

December 2012

## China's Internet Policies Within the Global Community

Omar Saleem

Follow this and additional works at: <https://scholarship.law.ufl.edu/jtlp>

---

### Recommended Citation

Saleem, Omar (2012) "China's Internet Policies Within the Global Community," *Journal of Technology Law & Policy*. Vol. 17: Iss. 2, Article 3.

Available at: <https://scholarship.law.ufl.edu/jtlp/vol17/iss2/3>

This Article is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in *Journal of Technology Law & Policy* by an authorized editor of UF Law Scholarship Repository. For more information, please contact [kaleita@law.ufl.edu](mailto:kaleita@law.ufl.edu).

# CHINA'S INTERNET POLICIES WITHIN THE GLOBAL COMMUNITY

Omar Saleem\*

I. CHINA'S INTERNET STRUCTURE.....	301
II. INTERNET CONTROL DEBATE.....	302
III. GLOBAL TECHNOLOGY SOCIETY.....	304
IV. CHINA REPORT.....	312

China is often perceived as a land of contradiction replete with economic opportunities and political authoritarianism. With many overlapping strategic interests, China has been described as a competitor and inevitable foe, not a strategic partner, to the United States.<sup>1</sup> China perceives the United States as butting into Asian affairs.<sup>2</sup> The U.S. perception is that China's socio-economic, political, and legal

---

\* Professor of Law, Florida A&M University College of Law, Orlando, Florida; LL.M. 1992 Columbia University School of Law; J.D., 1988 North Carolina Central University School of Law; B.A., 1985 City University of New York at Queens College.

1. See Confirmation Hearing by Sec'y of State—Designate Colin L. Powell Before the S. Comm. On Foreign Relations, 107th Cong. (Jan. 17, 2001), available at <http://www.gpo.gov/fdsys/pkg/CHRG-107shrg71536/pdf/CHRG-107shrg71536.pdf>; see also SEAN LEONARD, *THE DRAGON AWAKENS CHINA'S LONG MARCH TO GENEVA* 62 (1999) (noting China's increasing economic strength will inevitably lead to stronger military power, territorial acquisitions, and intimidation throughout Asia, which causes unease in the Asia-Pacific and the United States); Ken Dilanian, *China's Might on U.S. Radar*, ORLANDO SENTINEL, Jan. 7, 2011, at A3 (discussing U.S. concern that China may have closed the military gap enough to threaten the U.S. freedom of action in the western Pacific Ocean). In fact, as early as the late 1800s, Chinese immigrants to the United States were perceived as an aggressive encroachment by a horde of Chinese people crowding in upon U.S. citizens. See Gabriel J. Chin, *Unexplainable on Grounds of Race: Doubts About Yick Wo*, 5 U. ILL. L. REV. 1386-87 (2008) (citing *Chae Chan Ping v. United States*, 130 U.S. 581, 594 (1889)).

2. See, e.g., Zhu Feng, *Sino-U.S. Leadership Meeting Sets New Directions for Bilateral Relations*, CHINA TODAY, Mar. 1, 2011, at 31, 32 (noting that China has concerns about currency wars, Taiwan, disputes in the South China Sea, military exercises in the Yellow Sea, DPRK tensions, and U.S. alliance with Japan); M. Ulric Killion, *China Internet Tax: Issues of Particularism, Liberalization, and Integration*, 11 MSU-DCL J. INT'L L. 369, 379-80 (2002) (stating that China perceives U.S. neo-imperialism as a new threat to China's internal security, legal reforms and economic development).

infrastructures fail to protect the individual rights of Chinese citizens.<sup>3</sup> Accordingly, the criticism is that China's governmental violations of individual rights are copiously depicted in its controls over the Internet.<sup>4</sup> Purportedly, the logic follows, that China's governmental controls over the Internet undermine the human and civil rights of Chinese citizens in violation of international law.<sup>5</sup> This Article will examine that hypothesis within the construct of the World Summits on the Information Society assembled 2003 in Geneva and 2005 in Tunis.<sup>6</sup> Both Summits will serve to qualify the permissible scope and nature of the Chinese government's Internet activities.<sup>7</sup> This limited discourse concedes that there are vast reaches of online activities which encompass website design, business, consumer affairs, technical issues, copyrights, trademarks, patents, constitutional and privacy rights, contracts, and employment. Any attempt, however, at discussing the China's governmental online practices in totality would prove beyond the scope of this Article.

---

3. Some critics of U.S.-China relations are also cautious of China's growing military might. See RICHARD BERNSTEIN & ROSS H. MUNRO, *THE COMING CONFLICT WITH CHINA* 20–21 (1998).

4. See generally 2008 CONG.-EXEC. COMMISSION ON CHINA ANN. REP. NO. 44-748, at 4, 57, 60–65 (2d Sess. 2008), available at <http://www.cecc.gov>; see also Geremie R. Barne & Sang Ye, *The Great Firewall of China*, WIRE, June 1997 (indicating that China has sought to control the Internet via its architecture which limits telecommunication connections with the outside world).

5. Amnesty International USA (AIU) has purportedly compiled numerous records of instances in which the Chinese government has restricted the free expression of opinion and circulation of information in violation of international standards. AIU claims people whose rights have been violated include those “[w]ho have expressed views or circulated information via the Internet or email. The Internet, email and Bulletin Board Service (BBS) have been used by dissidents, Falun Gong practitioners, Tibetan exiles and others to circulate information or protest . . .” AMNESTY INTERNATIONAL USA, *PEOPLE’S REPUBLIC OF CHINA: STATE CONTROL OF THE INTERNET IN CHINA*, Amnesty International USA 3 (2002), available at <http://www.amnesty.org/en/library/info/ASA17/007/2002/en> (last visited Nov. 7, 2012) [hereinafter AIU]; see also HUMAN RIGHTS WATCH, *FREEDOM OF EXPRESSION AND THE INTERNET IN CHINA* (2001), available at <http://www.hrw.org/background/asia/china-bck-0701.htm> (examining the Chinese government's closures of Internet cafes and the detention of Internet users as well as providing several vignettes of individuals criminally sentenced or posting material on the Internet).

6. See WORLD SUMMIT ON THE INFORMATION SOCIETY, <http://www.itu.int/wsis> (last visited July 24, 2012).

7. In the United States, individual or public protected interests and specific harms and evils are defined within the scope of constitutional rights. See *Stanley v. Georgia*, 394 U.S. 557, 564, 568 (1969) (holding that the punishment for the private acquisition of pornography violated the constitutional right to freedom of thought); see also *Bowers v. Hardwick*, 478 U.S. 186, 190 (1986) (placing the debate about the right to homosexual sex within the construct of a constitutional right to privacy); *Washington v. Glucksberg*, 521 U.S. 702, 722–23 (1997) (deciding that the criminalization of assisted suicide failed to violate any recognizable constitutional right to die).

## I. CHINA'S INTERNET STRUCTURE

The growth of China's population, now in excess of one billion people, has precipitated remarkable growth in Internet usage.<sup>8</sup> Near the close of the twentieth century, China's Internet usage approximately doubled every 6 months.<sup>9</sup> Between the years 1999 and 2007 the number of Internet users in China increased exponentially from 2 million to 137 million.<sup>10</sup> During that time frame, predictions indicated that by 2010 that number would reach 200 million.<sup>11</sup> Cognizant of the impending vast Internet growth, the Chinese government at the onset embarked upon the unenviable task of Internet regulation.<sup>12</sup>

The regulations have encompassed both access and dissemination of online communications via the establishment of a vast communication gateway. Numerous government agencies are intertwined within an ostensibly and perplexing regulatory scheme.<sup>13</sup> The various government agencies adhere to specified regulations.<sup>14</sup> The Regulations primarily establish a pyramid system for international access of China's Internet. At the pyramid's first tier is a sole international gateway through which all connections to overseas computers must pass.<sup>15</sup> The Regulations are supported by the Implementation Measure and interconnected

---

8. For a discussion about the exponential growth of China's population, see Omar Saleem, *Be Fruitful and Multiple, and Replenish the Earth, and Subdue It: Third World Population Growth and Global Warming*, 8 GEO. INT'L ENVTL. L. REV. 1, 28-29 (1995) (indicating that China is the most populous country in the world and that in the near future China's population will exceed 1.5 billion).

9. See Omar Saleem, *The Establishment of a U.S. Federal Data Protection Agency to Define and Regulate Internet Privacy and Its Impact on U.S.-China Relations: Marco Polo Where Are You?*, 19 J. MARSHALL J. COMPUTER & INFO. L. 169, 185 (2000). But see Philip Tinari, *Web Use in China Slows*, WALL ST. J., July 20, 2004, <http://online.wsj.com/article/0,,SB109033408265568478,00.html> (stating that Internet growth in China slowed due to governmental control over access points such as Internet cafes and the growth of cell phone text messaging).

10. Saleem, *supra* note 9, at 185; see also ROB GIFFORD, CHINA ROAD: A JOURNEY INTO THE FUTURE OF A RISING POWER 197 (2007) (asserting the Internet has changed Chinese society because people are accessing information that was previously unavailable).

11. JEREMY HAFT, ALL THE TEA IN CHINA: HOW TO BUY, SELL AND MAKE MONEY ON THE MAINLAND 133 (2007).

12. Richard Cullen & Pinky D.W. Choy, *The Internet in China*, 13 COLUM. J. ASIAN L. 99, 109-11 (1999).

13. Government regulation in China is innately Byzantine due to China's vast geography and demographics. China consists of "thirty administrative units, five autonomous regions, twenty-two provinces, three self-governing megacities" with over 40 million inhabitants. See WILLEM VAN KEMENADE, CHINA, HONG KONG, TAIWAN, INC. 257 (1997).

14. Jack Linchaun, *Virtual Censorship in China: Keeping the Gate Between the Cyberspaces*, 4 INT'L J. COMMUN. L. & POL'Y 1, 10-15 (2000).

15. Jiang-yu Wang, *The Internet and E-Commerce in China: Regulations, Judicial Views, and Government Policies*, 18 COMPUTER & INTERNET L. 12 (2001).

networks.<sup>16</sup> These interconnected networks constitute the second-tier in China's network pyramid. The interconnected networks, all government owned, enable the Chinese government to filter communications.<sup>17</sup> Internet Service Providers (ISPs) must meet certain requirements for a special business permit to comply with government directives. At the pyramid's base are millions of China's Internet users who are required to register with a local public security bureau.<sup>18</sup> In sum, the elaborate pyramid scheme of Internet access and dissemination is designed to block unwanted foreign websites and to monitor Chinese citizens' Internet activities.<sup>19</sup>

Consequently, China's government regulates the access and dissemination of Internet communications to filter information, mandates Internet user registration and user agreements, prevents conduct that threatens the state's prohibitions against pornography, and monitors ISPs and their subscribers,<sup>20</sup> all of which raises concerns about whether such government practices unduly infringe upon the individual rights of Chinese citizens.<sup>21</sup>

## II. INTERNET CONTROL DEBATE

The Chinese government's Internet-regulation practices of controlling both access and dissemination of Internet communications highlights the debate among Western theorists about whether the state can or should regulate the Internet. Cyber-libertarian John Perry Barlow advocated an Internet that has neither sovereign interference nor state regulation.<sup>22</sup> In Barlow's view the state has no right to regulate the

---

16. Richard Cullen & D.W. Choy, *China's Media: The Impact of the Internet*, 6 SAN DIEGO INT'L L.J. 323, 326-27 (2005).

17. *Id.* at 329-31.

18. See Scott E. Feir, *Regulations Restricting Internet Access: Attempted Repair of Rupture in China's Great Wall Restraining the Free Exchange of Ideas*, 6 PAC. RIM. L. & POL'Y 361, 368 (1997).

19. For a detailed description of China's Internet structure and regulating bodies, see generally Jason LaCharite, *Electronic Decentralisation in China: A Critical Analysis of Internet Filtering Policies in the People's Republic of China*, 37 AUSTRAL. J. POL. SCI. 333, 335 (2005); Feir, *supra* note 18, at 368.

20. LaCharite, *supra* note 19, at 334; see also Barme & Ye, *supra* note 4; Ewan W. Rose, *Will China Allow Itself to Enter the New Economy*, 11 DUKE J. COMP & INT'L L. 451, 453-55 (2001).

21. See TED C. FISHMAN, CHINA, INC.: HOW THE RISE OF THE NEXT SUPERPOWER CHALLENGES AMERICA AND THE WORLD 284-85 (2005) (stating that China's Internet blockage demonstrates that, on a national level, China is a "land of ironfisted political repression and, on the local level China is pervasive with government gangsterism").

22. JOHN PERRY BARLOW, A DECLARATION OF INDEPENDENCE FOR CYBERSPACE (1996), <https://projects.eff.org/~barlow/Declaration-Final.html>.

Internet because Internet users have no elected government and the global social cyberspace is comprised of the people and is free of tyrants.<sup>23</sup> According to Barlow, governments lack both the authority and ability to regulate the Internet.<sup>24</sup> Other cyber-libertarians, such as David R. Johnson and David Post, expanded upon Barlow's premise of freedom of the Internet, basing their position on a "power-proximity-legitimacy-notice" paradigm, and surmised that governments are unable to regulate online transactions and that it is illegitimate for governments to regulate activities beyond their borders.<sup>25</sup>

In response to the cyber-libertarians, Judge Frank Easterbrook essentially argues that cyberspace can function satisfactorily via the clarification of existing laws, the creation of property rights, and the facilitation of bargaining institutions. In Easterbrook's view the Internet presented nothing new with respect to the sovereign's authority or power to regulate and when a property right or prohibition exists laws are enforceable and the sovereign has authority to regulate access and dissemination of information whether the medium of expression appears on the Internet, newspapers, or other printed publications.<sup>26</sup> The Johnson-Post position was further challenged by Jack L. Goldsmith who asserted that cross-cultural communications have occurred long before the Internet and that existing laws and technology were capable of providing rules for cyberspace governance.<sup>27</sup> Goldsmith's reliance on technological mechanisms to regulate the Internet is also at the crux of Lawrence Lessig's position concerning the use of code or architecture as a viable method to regulate the Internet.

In Lessig's view, discussions about whether the state should regulate the Internet are moot because the state already regulates conduct on the Internet. In his view regulation of the Internet, or any human behavior in the physical or cyberspace, occurs through four different modes: laws, markets, norms and code/architecture.<sup>28</sup> According to Lessig, architectural design or code provides the most effective means to regulate conduct in both the physical world and on the Internet.<sup>29</sup> He further posits that debates about whether the Internet can or should endure regulation are moot because states are already controlling the

---

23. *Id.*

24. *Id.*

25. See generally David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

26. See generally Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207. This position is similar to the Supreme Court ruling in *Reno v. ACLU*, 521 U.S. 844 (1997) in which the Court stated that speech on the Internet is entitled to the same full First Amendment protections afforded to newspapers and other printed publications.

27. See Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

28. LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 87-88 (2000).

29. *Id.* at 89.

Internet via software, code, or other architectural means.<sup>30</sup>

The debate among Barlow, Johnson-Post, Easterbrook, Goldsmith, and Lessig oscillates between discussions of a utopian world of uncontrolled ideas with individual rights and an austere pragmatism lodged in market concerns, property rights and state security.<sup>31</sup> The jurisprudential tension in this discourse is manifested in U.S. Supreme Court decisions. The Supreme Court has struck down domestic regulations of Internet pornography in the interests of free speech and individual rights consistent with the liberalism approach advocated by Barlow, Lessig and Johnson-Post.<sup>32</sup> In juxtaposition, individual rights have succumbed to the Court's interests in facilitating Internet economic growth via an Internet tax moratorium, and immunity for ISPs in comport with the economic pragmatism expounded by both Easterbrook and Goldsmith.<sup>33</sup>

In the main, within the United States there has been considerable discourse about the "how," "whether," and "why" behind Internet regulation. Despite the domestic debates and inconsistent laws governing U.S. Internet regulation there is a general U.S. perception that the Internet regulatory practices in China are reprehensible and in violation of the individual rights of Chinese citizens. According to U.S. critics, the Chinese government has obdurately embarked upon a path contrary to the global community, and created a cyberspace replete with filtering, monitoring, oversight, and criminal prosecution. The pivotal question presented in this Article is whether the Chinese government's Internet-related regulatory practices are in violation of international norms as proposed in the World Summits on Information Technology.

### III. GLOBAL TECHNOLOGY SOCIETY

Preceding the arrival of the Internet there has been consternation between technology and the law. The historical evolution of communication in forms such as written letters, telegraphy, and the

---

30. *Id.*

31. See YVES POULLET, *Some Considerations on Cyberspace Law*, in THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 147 (Bruno de Padirac & Teresa Fuentes-Comacho eds., 2000).

32. See *Reno v. ACLU*, 521 U.S. 844 (1997).

33. See *Quill Corp. v. North Dakota*, 504 U.S. 298 (1992) (prohibiting the collection of sales tax for transactions made by mail or common carrier outside of the state that lacks a "substantial nexus"). In order to facilitate investments and free discussion on the Internet, Congress enacted the Communications Decency Act, which has granted ISPs far reaching protections from liability as publishers. See *Communications Decency Act*, 47 U.S.C. § 230 (1998); *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997); *Blumenthal v. Drudge*, 992 F. Supp. 44, 50 (D.D.C. 1998).

telephone each highlight a disjoint between law and technology. The U.S. Supreme Court has addressed the prohibition of mail, namely, a 1877 circular about a lottery;<sup>34</sup> the disclosure of telegram contents to someone other than the authorized recipient;<sup>35</sup> and, by the 1890s, the taping of telephone conversations.<sup>36</sup> Technology has historically outpaced the legal system. Following the First World War, for example, bank robbers began using the Thompson sub-machine gun and the automobile to facilitate escapes from law enforcement. A notable example is depicted in the conduct of the infamous criminal, John Dillinger, who eluded police using both the automobile and Thompson submachine gun.<sup>37</sup>

Jurisprudentially, the Fourth Amendment to the U.S. Constitution has been contested in an effort to reconcile individual rights with police surveillances technology. Police technological surveillances, which have discombobulated Fourth Amendment scholars, have included technology-related eavesdropping cases dated post World War II,<sup>38</sup> and includes electronic tracking devices known as beepers,<sup>39</sup> pen-registers,<sup>40</sup>

---

34. Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 *Miss. L.J.* 1, 9 (2005).

35. *Id.* at 13.

36. *Id.* at 20–21.

37. BRYAN BURROUGH, *PUBLIC ENEMIES* 17 (2004).

38. See *Goldman v. United States*, 316 U.S. 129, 133 (1942) (holding government use of detectaphone technology against an outer wall for listening to a suspect's conversation was not a Fourth Amendment violation); *On Lee v. United States*, 343 U.S. 747, 754–55 (1952) (holding an electronic transmission to a nearby police officer was not a search when the speaker consented to the informer's presence and spoke confidently and indiscreetly); *Silverman v. United States*, 365 U.S. 505, 512 (1961) (holding insertion of a spike mike into a wall to hear conversations through heating ducts was a search); *Lopez v. United States*, 373 U.S. 427, 438 (1963) (holding consent to a government agent's presence and assumptions of the risk by the suspect was not a Fourth Amendment violation when government agents recorded the suspect's bribe); *Clinton v. Virginia*, 377 U.S. 158, 158 (1964) (holding a thumbtack-sized penetration into a wall as part of a listening device was a search within the Fourth Amendment); *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (holding that listening to and recording of the suspect's inculpatory statements by an informant in a hotel was not a search when the suspect relied upon his own misplaced confidence); *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (providing that one has a privacy right protected by the Fourth Amendment when the person exhibits an actual (subjective) expectation of privacy and that the expectation be one that society is prepared to recognize as reasonable); *United States v. White*, 401 U.S. 745, 754 (1971) (holding that when the conduct of the government agent fails to violate the Fourth Amendment without electronic equipment then the simultaneous recording of the same conversation fails to violate the Fourth Amendment as well).

39. Compare *United States v. Knotts*, 460 U.S. 276, 285 (1983) (holding that attaching an electronic tracking device to a container of chemicals to monitor a suspect's movements in public was not a search), with *United States v. Karo*, 468 U.S. 705, 717 (1984) (holding that the government's use of an electronic tracking device to gather information inside the home was a search).

40. See *Smith v. Maryland*, 442 U.S. 735, 745–46 (1979) (holding that pen register



aerial views,<sup>41</sup> cameras,<sup>42</sup> thermal-imaging devices,<sup>43</sup> and GPS tracking.<sup>44</sup>

At the dawn of the new millennium, the historical tug of war between law and technology has truly taken on another dimension. The impact of the Internet on law exceeds the impact of technology utilized by Dillinger and police surveillance techniques. The Internet has vastly redefined the nature of human conduct and technology. Internet usage in lieu of "snail mail," telephone calls, fax machines, office visits and house calls is fascinatingly similar to the famous comedian Groucho Marx's 1943 description of the benefits of radio in contrast to theater, in which he characterizes radio as "the poor man's theatre" with a nominal admission price.<sup>45</sup> The Internet, similar to the impact of radio, has created a mode of communication that is both widespread and inexpensive. Ideally, and at relatively low costs, an Internet user has access to e-mail, list servers, USENET groups, real-time chat, real-time remote computer utilization, and remote information retrieval.<sup>46</sup> This occurs all within a massive global community with convenient, instantaneous and translatable communications accessible to millions.

The cheap cost of the Internet has established a global virtual community that exceeds all previous modes of communication and has altered human perceptions of time and space. This alteration is remarkably similar to Albert Einstein's impact on theoretical physics via his theories of relativity. Before Einstein, the perception of the universe was based on the Newtonian principle that space and time were

---

mechanical devices used to record numbers dialed by a suspect on a telephone does not constitute a search for Fourth Amendment purposes).

41. See *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (holding police's use of an airplane flying 1000 feet within navigable airspace over a suspect's home did not constitute a search); *Florida v. Riley*, 488 U.S. 445, 451 (1989) (holding police surveillance from a helicopter at 400 feet above a suspect's premises did not constitute a search for Fourth Amendment purposes).

42. See *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986) (holding that when agents took aerial photographs of a large outdoor industrial complex, the agents violated the Fourth Amendment due to the nature of the place being surveilled, the information revealed, and the nature of the surveillance.).

43. See *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding the use of sense-enhancing thermal imaging technology to gather information about a home's interior that could not be otherwise obtained without physical invasion into the home constituted a Fourth Amendment search).

44. See *United States v. Jones*, 132 S. Ct. 945, 954 (2012) (holding government installations of a Global-Positioning-System (GPS) to monitor a vehicle's movement constitutes a search).

45. STEPHAN KANFER, *THE ESSENTIAL GROUCHO* 187 (2000).

46. See Peter S. Menell, *Knowledge Accessibility and Preservation Policy for the Digital Age*, 44 HOUS. L. REV. 1013, 1043 (2007) (explaining the Internet enables worldwide effortless communications and greater connection among individuals and groups).

separate and absolute.<sup>47</sup> Einstein proved that space and time are interwoven and relative.<sup>48</sup> Similar to Einstein's celestial world, the Internet has fashioned a vastly interwoven and relative network of computers stretching across vast geographical areas and purports to challenge "relative" views of morality, democracy, economic growth, and freedom.<sup>49</sup>

The extensively interwoven and "relative" aspects of the Internet have presented challenges within the global community.<sup>50</sup> The United Nations identified issues, such as SPAM, network security, privacy, domain names, servers, technical underpinnings, content, free speech, and intellectual property, all of which globally impact Internet users and governments.<sup>51</sup> The United Nations further acknowledged that solutions

---

47. See Omar Saleem, *The Physics of Fourth Amendment Privacy Rights*, 32 T. MARSHALL L. REV. 147, 160 (explaining how Einstein verified that the universe is interactive and fluid and that space is more than a mere background; rather it is an active participant).

48. BRIAN GREENE, *THE ELEGANT UNIVERSE* 51 (1st ed. 1999).

49. Areas which have increasing variability among states within the United States and between the United States and foreign nations are free speech and spam. See *Reno v. ACLU*, 521 U.S. 844, 876 (1977) (addressing the domestic conflicts in regulating indecent and patently offensive speech); see also *Mainstream Loudoun v. Bd. of Tr. of the Loudoun Cnty. Library*, 24 F. Supp. 2d 552 (E.D. Va. 1998); *Am. Lib. Ass'n v. Pataki*, 969 F. Supp. 160, 174 (S.D.N.Y. 1997) (discussing the domestic conflicts in regulating obscenity); *Yahoo!, Inc. v. LaLigue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001), *rev'd and remanded by Yahoo!, Inc. v. La LaLigue Contre Le Racisme et L'Antisemitisme*, 433 F.3d 1199 (9th Cir. 2007) (holding U.S. law rather than French law governs Yahoo!'s right with respect to content (Nazi merchandise on U.S. based services)); JONATHAN D. MART, *LAW OF THE WEB* 10–28 (2003) (providing extensive list of cases in which States have sought to restrict online content). For a discussion about the differing domestic and foreign efforts to regulate spam, see DOUG ISENBERG, *THE GIGA LAW GUIDE TO INTERNET LAW* 263–67 (2002); see also ROY J. GIRASA, *CYBERLAW NATIONAL AND INTERNATIONAL PERSPECTIVES* 84 (Melissa Steffens et al. eds., 2002). On a global level, the competing moral interests inherent in the Internet was illustrated in a dispute concerning online gambling between the governments of Antigua and Barbados and the United States, which was adjudicated at the World Trade Organization (WTO). The U.S. position was that Internet gambling is illegal—therefore morally reprehensible—because the conduct occurs in places such as Antigua and Costa Rica and is beyond the regulatory authority of U.S. federal agencies. In opposition to the U.S. position, the governments of Antigua and Barbados developed online gambling to boost its economy and advocated that any efforts by the United States to curtail online gambling adversely impacts both jobs and revenues in Antigua and Barbados. The WTO agreed with Antigua and Barbados and ruled in their favor. See Liz Benston, *WTO Ruling Details Remain Secret*, LAS VEGAS SUN, Mar. 25, 2004, available at <http://www.casinocitytimes.com/news/article/wto-ruling-details-remain-secret-141805>.

50. See *The Use of the Internet by Islamic Extremists: Testimony Before the H. Permanent Select Comm. on Intelligence*, 109th Cong. 1 (2006) (testimony of Dr. Bruce Hoffman, RAND Corp.), available at [http://www.rand.org/pubs/testimonies/2006/RAND\\_CT262-1.pdf](http://www.rand.org/pubs/testimonies/2006/RAND_CT262-1.pdf) (stating the Internet has altered communications and enabled the world-wide inexpensive distribution of information in real-time).

51. Declan McCullagh, *United Nations Ponders Net's Future*, CNET News (Mar. 26 2004), <http://news.com.com/2100-1028-5179694.htm1>. Another global concern is cybercrime.

to these issues required global inclusion rather than standards mandated by the United States, Canada, Europe, and Japan.<sup>52</sup> The United Nations also acknowledged that any coordinated efforts and archetype designed to regulate the sprawling global Internet network “must be made accessible and responsive to the needs of all the world’s people.”<sup>53</sup> The U.N. position recognizes the “relative” nature of values, the interplay between domestic and global values, and the tension in reconciling human rights, individual freedoms, and economic development with states’ concerns of accountability, national security, and sovereignty.<sup>54</sup> Countries throughout the world held two world summits in support of the United Nations’ position to establish a global information society.<sup>55</sup> The Summits were termed the World Summit on the Information Society (WSIS).<sup>56</sup> The first summit was held in Geneva in 2003, and the second summit was held 2005 in Tunis.<sup>57</sup>

The WSIS held in Geneva was an historical, multi-stakeholder global effort by participants to develop a shared vision of an information society that empowers and benefits all people. The Summit participants included over 11,000 delegates<sup>58</sup> consisting of nation states,<sup>59</sup> U.N. bodies,<sup>60</sup> specialized agencies,<sup>61</sup> and intergovernmental

---

*See* Convention of Cybercrime, Aug. 5, 2006, Council of Europe, No. 185, 23 XI. 2001, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (Convention on Cybercrime to harmonize anti-cybercrime laws and establish uniform agreement and cooperation in cybercrime investigations.).

52. A global approach is practical because at the dawn of the new millennium more than half of the world’s Internet users were outside the United States. *See* A. HUGH SCOTT, *COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW* 12 (2001).

53. McCullagh, *supra* note 51.

54. Dianna Kempe, Presentation at the University of Dayton: Law in a Wired Society – The Information Revolution and the Evolution of Law (Mar. 23, 2001).

55. *About WSIS*, WORLD SUMMIT ON THE INFORMATION SOCIETY, <http://www.itu.int/wsis/basic/about.html> (last visited Oct. 10, 2012) [hereinafter WORLD SUMMIT ON THE INFORMATION SOCIETY].

56. *Id.*

57. *Id.*

58. *Id.*

59. The following states were represented: Afghanistan, Albania, Algeria, Angola, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahrain, Bangladesh, Barbados, Belarus, Belgium, Benin, Bhutan, Bosnia and Herzegovia, Botswana, Brazil, Brunei Darussalam, Bulgaria, Burkina Faso, Burundi, Cambodia, Cameroon, Canada, Capeverde, Central African Rep., Chad, Chile, China, Colombia, Comoros, Congo (Rep. of the), Costa Rica, Côte d’Ivoire, Croatia, Cuba, Cyprus, Czech Rep., Dem. People’s Rep. of the Congo, Dem. People’s Rep. of Korea, Denmark, Djibouti, Dominican Rep., Ecuador, Egypt, El Salvador, Equatorial Guinea, Entrea, Estonia, Ethiopia, Fiji, Finland, France, Gabon, Gambia, Georgia, Germany, Ghana, Greece, Guatemala, Guinea, Haiti, Holy See, Honduras, Hungary, Iceland, India, Indonesia, Iran (Islamic Rep. of), Iraq, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Lau People’s Dem. Rep., Latvia, Lebanon, Lesotho, Liechtenstein, Lithuania, Luxembourg, Madagascar, Malawi, Malaysia, Maldives, Mali, Malta, Mauritania,

organizations.<sup>62</sup> The participants produced a Draft Declaration of Principles (Draft Declaration), which delineated a common vision, key principles, and the goal of a true shared knowledge society.<sup>63</sup> The Draft Declaration outlined a “Common Vision of the Information Society” comprised of certain recognitions, challenges, reaffirmations, awareness of issues, commitments, resolutions, attentiveness to special needs, and reservation of rights.<sup>64</sup> The participants recognized a shared vision of a global information society, which would be people-centered, inclusive and development-centered, “where everyone can create, access, utilize,

---

Mauritius, Mexico, Micronesia (Federated States of), Monaco, Mongolia, Morocco, Mozambique, Myanmar, Namibia, Nepal, Netherlands, New Zealand, Nicaragua, Niger, Nigeria, Norway, Oman, Pakistan, Palau, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Rep. of Korea, Rep. of Moldova, Romania, Russian Federation, Rwanda, Samoa, San Marino, Saudi Arabia, Senegal, Serbia and Montenegro, Sierra Leone, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Sudan, Suriname, Swaziland, Sweden, Switzerland, Syrian Arab Rep., Thailand, The Former Yugoslav Rep. of Madagascar, Timor-Leste, Togo, Tonga, Trinidad and Tobago, Tunisia, Turkey, Uganda, Ukraine, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United Rep. of Tanzania, United States of America, Uruguay, Uzbekistan, Venezuela, Viet Nam, Yemen, Zambia, Zimbabwe. See *Final List of Participants*, WORLD SUMMIT ON THE INFORMATION SOCIETY, [http://www.itu.int/wsis/docs/geneva/summit\\_participants.pdf](http://www.itu.int/wsis/docs/geneva/summit_participants.pdf) (last visited Oct. 10, 2012).

60. The following U.N. bodies were represented: U.N. Secretariat, U.N. Human Settlements Programme, Joint U.N. Programme on HIV/AIDS, U.N. Conference on Trade and Development, U.N. Development Programme, Economic Commission for Africa, Economic Commission for Europe, Economic Commission for Latin America and the Caribbean, Economic and Social Commission for Asia and the Pacific, Economic and Social Commission for Western Asia; U.N. Population Fund, U.N. Children's Fund, U.N. Development Fund for Women; U.N. Institute for Training and Research, Non-Governmental Liaison Service, U.N. University, U.N. Office at Geneva, U.N. Volunteers. *Id.*

61. The following specialized agencies were represented: Food and Agriculture Organization; International Labour Organization; The World Bank; U.N. Educational, Scientific and Cultural Organization; U.N. Industrial Development Organization; Universal Postal Union; World Health Organization; World Intellectual Property Organization; and World Meteorological Organization. *Id.*

62. The following invited intergovernmental organizations were represented: Asia Pacific Telecommunity, Asian Development Bank, African Telecommunications Union, Commonwealth of Independent States, Economic Commission for Europe, Inter-American Developmental Bank, Inter-Parliamentary Union, League of Arab States, Organization for Economic Cooperation and Development, Organization of the Islamic Conference, International Organization of la Francophonie. *Id.* In addition, a large number of non-governmental organizations and business sector entities, including ITU Sector Members, attended the session. See *Invited Intergovernmental Organizations for WSIS*, WORLD SUMMIT ON THE INFORMATION SOCIETY, <http://www.itu.int/wsis/participation/accreditation/lists/io.pdf> (last visited Oct. 10, 2012).

63. See WORLD SUMMIT ON THE INFORMATION SOCIETY, DRAFT DECLARATION OF PRINCIPLES DOCUMENT (2003), available at <http://www.dinf.ne.jp/doc/english/prompt/031217/wsis.html> [hereinafter *Draft Declaration*].

64. *Id.*

and share information and knowledge . . . to achieve their full potential.”<sup>65</sup> The common vision was designed to promote sustainable development and to improve the quality of life in the spirit of the Charter of the United Nations and the Universal Declaration of Human Rights.<sup>66</sup>

Along with the common vision, the Draft Declaration listed major challenges and expressed an “awareness of issues” confronting the establishment of a global information society.<sup>67</sup> The challenges were perceived as global in nature and exemplified the gap between the industrial and developing nations. The challenges included global poverty and hunger, illiteracy, gender inequality, child mortality, maternal health, HIV/AIDS, malaria, sustainable development, and the absence of peace, justice, and prosperity.<sup>68</sup> The Geneva Summit Participants further understood that certain global issues essentially render Information and Communication Technologies (ICTs) irrelevant for the disadvantaged and oppressed in developing countries.<sup>69</sup> Cognizant of the challenges ahead, the Geneva Summit Participants articulated an awareness of certain basic truths.<sup>70</sup> The Participants noted that ICTs are not ends in themselves, rather they are tools which immensely impact individuals’ lives and can facilitate dialogue that may lead to economic growth.<sup>71</sup> The WSIS Geneva Summit Participants were also aware of, and addressed, the digital divide crisis between “developed and developing countries and within societies.”<sup>72</sup>

The challenges and awareness of issues facilitated the WSIS Geneva Summit Participants’ reaffirmation of certain fundamental rights.<sup>73</sup> They reaffirmed the international community’s commitment to human rights and fundamental freedoms, economic development, democracy,

---

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*; see also AMY CHUA, *WORLD ON FIRE 7* (2004) (stating that one-third of 80 million residents of the Philippines exist on \$2.00 a day, and further arguing that the global spread of free markets and democracy has caused global anti-Americanism); cf. THOMAS L. FRIEDMAN, *THE LEXUS AND THE OLIVE TREE* (2000). Despite global Internet access, there is a digital divide in which poor nations lack the means to provide Internet access to its citizens. For a discussion on the global digital divide, see James Hall, *Poverty an Impediment to Internet Growth in Africa*, IPS UN J., July 21, 2003, available at <http://www.ipsnews.net/2003/07/technology-africa-poverty-an-impediment-to-internet-growth/> (stating that although the African Continent accounts for approximately 13% of the world’s population, only 0.6% of Internet users worldwide are in Africa and that 50% of Africa’s population live below the poverty line on \$1.00 per day).

73. See *Draft Declaration*, *supra* note 63.

good governance at all levels as interdependent and mutually reinforcing, respect for the rule of law in international and national affairs, freedom of expression, full development of personality, morality, public order, general welfare in a democratic society, human dignity, and empowerment of women.<sup>74</sup>

The WSIS Geneva Summit participants sought to minimize the numerous challenges with the recognition of the significant role of science, education, and the need for new forms of solidarity, partnership and cooperation among governments, and other stakeholders in the private sector, civil society, and international organizations.<sup>75</sup> There was a further resolve to empower the poor, particularly those in remote areas, to utilize ICTs to eradicate poverty, and to preserve indigenous peoples and their heritage and cultural legacy.<sup>76</sup> The WSIS Geneva Summit participants devoted special attention to the marginalized and vulnerable groups in societies, the needs of the people of developing countries, and the threats to development in those nations.<sup>77</sup> Along these lines, the Draft Declaration incorporated by reference relevant international documents such as the Charter of the United Nations, the Universal Declaration of Human Rights, the Millennium Declaration, the Johannesburg Declaration and Plan of Implementation, the Monterrey Consensus, and the Vienna Declaration.<sup>78</sup>

The “Key Principles” section of the Draft Declaration, consisting of sixty-seven paragraphs, is both extensive and ambitious.<sup>79</sup> The section is primarily a quest for all stakeholders to work together to improve information access. The stakeholders in the global information society are the private sector, civil society, international organizations, and governments.<sup>80</sup> These stakeholders are instructed to collaborate to build a people-centered information society with equitable and affordable access.

Two years after the Geneva Summit the participants held the Tunis Summit in 2005, which constituted the second phase of the WSIS.<sup>81</sup> The 2005 Tunis Summit participants expressed unequivocal support for the 2003 WSIS in Geneva.<sup>82</sup> The Tunis Commitment provisions also stressed such concerns as: people-centeredness, inclusion, development, human rights, fundamental freedoms, democracy, sustainable

---

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.* at 16-18 (Second phase of the WSIS, Nov. 2005).

82. *Id.* Statements, WSIS.

development, freedom of expression, free flow of information, poverty eradication, links with other U.N. conferences and summits, closing the digital divide, Internet governance, development (economic, social, and cultural), and entrepreneurship.<sup>83</sup> Furthermore, there was recognition of the need to prevent abuse of information resources, to foster human rights, and to tend to special needs (developing nations, heritage preservation, rights of women and children, poverty eradication, and cultural diversity).<sup>84</sup>

Along with a commitment section, the WSIS in Tunis recognized the financial mechanisms involved in meeting the challenges of ICTs.<sup>85</sup> Such challenges were rooted in recognition of a digital divide, limited resources, technology transfer, development, and Internet governance.<sup>86</sup> The Internet governance concerns are enumerated in articles 29 thru 82 of the Tunis WSIS Agenda.<sup>87</sup> While the Agenda affirms the Geneva WSIS, it also recognizes sovereign rights of states, cybersecurity, social and economic development of each country, cybercrime, spam, Internet instability and security (while protecting human rights), terrorism, Internet threats and vulnerabilities, rights of individuals, national laws, digital divide, national strategies for ICT integration, and the maximization of the interests and development of developing countries.<sup>88</sup>

#### IV. CHINA REPORT

The pivotal inquiry arising from the WSIS is whether China's governmental Internet practices comport with the WSIS participants' common visions, key principles, and the goal of a true/shared knowledge society. Posed differently, the inquiry becomes whether China has merely fostered an Internet society that controls what people read and think.<sup>89</sup>

The development of Internet regulation in China is juxtaposed with the reality that, although China is an ancient country, its so-called modern legal system developed in the late 1970s after China opened up

---

83. *Tunis Commitment Document*, WORLD SUMMIT ON THE INFORMATION SOCIETY (Nov. 18, 2005), available at <http://www.itu.int/wsisis/docs2/tunis/off/7.html> [hereinafter *Tunis Commitment Document*].

84. For sources on the affirmations, commitments, and recognitions listed, see *id.*

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. See RAJ BHALA, INTERNATIONAL TRADE LAW: THEORY AND PRACTICE 186 (2d ed. 2001).

to the world.<sup>90</sup> Contemporary China has a commercial legal system similar to France, Germany, Japan, and Taiwan.<sup>91</sup> This leads to the conjecture that China's domestic laws should comport with Western practices to protect online privacy. Although similar to the western system in certain respects, China's legal system is "a market economy with socialist characteristics."<sup>92</sup>

In the United Kingdom and United States, systems of government consist of three separate branches, all of which provide a system of checks and balances against one another. In China, however, there is a dominant legislative branch called the National Peoples Congress (NPC).<sup>93</sup> China's Constitution provides that all the power in the People's Republic of China belongs to the people and that the NPC is the highest body through which the people exercise state power.<sup>94</sup> The NPC has approximately 3000 delegates elected by various provinces, autonomous regions, and municipalities.<sup>95</sup> The NPC, along with its Standing Committee consisting of 175 individuals elected by the NPC, interprets and has the power to implement the Constitution and enact, interpret, and amend the laws.<sup>96</sup> The other organs of state power, subordinate to the NPC, include the President, the State Council, the Supreme People's Court, the Supreme People's Procuratorate, and the Central Military Commission.<sup>97</sup>

The United States and China clearly have different political structures. China lacks a democratic system similar to the West.<sup>98</sup> In

90. See generally Xiang Gao, *The Fraud Rule in Law of Letters of Credit in the P.R.C.*, 41 INT'L LAW. 1067 (2007) (explaining the development of the procedural and substantive legal system in China as it relates to letters of credit).

91. See John S. Mo, *The Code of Contract Law of the People's Republic of China and the Vienna Sales Convention*, 15 AM. U. INT'L L. REV. 209, 211 (1999).

92. For a detailed analysis of China's legal system, see RONALD BROWN, *UNDERSTANDING CHINESE COURTS AND THE LEGAL PROCESS: LAW AND CHINESE CHARACTERISTICS*, at xx-xxi (1st ed. 1997); see also *Alphabetical Index of the Political Entities and Corresponding Legal Systems*, JURIGLOBE-WORLD LEGAL SYSTEMS RESEARCH GROUP, available at <http://www.juriglobe.ca/eng/sys-juri/index-alpha.php> (last visited Oct. 10, 2012) (indicating China is among a significant number of countries which has a mixed system of law that includes both civil law and customary law).

93. See *Organization*, THE NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA, [http://www.npc.gov.cn/englishnpc/Organization/node\\_2846.htm](http://www.npc.gov.cn/englishnpc/Organization/node_2846.htm) (last visited Nov. 20, 2012).

94. See XIANFA arts. 57-58 (1982) (China).

95. *Id.* art. 59; see also *The National People's Congress: What Makes a Rubber Stamp?*, ECONOMIST (Mar. 5, 2012), <http://www.economist.com/blogs/analects/2012/03/national-peoples-congress>.

96. XIANFA arts. 65-67; see also *Organization - Standing Committee*, THE NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA, [http://www.npc.gov.cn/englishnpc/Organization/node\\_2847.htm](http://www.npc.gov.cn/englishnpc/Organization/node_2847.htm) (last visited Nov. 20, 2012).

97. See PEOPLE'S REPUBLIC OF CHINA YEARBOOK 1989-1999, at 37-72 (1999).

98. Americans tend to view constitutional and common law rights "to be universal, a



enacting its Code of Criminal Procedure, for example, China indicated that it adopts “Marxism-Leninism-Mao Zedong thought as its guide and the Constitution as its basis . . . in carrying out the people’s democratic dictatorship.”<sup>99</sup> This form of proletariat democracy derives from leadership by the proletariat based on worker-peasant alliance focused on striking the enemy and protecting the people.<sup>100</sup> The discourse concerning a world information society falls short if China’s Internet practices are simply contrasted with U.S. political rhetoric. This is because the more relevant inquiry is whether China’s Internet practices comply with the international standards synthesized by the 2003 Geneva and 2005 Tunis WSIS, which incorporated the cultural perspectives of more than 11,000 delegates representing 175 countries.<sup>101</sup>

China’s Internet regulatory practices are numerous and pervasive.<sup>102</sup> China has held ISPs liable when a plaintiff requested a bulletin board operator to remove defamatory statements about the plaintiff, and the operator failed to do so.<sup>103</sup> A Chinese province required Internet café users to buy access cards to enable the police to monitor the users’ activities, block certain sites, track sites visited, and filter email for forbidden content.<sup>104</sup> China has threatened to criminally charge bloggers who have failed to register with the government.<sup>105</sup> In order to secure blogger registration, the Chinese government utilizes a webcrawler program to monitor and report unregistered bloggers.<sup>106</sup> China has

codification of liberty’s meaning, constraining all levels of government and applicable to all people within the boundaries of [democratic society].” See BARACK OBAMA, *THE AUDACITY OF HOPE* 86 (2006). *But see* CHUA, *supra* note 72, at 13 (stating the concept of “democracy” is difficult to define because a single interpretation of the term is nonexistent); *see also* RANDALL PEERENBOOM, *ASIAN DISCOURSES OF RULE OF LAW* 137 (2004) (China is unlikely “to embrace democracy in the near future,” and even if it does, it will “not necessarily become a liberal democracy.”).

99. See FADIAN art. 1. For the English translation, see 26 *THE AMERICAN SERIES OF FOREIGN PENAL CODES* 84 (1985).

100. *Id.*

101. See *WORLD SUMMIT ON THE INFORMATION SOCIETY*, *supra* note 55.

102. According to Human Rights, Watch between 1994 and 2000, China established approximately 60 regulations to control Internet content or access. *Freedom of Expression and the Internet in China: A Human Rights Watch Backgrounder*, HUMAN RIGHTS WATCH, <http://www.hrw.org/backgrounder/asia/china-bck-0701.htm> (last visited Dec. 21, 2012).

103. See Li Fangchao, *Man Wins Online Defamation Case*, CHINADAILY.COM (Dec. 14, 2004), [http://www.chinadaily.com.cn/english/doc/2004-12/14/content\\_400008.htm](http://www.chinadaily.com.cn/english/doc/2004-12/14/content_400008.htm).

104. See JONATHAN D. HART, *INTERNET LAW: A FIELD GUIDE* 447 (5th ed. 2007) (citing *Chinese Net Café Users Must Get ID Cards*, SAN JOSE MERCY NEWS, Nov. 5, 2002, at 2C); *see also* ANDREW ROSS, *FAST BOAT TO CHINA CORPORATE FLIGHT AND THE CONSEQUENCES OF FREE TRADE LESSONS FROM SHANGHAI* 134 (2006) (stating that China’s networks are controlled by a government that views every Internet packet of information entering or leaving the country).

105. See Bill Thompson, *A Little Less Censorship?*, BBC.COM (June 10, 2005), <http://news.bbc.co.uk/2/hi/technology/4080886.stm>.

106. *Id.*

deemed spam as subversive, pornographic, and anti-government.<sup>107</sup> China has also promulgated the Commercial Encryption Management Regulations that require all foreign companies, as a matter of law, to register encryption technology, and forbid foreign companies from importing or distributing unregistered encryption technology in China.<sup>108</sup>

The above regulatory practices demonstrate that China's government has imposed ISP liability, blocked sites, mandated blogger registration, deemed spam as subversive and pornographic, and required companies to register encryption technology. Are such regulatory practices in violation of the WSIS? In both Geneva and Tunis, the WSIS participants emphasized that connectivity in a global information society should be "in conformity with the domestic legislation of each country."<sup>109</sup> In other words, each nation has the sovereign right to establish policies governing the Internet, and such policies while in conformity with International standards should also respect and foster domestic policies.

The WSIS, for example, emphasized "particular attention to the special needs of girls and women."<sup>110</sup> The Chinese government's restrictions on spam, as it relates to pornography, comport with the WSIS concerns for women and children. China, in the interests of blocking pornography, blocked access to certain sites and stopped doing business with certain companies.<sup>111</sup> While blocking sites and stifling business seemingly fails to facilitate an information society, such governmental practices are in compliance with the Internet governance concerns enumerated in articles 29 through 82 of the Tunis WSIS agenda concerning human rights, the rights of women and children, poverty eradication, state sovereignty, cyber-security, social development, cybercrime, spam, and respect for national laws.<sup>112</sup> In 2009, when China blocked sites and stifled certain business interests, there were 650 million cellphone users in china, 50 million of which were primary and middle-school children.<sup>113</sup> Also, in 2009 there were 400 million Internet users in China, most of whom were 20-29 years

---

107. See Donna Buenaventura, *China Vows to Curb Junk Email*, SILICONVALLEY.COM (Feb. 2, 2004), <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/7855530.htm>.

108. See BHALA, *supra* note 89, at 186.

109. See *Draft Declaration*, *supra* note 63; *Tunis Commitment Document*, *supra* note 83.

110. *Id.*

111. Yuan Yuan, *The Big News on the Web in 2009*, BEIJING REV., Dec. 31, 2009, at 21, available at [http://www.bjreview.com.cn/special/2009-12/26/content\\_236926.htm](http://www.bjreview.com.cn/special/2009-12/26/content_236926.htm).

112. See World Summit on the Information Society, *Tunis Agenda for the Information Society Document WSIS-05/TUNIS/DOC/6(Rev. 1)-E*, arts. 29-82 (Nov. 18, 2005), available at <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>.

113. Yuan, *supra* note 111, at 21.

old, with online usage amounting to 17.9 hours per week.<sup>114</sup> As far back as 2006, China's Internet usage was first in the world.<sup>115</sup> The Chinese government used software called Green Dam Youth to block sites as part of a campaign to prevent the Internet from "poisoning youthful people with harmful content."<sup>116</sup> In the interests of preventing vicious rumors about citizens and protecting the public rights and interests, China has also required real-name registration of bloggers in micro-blogs like Twitter.<sup>117</sup> Neither blocking sites nor real name registration would be in violation of the WSIS when the state's interests are in social harmony and balancing individual's privacy rights against one another.

In both the United States and China, pornography is an issue inextricably tied to free speech, cultural integrity, and social values. Although pornographic restrictions may hinder speech, free speech rights lack an absolute protection in both the United States and China. In restricting Internet speech China has asserted interests in the protection of cultural values and the protection of women as justifications to curtail Internet pornography. Both justifications are clearly in agreement with the spirit of the WSIS participants to acknowledge the "needs of girls and women" (among other legitimate policies).<sup>118</sup> Although standards and values vary globally, the protection of women, especially young women, is a global concern. Juveniles generally lack maturity, full character development, and are more vulnerable than adults. Concerning women and pornography, there are the corollary crimes such as drugs and human trafficking. Organized crime is a \$2 trillion industry, with human trafficking representing a significant share of the flow of organized crime.<sup>119</sup> It is estimated that tens of thousands of people are taken from their homes every year: 79% of them are taken for sexual exploitation, and among that number 66%

---

114. Zan Jifang, *Life on the Internet*, BEIJING REV., Oct. 14, 2010, at 38–39, available at [http://www.bjreview.com.cn/special/2009-12/26/content\\_236926.htm](http://www.bjreview.com.cn/special/2009-12/26/content_236926.htm); see also *The Internet in China: Alternative Reality*, ECONOMIST, Feb. 2008, at 69 [hereinafter *The Internet in China*], available at <http://www.economist.com/node/10608655> (stating that in 2008 more than 70% of Internet users in China were under 30 years of age and China's Internet users used the Internet primarily for films, television shows, music, accessing the Internet on cell phones, and online multiplayer games).

115. Jifang, *supra* note 114; *The Internet in China*, *supra* note 114.

116. Yuan, *supra* note 111, at 21. Data is conflicting as to whether parents supported or disapproved of the Green Dam Youth Escort software. *Id.*

117. Li Shigong, *Is Real-Name Registration Necessary for Micro-Blogs?*, BEIJING REV., Feb. 2, 2012, at 28, available at [http://www.bjreview.com.cn/forum/txt/2012-01/30/content\\_422194.htm](http://www.bjreview.com.cn/forum/txt/2012-01/30/content_422194.htm).

118. See *Draft Declaration*, *supra* note 63.

119. See Patrick Di Justo et al., *Organized Crime: The World's Largest Social Network*, WIRED, Feb. 2011, at 78, available at [http://www.wired.com/magazine/2011/01/ff\\_orgchart\\_crime/](http://www.wired.com/magazine/2011/01/ff_orgchart_crime/).

are women and 13% are girls.<sup>120</sup> It is estimated that trafficking humans to Europe is a \$1.25 billion industry and global child pornography is a \$250 million industry.<sup>121</sup> Efforts to curtail spam, filter email, regulate encryption, and limit business activities in the interests of protecting women and children, are acceptable within the provisions of the WSIS.<sup>122</sup> Such government regulations find support in Catharine A. MacKinnon's vivid description from a Minneapolis City Council proceeding on the impact of pornography on women (drawing parallels to the Nuremberg trial):

The studies of researchers and clinicians documented the same reality [as Nuremberg] women documented from life: pornography increases attitudes and behaviors of aggression and other discrimination by men against women.

....

Women told how pornography was used to break their self-esteem, to train them to sexual submission, to season them to forced sex, intimidate them out of job opportunities, blackmail them into prostitution, and keep them there, terrorize and humiliate them into sexual compliance, and silence their dissent. They told of being used to make pornography under coercion, of the force that gave them no choice about viewing pornography or performing sex. They told how pornography stimulates and condones rape, battery, sexual harassment, sexual abuse of children, and forced prostitution.<sup>123</sup>

MacKinnon describes prostitution as female slavery because it institutionalizes the subhuman status of women.<sup>124</sup> In theory, the WCIS participants would adhere to Mackinnon's rationale in its support of China's regulation of spam and other regulations as they relate to the intent to protect women from oppression. China's adherence to regulation of spam and other similar threats would be in the interests of the WSIS's focus on human dignity, gender equality, HIV/AIDS prevention, full development of personality, empowerment of women, and national affairs.

Along with free speech rights, the WSIS indicated that confidence and security in ICTs is accomplished by strengthening information security, assuring network security, and establishing authentication, all

---

120. *Id.* at 80.

121. *Id.*

122. *See Draft Declaration, supra* note 63.

123. CATHARINE A. MACKINNON, ARE WOMEN HUMAN? 115–16 (2006).

124. *Id.*

while simultaneously protecting consumers and privacy concerns.<sup>125</sup> Indeed, China's Internet regulatory practices raise concerns about the privacy rights of its citizens. In the global information technology age, threats to individual privacy are of monumental concern.<sup>126</sup> The United Nations noted that most nations grapple with, among other concerns, the tension between network security and protecting individual privacy.<sup>127</sup> In the United States, the word privacy is absent from the U.S. Constitution; rather, privacy in the United States stems from a multitude of sources such as common law, evidence, statutory provisions, and state and federal constitutions.<sup>128</sup> In the United States, privacy rights are balanced against state interests.<sup>129</sup> This balancing test is typified in Fourth Amendment criminal procedure jurisprudence protections against unreasonable searches and seizures. The Fourth Amendment to the U.S. Constitution provides, in relevant part, "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated . . . ."<sup>130</sup>

Between 1967 and 1968, the U.S. Supreme Court decided three major cases that altered the course of Fourth Amendment jurisprudence and firmly established a balancing test to gauge whether a search was unreasonable. The cases were *Camara v. Municipal Court*,<sup>131</sup> *Katz v. United States*,<sup>132</sup> and *Terry v. Ohio*.<sup>133</sup> As a result, the Court began to balance the individual's right to be left alone against the police need for effective law enforcement. The result has been a hodgepodge of cases attempting to grapple with the impact of technology on Fourth Amendment jurisprudence. The disjunction in Fourth Amendment jurisprudence is escalated by Court decisions which dismiss the subjective bad-faith of the police, while other cases allow consideration of the good faith of the police to ascertain whether there is a Fourth

---

125. See *Draft Declaration*, *supra* note 63.

126. Indeed, privacy in the global Internet age is a concern of all nations. See DANIEL J. SOLOVE ET AL., *INFORMATION PRIVACY LAW* 38 (2d ed. 2006) ("The Organization of Economic Cooperation and Development (OECD) developed an extensive series of privacy guidelines in 1980 that formed the basis for privacy laws in North America, Europe, and East Asia.").

127. See *Draft Declaration*, *supra* note 63 and accompanying text.

128. See U.S. CONST. amend. IV.

129. See *Aid for Women v. Foulston*, 441 F.3d 1101, 1119 (10th Cir. 2006).

130. U.S. CONST. amend. IV.

131. *Camara v. Mun. Court*, 387 U.S. 523, 536–37 (1967) (establishing the balancing test to determine whether a search is unreasonable).

132. *Katz v. United States*, 389 U.S. 347, 350–51 (1967) (defining a search for Fourth Amendment purposes).

133. *Terry v. Ohio*, 392 U.S. 1, 20 (1968) (allowing for a stop and frisk of a suspect based on reasonable suspicion rather than probable cause). The Court later drew a bright line in deciding that a person is in custody and police conduct is beyond the scope of a Terry Stop when police place a suspect in a police car and drive him to the station without probable cause. See *Dunaway v. New York*, 442 U.S. 200, 212–13 (1979).

Amendment violation. The Supreme Court in cases such as *Whren v. United States*,<sup>134</sup> *Atwater v. City of Lago Vista*,<sup>135</sup> and *Horton v. California*<sup>136</sup> involved questionable police motivations tantamount to bad faith, but the Court held that the subjective intent of the officer is not dispositive for Fourth Amendment purposes.<sup>137</sup> The same Court, however, in cases such as *Maryland v. Garrison*<sup>138</sup> and *United States v. Leon*,<sup>139</sup> allowed for the good faith of the officer to come into consideration when a defendant seeks to exclude the evidence based on a constitutional violation.<sup>140</sup> In the main, Fourth Amendment jurisprudence has been in flux.<sup>141</sup> The cases are inconsistent in balancing the need to search or seize against the privacy or possessory invasion the search or seizure entails. The outcome is the establishment of a balancing test often difficult to implement and more frequently construed against individual privacy interests.<sup>142</sup>

In similar fashion, China's effort to balance individual privacy rights and governmental intrusions is a challenge. In actuality, the challenge occurs worldwide within nations.<sup>143</sup> A cursory and one-dimensional

134. *Whren v. United States*, 517 U.S. 806, 813 (1996) (holding, in part, that the actual motivations of the officer are irrelevant to the inquiry of constitutional reasonableness).

135. *Atwater v. City of Lago Vista*, 532 U.S. 318, 360 (2001) (O'Connor, J., dissenting) (arguing that arresting the defendant for minor traffic offense constituted a "pointless indignity").

136. *Horton v. California*, 496 U.S. 128, 130, 138 (1990) (eliminating the Fourth Amendment inadvertence requirement and stating that the subjective state of mind of the officer is irrelevant and that police officers are presumed to not lie).

137. The one notable exception to the general rule that the officer's subjective intent is irrelevant is in the area of police inventory searches. Such searches are beyond the warrant exception if conducted for the purpose of gathering criminal evidence. See *Colorado v. Bertine*, 479 U.S. 367, 372–73 (1987). See also *Florida v. J.L.*, 529 U.S. 266, 271 (2000) (in which the Court considered the officers' conduct as somewhat dishonest).

138. *Maryland v. Garrison*, 480 U.S. 79, 87–88 (1987) (allowing for the subjective good faith of the officer when a warrant is either issued or executed improperly).

139. *United States v. Leon*, 468 U.S. 897, 920–22 (1984) (establishing the good faith exception to the exclusionary rule).

140. For an excellent discussion on the contradiction of considering police good faith and ignoring police bad faith, see MACLIN TRACEY, *United States v. Whren: The Fourth Amendment Problem with Pretextual Traffic Stops*, in *WE DISSENT TALKING BACK TO THE REHNQUIST COURT* 90 (Michael Avery ed., 2009). Beyond the Fourth Amendment, the Court has limited good faith in the context of Fifth Amendment Miranda warnings. See *Brown v. Illinois*, 422 U.S. 590, 601 (1975) (holding that an arrest without probable cause, which produces a confession, fails the attenuation test simply because the individual was Mirandized).

141. *Saleem*, *supra* note 47, at 147 (discussing the historical parallels between Physics and Fourth Amendment jurisprudence and how both fields are currently at a crossroad).

142. See ELLEN ALDERMAN & CAROLINE KENNEDY, *THE RIGHT TO PRIVACY*, at xiii (1995).

143. Islamic countries such as Singapore, Iran, Kuwait, Tunisia, and Saudi Arabia also restrict blogger content and criminally punish improper blogger statements. See HART, *supra* note 104, at 57 (citing *Singapore Blogger Convicted for Racist Posting*, BANGKOK POST, Oct. 27, 2005); see also Richard Winfield & Kristin Mendoza, *Does China Hope to Remap the*

view of China's Internet-pyramid paradigm and censorship practices would possibly lead to the inference that privacy rights are nonexistent in China. Culturally, China has recognized a substantive right to privacy traced back to ancient China.<sup>144</sup> In addition, the contemporary Chinese Constitution provides for freedom of speech (article 35), freedom of religion (article 36), freedom of person (article 37), freedom from insult (article 38), freedom of the home (article 39), and privacy (article 40).<sup>145</sup> China, dissimilar to the United States, has the word "privacy" in its Constitution.<sup>146</sup> Article 40 for privacy of correspondence provides:

No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of State security or of investigation into criminal offenses, public security of procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law.<sup>147</sup>

China's Constitution clearly specifies that there is a constitutional right to privacy in China, although that right is not absolute. After its adoption, and between 1982 and 2000, China's Constitution has been amended four times to accord human rights, due process, and an impartial legal system.<sup>148</sup> Similar to constitutional rights in the United States, an individual's privacy rights in China are balanced against governmental interests.<sup>149</sup> In China, the interests balanced against an

---

*Internet in Its Own Image?*, 2 J. INT'L MEDIA & ENT. L. 85, 94 (2008) (indicating that countries throughout Asia, the Middle East, and Africa filter the Internet using U.S.-made technology).

144. See generally *An International Survey of Privacy Laws and Practice*, GLOBAL INTERNET LIBERTY CAMPAIGN, <http://www.gilc.org/privacy/survey/intro.html> (last visited Sept. 21, 2012).

145. See XIANFA arts. 35–40 (1982) (China), translated at <http://english.people.com.cn/constitution/constitution.html>.

146. See ALDERMAN & KENNEDY, *supra* note 142, at xiii (stating, "The word 'privacy' does not appear in the United States Constitution."). In the United States, privacy is more wide-ranging and has roots in common law, constitutional interpretation, statutes and international law. See DANIEL J. SOLOVE & MARC ROTENBERG, *INFORMATION PRIVACY LAW 2* (2006); see also ROBERT ELLIS SMITH, *COMPILATION OF STATE AND FEDERAL PRIVACY LAW*, at xii (1998) (describing U.S. state and federal privacy laws).

147. XIANFA art. 40.

148. See Mark Moedritzer et al., *Judgments 'Made in China' but Enforceable in the United States?: Obtaining Recognition and Enforcement in the United States of Monetary Judgments Entered in China Against U.S. Companies Doing Business Abroad*, 44 INT'L LAW. 817, 823 (2010).

149. See *Camara v. Mun. Court*, 387 U.S. 523, 536–37 (1967) (stating that "[T]here can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails. . . ."); see also Russell L. Weaver, *The Internet, Free Speech, and Criminal Law: Is it Time for a New International Treaty on the Internet?*, 44 TEX. TECH L.R. 197, 200 (2011) (indicating that constitutional rights, such as the right to expression,

individual's privacy right are enumerated in article 40 and include "needs of State security or of investigation into criminal offenses, [and] public security of procuratorial organs. . . ." <sup>150</sup> The Chinese government has emphatically stated it has a legitimate interest in quashing dissidents, maintaining social order, and screening information that is politically harmful to the state. <sup>151</sup> Privacy *vis-à-vis* state security is demonstrated in a popular case arising out of the 1989 Tiananmen Square protest.

Political activist Huang Qi published information about the 1989 Tiananmen Square crackdown on his web site, and the Chinese government charged him with "subverting state power" and he faced a sentence of life imprisonment. <sup>152</sup> The Chinese government indicated that although the Internet has healthy and beneficial information, it also contains information that is reactionary, superstitious, and pornographic. <sup>153</sup> The government vowed to battle the "enemies of the state" who use the Internet to undermine the state, and promulgated regulations restricting the "transfer of state secrets on bulletin board systems, in chat rooms or through Internet news groups." <sup>154</sup> The rationale is that social control through a Communist dictatorship is the key towards a successful democracy. <sup>155</sup> The Chinese government's position complies with the WSIS recognition that the global information society should be in conformity with the domestic laws of each country and that a country has legitimate reason to combat cyber-security, cybercrime, and to perpetuate social development and national laws.

China is a rather unique country due to its population, and the harsh reality is that individual rights may yield to overall social harmony. With a population of 1.295 billion people in 2000, and growing, China has particular concerns distinct from U.S. concerns. <sup>156</sup> The Beijing-

are not absolute in any country) (internal citations omitted).

150. XIANFA art. 40.

151. See generally Steven Schwankert & Jonathan S. Landreth, *China Tightens Control Over Web Site Publishing*, VIRTUAL CHINA, <http://www.virtualchina.com/news/jan00/0128/012800-regulation2-ss-jsl1.html> (noting that laws promulgated in China balance individual rights against the state's interests).

152. See *China Says Provinces Setting Up Internet Police*, REUTERS, Aug. 6, 2000, available at <http://archives.cnn.com/2000/ASIANOW/east/08/05/internet.china.reut/>.

153. See *China Vows to Battle "Enemy Forces" on Internet*, REUTERS, Aug. 9, 2000, available at <http://www.insidechina.com/news.php3?id=187292>.

154. Schwankert & Landreth, *supra* note 151.

155. CHIH-YU SHIH, *COLLECTIVE DEMOCRACY: POLITICAL AND LEGAL REFORM IN CHINA* 59 (1999).

156. Li Li, *Charting Population Shifts China's Once-In-A-Decade Census Will Release Information Essential For Making Policies*, BEIJING REV., Nov. 18, 2010, at 22–23, available at [http://www.bjreview.com.cn/nation/txt/2010-11/15/content\\_312127.htm#](http://www.bjreview.com.cn/nation/txt/2010-11/15/content_312127.htm#) (providing the following population growth data in China in 1963, 580 million; in 1964, 690 million; in 1982, 1.03 billion; in 1990, 1.13 billion).



based web-browser Maxathon (which means maximum), depicts an example of China's exponential population growth. In 2009, Maxathon was among the world's largest Internet browsers after Internet Explorer, Firefox, Safari, and Google.<sup>157</sup> With such a massive population and such high Internet usage, China will continue its practice of monitoring. Even before the Internet and its population growth, China has monitored its citizens. In fact, China's monitoring of citizens dates back to the 4th century B.C.<sup>158</sup> while its huge population dates back to 1600 A.D.<sup>159</sup> Consequently, the American concept of self is rooted in individualism, while the concept of self in Chinese tradition places a higher value on group cooperation.<sup>160</sup> A well-known Chinese expression is "He' wi'e gui," which translates into "harmony is priority." This expression reflects the reality that, culturally, China prefers stability over revolution.<sup>161</sup>

When viewed with the WSIS as a backdrop, China's domestic policy of "cyber-snooping" comports with WSIS standards. Network security is inextricably linked to state security due to the prevalence of economic transactions on the Internet and the terrorist and other criminal threats to those transactions. In fact, China's enormous economic growth since 1970 has precipitated threats to state security such as massive illicit economies and organized crime.<sup>162</sup> Under the rationale of state security,

157. Tang Yuankai, *Browsing to the Max: A Beijing-Based Web Browser is Gaining Global Market Share*, BEIJING REV., Dec. 10, 2009, at 42, available at [http://www.bjreview.com.cn/e-mail/2009-12/07/content\\_233544.htm](http://www.bjreview.com.cn/e-mail/2009-12/07/content_233544.htm).

158. W.J.F. Jenner, *China and Freedom*, in ASIAN FREEDOMS: THE IDEA OF FREEDOM IN EAST AND SOUTHEAST ASIA 65, 75–76 (David Kelly & Anthony Reid eds., 1998).

159. See JONATHAN D. SPENCE, *THE SEARCH FOR MODERN CHINA* 7 (2d ed. 1999).

In the year A.D. 1600, the empire of China was the largest . . . of all the unified realms on earth. The extent of its territorial domains was unparalleled at a time when Russia was only just beginning to coalesce as a country, India was fragmented . . . and a grim combination of infectious disease and Spanish conquerors had laid low . . . the empires of Mexico and Peru. And China's population of some 120 million was far larger than that of all the European countries combined.

*Id.*

160. See *Some General Differences Between Chinese and American Cultures*, PRE-DEPARTURE ORIENTATION FOR CHINESE STUDENTS, <http://china-nafsa.aief-usa.org/culture/differences.htm> (last visited Sept. 27, 2012).

161. *Dear President*, WIRED 160, 163 (Oct. 2008), available at [http://www.wired.com/politics/law/magazine/16-10/sl\\_intro](http://www.wired.com/politics/law/magazine/16-10/sl_intro).

162. Vanda Felbab-Brown, *The Political Economy of Illegal Domains in India and China*, 43 INT'L LAW. 1411, 1415–20 (2009); see also Peter K. Yu, *Enforcement, Economics and Estimates* 6 (Drake Univ. Law Sch. Research Paper No. 11-27, 2010), available at <http://ssrn.com/abstract=1711184> (stating that China is an ideal environment for pirates and counterfeiters because, globally, China makes 70% of the world's toys, half its shoes, a third of its luggage,

China would be in compliance with the WSIS in enforcing government snooping, site blockage, eradication of spam, and restrictions on foreign encryption technology by corporations.

In addition, China's government surveillance has also been linked to micro-blogs, in which the government regulations require users to register using their real names and personal information.<sup>163</sup> Arguably, such regulations threaten free speech, yet, were proper under the WSIS when designed—from the China governmental policy perspective—to halt the plague of harmful rumors, which damage both individual and public rights and interests.<sup>164</sup> The required real name and personal information registration for micro-blogs by the Chinese government fosters what China would term a “responsible” Internet. Thus the right of anonymity is inextricably bound to coordinate concerns of individual autonomy and accountability.<sup>165</sup> In zealous fashion, China imposes Ann Wells Branscomb's paradigm by embracing the strong position that persons should be responsible for Internet communications.

Ann Wells Branscomb defines anonymity as the point where “no one could trace the source of an electronic message.”<sup>166</sup> She linked privacy law to autonomy, which she defined as “the right to exert some modicum of control over one's electronic environment.”<sup>167</sup> She further stated, “Accountability refers to the acceptance of responsibility for one's actions.”<sup>168</sup> In her paradigm, Branscomb seeks to effectuate a balance between Internet-based communications and responsible social behavior on the Internet. She essentially posits that there is a need for guiding principles and ethical standards. She would essentially advocate for rules governing Internet communications. Her approach of regulating speech, however, sparks criticism. With the backdrop of a multi-cultural society, the United States has historically grappled with the right to free speech versus the right of the victim of such speech.<sup>169</sup> An ample retort is that although one person may have the desire to

---

half of its microwave ovens, a third of its TVs and air conditioners, a quarter of its washers, a fifth of its refrigerators).

163. See Kristen Farrell, *The Big Mamas are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression*, 15 MICH. ST. J. INT'L L. 577, 584–88 (2007) (discussing how China censors and requires customer's personal information).

164. Shigong, *supra* note 117.

165. See Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE. L.J. 1639, 1641–45 (1995) (examining the conflicts and questions the First Amendment provokes in cyberspace).

166. *Id.* at 1641.

167. *Id.* at 1644.

168. *Id.* at 1645.

169. See JEANNINE BELL, *POLICING HATRED: LAW ENFORCEMENT, CIVIL RIGHTS AND HATE CRIME* 19 (2004) (arguing that the Supreme Court has taken the position that the state may punish discriminatory conduct, but not solely punish hate speech).

communicate anonymously, that same person may have to accept responsibility for certain actions to facilitate a true democracy.<sup>170</sup> As eloquently stated, by Richard Delgado, “words do cause harm.”<sup>171</sup> Where morals and advocacy fail codification of law may be appropriate.<sup>172</sup>

China’s regulations structured to protect individual and public interests comply with the WSIS Declaration. Globally, Internet surveillance has become a means of warfare to preserve the state.<sup>173</sup> China’s position was amply depicted by Jichuan Wu, head of the Ministry of Information Industry (MII), who once remarked there is no conflict between Internet access for Chinese citizens and censorship.<sup>174</sup> His view is in direct opposition to the U.S. perspective espoused by Justice Potter Stewart, dissenting in *Ginzburg v. United States*, in which he stated, “[c]ensorship reflects a society’s lack of confidence in itself. It is a hallmark of an authoritarian regime. . . .”<sup>175</sup>

The U.S. cases dealing with Internet speech have sought to encourage free speech on the Internet despite the harm to individual interests. In 1991, the U.S. District Court for the Southern District of New York decided in *Cubby, Inc. v. CompuServe, Inc.* that an ISP lacked liability for hosting defamatory content on one of its forums because ISPs are distributors rather than publishers of information.<sup>176</sup> Furthermore, CompuServe, as an ISP, did not know or have reason to know of the defamatory content.<sup>177</sup>

In 1995, the New York Supreme Court held in *Stratton Oakmont*,

170. In a true democracy, governments must regulate behavior. See Robert Post, *Racist Speech, Democracy, and the First Amendment*, 32 WM. & MARY L. REV. 267 (1991), reprinted in HENRY LOUIS GATES ET AL., *SPEAKING OF RACE, SPEAKING OF SEX: HATE SPEECH, CIVIL RIGHTS, AND CIVIL LIBERTIES* 115 (1994).

171. RICHARD DELGADO & JEAN STEFANCIC, *UNDERSTANDING WORDS THAT WOUND* (2004); see also LAURA J. LEDERER & RICHARD DELGADO, *THE PRICE WE PAY* 4–5 (1995) (stating that physical wounds can harm, but psychological wounds are lifelong).

172. See JON B. GOULD, *SPEAK NO EVIL: THE TRIUMPH OF HATE SPEECH REGULATION* 66–67 (2005) (providing a sphere of formal law and social pressure which encompasses moral views, contact zones representing advocacy in a free society, and codified law).

173. See generally FRANK WEBSTER, *THEORIES OF INFORMATION SOCIETY* 52–73 (1995).

174. Compare ROBERT BURDERI & GREGORY T. HUANG, *GUANXI (THE ART OF RELATIONSHIPS) MICROSOFT, CHINA, AND BILL GATE’S PLAN TO WIN THE ROAD AHEAD* 57 (2006), with S. David Cooper, *The Dot.Com(munist) Revolution: Will the Internet Bring Democracy to China?*, 18 UCLA PAC. BASIN L.J. 98, 108 (2000) (arguing that censorship of the Internet will cause the fall of China’s communist system), and John H. Taylor, *The Internet in China: Embarking on the “Information Superhighway” With One Hand on the Wheel and the Other on the Plug*, 15 DICK. J. INT’L L. 621, 639–40 (1997) (predicting the exchange of ideas among students on the Internet will circumvent China’s governmental controls over the Internet).

175. *Ginzburg v. United States*, 383 U.S. 463, 498 (1966) (Potter, J., dissenting).

176. *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991).

177. *Id.*

*Inc. v. Prodigy Services Co.*, that an ISP was liable for defamatory speech on its bulletin board by an unidentified user.<sup>178</sup> In *Stratton*, the court decided the ISP was a publisher because it exercised editorial control over the content of its bulletin board messages via guidelines, enforcement of those guidelines, and the removal of offensive language.<sup>179</sup> The *Stratton* case proved to be an aberration. In response to ISP liability under *Stratton*, Congress promptly enacted the 1996 Communication Decency Act (CDA) to address ISP liability.<sup>180</sup> The CDA effectively overruled *Stratton* and eliminated ISP liability. The findings and policies behind the CDA were to foster a free Internet, true diversity of political discourse, minimize government regulation, promote the development of the Internet, maximize user control, remove user disincentives, and ensure enforcement of federal criminal law.<sup>181</sup>

The CDA's practical application was enforced a couple of years after *Stratton* in *Zeran v. America Online, Inc.*<sup>182</sup> In *Zeran*, an anonymous message was posted six days after the 1995 Oklahoma City bombing.<sup>183</sup> *Zeran* had nothing to do with the bulletin board posting.<sup>184</sup> The message advertised items, which glorified the bombing and encouraged interested persons to contact *Zeran*.<sup>185</sup> His home phone number was posted on the message bulletin board.<sup>186</sup> *Zeran* contacted his ISP, which was AOL, and asked that AOL remove the posting, with which AOL complied.<sup>187</sup> The content reemerged and *Zeran* again asked for its removal, and again the AOL complied.<sup>188</sup> A radio announcer read the message on an Oklahoma radio station and encouraged listeners to call the telephone number.<sup>189</sup> At that time, *Zeran* received threatening phone calls approximately every two minutes.<sup>190</sup> *Zeran* sued the ISP and the radio station for the defamatory remarks.<sup>191</sup> The Court held that *Zeran*

178. *Stratton Oakmont, Inc., v. Prodigy Servs. Co.*, 1995 WL 323710, at \*4 (N.Y. Sup. May 25, 1995), *superseded by statute as stated in* *Shiamili v. Real Estate Grp. of N.Y., Inc.*, 929 N.Y.S.2d 19 (N.Y. 2011).

179. *Stratton Oakmont*, 1995 WL 323710, at \*4.

180. Communications Decency Act of 1996, 47 U.S.C. § 230 (2012).

181. *Id.* § 230(b).

182. *Zeran v. Am. Online, Inc.* 129 F.3d 327, 330 (4th Cir. 1997) (holding section 230 of the CDA provides immunity for ISPs from any information generated by a third party); *see also* *Blumenthal v. Drudge*, 992 F. Supp. 44, 49–50 (D.D.C. 1998).

183. *Zeran*, 129 F.3d at 329.

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.*

191. *Id.*

was barred because the CDA provides ISPs with virtually absolute immunity.<sup>192</sup>

The U.S. position of a free-Internet lacking ISP liability is contrary to China's position. In China, democracy is based on Communist dictatorship. The United States would be remiss to embrace the position that western democratic ideas will prevail in the Asian political governing structures.<sup>193</sup> Contrary to the U.S. position of absolute immunity for ISPs and a lack of recourse for the victim, as in the *Zeran* decision, China takes a different approach towards ISP liability. China controls the Internet to prevent confusion, regulate content, protect national security, and promote economic growth.<sup>194</sup> China holds ISPs responsible for their wrongful conduct.<sup>195</sup> The measures China enacted related to content were designed to do the following: protect the Constitution; avoid threats to national security, prevent divulgence of state secrets, quash subversive conduct; honor state interests; prohibit hatred, race discrimination, and damage to unity among nationalities; foster the state's religious policies and restrict evil cults or feudal superstitions; protect against rumors and disruption to social order or social stability; and prohibit obscenity, pornography, gambling, violence, murder, or other criminal activities.<sup>196</sup> Viewed as a cultural difference, the U.S. approach of individualism is contrary to the Chinese approach of community interdependence and responsibility.<sup>197</sup> The WSIS standards are not in conflict with ISP liability because such liability protects individual rights, fosters economic development, and allows for the exercise of sovereign rights.

China's form of government falls short of atypical. Many Asian systems of government have been entrenched in cultural values inextricably bound to economic and political developments and assertive leadership.<sup>198</sup> Charismatic and assertive leaders, for example,

---

192. *Id.* at 335. Section 230 has provided immunity for more than ISPs. The immunity has extended to blogs, online forums, auction sites, parties forwarding defamatory emails, publishers, and entities that edited user reviews. See Catherine R. Gellis, 2011 *State of the Law Regarding Website Owner Liability for User-Generated Content*, 67 *BUS. LAW.* 305, 306–09 (Nov. 2011).

193. Jose E. Alvarez, *Contemporary Foreign Investment Law: An "Empire of Law" or the "Law of Empire?"*, 60 *ALA. L. REV.* 943, 947 (2009).

194. Hong Xue, *The Voice of China: A Story of Chinese Character Domain Names*, 12 *CARDOZO J. INT'L & COMP. L.* 559, 575–82 (2004).

195. See John V. Grobowski & Yiquiang Li, *Tort Liability Law of the People's Republic of China*, MARTINDALE.COM (Feb. 1, 2010), [http://www.martindale.com/government-law/article\\_Faegre-Benson-LLP\\_916960.htm](http://www.martindale.com/government-law/article_Faegre-Benson-LLP_916960.htm).

196. Xue, *supra* note 194, at 578–79.

197. See JOHN W. HEAD, *CHINA'S LEGAL SOUL: THE MODERN CHINESE LEGAL IDENTITY IN HISTORICAL CONTEXT* 104 (2009) (exploring how China filters external influences).

198. See ADEL SAFTY, *LEADERSHIP AND DEMOCRACY* 228 (2004) (discussing the correlation between Asian values and democracy).

have dominated contemporary politics in certain Asian systems with leaders who have exercised centralized power with supreme authority. Such notable leaders include: Chiang Kai-shek (Taiwan), Mao Tse-tung (China), Kim Il Sung (North Korea), Chi Minh (Vietnam), Lee Kuan (Singapore), Norodom Sihanouk (Cambodia), Ferdinand Marcos (Phillipines), Jawaharlal Nehru and Indira Gandhi (India), Ne Win (Burma), and Sukarno (Indonesia).<sup>199</sup> In the main, there is a tendency in Asia to embrace a concept of democracy based on harmony and cooperation rather than the western model of democracy based on individualism, competition, and confrontation.<sup>200</sup> Cultural or traditional values, mutual aid, harmony, cooperation, centralized and strong government, and charismatic leadership better defines Asian politics more than the individualism and individual rights advocated in the United States.

Global democracy, as a result has a distinct sinicism in the new millennium. Perhaps China's economic and political perspective is amply articulated by the statement by Deng Xiaoping: "Black cat, white cat, all that matters is that it catches mice."<sup>201</sup> Ideology is unimportant, all that matters is China's economic growth. China's intent to raise the living standards of its citizens was articulated by former President Deng Xiaoping's statement in the early 1990s when he stated, "To get rich is glorious."<sup>202</sup> The WSIS participants stressed economic growth, fair competition, investment opportunities, property protection, transparency, democracy, fundamental values, and freedom of

199. *Id.*

200. *Id.* at 230; see also B.V. RAO, HISTORY OF ASIA FROM EARLY TIMES TO THE PRESENT (2005) (outlining the Asia's subversion of democracy). In addition, Asian economic interdependence impacts the Asian political climate. See Robert Sutter, *Asia in the Balance: America and China's "Peaceful Rise,"* in CHINA CONTEMPORARY POLITICAL, ECONOMIC, AND INTERNATIONAL AFFAIRS 72-73 (2007).

201. THOMAS FRIEDMAN, HOT, FLAT, AND CROWDED 344 (2008). In the spirit of fostering economic growth, China has invested heavily worldwide, surpassing Japan's economy, and it is in contention with the United States to become the largest economy in the world. See Lutz-Christian Wolff, *Chinese Investments Overseas: Onshore Rules and Offshore Risk*, 45 INT'L LAW. 1029, 1030-32 (2011).

202. TIM CLISSOLD, MR. CHINA 25 (2005) (describing the trials and tribulations of conducting business in China). In China, the conception of law is different from the U.S. conception of law. As one author noted, in Western societies, "The law protects the rights of citizens and permits those citizens to shape their conduct in the knowledge that the law will be applied fairly, consistently and predictably. However, . . . in China, law follows policy rather than having an independent status." James Hugo Friend, *The Rocky Road Toward the Rule of Law in China: 1979-2000*, 20 N.W. J. INT'L L. & BUS. 369, 373 (2000). Professor Ronald Dworkin has stated that while western nations focus on individual rights, Asian nations focus on the economic and social needs of its citizens. See Charles Li, *Internet Control in China*, 8 INT'L J. COMM. L. & POL'Y 1, 10 (2004) (referencing Dworkin's remarks made after human rights lectures in China).

expression.<sup>203</sup> However, they further specified that “governments should intervene to correct market failures, to maintain fair competition, to attract investment, to enhance the development of the ICT infrastructure and applications, *to maximize economic and social benefits, and to serve national priorities.*”<sup>204</sup> Underpinning this lofty language is a focus on economic and social benefits and national priorities.<sup>205</sup> The Chinese government has a legitimate claim within the WSIS that their unique form of democratic-dictatorship is necessary to maximize economic and social benefits, maintain social harmony, foster economic progress, and secure a national priority of social stability. China’s focus on social harmony and economic prosperity has legitimacy. Furthermore, China’s democratic-dictatorship is in agreement the WSIS Summit’s participants’ emphasis that ICTs must comply with principles of legality, national laws and regulation, and relevant international agreements for the benefit of their populations and the preservation of cultural identities and cultural heritage.<sup>206</sup>

The corollaries of a democratic dictatorship are the aspects of culture, written language, philosophy, and tradition. Concerning written language, it has been proposed, “[b]ecause each Chinese ideograph carries from its cultural past its own distinct connotations . . . the Chinese script proved a major barrier to . . . foreign ideas and values in the Chinese culture.”<sup>207</sup> In effect, foreign ideas such as “western democracy” could only reach the Chinese through cultural filters. Such filters are culturally strong as depicted in China’s view that economic prosperity is possible without accepting democratic substantive processes.<sup>208</sup> Clearly, the United States and China differ in approach. However, the world community through the WSIS in both Geneva and Tunis deem that both the United States and China are correct in the realm of Internet governance.

---

203. *Draft Declaration*, *supra* note 63.

204. *See id.* (emphasis added).

205. China’s tremendous post-colonial efforts and economic growth is both intense and expansive. China has perpetuated a “no strings attached” approach as it deepens its economic ties with African countries such as Chad, Angola, Nigeria, Ivory Coast, Congo and Guinea. *See generally* Howard W. French & Lydia Polgreen, *China, Filling a Void, Drills for Riches in Chad*, N.Y. TIMES, Aug. 13, 2007, at A1, A9.

206. *See Draft Declaration*, *supra* note 63.

207. JOHN W. HEAD & YANPING WANG, *LAW CODES ON DYNASTIC CHINA* 83 (2005).

208. *See* WILL HUTTON, *THE WRITING ON THE WALL* 214 (2006) (arguing that China would wrong to embrace such an assumption).