THE REGULATORY FRAMEWORK CONCERNING ONLINE PROTECTION OF MINORS IN CHINA

Perspectives from the Green Dam Case



University of Oslo Faculty of Law

Candidate number: 8009

Supervisor: Lee A. Bygrave

Deadline for submission: 02/01/2011(month/date/year):

Number of words: 17,339 (max. 18.000)

Content

<u>1</u> II	NTRODUCTION	1
1.1	Background	1
1.2	Resources	6
2 <u>R</u>	REGULATORY FRAMEWORK CONCERNING INTERNET CONTENT IN C	CHINA
TODA	AY	8
2.1	Regulatory Authorities (Governments)	8
2.2	Private Sector (Industry)	14
2.3	Civil Society	16
2.4	Specific Bodies on Online Protection of Minors in China	17
<u>3</u> <u>C</u>	CONCERNS ABOUT CHINA'S REGULATORY SCHEME OF INTERNET	
	TENT IN LIGHT OF GREEN DAM CASE	20
3.1	Overview of Green Dam Case	20
3.1.1		20
3.1.2		22
3.1.3	3 Ending	26
3.2	Relevant Concerns Raised in Green Dam Case	27
3.2.1	Tension in China is different from the Western assumption	27
3.2.2	2 Coordination between government and industry is deficient	28
3.2.3	Interaction between government and civil society is poor	30
<u>4</u> <u>E</u>	CUROPEAN REGULATORY FRAMEWORK FOR ONLINE PROTECTION (<u>OF</u>
MINO	DC	32

4.1	Rationale	32
4.2	Approaches at the EU Level	33
4.2.	.1 Restricted Internet Content to minors in the EU	33
4.2.	.2 Regulatory Mechanisms	35
4.3	Case Study of EU Member States: Practice in UK	39
4.3.	.1 UK Legislation on Online Protection of Children	39
4.3.	.2 UK Regulatory Bodies	41
4.4	Inspirations of European Regulatory Scheme for China	42
<u>5</u> <u>4</u>	ALTERNATIVES FOR CHINA CONCERNING ONLINE PROTECTION OF	<u>'</u>
MIN(ORS	44
5.1	Role-switch of Chinese Regulatory Authorities	44
5.2	Promoting Coordination between Government and Private Sector	47
5.3	Facilitating Dialogues between Government and Civil society	50
5.4	Other Possible Propositions	53
<u>6</u> <u>c</u>	CONCLUSION	54
REFE	ERENCES	57

1 Introduction

1.1 Background

The emergence of the internet has dramatically and profoundly influenced the world. It urges countries irrevocably to shift into the information era. Access to a vast amount of information has become much easier than before and even some secret information previously held only by governments can become publically available through the struggles amidst internet multi-stakeholders ¹, i.e. Wikileaks. While enjoying the freedom of information brought by internet, people also faces some content that they may not want, e.g. hate speech, pornography, spam etc. Many of these concerns predate the internet, but they are turning out to be more troublesome due to the unique characteristics of the information technology evolution. One such issue is the online protection of minors ², which is (generally) the protection of the physical and psychological well-being of minors by shielding them from materials distributed by means of the World Wide Web which are harmful to them³.

To address the challenges posed by internet, informal and voluntary governance such as "netiquette" no longer work adequately. The *Declaration of the Independence of*

¹ The main internet multi-stakeholders are governments, private sector and civil society. This is in accordance with the working definition of 'internet governance' by the Working Group on Internet Governance (WGIG) which is 'the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.' For details about WGIG and the follow-up Tunis Declaration, see further A. Hubbard and Lee A. Bygrave, 'Internet governance goes global', in Lee A. Bygrave and Jon Bing (eds.), *Internet Governance Infrastructure and Institutions*, Oxford University Press 2009, p. 224, 227

² The definition of minors differs from country to country. In China it is any person under 18 years of age (Article 2, Law of People's Republic of China on the Protection of Minors 2006)

³ Cf. Child Online Protection Act 1998, Pub. L. No. 105-227, 112 Stat. 2681-736 [codified at 47 U.S.C. § 231 (2000)]

Cyberspace proclaimed by John Berry Barlow⁴ is an old story now. The government no longer merely a player in internet governance, but has an increasingly significant role. Since the population of internet users began to skyrocket, governmental policy initiatives were introduced into internet governance, particularly for internet content regulation. As a public interest, the online protection of minors is high on the governments' agendas and is complicated in the regard that it involves different players, which brings difficulty in balancing opposing interests in the regulatory regime. For example, the online protection of minors calls for restrictions on the transmission of internet content. This would inevitably result in conflicts with other fundamental rights, *inter alia*, free speech. The governments' attempt to create regulations in this domain has frequently run into obstacles.

As a pioneer in the internet realm, the United States first proposed legislative initiatives to crack down online access to harmful information by children. Such attempts have been carefully examined in libertarian frameworks under which the US regulatory mode for internet content largely relies upon self-regulatory mechanisms⁵. The first noticeable attempt by the US Congress to prohibit availability of online obscene materials to minors was the *Communications Decency Act* (CDA) 1996 6. A lawsuit was soon filed against two sections of CDA after it was enacted. It was struck down on the grounds that it would impair the rights of free speech under the first Amendment of the US Constitution⁷. Later the enforcement of the *Child Online Protection Act*⁸ (COPA) 1998 was enjoined by the court on the same grounds. The Court held that the "strict scrutiny test" in COPA might prevent online publishers from publishing some material that adults have a right to access. The Court also pointed out that the least restrictive means possible to protect children is the blocking software installed on home computers by parents, which would not prevent free

 $^{^4\,}$ See further https://projects.eff.org/~barlow/Declaration-Final.html accessed October 2010

⁵ See further B. Frydman, L. Hennebel and G. Lewkowicz, 'Public Strategies for Internet Co-regulation in the United States, Europe and China', *Working Papers du Centre Perelman de philosophie du droit, n*° 2007/6, available at http://www.philodroit.be/IMG/pdf/BF-LH-GL-WP2007-6.pdf accessed October 2010

⁶ Pub. L. No. 104-104, 110 Stat. 133 [codified as amended at 47 U.S.C. § 223 (2000)]

⁷ Reno v. American Civil Liberties Union, 117 S.Ct. 2329, 2332 (1997)

⁸ Supra note 3

speech⁹.

The European approach to online protection of minors is somewhat different to that of the US. As opposed to the US, the EU regulatory authorities play a significant role in the control of internet content. For example, the *Directive on Electronic Commerce* (ECD)¹⁰, it stresses the essentiality of legislation at the EU level¹¹. It also leaves room for state intervention in certain restrictions, liabilities, and penalties¹². Again, unlike the US regulatory authorities who cooperate with the industry to achieve specific goals on certain issues, the EU regulatory authorities define general rules applicable to any kind of illegal or harmful materials¹³. Further, the EU regulatory authorities and the governments of some EU Member States fund non-profit organizations like hotlines and watchdogs, to track and report the harmful content actively, e.g. the German association "Jugendschutz".

What about in China, the "authoritarian country"? In 2008, the Chinese government issued a notification to pre-install a web-filtering software "Green Dam-Youth Escort" (hereinafter, "Green Dam"), aiming to prohibit the dissemination of harmful online information to minors. This was the first time that the Chinese government launched an official plan in this area. However, it soon aroused heated controversies. A great number of Chinese internet users were against this order and finally government had to postpone the plan. As always, this plan drew lots of attention from the international community. Many western media published this news and assumed the plan was another attempt of Chinese government to restrict Chinese citizen's access to online information 14, just as the

⁹ Ashcroft v. American Civil Liberties Union, 542 U.S. 656 (2004)

¹⁰ Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17.7.2000, p.1-16, adopted 8 June 2000

¹¹ *Ibid*, Recital 3, 32, see also chapter I 'General Provisions' and Chapter II 'Principles'

¹² Supra note 10. Recital 21, 22, 24, 26, 34,35,36, see also Article 3(4), Article 12(3)

¹³ Supra note 5

¹⁴ Ref. Geoffrey A. Fowler and B. Worthen, 'New China Web-Filtering Rules Still Murky', *The Wall Street Journal*, 9 June 2009, available at http://online.wsj.com/article/SB124450534684996071.html accessed October 2010

configuration of the web-filtering system "Great Firewall¹⁵" in China. When confronted with western criticisms, typically the Chinese government refutes this attention by asserting that western opinions derogate from the context and reality of China and claiming that the internet in China is ruled under Chinese laws. Such gaps of opinion between China and Western countries come out of rather complicated backgrounds and are beyond the scope of this paper.

But what is the true situation of internet governance in China today? To bridge the gaps between China and Western world, it is important to examine the facts relevant to this matter in China. This examination serves as the point of departure for this paper and will help the pertinent analysis on the Green Dam project.

When it comes to the true situation of internet governance in China, one point should not be neglected—China's accomplishments on the construction of internet infrastructures (network facilities, i.e. cables, local loop), the precondition for freedom of information. Since the inception of the national development strategy of internet infrastructure, Chinese government has been dedicated to it for years. As a result, internet access is available in most parts of the geographically vast country, which aids the fast growing number of internet users in China. According to the 26th Statistical Reports on the Internet Development in China¹⁶, up to June 2010 the number of Chinese internet users was 42 million (27.2 million of them access the internet via mobile phone). The statistic reflects the success, at least partly, of China's internet development policy.

As referred to in the preceding paragraph, Chinese government's control on internet access is what most concerns western media and academics, though such control also exists in

Published by China Internet Network Information Center (CNNIC), available at http://research.cnnic.cn/img/h000/h12/attach201007151358080.pdf (Chinese) accessed July 2010 *

¹⁵ See Bygrave, supra note 1, at 70, L. Solum, 'Models of Internet Governance'

most countries of the world¹⁷. Yet the impact of such control to Chinese netizens is perhaps exaggerated since most westerners ignore, or do not know the fact of the failure of such controls due to the technology aids available to internet users. The chief Editor of Finance Times (Asia), David Pilling, has been fully aware of this, stating that:

With a little technical savvy or a dollar a week for a virtual private network (VPN), anyone in China can breach the Great Firewall and see the same information as freedom-surfers in London or New York¹⁸.

With the most internet users in the world, a large amount of information is transmitted and shared via internet every day in China. Nowadays, China's society is in a gradual transition from the past. A growing number of Chinese netizens publicly lobby and this impacts both personal life, i.e. the phenomenon of cyber manhunt¹⁹, and public policies, i.e. change of government orders (Green Dam is perhaps the most noticeable case but not the first), deposition of government officials, etc. The public opinion from internet users also weighs more heavily in the process of policy-making. Like it or not, the transitional scenarios brought by the emergence of digital technology have to be kept in the mind of the Chinese government. However, such considerations under current regulatory regime are still in chaos.

-

¹⁷ Ref. R. Deibert, J. Palfrey, R. Rohozinsiki and J. Zittrain (eds.), *Access Controlled, The Shaping of Power, Rights and Rule in Cyberspace*, The MIT Press, 2010

¹⁸ David Pilling, 'Democracy's Demise in Asia is Exaggerated', *The Financial Times Journal*, 6 May 2010, available at http://www.ftchinese.com/story/001032485/en?page=2 accessed 20 October 2010

¹⁹ Also known as "Human Flesh Search Engine", it is a Chinese internet phenomenon of massive searching by internet users rather than by machines (i.e. Google). It originated in a Chinese entertainment web www.mop.com, once a mop user ask a question, the others who answer it could get Mop Money as reward for sharing his/her knowledge/experience. The application of this search mode gradually extends to social events and becomes a form of online vigilante justice in which internet users hunt down and punish people who have attracted their wrath. Without rules human flesh search could constitute invasion of personal privacy. Ref. Tom Downey, 'Human Flesh Search Engine in China', *The New York Times Magazine*, 3 March 2010, available at http://www.nytimes.com/2010/03/07/magazine/07Human-t.html, accessed 28 December 2010

Due to the Chinese convention and culture, usually the protective measures benefiting children will be supported by the Chinese people in every possible way. Then why was the Green Dam project, which aimed to forbid the transmission of child sexual offensive words/pictures, so strongly resisted by Chinese internet users? Faced with the digital technology challenges, how can China best integrate the aspirations of the stakeholders into the whole regulatory scheme while still keep unique Chinese culture? According to the experiences of other superpowers tackling this issue, especially that of the US (bottom-up) and the EU (top-down), which model will suit China most? After experiencing similar transition from long history to modern society, what are the European inspirations for China?

This paper will seek to answer these questions, mainly from the legal point of view rather than political or technological, though such issues are also involved. In doing so, Chapter II will examine the regulatory framework concerning internet content in China today. Chapter III will illustrate the Green Dam case and analyze the relevant concern on the framework elaborated in Chapter II. As a good example of online protection of minors, Chapter IV will sketch the European regulatory regime in this domain by examining the main policy documents and legal instruments at the EU level. Also, it will proceed to a case study on the UK, an EU Member State. In line with the features of China's society and institutions combined with European experience, Chapter V will offer alternatives for China in respect to online protection of minors. Chapter VI will sum up the answers to the questions proposed in this part according to preceding Chapters and discuss other possible further researches in this domain.

1.2 Resources

The majority of the legal resources in this research lie in books, online articles, scholarly publications, and official legal documents. The part of the EU policy documents mainly refers to EU internet-related Directives, Recommendations, plans, resolutions, declarations and other policy documents. The English translations of Chinese legislations are mainly from the Chinese database, *lawinfochina*, provided by Peking University, and *ChinaITLaw* (some provisions have been modified with my own understanding), if the specific resource

of the translation is not quoted. The Chinese academic' original works, reports and articles will be translated by me due to lack of official translation (with * remark in the footnotes).

Thank my supervisor Lee A. Bygrave for everything;

Thank Jon Bing, Professor of University of Oslo, to supervise me at an early stage of my thesis;

Thank Jeremy Scott Lunde, Katerina Shaw and Yue Liu for language help;

Thank Ge Yunsong, my professor at Peking University, Xiaofeng Wang, Beituan Wang, Zejun Yan, and Emmanuel Dymas Satrioprojo for the help of the materials searching and data collecting for this paper.

2 Regulatory Framework Concerning Internet Content in China Today

The working definition of WGIG on internet governance reinforces the concept of inclusiveness of the governments, the private sector and the civil society in the mechanisms of internet governance. This Chapter will examine the role of the multi-stakeholders in the regulatory framework of internet governance, mainly concerning internet content, in China today.

2.1 Regulatory Authorities (Governments)

China has been ruled under a centralized, top-down government mode for thousands of years. Today the internet governance paradigm in China is still government-lead. This system roughly runs under the principle of the rule of law. However, the regulations have rarely been examined under the constitution. This deficiency has been constantly criticized by the legal circles²⁰.

According to the *Constitution of the People's Republic of China* 2004, National People's Congress (NPC) is the supreme organ of state power of PRC. Standing Committee is permanent body of NPC²¹. They exercise the legislative power of the State²². However, the first attempt to regulate the internet content in China was neither initiated by NPC nor its Standing Committee. In 1997, the Ministry of Public Security promulgated the *Administrative Measures for Security Protection of the Information on International Computer Networks* (hereinafter, MPS 1997 33rd Decree), which was the first regulation concerning the internet content at a national level. Under this decree, producing, reproducing, accessing or transmitting certain materials over the internet is prohibited in

²⁰ Ref. Lei Wang, Constitutional Law Applied in Courts (宪法的司法化), China University of Politics and Law Press, 2000

²¹ Article 57, Constitution of People's Republic of China 2004

²² *Ibid*, Article 58

China. The list of prohibited materials includes those²³: (a) subversive of state power or the socialist system; (b) damaging to national unity; (c) inciting discrimination between nationalities; (d) disturbing to social order; (e) propagating feudal superstition; (f) related to pornography, gambling, or violence; (g) insulting or libelous; and (h) violating the Constitution and other laws. The provisions are quite general and the subsequent internet-related regulations transplant this article almost verbatim.

As a state legislative body, insofar no legislation enacted by NPC has been directly related to internet regulation. Not until 2000 did, its Standing Committee issue a resolution concerning state network security²⁴. The resolution criminalizes certain acts committed over the internet in four instances²⁵:

- (1) acts **which** impair the network operational security, including invading the computer database of national defense, inventing and spreading the computer viruses, and disconnecting the network illegally or without authorization;
- (2) acts **which** are against state security and social stability, including subverting state power or the socialist system, stealing or divulging state secrets, inciting ethnic discrimination and impairing the unity between nationalities, and establishing cult organization and contacting cult members;
- (3) acts **which** undermine public order and the order of the socialist market economy, including propagating false information of products, insulting and libelous, infringing intellectual property rights, distributing misleading financial information, and providing pornography websites and links or transmitting pornography texts, pictures and videos; and (4) acts **which** infringe civil rights, including humiliating or libeling with fabrications, illegally collecting, reproducing personal data, and stealing and blackmailing.

²³ Bygrave, supra note 1, at 67, see also Article 5, Measures for Security Protection Administration of the International Networking of Computer Information Networks 1997

Resolution of the Standing Committee of the National Peoples Congress on Safeguarding Computer Network Security, Adopted at the 19th Meeting of the Standing Committee of the Ninth National People's Congress on December 28, 2000, available at http://yy.china-b.com/hyfl/520854.html accessed July 2010

²⁵ *Ibid*, Provision 1, 2, 3, and 4

Comparing to MPS 1997 33rd Decree, the resolution extends the protection to new facets of economic rights and civil rights, i.e. intellectual property, personal privacy, etc.

The State Council is the Central People's Government of P.R.C, the executive arm of state power and the supreme body of state administrations²⁶. In 2000, the State Council stipulated the *Administrative Measures on Internet Information Service* and the *Regulation of the People's Republic of China on Telecommunications*. On a base level, these two legal instruments follow the routine of the MPS 1997 33rd Decree on internet content regulation²⁷. Only small changes in tone of expression and minor corrections of some items have been done, i.e. the item "damage the reputation of state administrations" in MPS Decree, is replaced by the "damage the state reputation". These modified provisions reflected the changes in governance ideas in China, but they were still too abstract to implement.

Pursuant to the NPC Standing Committee resolution, the prohibited internet materials are illustrated in the regulations adopted by State Administrations. The Ministry of Industry and Information Technology²⁸ (hereinafter, MIIT) is the regulatory authority to supervise the internet infrastructure and is responsible for supervision and regulation of the internet information service²⁹. Other State Administrations regulate the internet content on their sector-specific issues³⁰. Insofar, seven State Administrations have published policy documents concerning internet content (see Figure 1). Aforementioned harmful information has been re-addressed and is prohibited in internet-related stipulations of the MIIT³¹. The prohibited materials on the internet supplemented by the state administrations

²⁶ See Article 85, Constitution of People's Republic of China 2004

²⁷ See Article 15 in the Administrative Measures on Internet Information Service 2000, and Article 52 in the Regulation of the People's Republic of China on Telecommunications 2000

²⁸ The successor of the Ministry of Information Industry (MII) from April 2008

²⁹ Article 18, Administrative Measures on Internet Information Service 2000

³⁰ Supra note 29

³¹ See Article 9 in the Administration in Internet Electronic Messaging Services Provisions 2000, Article 27 in the Measures for Administration of Internet Domain Names 2004, Article 11 in the Measures for the Administration of Internet E-mail Services 2005

are still general, i.e. those that "are against public morality or the excellent national cultural traditions³²", and "impair the public interest.³³"

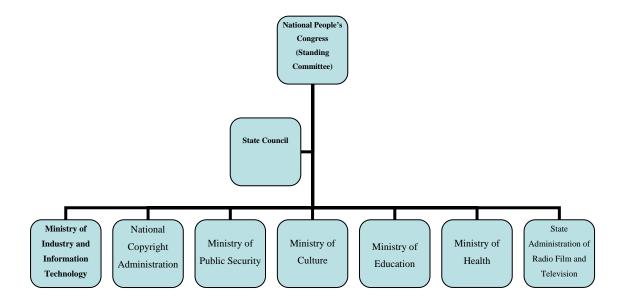


Figure 1 China's Regulatory Authorities on Internet Content

The supervision of internet information is probably the most noticeable issue because it may contradict freedom of expression. In fact in China it is ultimately exercised by the State Council Information Office, though it always coordinates regulation with MIIT. In 2005, they co-issued the *Measures on the Administration of Internet News Services*. In addition to prescribed materials, the Measures extends the scope of content that are prevented from online publication to include those ³⁴ (a) inciting illegal associations, parades, demonstrations, or assemblies that disturb public order; and (b) organizing activities in the name of illegal civil organizations. This extension is very questionable because freedom of speech, press, assembly, association, parades, and demonstration are

³² Article 17 in the Interim Provisions on the Administration of Internet Publication 2002 (promulgated by MIIT), Article 16 in the Administrative Rules about Audio-visual Programs Transmitted over Internet 2007 (SARFT), Article 17(9) in the Interim Provisions on the Administration of Internet Culture 2004 (MOC)

³³ Article 18 (7), Interim Measures for Administration on Education Websites and Online Schools 2000 (MOE)

³⁴ Article 19, Measures on the Administration of Internet News Services 2005

constitutional rights in China³⁵. Nonetheless, no litigation has been commenced against the Measures on the grounds that they are unconstitutional, unlike in the US.

The protection of intellectual property in digital environment is another important topic in China, due to the imperative needs from outside and in. In 2005, the National Copyright Administration of P.R China (NCAC) and MIIT co-published the *Measures for the Administrative Protection of Internet Copyright*. Later to fulfill the obligations as a WTO (World Trade Organization) member, the NCAC together with MIIT stipulated the *Ordinance on the Protection of the Right to Network Dissemination of Information* in 2006 to transpose the WIPO (World Intellectual Property Organization, the same below) Copyright Treaty and WIPO Performances and Phonograms Treaty into Chinese law. In addition, the Ordinance transplants superior experience to tackle online copyright issues. For example, with respect to internet content potentially in breach of copyright law, the ordinance adopts the "Notice and Takedown" procedure, which is borrowed from the US Digital Millennium Copyright Act 1998³⁶.

So far, the only decree to directly tackle the online protection of minors is the *Interim Provisions on the Administration of Internet Publication*, promulgated in 2002 by MIIT combined with the General Administration of Press and Publication³⁷. It indicates that minor-oriented internet publications should not contain any content that "induce minors to imitate the acts against social morality or the acts of illegalities or crimes, as well as any horrible or cruel content that impairs the physical and psychological health of the minors³⁸".

Referring to the prescribed legal documents, three points can be deduced from internet content regulation in China. First, Chinese internet-related regulations are mainly adopted

³⁵ Article 35, Constitution of People's Republic of China 2004

³⁶ DMCA, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998)

³⁷ General Administration of Press and Publication is another name of National Copyright Administration

³⁸ Article 18, Interim Provisions on the Administration of Internet Publication 2002

at the Chinese government level rather than at legislative body level, i.e. NPC or its Standing Committee. Second, Chinese provisions in respect to online illegal/harmful information are too general to implement. The specific meaning of those provisions needs further elaboration through legislation or interpretations by courts. Third, a large number of regulatory authorities involved in this field can potentially result in the problem of coordination and efficiency.

The coordination of Chinese regulatory authorities on policy-making leads to their co-implementation of the regulations. In terms of access to harmful internet information to children, the Chinese government has run a campaign against smutty and lewd pictures overwhelming the country's internet³⁹ from December 2009 to May 2010. Nine State Administrations executed this campaign. Up to late 2009, tens of internet service providers had opted in to the list providing pornography and thousands have been arrested in this drive⁴⁰. This joint action implies the importance that is put on the online protection of children in the Chinese political agendas. In some sense, such action was effective in providing a safer internet to children. Nevertheless, the effect of this campaign-style enforcement of regulations was negated by at least two factors. On one hand, the standard of "harmful/illegal" and "smutty/lewd" materials in this action was ambiguous. In actuality, police members that participated in the campaign confessed that they had difficulty in identifying the pornography content⁴¹. Hence, it possibly constituted a violation of the civil rights of the arrested. On the other hand, the crackdown of internet pornography in the campaign is temporary. The websites providing illegal/harmful content to minors cannot be effectively eliminated from the internet. New sites are emerging everyday and are impossible to be tracked down by government alone.

-

³⁹ Campaign webpage http://news.cctv.com/special/zhengzhidisuzhifeng/01/index.shtml accessed 15 November 2010

⁴⁰ Chris Buckley (Reporter), N. Macfie (eds.), "China says 5,394 arrested in Internet porn crackdown", *Reuters*, 31 December 2009, available at http://www.reuters.com/article/idUSTRE60004220100101 accessed 15 November 2010

⁴¹ Supra note 39, a superintendent of the Ministry of Public Security indicated his difficulty to tackle the erotica information due to the lack of legislation

To sum up, the central government is in a dominant position in China's paradigm of internet governance. This mode takes effect in capacity building and enabling roles in China, i.e. the success in internet infrastructure construction. However, the over-expanded function of the Chinese government weakens the role of judiciary/arbitration bodies when it comes to internet content regulation. The Chinese government's potentiality to violate the constitutional rights, and its pitfall to track and crack down the harmful websites, discredit its influence in this framework.

2.2 Private Sector (Industry)

The private sector consists of commercial, non-governmental entities, which also refers to "business entities", Private sector is not merely a market player, but is represented in political systems as an essential actor in internet governance, e.g. developing policy proposals and self-regulatory mechanisms, etc. After China entered the WTO, the number of multinational companies in China quickly grew and they provided significant impact in this field. Google was the first company trying to challenge scrutiny by the Chinese government in declaring it would shut down its operations in China and Though Google's motivation was questionable as Google probably got involved for political reasons, the controversies derived from this event testified the importance of business entities in the process of policy-making and implementation of the regulations concerning internet content in China.

While self-regulation mechanism of the private sector in digital circumstance is promoted in Western countries, it has been introduced to China as well, in the forms of founding self-regulatory bodies, developing and signing self-discipline agreements, etc, as elaborated briefly in the following. The Internet Society of China (ISC) is one of the biggest self-regulatory bodies in China's information industry. ISC was initiated in 2001 by internet service providers, telecommunication operators, PC manufacturers, research

⁴² Jeremy Malcolm, 'Multi-Stakeholder Governance and the Internet Governance Forum', Terminus Press Perth 2008, p. 104

⁴³ Ref. Tuan Nguyen, 'Google Threatens to Withdraw From China', *Tom's hardware US*, 13 January 2010, available at http://www.tomshardware.com/news/google-gmail-baidu-bing-china,9430.html accessed 5 January 2011

institutions and the academics⁴⁴. The goal of the ISC is to promote the development of the internet in China and help it actively interact with Global Internet Community. For industry, ISC is expected to be a platform for members to execute self-regulatory rules, create good reputations and protect legal rights of members, facilitate interaction and coordination with government, help with implementation of relevant policies and regulations, promote public awareness, etc.

In terms of harmful information conveyed via wireless device (mainly mobile phone), in 2004 three Chinese web portals⁴⁵ co-founded the Consumer Trusted Wireless Service (CTWS) self-discipline Alliance⁴⁶. This Alliance calls on wireless service providers to operate under the principle of good faith. It also designs an evaluation system to protect the consumers. After evaluation by the system, qualified wireless service providers are permitted to use the tag "CTWS" on their web pages. However, in reality this alliance does not attract many new members.

The Self-Discipline Guideline on Online Audio-Video Service⁴⁷, initiated in 2008 by China Central Television (CCTV), was set up according to the promulgation of the *Administrative Rules about Audio-visual Programs Transmitted over Internet* 2002. The first provision in this guideline states that signing parties should be fully aware that pornography, violence, vulgar audio and video programs have imposed negative effects on minors via internet. This sounds like another attempt in China, through industry, to ban online harmful audio-video content to children. However, the guideline encloses certain politically sensitive rules and it is trying to be legally binding. Further, the first signing members are state-owned audio-video companies, i.e. CCTV. Thus, it is more likely to be compulsory

⁴⁴ See further at http://www.isc.org.cn/isc_eIntroduction/index.htm accessed 15 November 2010

⁴⁵ They are Sina (新浪), Sohu (搜狐), and Netease (网易)

⁴⁶ See further 'Consumer Trusted Wireless Service self-discipline Alliance (中国无线互联网行业诚信自律同盟)' available at http://www.ctws.com.cn/ (Chinese) accessed 15 November 2010 *

⁴⁷ See further 'Self-Discipline Guideline on Online Audio-Video Service (中国互联网视听节目服务自律公约)', *CCTV news*, 22 February 2008, available at http://news.cctv.com/society/20080222/101453.shtml (Chinese), accessed November 2010 *

rather than self-disciplinary. According to the information of the websites, up to April 2008 no new parties other than CCTV have signed this agreement.

The ISC, CTWS self-discipline Alliance and the Guideline are three main self-regulatory attempts in China's information industry. Their operations and impacts indicate that the industry self-regulation on internet content in China is still at an early stage. The self-regulatory bodies are too weak to cooperate with the government. Instead, they could just follow the governmental intent and few independent responses have been disseminated to the government by these bodies. This is partly because the tradition and culture in China does not leave much room for industry to negotiate or create broad consensus with government (Chinese tradition discriminated against business). Another factor is that it takes time for industry to establish proper and effective self-regulatory mechanism. Now in China, the response from industry is either radical, e.g. Google example, or indifferent—many companies actually do not care to engage in non-commercial regulations concerning public interests, which will be further elaborated in Chapter VI.

2.3 Civil Society

The civil society is the non-commercial and non-governmental sector. Compared to private sector, the participation of Chinese civil society is more active and effective in the public interest domain. Nowadays, tens of million Chinese internet users express themselves via blogs, micro blogs (the same as twitter), and Bulletin Board System (BBS). The impact of the Chinese celebrities has leaped to a new high level by publishing their opinions online. Han Han, a boy born in 1980s, best-selling author and now a professional driver, was enlisted and finally ranked second in TIME annual "World's Most Influential People in 2010". His blog was accessed almost a million times with thousands of responses from internet users. Many youth like to check his blog soon after events happen in China. He

-

⁴⁸ See 'The 2010 TIME 100 Poll', *TIME*, 29 April 2010, available at http://www.time.com/time/specials/packages/article/0,28804,1972075 1976159 1976160,00.html, accessed November 2010

was described by TIME as "China's Literary Bad Boy" 49. China's internet policy is one of his favorite targets to criticize.

In addition to celebrities, the influence of ordinary internet users is rising quickly as well. Yet one should bear in mind that the increasing power of civil society in China is a two-edged sword. For one thing, ordinary internet users are receivers of internet content making them objects to be protected; for another, they can also be the internet content provider which makes them targets to be regulated. As "bad" administrative policies potentially contradict civil rights, they thus have to be terminated due to the mounted protests from internet users, which has caused some to rebuke that internet has kidnapped the government. This does not sound sensible since public opinion should be justifiably taken into account by the government. Nonetheless, the public opinion sometimes will constitute "civic violence" as well. It could even go far to interfere with Court decisions or to invade personal privacy, e.g. the prescribed cyber manhunt phenomenon. How to balance the impacts from civil society will be a pivotal issue for China in the long term.

2.4 Specific Bodies on Online Protection of Minors in China

China has not yet adopted specific regulation concerning the online protection of minors. The relevant provisions are scattered in various prescribed policy documents and judicial interpretation, which is another important source of law in China. Though precedent is not officially binding in China, as in common law countries, judicial interpretations are de facto binding since the Supreme Court has the power of final adjudication. This is not a perfect solution but it is rather flexible and is better than nothing. In actuality, judicial interpretations have been integrated into later related legislation.

_

⁴⁹ Simon Elegant, 'Han Han: China's Literary Bad Boy', *TIME*, 2 November 2009, available at http://www.time.com/time/magazine/article/0,9171,1931619,00.html, accessed 15 November 2010

⁵⁰ Ref. Weiguo Zhang, 'Alert: network cynical kidnap public opinion (警惕网络愤青绑架民意)', *JXNews*, 23 August 2010, available at http://jxcomment.jxnews.com.cn/system/2010/08/23/011461502.shtml, accessed January 2010 *

In 2010, the Supreme People's Court and the Supreme People's Procuratorate of PRC co-published an "Interpretation (II) concerning the application of laws in criminal cases of producing, reproducing, publishing, selling, and distributing electronic pornographic information via internet, mobile communication terminals and audio sets⁵¹" (hereinafter, Interpretation (II)). It criminalizes the transmission of online content concerning obscene electronic information of minors under fourteen year-old⁵². So far Interpretation (II) is the most specific rule in respect to online protection of minors in China. Yet it does not define what "pornography" is.

The practice in the online protection of minors has been in development in China. It has set up specific bodies and hotlines to attack online pornography, violence and other harmful information. Such bodies include China Internet Illegal Information Reporting Center⁵³ (CIIRC), Hotline 12321 set up by Ministry of Public Security, and Hotline 12390 set up by the Office of Anti-pornography and Anti-illegal publication of PRC. CIIRC is sponsored by China Internet Information Service Commission of ISC; the other two belong to the Chinese regulatory authorities.

As pointed out in preceding passages, the Chinese government plays a leading role in the regulatory scheme concerning internet content regulation. Industry exerts its effects, but as a whole, it is neither mature nor fully developed. The impact of civil society weighs more and more heavily in this scheme, but the proper way to integrate public opinion into policy-making still needs further exploration. The tension of this regulatory paradigm would be the same when it comes to the online protection of minors. This tension has many defects (some already analyzed) and the improvement is in dire need in China today since

⁵¹ Supreme People's Court Interpretation [2010] No. 3, 'Interpretation (II) concerning the application of laws in criminal cases of producing, reproducing, publishing, selling, and distributing electronic pornographic information via internet, mobile communication terminals and audio sets(最高人民法院,最高人民检察院关于办理互联网、移动通讯终端、声讯台制作、复制、出版、贱卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二))',23 February 2010, available at http://www.court.gov.cn/qwfb/sfjs/201002/t20100223_1741.htm (Chinese), accessed 15 November 2010 *

⁵² *Ibid*, Provision 2

⁵³ See further at http://ciirc.china.cn/, accessed 16 November 2010

these limits in the current model constantly give rise to conflicts among multi-stakeholders. It could result in big protests with the Green Dam case being typical amongst those. This will be described and analyzed in Chapter III.

3 Concerns about China's Regulatory Scheme of Internet Content in Light of Green Dam Case

3.1 Overview of Green Dam Case

3.1.1 Context

"Green" in Chinese represents safety and cleanliness, with respect to information it is contrary to the harmful content, especially violence and pornography. In the context of the internet, "green" is used by the Chinese government in relation to online contents for pornography and other illicit material.

The Chinese government is highly concerned with the online protection of minors; especially since erotic information is widespread in the internet and the rate of juvenile delinquency incidents incited by internet addiction quickly increases⁵⁴. In 2006, MIIT launched a "Sunshine Green Network Project", aiming to rectify problems in network environments. Later in January 2008, MIIT publicly tendered for web nanny software to filter pornographic content.

On 20 May 2008, MIIT announced the bid-winners who were Zhengzhou Jinhui Computer Engineering Co. Ltd. (hereinafter, Jinhui) with its product "Expert System to Block Pornography Images", and Beijing Dazheng Language Processing Co Ltd. with its product "Youth Escort—Management System of Internet Access", which is capable of word filtering. The two products were then integrated into one system "Green Dam—Youth Escort". To prohibit harmful information and alleviate the youth internet addiction, the software can block online pornographic and violent content, keep records of users' surfing

According to the statistics of a provincial Committee for Wellbeing of The Youth, about 60% juvenile crime in one of its districts is incited by internet addiction, and 37.5% youth accessed erotic websites in the country. Data provided by Beituan Wang

20

histories, control internet surfing time and prevent users from playing web-games. With RMB 41m (\$6m), MIIT procured one-year exclusive rights to freely distribute the software. One year later, the basic functions of the program were still free of charge with users only paying for updates, maintenance, etc.

On 1 April 2009, the *Notification Concerning the Installation of Green Internet Filtering Software on Campus Network of Primary and Secondary School*⁵⁵ was jointly released by Ministry of Education, Ministry of Finance, MIIT and State Council Information Office. It was the first official order to promote the use of Green Dam. The notification stressed the hazards of harmful information on campus networks, and required primary and secondary schools' awareness of preventing online harmful information from getting to students. Additionally, the notification required the installation of Green Damn on campus networks to be finished by the end of May 2009.

Later, on 19 May 2009 MIIT issued the *Notice Concerning the Pre-Installation of Internet Filtering Software on PCs* ⁵⁶ (MIIT Soft⁵⁷ [2009] No. 226), which stated that the pre-installation of Green Dam was in line with the national deployment of a crackdown on indecent online content and to protect the healthy development of minors. It declared that Green Dam has been effectively doing so, and required computer manufacturers and vendors to complete pre-testing and related work of Green Dam at the end of June 2009. Also, it was announced that new PCs going on sale in China from 1 July 2009 should pre-install Green Dam or include in the software pack⁵⁸. This immediately stirred ardent contentions in the industry and civil society.

⁵⁵ Ref. Notification in Chinese '教育部 财政部 工业和信息化部 国务院新闻办关于做好中小学校园网络绿色上网过滤软件安装使用工作的通知)' http://www.edu.cn/zc_6539/20090507/t20090507_377220.shtml accessed Nov 2010 *

⁵⁶ Ref. Notice in Chinese '关于计算机预装绿色上网过滤软件的通知'

http://miit.gov.cn/n11293472/n11293832/n12843926/12848268.html accessed 11 November 2010. *

⁵⁷ Here 'Soft' represents the Software Service Department of MIIT

⁵⁸ Supra note 56, Provision 4

3.1.2 Contentions

Firstly affected by *the Notice*, some PC manufacturers responded to MIIT with cooperative gesture. Lenovo Group, the largest PC manufacturer in China, stated it would facilitate the order and integrate GD software in its PCs sold in China from 1 July 2009⁵⁹. Another PC major, Dell denoted that it would work with government official to understand its application⁶⁰. Some other PC makers indicated similar intentions as well⁶¹.

The plan also got some proponents from the academics and the media. The deputy director of China Youth Research Center, Xiquan Deng held that it was necessary to build a "psychological Green Dam" for children⁶². Tao Ran, the Director of China Youth Mental Development Base, believed mandatory measures will help juveniles get rid of internet addiction. The secretary-general of China Youth Association on Network, Xianghong Hao praised that GD plan timely met the urgent need of parents⁶³. Bingguang Yan, a journalist of Xinhua.net, provided statistics from a survey on 1813 internet users that over 92% of them supported the Green Dam project, and over 70% were satisfied with Green Dam⁶⁴. However, he did not provide the specific source of the data.

_

⁵⁹ Ref. 'Lenovo said it would install Green Dam from 1 July and offer two options of installation (联想称将如期安装绿坝 提供两种安装方式)', 30 June 2009, http://www.techweb.com.cn/news/2009-06-30/414134.shtml, accessed January 2011.*

⁶⁰ Chris Lefkow, 'Microsoft: China Web filtering raises issues', *Agence France-Press (Washington)*, 9 June 2009, http://technology.inquirer.net/infotech/view/20090609-209562/Microsoft-China-Web-filtering-raises-issues accessed 11 November 2010

Ref. Joe Mcdonald, 'PC makers voluntarily supply Web filter in China', *USATODAY*, 2 July 2009, available at http://www.usatoday.com/tech/news/2009-07-02-china-pc_N.htm?csp=34&utm_source=feedburner&utm_medium =feed&utm_campaign=Feed:+usatoday-TechTopStories+(Tech+-+Top+Stories) accessed January 2011

⁶² Jun Liu(eds.), 'Expert: utilization of Green Dam helps to promote network morality for the youth (要把绿坝软件转变为青少年的网络道德能力)', 12 June 2009, http://news.xinhuanet.com/video/2009-06/12/content_11532181.htm, accessed 11 November 2010, *

⁶³ Shuquan Tang (eds.), 'Installation of web nanny software: necessary and a imperative need from parents (陶然:安装不良信息过滤软件很有必要 家长有迫切需求)', 11 June 2009, http://politics.people.com.cn/GB/1026/9455367.html, accessed 11 November 2010, *

⁶⁴ Bingguang Yan, 'What contentions on Green Dam for (过滤软件之争 争的是什么)', *Xinhua.Net*, 12 June 2009, http://news.xinhuanet.com/politics/2009-06/12/content_11532769.htm, accessed 11 November 2010, *

Yet these positive responses seemed just trivial compared to the protests against the GD plan. Criticisms of the program and the government flooded over the internet. For instance, the end-user agreement of the software underlined that GD "does not guarantee harmful information will be completely filtered, nor does it guarantee the filtered information is entirely harmful," and "producers will bear no liability to any economical or legal disputes raised by this product." Chinese netizens criticized that these items were ridiculous and questioned who would bear the loss, since they had no choice but to install GD due to *the Notice*⁶⁵.

Also, GD's technological deficiencies were continuously found by technology volunteers. First, the filtering function of pornographic images was problematic. Tests revealed that the pictures of cat "Garfield" and images of pink pigs would be filtered ⁶⁶(see a comic below), even the profile pictures of Chinese leaders would be blocked outside the "dam" ⁶⁷. On the contrary, colored nudity (black and red) can breach its filters ⁶⁸. Second, GD's compatibility was poor. The software could only work on Internet Explorer of Microsoft, and was invalid for use on Firefox ⁶⁹. Third, GD would interfere with normal operations of a PC, i.e. closing Notepad and WordPad ⁷⁰. The PC on which the software was installed the software was also found vulnerable to security and privacy risk, i.e. remote parties can execute arbitrary code and obtain control of any PC with the software ⁷¹. The software words-filtering

⁶⁵ Ref. Bi Hu, Shipeng Guo, 'Doraemon passed Garfield denied: Green Dam's good and bad (机器猫过关加菲猫过滤: 绿坝过滤软件是与非)', *iNFZM* (南方周末),11 June 2009, http://www.infzm.com/content/29902, accessed November 2010*

⁶⁶ Ibid

⁶⁷ Zhixiong Gu, 'Green Dam block pictures of leaders (绿坝软件封杀领导人相片)', MINGPAO, 21 June 2009, available at http://news.sina.com.hk/cgi-bin/nw/show.cgi/2/1/1/1174494/1.html accessed 11 November 2010, *

⁶⁸ Supra note 65

⁶⁹ See 'Overkill: absurd Green Dam (错杀良民 软件闹笑话)', *MINGPAO*, 11 June, available at http://news.sina.com.hk/cgi-bin/nw/show.cgi/94/1/1/1163832/1.html, accessed January 2011

⁷⁰ Supra note 65

⁷¹ S. Wolchok, R. Yao, and J. A. Halderman, 'Analysis of the Green Dam Censorware System', *University of Michigan*, 11 June 2009, http://www.cse.umich.edu/~jhalderm/pub/gd/, accessed November 2010

function was weak in accuracy as well, i.e. a mathematics ball game with words "touch ball and pat ball" would be blocked⁷².



Comic⁷³: Garfield saying to Green Dam, "Dude, you got the wrong guy"

Further, GD was involved in legal disputes. A number of blacklist files used by Green Dam were alleged to be copied from Cybersitter⁷⁴, a US net nanny software product. The US Company, Cybersitter LCC brought a lawsuit in US District Court with the latest news being the request for dismissal by the involved PC manufacturers was rejected by the court⁷⁵.

73 Li Zhang, 'Sick Green Dam (病态的绿坝软件)', IT Times Weekly Journal (IT 时代周刊), 5 August 2010, p. 80 *

⁷² Supra note 69

⁷⁴ Supra note 71

⁷⁵ Owen Fletcher, 'Green Dam Comes Back to Haunt Beijing', *The Wall Street Journal*, 2 December 2010, http://blogs.wsj.com/chinarealtime/2010/12/02/green-dam-comes-back-to-haunt-beijing/?KEYWORDS=%22Court%22++%22Green+Dam%22 accessed 12 December 2010

The statistics from a survey of 360 Software Encyclopedia, one of the biggest Chinese online test companies for PC security, attested to users' discontent with GD. Up to 8 January 2011, over 93% of respondents held a low opinion on the program and its rated score was 0.7/10 in this survey⁷⁶. This was in distinct contrast to the statistics provided by Binguang Yan, the journalist of Xinhua.net.

Though MIIT argued that the pre-installation of GD was for children's benefit, it was in vain to relieve the resentment. The statement "should pre-install Green Dam" in *the Notice* was interpreted as a mandatory requirement by Chinese media and this was strongly protested about by internet users. In response to the dissent, MIIT clarified that the "should" statement was a grammar mistake and the pre-installation was optional. Meanwhile, Jinhui proclaimed that users could feel free to uninstall GD. However, un-installation was found implausible because GD could not be completely removed from PCs.

In addition, the GD blacklist was controversial for containing politically sensitive words⁷⁷. Chinese netizens believed this violated their constitutional rights of supervising the government⁷⁸. Also, GD would block the online information which is harmful to minors but legal to adults. In fact, some adult netizens were excited about GD blacklist because it provided an overall list of porn websites, which was never anticipated by the government.

Witnessing the whole incident, Han Han condemned that the government was out of credibility in this project. He also satirized that the government should develop a chip directly transplanted into the youth's brain⁷⁹.

⁷⁶ Ref. 'Green Dam-Youth Escort', 360 Software Encyclopedia,

http://baike.360.cn/wiki/item/%C2%CC%B0%D3-%BB%A8%BC%BE%BB%A4%BA%BD?select=desc&page=2#msg, accessed 8 January 2011 *

-

⁷⁷ Supra note 69

⁷⁸ Article 41, Constitution of People's Republic of China 2004

⁷⁹ Han Han, 'Green Dam reminds you that the content below including harmful information (绿坝提醒你,以下内容含有不良信息)', *Sina*, 11 June 2009, http://blog.sina.com.cn/s/blog_4701280b0100dlh2.html, accessed 12 November *

As always, this internet-related GD plan drew attention from the western world. It even almost sparked friction over trade with the country. The US Embassy in Beijing expressed their concern about this program and lobbied Chinese counterparts to drop the requirement that computers sold in the country be equipped with Green Dam⁸⁰.

3.1.3 Ending

Due to the pressure mounted from inside and outside, on June 30 2009, a day before the deadline by which it had said it would require all new PCs to come with Green Dam installed, MIIT announced it would delay introduction of the software *indefinitely* to give PC makers more time to prepare⁸¹. A MIIT spokesman also assured that GD would not be used to collect user's data. From late March to mid June 2009, the software had been downloaded 3.27 million times, installed at approximately 2279 schools, and installed in more than 53 million PC units for home use⁸².

On 13 August 2009, Li Yizhong, the minister of MIIT⁸³, said that the demand that each computer in China must pre-install the GD software was "not thoughtful enough"⁸⁴. However, the government would continue to install GD software on PCs in schools, internet cafés and other public places. He also emphasized that the government would fully

⁸⁰ Ref. T. Braithwaite, J. Chaffin, K. Hille, 'US lodges WTO case against China', *The Financial Times*, 25 June 2009, http://www.ftchinese.com/story/001027177/en, accessed12 November 2010

⁸¹ K. Hille, 'China Backtracks on mandatory installation of PC software filter', *The Financial Times*, 14 August 2009, http://www.ftchinese.com/story/001028158/en accessed 12 November 2010

Ref. OpenNet Initiative, 'China's Green Dam: The Implications of Government Control Encroaching on the Home PC', June 2009 http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc, accessed October 2010

⁸³ Li Yizhong has officially resigned his position as Minister of Industry and Information Technology from 17 December 2010

⁸⁴ Xin Qin (eds.), 'Li Yizhong: the political expansion of Green Dam deviates the fact (李毅中谈'绿坝':问题扩大政治化不符合事实)', *CHINANEWS*, 13 August 2009,

http://www.chinanews.com/cj/cj-cyzh/news/2009/08-13/1816719.shtml accessed October 2010 *

respect everyone's freedom of choice and would absolutely not mandate the installation on all PCs sold⁸⁵.

On 13 July 2010, the GD project group in Beijing was laid off due to a lack of funding⁸⁶. This means that over 20 million users who installed the software were left without technology support and customer service after the closure of the project.

3.2 Relevant Concerns Raised in Green Dam Case

Online protection of minors is a global concern. As an old-fashioned country (sex is still a public topic taboo in China), it is not only the concern of Chinese government, but also of Chinese parents. The failure of the GD project is worth rethinking for China in order to draw some lessons from it. It clearly exposed the limits and weakness of China's regulatory mode on internet content, yet it also reflected some facts contrary to the western assumption on China.

3.2.1 Tension in China is different from the Western assumption

Internet control in China has been assumed to be especially tight for a long period in the western world. Hence, the GD project in western perspective naturally was thought of as another action by the Chinese government to reinforce such control. The essentiality of online protection of minors in China, as stated in the notice of MIIT, has not drawn much attention from western community. In addition, few westerners have experienced or observed the social and cultural ongoing changes in China.

The report "China's Green Dam: The Implications of Government Control Encroaching on the Home PC"⁸⁷ represented a typical western point of view on the GD plan. It described GD as "a new and powerful control mechanism to the existing filtering system⁸⁸". This

.

⁸⁵ Supra note 81

⁸⁶ Qihui Gao, 'Green Dam's Beijing team dismissed, 20m users influenced,' *Chinadaily*, 13 July 2010, http://www.chinadaily.com.cn/china/2010-07/13/content_10099986.htm, accessed 12 November 2010

⁸⁷ Supra note 82

⁸⁸ *Ibid*, 'Executive Summary' part

research group reiterated in a published book that GD is "far more powerful than the centralized filtering system China currently implements" Those conclusions sound like "pie-in-the-sky" since it was in sharp contrast to what actually happened in China—the fatal filtering flaws of GD was illustrated in numerous jokes among Chinese internet users.

One should not deny that the Chinese government has engaged in internet control, like many countries do, US, Russia, Japan, etc⁹⁰. The arrest of Julian Assange, the founder of Wikileaks, is arguably a good example of such control because the official UK reason for his arrest did not convince his supporters⁹¹. It might go too far to say that Western media likes demonizing China's motivations (and vice versa to some degree), but it does seem doubtful that much Western research is based upon the true conditions in China. For example, regarding the function of GD, obviously the public opinion in China is quite contrary to the conclusion of the OpenNet Initiative research group.

It is important that Western research does not restrict itself to presumptions, which easily turns into dreary clichés. In fact, the challenges to Chinese government in the digital era are enormous and even more complicated. The online protection of minors, the constitutional rights of free speech (the situation is officially tight now in China due to some unresolved historical incidents), the conflicts and balance between them, as converged in the GD case, are the same missions for China to accomplish as in other countries of the world.

3.2.2 Coordination between government and industry is deficient

Though a number of PC manufacturers announced that they will coordinate with Chinese government to implement the GD plan, their hesitations indicated their internal worries. The potential losses largely lay in the technology bugs of the program, let alone the legal and political risks. As a Chinese commentator questioned, "Is any PC manufacturer willing to integrate a 'bomb' in its products?" and "after one year of free use, the fee for GD will

1

⁸⁹ *Supra* note 17, p.472

⁹⁰ Supra note 17

⁹¹ Ref. Wikileaks, 'Julian Assange arrested in London', *Facebook*, 7 December 2010, http://www.facebook.com/wikileaks/posts/179574032055494, accessed 7 December 2010

go to PC makers or consumers—will they buy products that bring inconveniences to internet access and risks to PC security?⁹²" Obviously, MIIT did not think about these consequences before it issued the order.

In the GD event, the industry self-regulatory bodies, which are supposed to put forward recommendations to government on behalf of industry⁹³, did not do their job adequately. For example, ISC, a body with representatives of ICT majors, simply remained silent in this uproar and did not pass the industry's real concerns to government. Microsoft, an ISC member, was the only one warning that GD would raise issues of freedom of expression, privacy, and security, which "need to be properly addressed⁹⁴". However, this was Microsoft's "personal" combat, not that of the industry.

Since ISC, the largest industry self-regulatory body in China could not facilitate its goal, it goes without saying that neither could other smaller and weaker ones. ISC is an example of Chinese self-regulation mechanisms at an early stage. Examining ISC bylaws, one discovers that ISC is supervised by MIIT⁹⁵. Further, some departments of MIIT and other government offices are ISC board members⁹⁶. Such tight government-involvement in a self-regulatory body will arguably undermine the independence of the organization, and thus impair its efficient operation and corrective feedback capability.

Another deficiency of such coordination exposed in the GD plan was that the Chinese government has not made use of industry's technological advantage. The software evaluated as "can effectively filter harmful text and pictures⁹⁷" in *the Notice* was not a solidly based conclusion. Evidently, it was not assessed by technology professionals from the industry since volunteer groups could find out GD technology flaws quickly.

29

⁹² Rui Wen, 'Green Dam or Damn Filter (绿坝还是滤霸)', Software Engineer(软件工程师), Vol 8 2009, p. 24-25 *

⁹³ Ref. 'Goal of ISC', http://www.isc.org.cn/Society_zz.php accessed 20 November 2010, accessed 20 November 2010 *

⁹⁴ Supra note 60

Provision 4, Bylaws of ISC (2008), see http://www.isc.org.cn/Society_zc.php accessed 20 November 2010, *

⁹⁶ Ref. 'ISC Members', http://www.isc.org.cn/Society_hy.php accessed 20 November 2010, *

⁹⁷ Supra note 56

3.2.3 Interaction between government and civil society is poor

The conflict between government and civil society in the GD plan largely lies in the scope of the software pre-installation: where—all the PCs, and who—all of the people (both adults and minors). This plan could be named "Green Dam for All", which implies that the Chinese government has lagged behind the progress of civil society. As China's society has been transitioning from the past, the government still stands up to its old role as "parents" of citizens (established in Confucianism)—it has been used to making decision for citizens without providing enough communication beforehand.

There was no doubt that the GD plan tried to protect minors by cracking down indecent online content. However, it is rarely noted that the plan was not just specific to minors. This crackdown deviated from the real situation of civil society by impairing citizens' freedom of information since there was no legislation explicitly banning adults' access to such information. As the Minister Li Yizhong confessed, the GD plan was not thoughtful enough. MIIT did not take account of true interests of civil society and such a drawback was inevitable since no dialogues were facilitated with civil society beforehand.

In addition to incomprehensive considerations of balancing interests, the absence of special groups in the GD plan reflected this poor interaction again. Though government announced that the plan met the needs of parents, during the whole event no parents showed up and made their voices heard. Regarding the government's routines for such allegations, Chinese internet users named it the "delegated" phenomenon, which means that the government considers itself the delegate of people but actually it does not represent the real thoughts of people.

The openness feature of an information society enables Chinese internet users to tell what is right or wrong on their own. Concomitantly, the capability of government to make "right" decisions for civil society is declining. The lack of dialogues worsens the situation and it needs to change. But how and what to change still remains unknown. Also running under a top-down governance mode, the experience of Europe with online protection of

minors may provide useful guidance for China. This experience will be described in Chapter IV.

4 European Regulatory Framework for Online Protection of Minors

4.1 Rationale

The online protection of minors can lead to conflicts with free speech, which has been ensured as a fundamental right in the United Nations' Declaration of Human Rights and other treaties as well as national legislations. Some harmful internet content, e.g. obscenity, is not protected in the form of free speech⁹⁸. However, the definition of such harmful content with respect to minors varies from country to country. The US and EU are forerunners to look for the balance between the two, and that is what China has to go through today. Of the US and EU governance modes, the former with its marked libertarian background is quite different from the elite-governance culture in China. The European regulatory mode is more top-down than bottom-up and as such is probably closer to the Chinese traditions than is the US mode. Therefore, this Chapter concentrates on examining relevant European policy documents and measures as a reference point for China's policy development.

In 1996, Europe published a *Green Paper*⁹⁹ which marked the start of a debate, at the European level, on the ethical dimension of information society and on how public interest can be protected in the new services. The right of freedom of expression is a fundamental right enshrined in Article 10 of the *European Convention of Human Rights* (ECHR)¹⁰⁰. The protection of children has been identified as overriding public interest in Europe and is

⁹⁸ This is even so in the USA: Ref. *Roth v. United States*, 354 U.S. 476 (1957), which was a landmark case before the US Supreme Court which redefined the Constitutional test for determining what constitutes obscene material unprotected by the First Amendment

⁹⁹ Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Service, presented by the Commission of the European Communities, [COM(96) 483 final], Brussels 16.10.1996

¹⁰⁰ Convention for the Protection of Human Rights and Fundamental Freedoms, available at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm accessed 7 October 2010

among the priorities for legal protection. As in the US, the restrictions on the dissemination of internet content for protection of the minors often results in conflict to free speech. Yet ECHR also provides that the exercise of this right may be subjected to certain limitations for specified reasons. The Green Paper pinpoints that "the case law of European Court of Human Rights has developed the principle of proportionality, the crucial test of conformity of any restrictive measures with the fundamental principles laid down in the ECHR. Europe therefore has a basis for a common approach - the principle of freedom of expression and the test of proportionality ¹⁰¹". Follow on this common basis, a series of legal documents concerning online protection of minors at an EU level have been adopted and related resolutions have been developed.

4.2 Approaches at the EU Level

The online protection of minors in the EU is of fundamental importance for the development of new media service. However the approaches to this object are not isolated from another equally significant public interest, that is, the human dignity. Therefore, several facets of internet content were taken into account by the EU on the restrictions to minors and these considerations are implemented with specific measures.

4.2.1 Restricted Internet Content to minors in the EU

The EU legal documents mainly provide three categories of restricted internet content to minors: illegal content, harmful content and unwanted content.

As defined in the *Safer Internet Action Plan*¹⁰² (1999-2004), illegal content "must be dealt with at source by the police and the judicial authorities, whose activities are covered by national legislation and judicial cooperation agreements." Regarding the parties to restrict the illegal content, it supplements that "the industry can be of considerable assistance in restricting the circulation of illegal content (particularly in the case of child pornography, racism and anti-Semitism) by means of effective self-regulation schemes (such as codes of

.

¹⁰¹ Supra note 98, see part 'Summary'

Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, O.J. L 033, 06 Febrary 1999, p. 1-11, adopted 25 January 1999

conduct and hotlines) governed and supported by legislation, and with consumer backing 103".

The *Safer Internet Action Plan* also defines that harmful content is "both that which is authorized but has restricted circulation (e.g. for adults only) and content which could be offensive to some users, even if publication is not restricted because of freedom of speech¹⁰⁴." That is to say, harmful content is not necessarily illegal. For example, the access to adult erotica is not prohibited to adults by legislation but the transmission of such content to children will be harmful.

The unwanted content, as stated in *Safer Internet Plus Programme*¹⁰⁵ (2005-2008), is "notably those on unsolicited commercial e-mail/communications", in other words, "spam¹⁰⁶". It is not wanted by end-users for the invasion of privacy, frequently misleading or deceptive, shocking pornographic content, loss of time and financial cost to the user, the considerable cost to business¹⁰⁷. The content concerning racism is also listed as unwanted in this programme.

The actions to combat restricted internet content differ in accordance with their respective characteristics. The way to tackle illegal content generally complies with the existing judicial systems. The solutions to harmful and unwanted content present new challenges and the EU Internet Plans propose rough actions. The "action to combat harmful content first and foremost means developing technology (filtering tools and rating mechanisms) to enable users to reject such content by promoting awareness among parents and fostering

¹⁰³ Ibid

¹⁰⁴ Ibid

¹⁰⁵ Decision No 854/2005/EC of establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies, O.J. L 149, 11 June 2005, p. 1-13, adopted 11 May 2005

¹⁰⁶ Communication from the Commission on unsolicited commercial communications or 'spam', [COM/2004/0028 final], not published in O.J., adopted 22 January 2004

¹⁰⁷ Ibid

self-regulation, which could be an adequate way of protecting minors in particular ¹⁰⁸." In terms of unwanted content, the measures are more complicated including remedies and penalties, complaints mechanisms, monitoring established by the regulatory authorities; technical and self-regulatory action by market players; and consumer awareness-raising ¹⁰⁹.

4.2.2 Regulatory Mechanisms

Online protection of minors in Europe is mainly geared by policy initiatives of EU regulatory authorities at community level. From 1996, a series of relevant policy documents have been adopted in Europe. In 1998, the first legal instrument at the EU level concerning the content of online audiovisual and information services, the *Recommendation on Protection of Minors and Human Dignity* ¹¹⁰ (hereinafter, 1998 Recommendation) was published. It "calls on the Member States, the sectors and parties concerned, as well as the Commission, to take measures to increase the protection of minors" in the internet sector.

Later in 1999, the *Communication on Audiovisual Policy*¹¹¹ points out that "digitization not only means a quantum leap in the amount of audiovisual content and information available to the citizen; it also allows a wide range of new operators to participate in the production and distribution of this information", and it defines "the European Commission's priorities for the next five years and the aims and principles of the Community's audiovisual policy in the medium term¹¹²". Then, the EU launched the *Safer Internet Action Plan* (1999-2004), initiating campaigns in Member States to deal with child pornography. With the

¹⁰⁸ Supra note 102

¹⁰⁹ *Supra* note 106

¹¹⁰ Council Recommendation 98/560/EC on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, O. J. L 270, 7 October 1998, p. 48-55, adopted 24 September 1998

Communication from the Commission: Principles and guidelines for the Community's audiovisual policy in the digital age, [COM (1999) 657 final], not published in O.J., adopted 14 December 1999

¹¹² Ibid

implementation of the plan, a European network of hotlines and the rating and filtering tools were successfully instigated and well developed¹¹³.

As Internet penetration is still growing considerably in Europe and potentially dangerous content, especially for children, is continuing to develop, in 2004 the Commission adopted the *Proposal for Safer Internet Plus Programme*¹¹⁴. Meanwhile, the EU endorsed a general approach in *Proposals for protection of minors and human dignity*¹¹⁵ to tackle the new digital technologies. The Commission argued in the proposal that the need for a safe environment was greater than ever, especially when "taking into account the ever-increasing processing power and storage capacity of computers, and the fact that broadband technologies allow distribution of content such as video on 3G mobile telephones. ¹¹⁶" Later in 2006, the Recommendation on the protection of minors and human dignity ¹¹⁷ had been adopted (hereinafter, 2006 Recommendation). It provides guidelines to harmonize the implementation of the measures and practice concerning online service in Member States, which had been established and well enforced in the former legal documents. Furthermore, some measures have been stipulated in the EU Directives, i.e. the drawing up of codes of conduct regarding the protection to minors was included in the provision Article 16 1(e) of Directive on Electronic Commerce.

_

¹¹³ Ref. Communication from the Commission concerning the evaluation of the Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors, [COM/2003/0653 final]

¹¹⁴ Proposal for a decision on establishing a multiannual Community programme on promoting safer use of the Internet and new technologies, presented by the Commission, [COM (2004) 91 final], Brussels 12.03.2004

¹¹⁵ Proposal for a Recommendation on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry, [COM/2004/0341 final- COD 2004/0117], presented by the Commission

¹¹⁶ Ibid

Recommendation on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, O.J. L 378, 27 December 2006, p. 72-77, adopted 20 December 2006

In addition to the regulations, alternative regulatory mechanisms, inter alia, co-regulatory and self-regulatory instruments were highly promoted by the Community—the terms of "co-regulation" and "self-regulation" have been increasingly mentioned in EU policy documents. This paper will examine the most important ones and those that are related to the online protection of minors. The *Better Legislation Action Plan* ¹¹⁸ describes co-regulation and self-regulation as "tools which in specific circumstances can be used to achieve the objectives of the Treaty of the European Union while simplifying lawmaking activities and legislation itself." In the Second Evaluation Report on the 1998 Recommendation, the Commission commends that the Recommendation "has a cross-media approach and emphasizes the cross-border exchange of best practices and the development of co-regulatory and self-regulatory mechanisms."

The White Paper on European Governance and the Final Report of the Mandelkern Group on Better Regulation delineate that the EU's approach to co-regulation is inclined to a top-down mode 119 that "regulation enacts the global objectives, main implementation mechanisms, and methods for monitoring the application of a public policy, and private players are asked to intervene in order to define a comprehensive set of rules." In the Inter-institutional Agreement on Better Law-making 120, self-regulation is defined as "the possibility for economic operators, the social partners, non-governmental organizations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)".

The precise conditions and characteristics of co-regulation and self-regulation still demand further exploration. However, the relevant attempts in relation to the online protection of minors have been in practice. The 1998 Recommendation established guidelines for the

¹¹⁸ Communication from the Commission: Action plan "Simplifying and improving the regulatory environment", [COM/2002/0278 final]

E. Lievens, J. Dumortier, P. S. Ryan, 'The Co-Protection of Minors in New Media: A European Approach to Co-Regulation', UC Davis Journal of Juvenile Law & Policy, Vol. 10:1 Winter 2006

European Parliament, Council, Commission Interinstitutional agreement on better law-making, O. J. C 321, 31 December 2003, p. 1-5

development of national self-regulation to this goal. The proposed guidelines concern four key components of a national self-regulation framework ¹²¹: (1) consultation and representativeness of the parties concerned, (2) codes of conduct, (3) national bodies facilitating cooperation at a national level, and (4) national evaluation of self-regulation frameworks. Later, the *Recommendation on self-regulation concerning cyber content* ¹²² adopted in 2001 indicates that Member States should encourage the establishment of self-regulatory organizations and encourage such organizations to establish regulatory mechanisms within their remit, to participate in relevant legislative process ¹²³, etc. The EU Directive 2007/65/EC ¹²⁴ also assures the positive effects of self-regulation in the audiovisual media service sector ¹²⁵.

While self-regulation mechanisms are gradually developed in detail in the policy documents, co-regulation has been increasingly put forward as well. In the second evaluation report on 1998 Recommendation, the Commission indicates that co-regulation implies an appropriate level of involvement by public authorities and that there should be cooperation among public authorities, industry, and other interested parties. In particular, co-regulation often offers a better mechanism for achieving set objectives regarding the protection of minors, where many sensibilities must be taken into account ¹²⁶. In the proposal for the Safer Internet Plus Programme, it asserts that self-regulation does not exclude the need for legal underpinning and the approach is shifting from advocating pure self-regulation to endorsing some form of co-regulation. Inspired by self-regulatory and co-regulatory principles, the Safer Internet Action Plan was implemented through three

supra note 110, see part 'Annex'

Recommendation on self-regulation and user protection against illegal or harmful content on new communications and information services, [Rec(2001)8], adopted by the Committee of Ministers to member states on 5 September 2001 at the 762nd meeting of the Ministers' Deputies

¹²³ Supra note 109, Chapter 1 of Appendix

¹²⁴ Directive 2007/65/EC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television, broadcasting activities, O. J. L 332, 18 December 2007, p.27-45, adopted 11 December 2007

¹²⁵ Ibid, ref. Recital 36

¹²⁶ Supra note 119

main action lines: creating a safer environment through the development of hotlines and codes of conduct, developing filtering and rating systems, and increasing public awareness ¹²⁷. For example in the action item of filtering and rating software, it underlines that "filtering and rating systems must be internationally compatible and interoperable and developed with full cooperation of representatives of industry, consumers and users", and "the demonstration projects will involve industry (self-regulatory bodies, access and service providers, content providers, network operators, software houses), user, consumer and citizens rights groups and government bodies involved in industry regulation and law enforcement".

Another pivotal mechanism in this regime is evaluation procedures. Such procedures have been constantly implemented on the enforcement of recommendations, plans, etc, by independent expert group. This procedure largely ensures the Community will sum up and promote the successful experience and to examine and improve the failed aspects. Also, it partly helps to ensure consistency among various policies.

4.3 Case Study of EU Member States: Practice in UK

The UK developed its regulatory scheme on the online protection of minors in accordance with its unique social, political and cultural structure. In general, the UK government favors a co-regulatory approach in which there is a significant role to be played by industry self-regulation. As an EU Member State, the UK also launched its projects along with the EU's plan. Currently some UK solutions have already become leading models in this domain, e.g. the self-regulatory mechanism.

4.3.1 UK Legislation on Online Protection of Children 128

Unlike the US, the UK does not attempt to tackle the issue of children safety on the internet by enacting specific laws. Instead, the UK constantly amends the existing laws, *inter alia*, by extending the scope of the provisions to protect the children over the internet,

.

¹²⁷ Supra note 102

¹²⁸ The source of UK legislation is the UK official website www.legislation.gov.uk

particularly concerning child sex abuse. Under the Criminal Justice and Public Order Act 1994 (hereinafter, "CJPOA 1994"), it is an offence to publish an obscene article or to have an obscene article for publication for gain. The scope of "publication" has been extended to electronic transmissions to be applicable on the internet. In addition, to crackdown on new behaviors of child sex offenders by information technology, the CJPOA 1994 (section 84) introduced the concept of "pseudo-photographs" of children, which means an image, whether made by computer-graphics or otherwise howsoever appears to be a photograph.

Following the amendments of CJPOA 1994, the definition of "photograph" given in section 7(4) of the Protection of Children Act 1978 (hereinafter, PCA 1978) has been interpreted to include photographs in electronic data format. It is further amended by the Criminal Justice and Immigration Act 2008 (section 69) to include the photographs derived from a part of a photograph or pseudo-photograph (or a combination of either or both), and includes the data stored on a computer disc or by any other form of electronic means that can be converted into such an image.

Recent legislation has sought to protect young people from internet abuse through the introduction of a "grooming" clause. This new offence category was introduced in the Sexual Offences Act 2003 in England and Wales (the section of the Act having application also to Northern Ireland). Section 15 makes "meeting a child following sexual grooming" an offence; this applies to the internet, to other technologies such as mobile phones and to the 'real world' ¹²⁹. In addition, the non-photographic visual depictions, such as computer-generated images, of child sexual abuse, which are illegal under the Obscene Publications Act 1959, are prohibited to be transmitted over the internet by the Coroners and Justice Act 2009 (section 62-69) ¹³⁰.

_

¹²⁹ J. Davidson, P. Gottschalk (eds.), *Internet Child Abuse: Current Research and Policy*, Taylor & Francis e-Library 2010, p. 10

¹³⁰ See further at

http://www.iwf.org.uk/hotline/the-laws/non-photographic-child-sexual-abuse-images/coroners-and-justice-act-2009 accessed 29 November 2010

4.3.2 UK Regulatory Bodies

The UK Home Office takes lead responsibility for internet content issues which lies with other UK government departments¹³¹. It has launched groups and projects to protect the children from online harmful content. The Home Secretary's Internet Task Force 2001 was set up by Home Office for two aims (a) to make the UK the best and safest place in the world for children to use the Internet; (b) to help protect children the world over from abuse fuelled by criminal misuse of new technologies¹³².

The Child Exploitation and Online Protection Centre (CEOP) is dedicated to eradicating the sexual abuse of children over the internet. It was launched in April 2006 funded by the Government and the communications industry, which includes representatives from the police and other criminal justice agencies. It is part of UK law enforcement and can apply the full range of policing powers in tackling the sexual abuse of children, including tracking and bringing offenders to account either directly or in partnership with local and international forces. Police officers visit chat rooms posing as children in order to detect grooming behavior. False websites will be set up to attract sex offenders seeking to groom children 133.

The Internet Watch Foundation (hereinafter, IWF), was announced in September 1996 initially as a hotline with the support of the UK government and is part of the EU's *Safer Internet Plus Programme*¹³⁴. IWF is a self-regulatory body¹³⁵ and was an initiative from the UK industry in reaction to police pressures. The IWF has an e-mail, telephone and fax hotline so that users can report materials related to child pornography and other obscene materials. IWF works with the UK governments, online industry, and law enforcement,

Yaman Akdeniz, 'Internet Content Regulation: UK Government and the Control of Internet Content', *Computer Law & Security Report*, Vol. 17 no.5 2001, Elsevier Science Ltd., p.303-317

http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/crimpol/crimreduc/internet/index.html
accessed 24 November 2010

¹³³ See further http://www.ceop.police.uk accessed 24 November 2010

¹³⁴ Supra note 129, p. 5

¹³⁵ See further http://www.iwf.org.uk/about-iwf accessed 29 November 2010

compiles a list of web sites it deems illegal ("potential illegal") and transmits this information to the ISPs, such as British Telecommunication 136. The tactics carried out by the IWF in minimizing the availability of child sexual abuse content encloses the reporting mechanism for the public, "Notice and Takedown" system to remove the alleged illegal/harmful content, targeted and monitoring system to remove such content in newsgroups, and the mechanism to work with domain name registries and registrars ¹³⁷. As a founding member of INPHONE¹³⁸, IWF work with the internet hotlines around the world to ensure the swift action of reporting harmful content on the internet. To fulfill its functions, IWF worked with internet actors to publish the R3 Safety Net Agreement regarding rating, reporting and responsibility of online harmful content, supported the use of rating and filtering software like Platform for Internet Content Selections (PICS), and Netintelligence, and so on.

With amending the legislation and building various institutions, the UK has established a system integrated with the power of the government and the industry in this domain. Though in practice there are difficulties with the application of existing national laws to a global internet which does not have any borders, this system has been effective in cracking down on online child sex offenders in UK¹³⁹.

4.4 Inspirations of European Regulatory Scheme for China

Though the online protection of minors in Europe was also mainly initiated by regulatory authorities, the European mode is much more sophisticated than that of China. To be specific, the essences of the European Regulatory model lie in several aspects below:

1. EU legal system establishes principles for public interests balance and develops specific measures for counterparts;

¹³⁶ Supra note 17

¹³⁷ *Supra* note 133

¹³⁸ IPHONE was founded under the EU Safer Internet Action Plan, see further https://www.inhope.org/

¹³⁹ IWF Annual Report 2007 indicates that 'there has been a 10% rise in the number of reports processed comparing to 2006 figures... however, there has been... a 10% decrease in the number of domains depicting child sexual abuse'. Available at http://www.iwf.org.uk/accountability/annual-reports/2007-annual-report accessed January 2011

- 2. EU values communication among all players and integrate them into the whole regime;
- 3. EU adopts independent evaluation procedure to examine the effects of its policies.

The European approaches were essentially developed due to their human rights oriented background and the EU's difficulty in establishing an internal market and accomplishing harmonization of the measures at an EU level. This is not a problem for China. Yet the EU has provided China with practical experiences under the top-down regulatory mode, which will be elaborated in Part V.

5 Alternatives for China Concerning Online Protection of Minors

The aborted Green Dam project presented a major case to demonstrate the emerging impact of other stakeholders, particularly civil society, in affecting the internet policy-making process in China. However, solution on a case by case basis is not a good way to go.

China now is struggling with many issues in this context: legislation is deficient and inefficient; alternative regulatory mechanisms, *inter alia*, co-regulation and self-regulation, still lag behind; dialogues among multi-stakeholders are not well facilitated, and so on. Nevertheless, which and how alternatives should offer requires prudent considerations. European experiences in this area provide a good example for China on how to balance the interests among all the players. The specific standards on online protection of minors may diverge from Europe to China due to culture differences, but the general regulatory approaches are arguably not so far apart. With European experiences combined with the actual situation in China, this paper proposes alternatives below for China in general and in specific aspects.

5.1 Role-switch of Chinese Regulatory Authorities

All regulatory systems operate within a framework influenced by the legal sanction of the sovereign government. As a primary public interest, the online protection of minors especially demands the policy initiatives of the regulatory authorities (governments).

In general, the regulatory mode in China is top-down, as analyzed in Chapter II. Such a model has severe limits and hardly tackles the challenges addressed by the fast evolving digital technology. As Sahel has described, "Government lost specialized capabilities in some sectors. This is evident in telecommunications (and ICTs more widely) where

governments cannot expect to rival private sector expertise and resources ¹⁴⁰." The GD case was evidence for this view. Therefore, the role of the Chinese government has to change to a more effective and advanced model.

In Europe, regulatory authorities play a leading role in tackling child pornography and other harmful internet information access to minors. However, such a "leading" position does not weaken the role of other players. On the contrary, the EU's promotion of co-regulation and self-regulation has taken advantage of all internet actors under the principles, i.e. principle of transparency, independence and proportionality, etc, which are enshrined in European legislation and Case law.

In response to social transition in China today, it is critical that the Chinese government switches from its "dominant" position to a "leading" position. The specific meaning of such a switch is three-fold. First it means that the government intervention should operate in accordance with Chinese laws and due procedures. In the report of WGIG for the better understanding of the respective roles and responsibilities of stakeholders, it indicates that governments should have oversight functions¹⁴¹. However, such function as performed by the government in China is overacting, which has resulted in severe conflicts with civil society and feasibility difficulties in the industry. The policies and orders issued by Chinese government have frequently run into obstacles for they put too much weight on efficiency rather than justice and fair reason. These values are very important to a harmonious society and could only be assured via certain procedures under the rule of law.

For the online protection of minors, the EU published a series of policy documents, i.e. the Green Paper, declarations, communications, proposal, etc, to promote public awareness

¹⁴⁰ Jean-Jacques Sahel (Department of Trade and Industry, UK), 'A new policy-making paradigm for the Information Society', 2006, available at http://web.si.umich.edu/tprc/papers/2006/635/NewParadigmInfoSociety.pdf accessed 23
November 1 2010

¹⁴¹ C. Marsden, S. Simmons, J. Cave, E. Nason, N. Robinson, 'Options for and Effectiveness of Internet Self- and Co-Regulation, Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet', *Rand Europe*, 27 June 2007, p.10

first. Not until such concerns have been roughly shared by EU Member States, would "soft-law", i.e. the recommendations, be adopted, and the plans on the EU scale would be launched. For the Chinese government, launching a full-scale action or stipulating laws is not as difficult as the EU. Yet the complexity for the Chinese government to fulfill the task is not any less than in Europe. The culture diverges a lot in different areas of China and the preservation of cultural diversities is a primary interest of the political agenda¹⁴². This will necessarily lead to the trend of civil society involvement in the procedure of policy-making and implementation to form common awareness. Therefore, the Chinese government has to relinquish acute dominant-style measures and take utmost account of all parties concerned.

In doing so, first and foremost the Chinese government needs to focus on justice instead of efficiency and pay more attention to the procedures enshrined in the Chinese judicial system. In particular, the Chinese government should (a) consult more with legislative bodies, i.e. NPC and its Standing Committee, to restrain itself not breach the constitution ¹⁴³; (b) release guidelines rather than mandatory administrative measures in early stages; (c) initiate public hearing and expert evaluation in the process of any compulsory order/policy making and measures adopting, and so on. All these procedures should proceed with the principle of transparency and independence. For example, the results of the consultation with NPC/Standing Committee should be made publicly available by the government except in the case of state confidentiality; the expert group in evaluation procedures should be independent from any interference from government, group or individual.

In addition to regulating under the rule of law, the ex-ante and ex-post regulation mode that the government adopts concerning information service should be carefully chosen. For now, the restrictions exposed on the conveyance of information via the internet are run under ex-ante control, i.e. headlines of newspapers are pre-selected by the Chinese government before being published over the internet to ensure online information is not illegitimate or

.

¹⁴² Article 4, Constitution of the People's Republic of China 2004

NPC and its Standing Committee exercise the power to supervise the enforcement of the Constitution, see Article 62 (2), Article 67 (1), Constitution of the People's Republic of China 2004

harmful. This is not practical because the government is not competent enough to recognize such materials. Further, this would largely infringe the constitutional rights of civil society to supervise the government and thus leave room for government officials to manipulate the media for their own sake instead of for the country and Chinese people, which is inconsistent with objectives of the government. Therefore, the ex-ante mode should be only carefully used except in the case of child pornography 144, state confidentiality, etc.

An ex-post regulation mode on information services, viz. all information should be allowed for online publishing unless judicial bodies confirm it illegal or harmful and prohibit its transmission, will be an effective alternative for the Chinese government. First and foremost, an ex-post regulation mode leaves the issues to courts which are more capable of making convincible conclusions than government. Also, courts can develop specific standards of harmful information. If explicit and reasonable standards are provided, civil society could exercise the right of freedom of speech and the industry could be more motivated to innovate in information service. Additionally, the ex-post regulation mode can largely decrease the government's cost on mandatory administrative measures. Nonetheless, the ex-post model has exceptional cases, i.e. Chinese government is always stricter in cracking down on online pornography. Even the non-profit transmissions that do not constitute penal offense will be prohibited over the internet—China can keep the tradition.

The role-switch of Chinese government also indicates multiple approaches provided for the online protection of minors. The alternative regulatory measures, *inter alia*, co-regulation and self-regulation mechanisms could be promoted and enhanced in this regime. These measures will be discussed with the role of private sector and civil society below.

5.2 Promoting Coordination between Government and Private Sector WGIG also describes the private sector role including:

-

Article 2, Optional Protocol to the Convention on the Rights of the Child, adopted 25 May 2000, entered into force on 18 January 2002

¹⁴⁵ Supra note 140, p. 11

- Industry self-regulation.
- Development of best practices.
- Development of policy proposals, guidelines and tools for policymakers and other stakeholders.
- Research and development of technologies, standards and processes.
- Contribution to the drafting of national law and participation in national and international policy development.
- Arbitration and dispute resolution.

Following this scheme, the policy-making process will chime with the views of the private sector. The EU Directive 2007/65/EC indicates that experience "has shown that measures aimed at achieving public interest objectives in the emerging audiovisual media services sector are more effective if they are taken with the active support of the service providers themselves." Also "self-regulation constitutes a type of voluntary initiative which enables economic operators, social partners, non-governmental organizations or associations to adopt common guidelines amongst themselves and for themselves". And "effective self-regulation can play as a complement to the legislative and judicial and/or administrative mechanisms in place¹⁴⁶."

As examined in Chapter II, the weakness of the self-regulatory bodies in China lay largely in the lack of independence. For instance, two bureaus of MIIT are the trustee/board member of ISC¹⁴⁷, and so some other departments of government, i.e. the State Council Information Office and State Intellectual Property Office. This would arguably impair the independence of ISC. To assure the independence of self-regulation and co-regulation bodies, the Council of Europe ¹⁴⁸ offers a way as indicated in the *Freedom of*

-

¹⁴⁶ Supra note 125

They are Telecommunications Administration Bureau and Telecommunications Support Bureau of MIIT, Cf. http://www.isc.org.cn/isc_e/member.php and http://www.isc.org.cn/Society_hy.php accessed 2 December 2010, *

¹⁴⁸ Every of 27 EU Member States is also a party of the Council of Europe (CoE). Thus, the policy document of CoE is also binding to EU. In this sense, CoE also provides the European experiences which go beyond that of the EU.

Communication on the internet 2003 ¹⁴⁹, "such bodies would have to meet the requirements...on the independence and functions of regulatory authorities..., in particular with regard to their independence from political and economic powers and the possibility to subject their decisions to judicial review ¹⁵⁰." As an example, IWF, a self-regulation body of UK is governed by a board of ten consisting of an Independent Chair, six independent Trustees, and three industry Trustees ¹⁵¹—there are no UK government offices involved.

One may argue that self-regulatory bodies do not run as well as IWF not just in China, but also in the rest EU Member States excluding the UK. It is true that self-regulation has some defects. As Rand Europe Report points out, "the type of self-regulation espoused by industry and supported by for instance the 1998 Recommendation has suffered from the problems associated with the non-compulsory nature of self-regulation: outright lack of participation and/or failure to conform to minimum standards 152." Regarding the limits, the EU states that "However, while self-regulation might be a complementary method...it should not constitute a substitute for the obligations of the national legislator 153". Yet this does not mean that the government needs to get involved in self-regulatory organizations. Particularly in China, business entities have been around only for a few decades and are still much weaker compared to the powerful central government. Therefore, the government should encourage the industry to actively propose on policy-making.

Adoption of technological measures is a different issue upon which the Chinese government should work closely with the industry. The industry owns expertise and resources in fast-changing internet sector and is motivated to coordinate for better application of technological measures. In addition, "measures aimed at achieving public interest objectives in the emerging audiovisual media services sector are more effective if

_

¹⁴⁹ Freedom of Communication on the Internet, adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies and explanatory note, the Council of Europe

¹⁵⁰ *Ibid*, Principle 2 'Self-regulation and Co-regulation'

¹⁵¹ 'Governance of IWF', see http://www.iwf.org.uk/accountability/governance accessed 2 December 2010

¹⁵² *Supra* note 140, p.11-12

¹⁵³ Supra note 146

they are taken with the active support of the service providers themselves ¹⁵⁴."The hesitations of the PC makers regarding implementation of the GD plan proved this view as negative evidence. Such cooperation is necessary and the EU actually encourages the industry to provide the filtering and rating systems ¹⁵⁵. In the UK, the adoption of the rating software PICS developed by W3C was recommended by IWF. It was also sustained by the UK government who supported the deployment of the PICS and the development of rating systems ¹⁵⁶.

Last but not least, some measures, i.e. hotlines, will be more appropriate for the industry to execute than for governments to do alone. China has set up three hotlines in its crackdown of obscenity and two of them are managed by the government. Once the "illegal or harmful" materials are reported, the powerful government will take action. This may cause unnecessary loss and severe consequences if such information has not been confirmed so by judicial bodies. Such risks could be decreased if the industry self-regulatory bodies or co-regulatory bodies (with the government) manage the hotlines instead. Since the "Notice and Takedown" procedure has been adopted in the Chinese legal system and has been proved practical, it could be introduced to this regime as well¹⁵⁷. In terms of the risks on privatized censorship, the establishment of accountability and relevant system will roughly eliminate this concern.

5.3 Facilitating Dialogues between Government and Civil society

Under the elite-governed mode for thousands of years, Chinese government officials have been regarded intellectually and morally superior to citizens and capable to make decisions

¹⁵⁴ Ibid

¹⁵⁵ Ref. Safer Internet Action Plan (1999-2004)

¹⁵⁶ Supra note 132

The "Notice and Takedown" procedure in Chinese legal system lies in Article 14, 15, 16 and 17 of the Ordinance on the Protection of the Right to Network Dissemination of Information 2006. The procedure briefly consists of four steps: 1. right holder notifies Internet Service Provider (ISP) of the content that it believes infringes its rights (Article 14 "Notice"); 2. ISP removes the alleged infringement content (Article 15 "Takedown"); 3. uploader contests the claims of copyright ownership (Article 16 "Counter-notification"); 4. ISP restore the materials if the uploader files a valid counter-notification (Article 17 "Putback")

for them. In contrast, Chinese citizen's right of supervising the government has been weakened and even ignored for a long time. The emergence of the internet changes this tension. Chinese citizens are now increasingly involved in formal decision-making and informal lobbying process. The termination of orders and dismissal of government officials (mainly local ones), is not rarely seen in China today under the pressure of public opinions from internet users. Sometimes public opinions even affect the judicial decisions. Experienced by "civic violence" (i.e. Culture Revolution 1966-1976), China is now very careful of the civic participation in state key issues. The open characteristics of the internet catalyze the progress of civil society and the citizens are becoming more mature than before. Thus, there is the possibility to facilitate better dialogues between the government and civil society in China—dialogues have been going on but not so well now. The conflict in GD case was miniature.

One decisive factor of the conflict in the GD plan is that the interest of the adult group was unnecessarily deprived by the government in the name of protecting children. If the government communicated with the civil society beforehand, instead of producing the order alone, more specific rules might have been developed and adopted. Then the government would not have had to suffer such failure. However, this scenario could not happen if the role and responsibilities of civil society has not been fully realized by the government.

As a reference, the WGIG report indicates that the role and responsibilities of civil society includes ¹⁵⁸:

- Awareness-raising and capacity-building (knowledge, training, skills sharing).
- Promoting various public interest objectives.
- Contributing to policy processes and policies that are more bottom-up, people-centred and inclusive.
- Contributing to shaping visions of human-centred information societies based on human rights, sustainable development, social justice and empowerment.

-

¹⁵⁸ Supra note 140

- Helping to ensure that political and market forces are accountable to the needs of all members of society.
- Encouraging social responsibility and good governance practice.

Inspired by the report combined with European experiences, the Chinese government and civil society could incorporate those in several aspects. First, rating systems should be introduced into the regime of online protection of minors for the interests balance. The restrictions on internet content should correspond with their labels, such as the illegal content—obscenity, child pornography, violence, etc; the harmful content, such as the adult erotica, which should be prohibited to be conveyed to minors but allowed for adults; and the unwanted content, like spam or some other kinds of content, which is up to the internet users preferences. With rating systems, both adult rights and the protection of minors could be assured.

Second, Chinese government should encourage the awareness of specific institutions, like primary and secondary schools, and some people, like educators and parents, on the object. Since schools are especially important for the physical and psychological health of minors, the installation of filtering software in campus network terminals should be mandatory. So follows for internet cafes and other public places which have minor-age consumers. The Chinese government could also encourage parents to install the web-nanny software on home PCs, and adopt similar measures on broadcasting and TV service.

Third, Chinese government can initiate the training projects for child regarding the features of child sex abuse behavior. In accordance with the UK Home Office report, the majority of child sex offenders are known to their victims. They are often a member of the family, a friend of the victim, or a friend of the victim's family¹⁵⁹. Therefore, some relevant training could be provided to children to cut off the production of the online child pornography. Such practices should be especially cooperated with the parents.

-

Ref. 'UK Child Sex Offender Disclosure Scheme', see
http://www.homeoffice.gov.uk/crime/child-sex-offender-disclosure/ accessed 24 November 2010

5.4 Other Possible Propositions

To prevent minors from accessing online harmful information is not easy and national measures are not sufficient since the internet is borderless. Therefore, China should take part in international cooperation as well. For example, some EU projects like the Safer Internet Plans and are open to other countries and regions. Again, since some illegal websites are not located in China, international joint action will be necessary sometimes. At the EU level, such organization is already set up, e.g. INPHONE ¹⁶⁰. International coordination will be good for decreasing online child sex offense content globally and for experience-sharing.

_

 $^{^{160}}$ INHOPE is the International Association of Internet Hotlines, see https://www.inhope.org/accessed November 2010

6 Conclusion

The online protection of minors has been acknowledged as a compelling public interest by the US Supreme Court and highly ranked in the EU political agendas. In China it attracts holistic concerns because of the tradition and the fact that many Chinese families only have one child. However, the restrictions on the transmission of information over the internet would unavoidably lead to a collision with free speech, which is a fundamental human right enshrined in constitutional legislations. The collision is particularly sensitive and complex in China for its exceptional culture and politics features. The numerous disputes in GD case underlined the different layers of complexity in this area for China.

It is clear that meeting the aspirations of all internet actors in China demands profound changes in the current regulatory mode. The Green Dam incident was a signal of the limits to overkill control on the internet by the Chinese government. A fact that Chinese government has to face is that the superiority rooted in government officials has becoming increasingly outdated in the digital era. With leaps of economics and education development in China, the elites have emerged in all industries. Additionally, the availability of access to infinite online information enables Chinese grassroots to think more independently. Hence, the stereotyped regulatory mechanisms have now gradually backed into a corner when confronted with the complexities in information society.

The good news is that the Chinese government has embarked on reforms. As the GD plan indicates, the Chinese government began to compromise to other players in this arena. The ongoing renovation in China today, as President Hu Jintao proposed in 2007, emphasizes that China should "accelerate the reform of the administrative system and build a

service-oriented government."¹⁶¹ The service-oriented government arguably indicates the absence of prior state control and more reliance on the co-regulation with civil society and private sector and the self-regulation of the internet actors.

Yet the Chinese government still needs to mandate steering functions for the private sector. Currently, most enterprises in China are profit-oriented rather than being socially responsible. The awareness of public interests in the industry has been diluted and can sometimes lead in the opposite direction¹⁶². This is no exception when it comes to the online protection of minors. Hence, state intervention needs to remain in the industry in some aspects for now. Yet the Chinese government should exercise such intervention in accordance with the principle of proportionality that is not going beyond to a necessary level. For instance, it should not ignore the fair response from the industry as it wrongly did in the GD plan.

China now stands at a crossroad. After the priority of economics has overridden the country for decades, the essentialities of improvements on social and legal system rise to a brand new level. The internet has become a primary channel for such expressions. In essence, the GD incident not just represented the contradiction amongst the interests of multi-stakeholders, but also represented the widespread distrust of Chinese netizens regarding the government for its censorship over the internet. This largely depends on that how China modernizes its regulatory system, in particular how makes its Constitution work effectively. However, case study and small-scale experiment of renovation are always a smooth and proper way before any fundamental reforms extended to this vast and populous country. The online protection of minors could be a start for China.

¹⁶¹ Hu Jintao, 'Highly Hold the Great Banner of Socialism with Chinese Characteristics and Strive for New Victories in Building a Moderately Prosperous Society in all', Report to the 17th Party Congress, 15 October 2007, available at http://www.china.org.cn/english/congress/229611.htm#6 accessed 5 December 2010

As an example, the food safety is a severe problem in China, i.e. the milk scandal event, Ref. A. Ramzy and Lin Yang, 'Tainted-baby—milk scandal in China', *TIME*, 16 September 2008, available at http://www.time.com/time/world/article/0,8599,1841535,00.html, accessed 11 January 2011

The online protection of minors as a public interest should not stop because of the failure of the GD project. China, especially the Chinese government, should draw lessons from this case to improve the mechanisms and carry on. The EU and the US are culturally and politically different from China. Yet they provide relatively successful experiences in this area, in policy-making and institution-building to balance those fundamental rights and interests of multi-stakeholders. This paper mainly examined the relevant experience in the EU and one of its Member States. Nonetheless, there are no perfect solutions—some measures are also controversial and still developing in Europe. Thus, more specific studies could be carried on for more tailored solutions in China. In addition, this paper focused on the EU top-down regulatory mode. The US bottom-up mechanism, which is also adopted by the EU sometimes, deserves further explorations to supplement the paradigm in China.

It has taken China decades to revive its economics; it will take much longer to modernize its regulatory system while still keeping the essence of its tradition and culture. No other country, with the size of China, inherits and develops its own civilization well for tens of centuries. Thus, this process will not be easy or short. With its unique culture and history, China is now especially struggling with these challenges because no other country has exactly the same background as China. The tension of the online protection of minors reflected in the Green Dam case is a trivial facet of the progress but rather typical. Now perhaps the time is ripe for China to abandon some old stereotypes and adopt proved superior alternatives into its regulatory framework concerning internet content, under which the mission of online protection of minors could be successfully accomplished in the country.

References

List of Judgements/Decisions

- 1. Ashcroft V. American Civil Liberties Union, 542 U.S. 656 (2004)
- 2. Reno v. American Civil Liberties Union, 117 S.Ct. 2329, 2332 (1997)
- 3. Roth v. United States, 354 U.S. 476 (1957)
- 4. Interpretation (II) concerning the application of laws in criminal cases of producing, reproducing, publishing, selling, and distributing electronic pornographic information via internet, mobile communication terminals and audio sets (最高人民法院,最高人民检察院关于办理互联网、移动通讯终端、声讯台制作、复制、出版、贱卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二))
- —Supreme People's Court Interpretation [2010] No.3 (法释 [2010] 3 号)

Treaties/Statutes

United Nations

1. Optional Protocol to the Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000, entered into force on 18 January 2002

Europe

- 1. Convention for the Protection of Human Rights and Fundamental Freedoms
- Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

- 3. Directive 2007/65/EC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television, broadcasting activities
- 4. Council Recommendation 98/560/EC on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity
- Recommendation on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry 2006
- 6. Recommendation on self-regulation and user protection against illegal or harmful content on new communications and information services, [Rec(2001)8], adopted by the Committee of Ministers
- Decision No 276/1999/EC of adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks
- 8. Decision No 854/2005/EC of establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies
- 9. Communication from the Commission on unsolicited commercial communications or 'spam', [COM/2004/0028 final]
- 10. Communication from the Commission: Principles and guidelines for the Community's audiovisual policy in the digital age, [COM (1999) 657 final]
- 11. Communication from the Commission: Action plan "Simplifying and improving the regulatory environment", [COM/2002/0278 final]
- 12. Communication from the Commission concerning the evaluation of the Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors, [COM/2003/0653 final]

- 13. Proposal for a decision on establishing a multiannual Community programme on promoting safer use of the Internet and new technologies, presented by the Commission, [COM (2004) 91 final]
- 14. Proposal for a Recommendation on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry, [COM/2004/0341 final- COD 2004/0117]
- 15. Inter-institutional agreement on better law-making (2003/C 321/01)
- 16. Freedom of Communication on the Internet 2003, adopted by the Committee of Ministers, Council of Europe

P.R China

- 1. Constitution of People's Republic of China 2004
- Resolution of the Standing Committee of the National Peoples Congress on Safeguarding Computer Network Security 2000
- 3. Regulation of the People's Republic of China on Telecommunications 2000
- 4. Law of People's Republic of China on the Protection of Minors 2006
- Measures for Security Protection Administration of the International Networking of Computer Information Networks 1997
- 6. Administration in Internet Electronic Messaging Services Provisions 2000
- 7. Administrative Measures on Internet Information Service 2000
- 8. Interim Measures for Administration on Education Websites and Online Schools 2000
- 9. Interim Provisions on the Administration of Internet Publication 2002
- 10. Interim Provisions on the Administration of Internet Culture 2004
- 11. Measures for Administration of Internet Domain Names 2004
- 12. Measures for the Administration of Internet E-mail Services 2005
- 13. Measures on the Administration of Internet News Services 2005
- 14. Administrative Rules about Audio-visual Programs Transmitted over Internet 2007

United States

1. The Communications Decency Act 1996

- 2. The Child Online Protection Act 1998
- 3. The Digital Millennium Copyright Act 1998

United Kingdom

- 1. The Obscene Publications Act 1959
- 2. The Protection of Children Act 1978
- 3. The Criminal Justice and Public Order Act 1994
- 4. The Sexual Offences Act 2003
- 5. The Criminal Justice and Immigration Act 2008
- 6. The Coroners and Justice Act 2009

Secondary Literature

- 1. Y. Akdeniz, 'Internet Content Regulation: UK Government and the Control of Internet Content', *Computer Law & Security Report*, Vol. 17 no.5 2001
- 2. T. Braithwaite, J. Chaffin, K. Hille, 'US lodges WTO case against China', *The Financial Times*, 25 June 2009
- 3. Chris Buckley (Reporter), N. Macfie (eds.), 'China says 5,394 arrested in Internet porn crackdown', *Reuters*, 31 December 2009
- 4. Lee A. Bygrave and Jon Bing (eds.), *Internet Governance Infrastructure and Institutions*, Oxford University Press 2009
- J. Davidson, P. Gottschalk (eds.), Internet Child Abuse: Current Research and Policy, Taylor & Francis e-Library 2010
- 6. R. Deibert, J. Palfrey, R. Rohozinsiki and J. Zittrain (eds.), *Access Controlled, The Shaping of Power, Rights and Rule in Cyberspace*, The MIT Press, 2010
- 7. Tom Downey, 'Human Flesh Search Engine in China', *The New York Times Magazine*, 3 March 2010
- 8. Simon Elegant, 'Han Han: China's Literary Bad Boy', *TIME*, 2 November 2009
- 9. Owen Fletcher, 'Green Dam Comes Back to Haunt Beijing', *The Wall Street Journal*, 2 December 2010

- 10. Geoffrey A. Fowler and B. Worthen, 'New China Web-Filtering Rules Still Murky', *The Wall Street Journal*, 9 June 2009
- 11. B. Frydman, L. Hennebel and G. Lewkowicz, 'Public Strategies for Internet Co-regulation in the United States, Europe and China', *Working Papers du Centre Perelman de philosophie du droit, n*° 2007/6
- Qihui Gao, 'Green Dam's Beijing team dismissed, 20m users influenced,' *Chinadaily*,
 July 2010
- 13. Zhixiong Gu, 'Green Dam block pictures of leaders (绿坝软件封杀领导人相片)', *MINGPAO*, 21 June 2009
- 14. Han Han, 'Green Dam reminds you that the content below including harmful information (绿坝提醒你,以下内容含有不良信息)', *Sina*, 11 June 2009
- 15. K. Hille, 'China Backtracks on mandatory installation of PC software filter', *The Financial Times*, 14 August 2009
- 16. Bi Hu, Shipeng Guo, 'Doraemon passed Garfield denied: Green Dam's good and bad (机器猫过关加菲猫过滤:绿坝过滤软件是与非)', *iNFZM* (南方周末),11 June 2009
- 17. Hu Jintao, 'Hold High the Great Banner of Socialism with Chinese Characteristics and Strive for New Victories in Building a Moderately Prosperous Society in all', Report to the 17th Party Congress, 15 October 2007
- 18. Chris Lefkow, 'Microsoft: China Web filtering raises issues', *Agence France-Press* (Washington), 9 June 2009
- 19. Jun Liu(eds.), 'Expert: utilization of Green Dam helps to promote network morality for the youth (要把绿坝软件转变为青少年的网络道德能力)', 12 June 2009
- 20. Jeremy Malcolm, 'Multi-Stakeholder Governance and the Internet Governance Forum', Terminus Press Perth 2008
- 21. C. Marsden, S. Simmons, J. Cave, E. Nason, N. Robinson, 'Options for and Effectiveness of Internet Self- and Co-Regulation, Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet', *Rand Europe*, 27 June 2007
- 22. Joe Mcdonald, 'PC makers voluntarily supply Web filter in China', *USATODAY*, 2 July 2009

- 23. Tuan Nguyen, 'Google Threatens to Withdraw From China', *Tom's hardware US*, 13 January 2010
- 24. David Pilling, 'Democracy's Demise in Asia is Exaggerated', *The Financial Times Journal*, 6 May 2010
- 25. Xin Qin (eds.), 'Li Yizhong: the political expansion of Green Dam deviates the fact (李毅中谈'绿坝':问题扩大政治化不符合事实)', *CHINANEWS*, 13 August 2009
- 26. A. Ramzy and Lin Yang, 'Tainted-baby—milk scandal in China', *TIME*, 16 September 2008
- 27. Jean-Jacques Sahel (Department of Trade and Industry, UK), 'A new policy-making paradigm for the Information Society', 2006
- 28. Shuquan Tang (eds.), 'Installation of web nanny software: necessary and a imperative need from parents (陶然:安装不良信息过滤软件很有必要 家长有迫切需求)', 11 June 2009
- 29. Lei Wang, Constitutional Law Applied in Courts (宪法的司法化), China University of Politics and Law Press, 2000
- 30. Rui Wen, 'Green Dam or Damn Filter (绿坝还是滤霸)', Software Engineer(软件工程师), Vol 8 2009
- 31. S. Wolchok, R. Yao, and J. A. Halderman, 'Analysis of the Green Dam Censorware System', *University of Michigan*, 11 June 2009
- 32. Bingguang Yan, 'What contentions on Green Dam for (过滤软件之争 争的是什么)', *Xinhua.Net*, 12 June 2009
- 33. Weiguo Zhang, 'Alert on Network Cynical kidnap Public Opinion (警惕网络愤青绑架民意)', *JXNews*, 23 August 2010
- 34. Li Zhang, 'Sick Green Dam (病态的绿坝软件)', IT Times Weekly Journal (IT 时代周刊), 5 August 2010
- 35. OpenNet Initiative, 'China's Green Dam: The Implications of Government Control Encroaching on the Home PC', 2008
- 36. Wikileaks, 'Julian Assange arrested in London', Facebook, 7 December 2010