 March 2014) 23.

Jyh-An Lee and Ching-Yi Liu, 'Real-Name Registration Rules and the Fading Digital Anonymity in China' (2015) 25 *Washington International Law Journal* 1.

Kristen Farrell, 'The Big Mamas Are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression' (2007) 15 *Michigan State Journal of International Law* 577.

Mission to the Republic of Korea, UN Doc A/HRC/17/27/Add.2, addendum 2, 9 [32].

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

OpenNet Initiative, *China: Country Profile* (9 August 2012) OpenNet Initiative <http://access.opennet.net/wp-content/uploads/2011/12/accessc ontested-china.pdf> 276, 280; citing «互联网信息服务管理办法» [Measures for Managing Internet Information Services] (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000, art 20.

Park Sungwoo and Kim Miju, 'Court says Web portals are responsible for comments' *Korea JoongAng Daily* (online), 18 April 2009 <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2903746>.

Philip Chwee, 'Bringing in a New Scale: Proposing a Global Metric of Internet Censorship' (2015) 38 *Fordham International Law Journal* 825.

ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False>.

Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (16 May 2011) 7 [21].

Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the*

promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (21 March 2011) addendum 2 ('Mission to the Republic of Korea') 9 [32].

Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17th sess, Agenda Item 3, UN Doc A/HRC/17/27 (16 May 2011) 8 [24].

Yun-han Chu et al., *How East Asians View Democracy* (Columbia University Press, 2008) 28, cited in Fish, above n 4, 50.

CONVENTIONS

International Covenant on Civil and Political Rights, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976) art 19.

International Covenant on Civil and Political Rights, opened for signature 16 December 1966 999 UNTS 171 (entered into force 23 March 1976) art 12, General Comment 27, [43], quoted in Li, above n 18.

LEGISLATIONS

Act on Promotion of Information and Communications Network Utilization and Information Protection, etc (Republic of Korea) 18 August 2012, art 44-2(6).

Cybersecurity Law (Draft)] (People's Republic of China) National People's Congress Standing Committee, 7 July 2015, art 20 [unofficial English translation found here: <http://chinalawtranslate.com/cybersecuritydraft/?lang=en>

Framework Act on Telecommunications (Republic of Korea) 24 January 2011

Measures for Managing Internet Information Services (People's Republic of China) National People's Congress Standing Committee, Order No 292, 20 September 2000.

National Security Act (Republic of Korea) 1948.