Telecommunications Policy 35 (2011) 603–616

Contents lists available at ScienceDirect

Telecommunications Policy

URL: www.elsevierbusinessandmanagement.com/locate/telpol

A comparative study of online privacy regulations in the U.S. and China

Yanfang Wu [a], Tuenyu Lau [b], David J. Atkin [c,*], Carolyn A. Lin [d]

[a] Culture and Communication School, Beijing Central University of Finance and Economics, Beijing, China
[b] U.S.–China Institute, University of Southern California, 3535 South Figueroa Street, Los Angeles, CA 90089, USA
[c] Dept. of Communication Sciences, 850 Bolton Rd, Unit 85, University of Connecticut, Storrs, CT 06268, USA
[d] Graduate School and Dept. of Communication Sciences, University of Connecticut, Storrs, CT, USA

ARTICLE INFO

Available online 22 June 2011

Keywords:
Internet
Privacy
China
United States

ABSTRACT

Online privacy seeks to protect the identity of individuals who use the internet to collect information or express opinions. However, given the proliferating vehicles through which one's identity can be ascertained, the question remains as to what policies can most effectively protect personal identity. This paper explores the similarities and differences with online privacy regulation in the United States and China. The scope of privacy measures examined here ranges from government to personal levels, from communication and finance to personal records, for adults and children. As might be expected in a democracy, American legislative initiatives are more comprehensive and far-reaching than those of their Chinese counterparts. In China, there was until recently no specific right of privacy specified in dedicated legislation, with privacy having been instead protected under the right of reputation in the Civil law. Policy implications stemming from these competing models are evaluated. Study findings underscore the notion that privacy should be a universally established individual right, and that both countries are moving—at least in rhetorical terms—to strengthen it as such.

1. Introduction

The notion of online privacy encompasses measures that can be taken, over time, to protect the identity of individuals using the internet to collect information or express opinions. In an ideal online world, of course, users can choose not to reveal their identities (Allen, 2001). However, given the rise of technologies that enable the detection of a user's identity, policymakers are grappling with issues concerning the protection of personal privacy. The stakes in this ongoing policy debate are high, given the growth of global e-commerce, telecommuting and other economic engines powering the global information economy (Rogers, 2002; Delbert, Palfrey, Rohozinski, & Zittrain, 2008, 2010).

China's mandate that all computers sold after July 1, 2009 include the "Green Dam" filter—a software patch that could also be used to monitor a user's online movements—generated a public furor that prompted the government to delay its implementation (Watts & Branigan, 2009). That same month in the U.S., the *New York Times* reported that Amazon "conveyed a publishers change-of-heart to owners of its Kindle e-book reader: some purchasers of Orwell's *1984* found it removed from their devices, with nothing to show for their purchase other than a refund" (Zittrain, 2009, p. 1).

* Corresponding author. Tel.: +1 960 486 3090; fax: +1 860 486 5422.
E-mail addresses: y_f_wu@yahoo.com (Y. Wu), tylau@stanfordalumni.org (T. Lau), david.atkin@uconn.edu (D.J. Atkin), carolyn.lin@uconn.edu (C.A. Lin).

0308-5961/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.telpol.2011.05.002

These examples underscore a growing concern over the kinds of privacy issues that captivated Orwell, and which now confront governments across the globe. Given that America's libertarian press traditions provide a clear contrast to China's paternalistic approach, it's useful to explore the similarities and differences in online privacy regulation between the two economic superpowers. As emerging online channels spur global electronic commerce—based on converging technical standards—a fuller appreciation of these differences can help policymakers better understand prospects for developing a universally established individual right to privacy.

2. Online privacy defined

Conceptions of online privacy flow from those established in conjunction with traditional media over the past two centuries. The seminal treatise on privacy is Warren and Brandeis' (1890) law review essay entitled The Right to Privacy. At that time, the authors noted the need to "protect the privacy of private life" (Warren & Brandeis, 1890, p. 215) in response to the diffusion of newspapers and high-speed cameras. Such innovations were seen to penetrate the "the sacred precincts of private and domestic life" (Warren & Brandeis, 1890, p. 195).

Although dimensions of privacy have been debated for generations, theorists offer widely varying conceptual definitions. Margulis (1977, 2003) emphasizes variegated dimensions relating to privacy in attitudinal, behavioral and process terms, noting that "Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (Margulis, 1977, p. 10).[1] As these various and several definitions suggest, privacy interests and rights are undergoing considerable change in the modern era.

In particular, modern communications such as instant messaging, e-mails, and blogs bring new perspectives to privacy, helping to define a new realm of online privacy. Lee's (2007) conceptualization of privacy in the context of online or Internet communications encompasses the notion of intrusion, or an interest in controlling Internet access to one's self in order to maintain solitude. Unwanted intrusions might entail artifacts including spam, pop-ups, junk (unsolicited) faxes, and viruses. Such conceptions consider surveillance as a distinct category relative to Internet privacy concerns, given the capabilities of the Internet to monitor and track users (Lee, 2000). This differs from other telematic violations of personal solitude, such as a ringing telephone (Lee & LaRose, 1994).

As noted by Zittrain (2008), personal information theft or misuse lies at the core of online privacy, given that information represents an increasingly valuable commodity that is now being collected, cataloged, and traded in ways never before envisaged. The modern right to privacy thus also entails the right to control personal information even after it has been disclosed to others (e.g., Margulis, 2003; NOCPA, 2007). Given the increased ability for computers to collect, assemble, and distribute personal information, several scholars (DeCew, 1997; Lee, 2000, 2007; Lin & Atkin, 2007) now consider information privacy as the primary privacy concern.[2]

Despite the ongoing evolution of privacy embodied in law over the years, the concept has yet to enjoy any explicit constitutional protection in the U.S. (Margulis, 1977, 2003). Jurists invoke instead such provisions as the Fourth Amendment, which forbids unwarranted government searches and seizures. The courts consider such factors as "whether one has a reasonable expectation of privacy in the case of government infringements" (Lee, 2007, p. 259). As she and other commentators suggest, the lack of constitutional clarity here ensures a continual evolution in legal statutes and perpetual debates concerning digital information privacy.

3. Current online technology use trends

Under authoritarian political systems such as the China's one, media content is highly censored (Anokwa, Lin, & Salwen, 2003; Delbert et al., 2008, 2010). Yet, as Bill Gates (2000, p. 1) famously observed, "(t)he Internet is a constantly changing global network that knows no borders." The Internet thus presents an intriguing case where Western-inspired open media flows collide with more restrictive authoritarian information management practices, one where user privacy represents a key battleground.

According to East-West Connect (2010), some 384 million Chinese (or nearly 30% of the population) uses the Internet, helping propel the country ahead of the United States' 211 million users (CNNIC, 2007). By 2011, China's online population was projected to be double that of the U.S., reaching some 420 million users (CNNIC, 2010). Within China's online

[1] Privacy definitions also vary across disciplines, as outlined in Lee's (2007, p. 259) overview:

"Psychologists and sociologists, for example, focus on such notions as intimacy and personal space (e.g., Derlega & Chaikin, 1977; Pedersen, 1979). Legal practitioners focus on privacy as a "right" against government interference (e.g., Gavison, 1980; Tribe, 1988; Warren and Brandeis, 1890). Communications scholars consider privacy in the context of interpersonal communications and relative to the changing dynamics posed by communications technologies (e.g., Burgoon, 1982)."

[2] Privacy dimensions flowing from control over information about oneself are also at the core of definitions offered by DeCew (1997) and Bonavia and Morton (1998). In a variation on this theme, Laufer and Wolfe (1977) classified such interests as *information management* in reference to a user's ability to control the disclosure of his or her personal information. Focusing on the Internet, Lee (2007, p. 264) places these privacy interests in the context of maintaining user autonomy—or control over information—"which becomes especially salient as data mining, collection, sharing, hacking, and theft become major threats."

population, 78.7% read news online, and 30.4% use online forums or bulletin board systems (BBSs). The 2010 Chinese user profile (East-West Connect, 2010) also revealed that

- the number of online shoppers in China reached 108 million, pushing the total value of online shopping transactions to 250 billion Yuan (roughly $36.5 billion USD), roughly double the 2008 levels;
- the number of social networking site users reached 176 million (or 46% of the domestic Internet users).[3]

At present, a user who enters their name in Google will likely find such personal information as their position, education background, address, email, etc. in nanoseconds. In addition, one's personal information can be disclosed by blogs, podcasts, social network sites, and the like. BBC Watchdog recently warned people not to upload personal information on Facebook, a popular social networking site, since hackers could open a bank account by combining the online personal information with that available from other sites. As Gibson (1995, p. 1) notes, "the internet is transnational. Cyberspace has no borders." Given the ongoing diffusion of telematics, personal data and privacy are under unprecedented threat globally.

Internet regulation, however, continues to lag far behind the technology itself. Research on online journalism and privacy also remains scarce, with the bulk of work focusing on such topics as e-commerce (Lin & Atkin, 2007). Since most online privacy complaints address personal information releases (e.g., DeCew, 1997; Zittrain, 2008), this comparative analysis focuses on personal information protection.

4. Current study

In recent years, advances in computer technology have made it possible for detailed information about people to be compiled and shared more easily and cost-effectively than ever before. Although these electronic facilities produce benefits for individual consumers and the larger society, particularly as personal information becomes more accessible, the accompanying affordances for data mining and electronic surveillance enable personal information to be processed and distributed easily and with little accountability (Green, 2001). Lee (2007, p. 272) maintains that the personal release of (and outsider access to) private information can be "imposed on individuals by various public, social and commercial institutions with or without prior negotiation or informed consent."

In China, the rapidly expanding Internet has made people's privacy increasingly less secure. One estimate suggests that 30,000 government censors monitor the content of blogs, chatrooms, e-mails, and web pages, contributing to a surveillance network known as *The Great Firewall of China* (Zittrain, 2008). These Internet enforcers facilitate the removal of anti-government postings, blogs, and international sites that are deemed to be unfavorable. This governmental "raised eyebrow" presents privacy concerns, even prompting users to engage in self-censorship in all manner of online communication.

According to a survey by *China Youth Daily*, more than 55% of interviewees believe it is becoming harder to protect privacy; some 29.3% of interviewees report that their personal information has been randomly released, while 15.1% revealed they were under digital surveillance in their offices (Survey reveals, 2002). A survey by Oriental Horizon, CCTV in April 2005, suggests that 74% of respondents have experienced personal information exposure. Fully 90% of releases involve contact information such as telephone numbers and employment information. Some 42% of disclosure channels involve online registration, 25% are through job-hunting, 16% are from car, housing, or insurance purchases, and 10% can be traced back to hospital records.

Concerns over how this information is managed remain prominent in the U.S., where identity theft topped the list of respondent concerns for the 11th consecutive year in 2011, nearly half (42%) of the 516,740 complaints lodged in the FTC's Consumer Sentinel database centered on fraud and 214,905 involved identity theft reports (FTC, 2004). At the turn of the millennium, a study by the UCLA Center for Communication Policy found that 64% of Internet users "strongly agreed" or "agreed" that logging onto the Internet puts their privacy at risk (Ang, 2001).

In addition, Internet technology facilitates the process of news gathering, processing, and publishing. Evolving technologies such as digital video, cameras, and cell-phones allow more and more citizens who are interested in journalism to participate by posting or broadcasting on the web. The section to follow explores privacy implications stemming from the fact that, during this citizen–journalist era, any user can be the source of news.

5. Online modalities and privacy

According to a report from the Communication and Development Center of China Internet Association, the number of blogs all over the world surpassed 100,000,000 in 2005. The blogosphere is also developing rapidly in China, with the number of Chinese bloggers reaching 107,000,000 (see People, 2010). Several bloggers or posters fail to provide any

[3] In addition, Chinese internet users spend much more time online than with traditional media. According to a report by Eppanel, the Media contact rate for Chinese internet users is 48.4% for the internet, 24.2% for TV, 10.5% for newspapers, and 6.5% for radio (Epanel, 2007). These levels are approaching those found in the U.S., where 71% of American adults use the internet, while 72% of internet users report that they go to the internet to get news (PEW, 2007).

consideration to their subject's privacy. These emerging content providers may fulfill voyeuristic gratifications; they often do so, however, at the cost of violating a third party's privacy (Bucy, Gantz, & Wang., 2007).

In the U.S., YouTube is the most popular site for viewing online videos, sharing favorite videos with people, and commenting on favorite videos. Estimates suggest that over 100,000 videos are uploaded to YouTube.com every day (Lin & Atkin, 2007). Facebook, the leading online social network, recently surpassed the 500,000,000 user mark. Unlike traditional media, online posting sites, Blogs, Podcasts, and BBS do not experience filtering before publication. When a pair of students secretly webcast a gay sexual encounter online involving Tyler Clemente in 2010, they were prosecuted for violating his privacy after the Rutgers University freshmen committed suicide a few days later (Kaysen, 2011).

Another threat to privacy comes from the subscription-based business model. With the declining advertising profit margins in major media, an increasing number of news websites are turning to subscription-based business model. The *Wall Street Journal* represents a typical of subscription-based business. Increasingly, websites are requiring registration before a user can get the news, which can lead to more privacy violation cases in the online news field. The section to follow explores privacy implications stemming from these emerging Internet services.

6. Understanding forms of privacy violation by online content

The difference between online privacy and traditional privacy is that most of the online privacy cases involve disclosing important personal information. Online violations of privacy typically fall into the following categories.

6.1. Collecting personal information without notification

Websites may use tracking software such as cookies to track customers while they surf online. Cookies can track online user behavior to determine a user's navigation through the site such as the number of pages accessed and the time spent on individual pages (Whitman, 2001). Some of the most popular news sites utilize cookies, including the *New York Times* Online and CNN (Hong, 2005).

6.2. Profit by selling personal information

Websites can make a profit by selling personal information. Selling personal information is more harmful than illegal collection of information. The murder of Amy Boyer in 1999 is a typical case in point. In this case, the murderer stalked Amy Boyer in New Hampshire, obtaining her SSN from an internet-based investigation and information service for only $45.[4]

6.3. Personal information redevelopment

Although this collected personal information cannot be used for purposes beyond customer service without the registrant's permission, websites typically build databases for future use. While privacy advocates argue that the collection of such information constitutes a violation of one's privacy, the online industry contends that the collection of such information helps sites tailor information to each visitor and, thus, enhances the online experience (Hong, 2005).

7. Section summary

Policy implications stemming from online privacy violations have been most extensively researched in the West. The concept of privacy encompasses variegated facets: individual privacy regarding the integrity of the body; privacy regarding individual behavior; privacy regarding personal communication; and privacy regarding individual data. All of these areas of privacy are coming under increasing threat in the information age (Clarke, 1999; Zittrain, 2008). While privacy practices of e-commerce sites have been central to FTC investigations into online privacy practices, those of online media sites have received less scrutiny (Hong, 2005).

Uncertainty over privacy protection is even greater in China. Under her authoritarian press system, privacy was never well-protected in traditional media age, to say nothing of the new media arenas (Anowkwa et al., 2003). In general terms, then, online privacy enjoys only a modicum of legislative protection in China (e.g., Zittrain, 2009).

On balance, the definition and volume of privacy changes within particular media use contexts, although most of the studies addressing online privacy concerns tend to rely on offline literature reviews (Lee, 2007). Moor (1997) and Raab and Bennett (1998) propose moving the study of the nature of privacy, privacy risks, and privacy protection, from an adversarial paradigm towards a situational paradigm, especially in the context of the internet. These contextual factors are crucial to understanding nuances in privacy regulation in the new media environment, and further underscore the importance of comparative research that can account for differences in culture as well as social and legal systems.

[4] Consistent with longstanding traditions shielding common carriers from liability when acting as a third party content provider, the Fifth Circuit Court in *Doe v. MySpace* (528F. 3d 413 [5th Cir, 2008]) held that online service providers cannot be held liable for crimes committed by users. The court affirmed a lower court finding of MySpace's immunity, under the Communications Decency Act of 1996, from liability stemming from the sexual assault of a minor. This same logic may well shield online providers from liability when criminals make use of postings that are initiated or authorized by users.

The analytical model proposed here focuses on these issues, but concentrates on comparative perspectives between China and the U.S.

8. Analysis

The present study consulted used primary legal documents to research online privacy in China and the U.S. These traditional sources were supplemented by more timely online postings through such modalities as blogs and BBS's in order to better understand ongoing user policy concerns (e.g., an AOL user commented on August 6, 2006 at 6:18 pm, *Shame, Shame on AOL,* in his Pacificdave blog). Regulations were then reviewed from government agencies as well as self-regulatory charters. This second level of analysis helps inform the comparative analytical foundation, which is described in turn.

9. Conceptual framework

The proposed model explores interdependent relationships between the government, media institutions, and end-users to compare similarities and differences between the two countries. In the proposed framework, the government sets regulations and articulates agency guidelines underpinning the regulatory process. One key distinction is that the judiciary constitutes an independent entity in the U.S. while, in China, the courts are a subsidiary of the ruling government.

Krasnow, Longley, and Terry's (1982) seminal broadcast regulation model casts policymaking as a function of five key stakeholders in the U.S.: industry groups, citizen's groups, administrative authorities (e.g., the FCC), and major branches of government (the legislative, executive, and judicial branches). Accordingly, a given initiative (e.g., privacy safeguards) is not likely to be adopted as a formal policy until it enjoys the support of a majority of these stakeholders. The present model expands on this approach, consolidating representative government institutions (i.e., executive, administrative, and legislative branches) and tailoring citizen's and industry groups to suit the online environment. Consolidated under the rubric of institutional actors here, the interest group category can include coalitions favoring online privacy (e.g., the Electronic Frontiers Foundation) and scholars.

These stakeholders act ostensibly on the behalf of public end-users, a class that includes individual citizens who are affected and the general public (e.g., opinion polls on attitudes towards online privacy and citizens' rights). In Fig. 1, the three parties are mutually influenced and dependent on each other. Their mutual influences reach a triangular equilibrium balance, one that combines to produce online privacy regulations. The difference between the two diagrams is that in the U.S., aside from the three parties—government, industry groups, and citizens—there is another independent force that

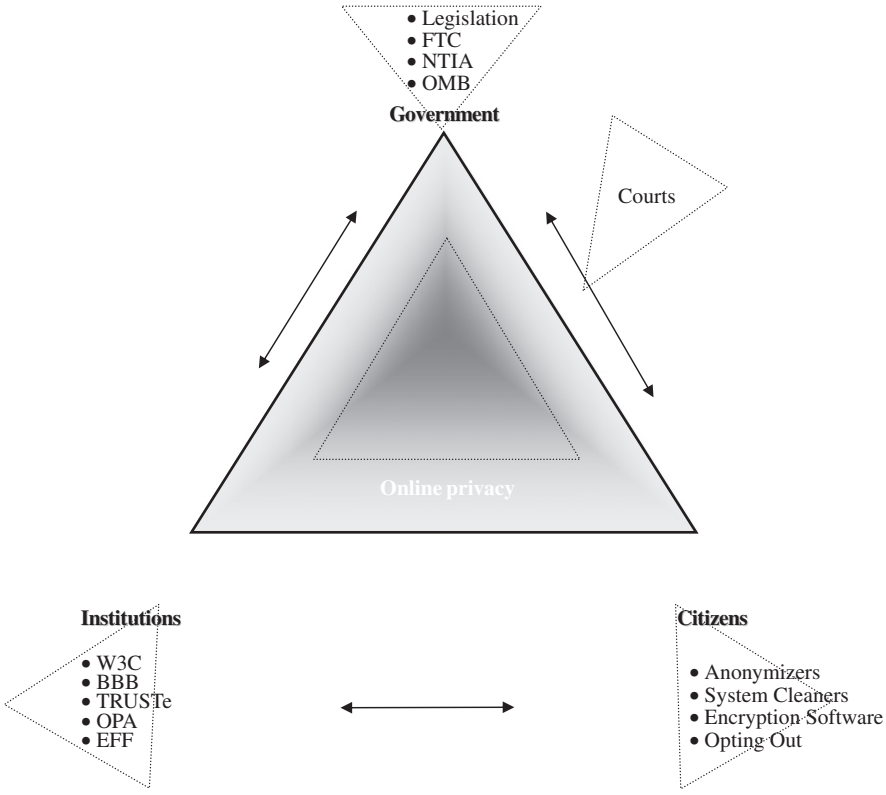

Fig. 1. The relationships between government, institutions, and end-users in the U.S.

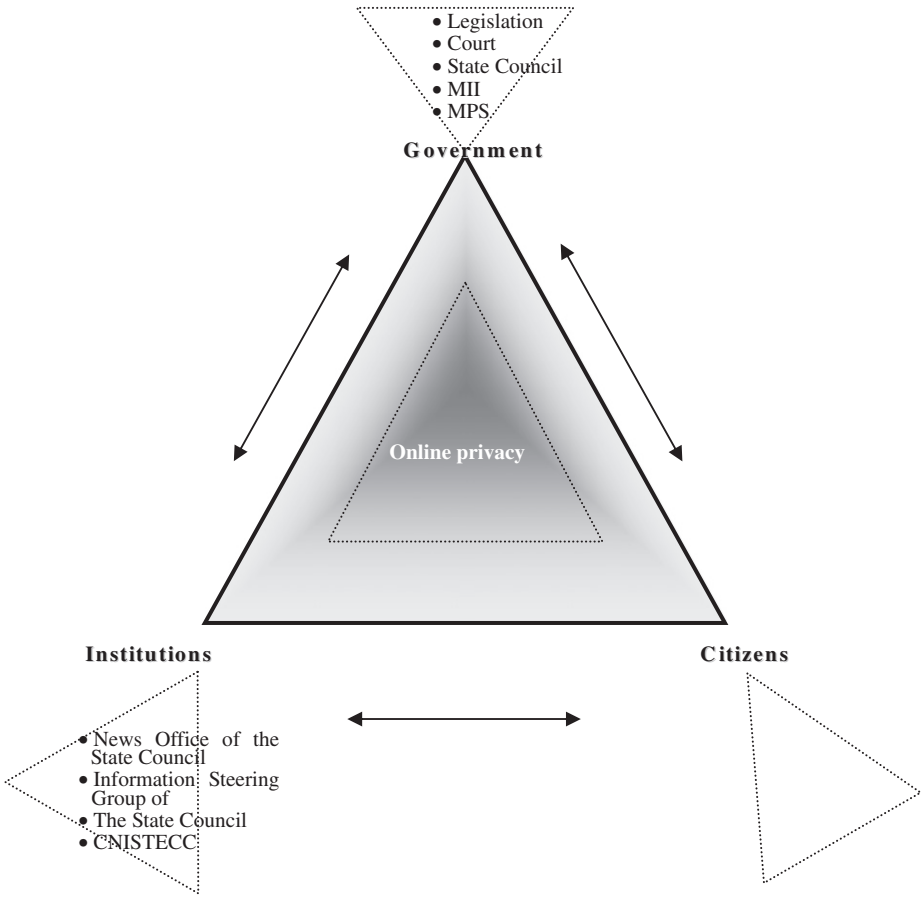

Fig. 2. The relationships between government, institutions, and end-users in China.

helps to facilitate online privacy regulation: the courts. Court cases obviously help to gradually accrete a standing body of applicable case-law vis. online privacy regulation, and—through their review powers—contribute to the legislative process.[5] Comparative policy research (e.g., Lau, Atkin, & Lin, 2008) underscores that this system observes a unique tradition in the U.S., one that benefits from online privacy protection (Fig. 2).

9.1. Government regulation in the U.S. and China

The U.S. has passed some landmark legislative initiatives on privacy, which can be classified in the following domains: privacy of communications (the 1986 Electronic Communications Privacy Act[6] and the Telephone Consumer Protection Act of 1991[7]); privacy of financial information (the 1970 Fair Credit Reporting Act[8]); privacy of government collections (the Privacy Act of 1974[9]); privacy of medical records (the Health Insurance Portability and Accountability Act of 1996[10]); privacy of other personal records (the Video Privacy Protection Act of 1988[11]), and the Cable Communication Policy Act of 1984.[12] All of these measures are related to some aspect of privacy protection (e.g., billing records for subscribers under the Cable Act), but they illustrate how such provisions are scattered across different media and information use contexts.

[5] Although Chinese courts may also review privacy cases, they are classified differently because the country lacks an independent judiciary. For a comprehensive discussion on U.S. privacy law origins in constitutional, common, and tort law—and how it's handled by various levels of federal, state and local courts in the U.S—see Lee (2007).

[6] http://www.ftc.gov/os/statutes/031224fcra.pdf.

[7] http://www.epic.org/privacy/laws/privacy_act.html

[8] http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf.

[9] http://www.loc.gov/law/find/hearings/pdf/00183854811.pdf.

[10] http://buskegroup.com/Conducting_a_Community_Needs_Assessment.pdf.

[11] http://www.ftc.gov/privacy/index.html.

[12] The NTIA believes that it will become increasingly difficult to apply existing privacy laws and regulations to communications service providers as services and sectors converge, and as new technologies evolve. See Privacy and the NII, safeguarding telecommunications-related personal information, Oct., 1995, read more from http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.

Aside from legislative bodies, some government institutions, such as the FTC and NTIA, help oversee privacy administration. The Federal Trade Commission (FTC) is a federal agency that enforces laws and regulations that affect the national marketplace and privacy oversight is central to its FTC's consumer protection mission. Under the FTC Act, the Commission guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use, and secure consumers' personal information (i.e., pretexting). Under the Gramm-Leach-Bliley Act, the Commission has implemented rules concerning financial privacy notices and the administrative, technical, and physical safeguarding of personal information, and it aggressively enforces strictures against pretexting. The Commission also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act.[13]

The NTIA is an agency of the U.S. Department of Commerce. In 1995, the NTIA published a report titled Privacy and the NII, which outlines safeguards for telecommunications-related personal information. The NTIA provided an analysis of the state of privacy in the U.S. as it relates to existing and future communications services and recommended a framework for safeguarding telecommunications-related personal information (TRPI). To rectify limitations in existing telecommunications privacy law and to provide consumers with a uniform privacy standard for TRPI, the NTIA proposed a framework that draws upon the Information Infrastructure Task Force's National Information Infrastructure (NII) Principles for Providing and Using Personal Information. This framework has two fundamental elements—provider notice and customer consent. Still, the NTIA's role in actual enforcement is limited, as it lacks the clout and the constituency of the FCC.

Among the many notions of privacy, the growth of the NII primarily raises concerns about information privacy, which is our primary focus here.[14] Still, as we'll explore later, backbone legislation like the Electronic Communication Policy Act 1986 has been updated with specific measures over time. For instance, the Communications Assistance for Law Enforcement Act (CALEA) of 1994s provisions on wiretapping was updated via the Patriot Act in 2001.[15] Also, in 1999, the Office of Management and Budget (OMB) in White House created the office of the Chief Counselor for Privacy to coordinate the federal government's response to privacy issues.

In China, privacy appeals have been judged and protected under the right of reputation based on Answering to the General Principles of The Civil Law of The People's Republic of China, January 26, 1988. Obviously, such measures cannot keep pace with the burgeoning the internet. The Chinese government nevertheless acknowledged the importance of personal information protection in the information age—at least in rhetorical terms—by establishing a working group to draft the Personal Information Protection Act. However, during the interim when the Act was being published, people had to rely on temporary regulations. For example, according to the clause 18 of the Computer Information Network International Internet Management Temporary Regulations, which was published by the State Council on December 17, 1997, "It is forbidden to have unauthorized access to a computer system to change other people's information, to send out information under other people's name, or invade other people's privacy." The privacy legislation is, however, far from complete.

As Zittrain (2009, p. 1) observes, such offerings of personal information contribute to a growing data "cloud" that makes it easier for authoritarian regimes to spy on their own citizens:

> "The cloud can be even more dangerous abroad, as it makes it much easier for authoritarian regimes to spy on their citizens. The Chinese government has used the Chinese version of Skype instant messaging software to monitor text conversations and block undesirable words and phrases. It and other authoritarian regimes routinely monitor all Internet traffic—which, except for e-commerce and banking transactions, is rarely encrypted against prying eyes."

In addition, the Chinese system offers no specific role taker, which explains why some government departments published internet regulations in a piecemeal fashion. For example, on December 30, 1997, the Ministry of Public Security issued the State Council approved The Management of the Security of International Computer Network Information Networking. In August, 1998, the Ministry of Public Security officially formed the Public Information Network Security Supervision Bureau. It takes the responsibility for maintaining computer network securities, striking against crime in cyberspace, and supervising the security protection of computer information systems. On September 11, 2005, the News Office of the State Council and Ministry of Information Industry jointly issued Regulations for Administering the Internet News and Information Services and the regulation came into effect on the same day. Not to be outdone, on March 6, 1998, the Informatization Steering Group of the State Council issued directive on Implementing Rules for Interim Regulations of the People's Republic of China on the Management of International Computer Information Networking. The rules went into effect as of the date of promulgation. In the February of 1999, the China National Information Security Testing Evaluation & Certification Center (CNISTEC) was established.

[13] CALEA aims to "preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities." Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994), codified at 47 U.S.C. §§1001-10.

[14] Only 28% of the B2C websites—which collect vast amounts of personal data—have privacy policies. From the perspective of the contents of privacy disclosures, among the most popular Chinese websites, only 8% implemented notice, choice, access, and security at the same time.

[15] By collecting the personal information of news users, online news sites can build user profiles that allow for personalizing content to individual visitors or selling site visitor information to third parties (Hong, 2005; Li, 2007).

9.2. Self-regulation in the U.S. and China

The U.S. has tried such license programs as TRUSTe, P3P, etc. The Seal program was put forward by online versions of the Better Business Bureau, representing a traditional self-regulatory bureau with a long history. Its online version certifies eligible Web sites, holding sites to baseline privacy standards. The program requires its licensees to implement certain fair information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Websites. TRUSTe is an independent, non-profit organization whose mission is to build trust and confidence in the Internet by promoting the use of fair information practices.

The Platform for Privacy Preferences Project (P3P) was initiated by the World Wide Web Consortium (W3C). It is an international consortium where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C's mission is "To lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web."[16] Industry leaders who have or will soon make their browsers or websites compliant with the new Platform for Privacy Preferences include Microsoft, America Online, Engage technologies, IBM, and P&G.[17]

In addition, the U.S. has a universal online privacy protection organization—the Online Privacy Alliance (OPA). The alliance will lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce. OPA will also identify and advance effective online privacy policies across the private sector, and support and foster the development and use of self-regulatory enforcement mechanisms and activities; in this way, they can promote user empowerment technology tools—particularly those designed to protect individual privacy—and support compliance with and strong enforcement of applicable laws, regulations, etc.[18]

China does not have a universal specific self-regulation organization dedicated to online privacy. Several departments of the government have issued certain rules on information networking. For example, on March 6, 1998, the Informatization Steering Group of the State Council issued Implementing Rules for Interim Regulations of the People's Republic of China on the Management of International Computer Information Networking. Created by the Internet News & Information Service Working Committee (INISWC) of the Internet Society of China, the website of net.china.cn was launched in Beijing on June 10, 2004. The website was named an Illegal and Inappropriate Information Report Center, providing a channel for the public to report suspected illegal or offensive Internet activity and material, and to maintain public interests. The opening of this website represents another essential step to strengthen self-discipline and public supervision of the Internet industry.

Kong's (2007) survey of Chinese websites reveals that virtually all of them collect personal data—although only 50% post privacy policies or discrete privacy statements—prompting him to conclude that website awareness of personal data protection is extremely weak. Some self-regulation projects are carried on partly by the government. For example, one project was initiated on December 7, 2000 jointly by the Ministry of Culture, the Central Committee of Communist Youth League, the State Administration of Radio Film and Television, National Students' Federation, the State Office of Informatization Promotion, Guangming Daily, China Telecom and China Mobile, namely the Internet Manners and Culture Project. Launched in Beijing, the project was framed along the theme of "Civilized website accessing, civilized network establishment and civilized Internet environment." On November 29, 2004, the Internet Trust and Self-discipline Alliance, co-established by Internet companies Sina, Sohu, and Netease, proclaimed self-disciplinary regulations for China's Internet wireless service providers (SPs), representing the continued and serious efforts put into the self-discipline of the Internet wireless SPs in China.

Still, China has substantially enhanced her legal and regulatory protections for personal information in recent years. Since 2003, the Personal Information Protection Law has been included in the legislative agenda of the State Council. On August 25, 2008, the seventh amendment to the Criminal Law was proposed to the Standing Committee of the National People's Congress for approval; it holds those committing leaking, stealing, or buying personal information of citizens criminally accountable. Legislation enabling the Personal Information Protection Law was designed to enhance protections for online privacy and play a positive role in enhancing the self-regulation of Internet enterprises.

With regard to ongoing administrative reforms, the relationship between the Chinese government and the judiciary has changed dramatically since 2008. The Central Committee of the Chinese Communist Party published the Document on Deepening the Reform of Administrative Systems early that year. The State Council then crafted the Decision on Strengthening Law-based Administration of City and Country Procedures and new assessment systems on law-based administration. All of these changes further reshaped the relationship between China's government and the legal system,

[16] The P3P enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit. Using P3P, Internet users will be able to configure their browsers or other software to meet certain privacy standards. The browsers will then automatically avoid web sites that do not meet those standards.

[17] Several media structures are peculiar to China, in that most of the news organizations are state-owned (in whole or part), although private owned news corporations are steadily proliferating.

[18] See OPA mission (2011).

helping facilitate the transition to a law-based administration. As Hu Jintao's report to the 17th Party Congress, VI (5) outlines (Hu, 2007)

> "…We need to carry out government administration in accordance with the law. We need to deepen the reform of the judiciary system, optimize the distribution of judicial functions and powers, standardize judicial practices, and build a fair, efficient and authoritative socialist judiciary system to ensure that courts and procuratorates exercise their respective powers independently and impartially in accordance with the law."

Building on that effort, the Standing Committee of the National People's Congress recently passed the Tort Liability Law of the People's Republic of China; the measure's final approval did not come until seven years after the comprehensive tort law draft was introduced in 2002. The measure thus pulls together doctrines and provisions previously found in disparate court rulings, regulations, or opinions in order to strengthen the legal basis for China's civil code as well. In particular, as Growbowski and Li (2010, p. 1) observe

> "Article 2 provides that tortious liability arises upon the infringement of "civil rights and interests, "an extremely broad category that includes personal and property rights and interests such as the right to life, the right to health, rights associated with names, reputation rights, honorary rights, the right to one's image, *the right to privacy*, the right to marital autonomy, the right to guardianship, ownership rights, usufruct, collateral rights, copyrights, patent rights, exclusive rights to use trademarks, discovery rights, equity rights and inheritance rights (emphasis added)."

The Tort Liability Law recognizes an independent right of privacy for the first time in Chinese legislative history. Article 2 of this new law expressly includes the right of privacy in the list of protected civil rights and interests, and thus subjects infringement of this privacy right to tort liability, including paying damages for actual losses (in the event that the actual losses are difficult to be quantified, then the damages will be granted by reference to the unlawful profits that may arise from such violation) and compensation for any emotional harms.

In provisions concerning medical malpractice, this new law also obligates the medical institutions to treat the private data of a patient in extreme confidence and prohibits any disclosure of such information without the authorization of the patient. Additionally, according to Article 36 of the Tort Liability Law, a website operator that acknowledges that a party's civil rights are being infringed through contents posted on its website and fails to take necessary corrective measures to stop such infringement is jointly and severally liable with the infringing party. (In practice, infringement of the right of privacy is one of the most common website torts.) Moreover, if a website operator is warned of such infringement by an affected party and fails to remove the contents or adopt other corrective measures, it will also be held jointly and severally liable with the infringing party.

Since the Tort Liability Law did not take effect until the time of this writing (late 2010), more time is needed to see how provisions related to privacy are interpreted and implemented. The fact that such terminology is being incorporated into a reform of this sort, however, stands testament to its salience in the government's plan to centralize and standardize tort laws as China deepens her involvement in the global information economy.

10. User concerns about online privacy

In the U.S., the F.T.C. is educating consumers and businesses about the importance of personal information privacy, including the security of personal information. Lee (2007, p. 264) recounts one online survey ($n=1500$ Internet users), which found that nearly 100% were "highly concerned about invasive promotional tactics and the collection of personal information on web sites," while 75% were also "highly concerned" about the tracking habits of web sites (Kandra & Brandt, 2003). Owing to these personal information protection concerns, some three-quarters of respondents report providing false data about their identity (Survey reveals, 2004). As a consequence, the Privacy and American Business (2004) reports that two-thirds of Americans are acting to protect their privacy. This might include such actions as removing one's personal information from a database, or declining to shop at stores that are aggressive in soliciting user data (see Lee, 2007).

In addition, users are employing software such as Anonymizers, System Cleaners, Encryption software and Opting Out, etc. to help them avoid online privacy violations.

Since China has no organization chartered to remind and educate citizens about online privacy, most do not know how to protect their online privacy (e.g., CNNIC, 2007).

11. Contrasting privacy regulation in the U.S. and China

Table 1 details how both the U.S. and the Chinese governments have published extensive legislation on online privacy regulation. The chief difference is that in the U.S., although there is no guarantee of privacy in the constitution, several measures regulate the collection, distribution, and use of personal information. Borrowing from Lee's (2007, p. 270) regulatory typology, these measures can be classified as follows:

- "In the realm of telecommunication, the Electronic Communication Privacy Act (EPCA, 1986) prohibits the intentional disclosure of the contents of a personal electronic communication intercepted by anyone, government, or private.

Table 1
Regulatory comparison charts contrasting the U.S. vs. China.

The U.S	
Government	
Department	**Legislation**
FTC	The Privacy Act of 1974 The Fair Credit Billing Act of 1974 The Cable Communication Policy Act of 1984 The 1986 Electronic Communications Privacy Act The Video Privacy Protection Act of 1988 The Telephone Consumer Protection Act of 1991 Communications Assistance for Law Enforcement Act of 1994 Telecommunications Act of 1996 Video Voyeurism Prevention Act of 2004 Internet Spyware Prevention Act of 2005 Enforce Gramm-Leach-Bliley Act Fair Credit Reporting Act Children's Online Privacy Protection Act CANSPAM Act of 2003 The Patriot Act
NTIA	
OMB, the White House Office of Management and Budget	
Self-regulation	
Institutions	**Oversight Function**
Online version of Better Business Bureau	Seal program
TRUSTe	
W3C	Platform for Privacy Preferences (P3P) standard
Online Privacy Alliance	
CPA WebTrust	
Network Advertisers Initiative (NAI)	
Liberty Alliance	
Privacy Exchange	
Privacy International	
Electronic Frontiers Foundation	
Citizens	
Anonymizers	
System Cleaners	
Encryption software	
Opting Out	
China	
Government	
Department	**Legislation**
The State Council	Answering to the General Principles of The Civil Law of The People's Republic of China, January 26, 1988 The Personal Information Protection Act is underway published Internet Management Method Rules for Administering the Internet Information Services (on September 25, 2000) Regulation on the Protection of the Right to Network Dissemination of Information (May 18, 2006)
The News Office of the State Council	Regulations for Administering the Internet News and Information Services 2005
The Informatization Steering Group of the State Council	Implementing Rules for Interim Regulations of the People's Republic of China on the Management of International Computer Information Networking (on March 6, 1998)
The Ministry of Industry and Information Technology	Measures for the Administration of Communication Network Security Protection (effective date March 1, 2010)
The Ministry of Public Security	In August 1998, the Ministry of Public Security officially formed the Public Information Network Security Supervision Bureau. It takes the responsibility of maintaining computer network securities, striking against crime in cyberspace, and supervising the security protection of computer information systems.
China National Information Security Testing Evaluation & Certification Center	
Self-regulation/semi-governmental	
Institutions	**Oversight function**
Internet News & Information Service Working Committee (INISWC)	Illegal and Inappropriate Information Report Center
Internet Trust and Self-discipline Alliance (2004)	Self-disciplinary regulations for China's Internet wireless service providers

- The Telecommunications Act of 1996 requires telephone companies to obtain customers' approval before using information about users' calling patterns to market new services (see Li, 2004).
- The Children's Online Privacy Protection Act of 1998 (COPPA, 2000) requires commercial websites and other online services directed at children to obtain consent prior to collecting information from children.
- The Cable Communications Policy Act of 1984 places fairly strong protections on the privacy of cable subscribers, stating that cable operators may not collect or disclose consumers' personally identifiable information without written or electronic consent (Section 551[b])."

The scope of privacy measures examined here ranges from governmental to personal levels—as well as communication and finance to personal records—for adults and children. As might be expected in a democratic system, American legislative initiatives are more comprehensive and far-reaching than those of their Chinese counterparts. In China, there was until recently no specific right of privacy specified in dedicated legislation, as privacy was protected instead under the right of reputation in the Civil law. Until now, China has not had an independent Right of Privacy Act, with regulation having relied on separate articles in different laws. The legislation concentrates more on public security than personal privacy. Only isolated clauses or rules mention the term "privacy".

With regard to government administration, both the Chinese and the U.S. governments rely on key institutions to oversee online privacy protection. In the U.S., the FTC and NTIA assume the main responsibilities to protect online privacy. Both of these bodies are affiliated with the Department of Commerce, and thus reflect a strong commercial orientation. The FTC deals with issues that touch the economic life of every American, representing the only federal agency with both consumer protection and competition jurisdiction in broad sectors of the economy. Privacy is a central element of the FTC's consumer protection mission. This explains why privacy is considered not only to be a human right, but also a property right as well. In that regard, online privacy is regarded as a right related to commerce. Online privacy cases involving the news media are thus resolved in the same way as in e-commerce, since in the U.S. since most of the news corporations are commercial operations.

In China, the Ministry of Information Industry and the Ministry of Public Security take charge of information regulation. The differences are that, in China, besides the Ministry of Information Industry, the Public Security Department is one of the main government institutions overseeing Internet management. Both bodies assume more responsibility for maintaining computer network security, striking against crime in cyberspace, and supervising the security protection of computer information systems than on personal information protection. The News Office of the State Council administers the Internet news and services, which underscores the Chinese government's recognition that internet news consumption can influence online privacy.

With regard to self-regulation, both countries offer several self-regulatory institutions that organize the companies or institutions together to manage online privacy. The U.S. relies more on self-regulation than legislation, which gives the corporations more freedom and conforms to the free market system. Several technological standards such as TRUSTe mark, seal program, P3P, etc., have been set up to guarantee consumers' online privacy. China also engages in self-regulation, but does so primarily through the auspices of the government (or which are at least related to government). They are not purely self-regulatory organizations. Up until now, there has been no confirmed technological standard similar to the TRUSTe program in China.

There remain large differences in terms of people's concerns regarding online privacy between the two countries. In the U.S., users generally express higher levels of online media literacy concerning the use of such software as anonymizers, system cleaners, encryption software, or opting out methods to protect their privacy. In China, although users express privacy concerns, relatively few realize that they can utilize technological ways to prevent online privacy violations (e.g., Li, 2007); the online users could benefit from more education on online personal information protection.

12. Discussion

On balance with regard to online privacy regulation, the U.S. follows a self-regulatory model, one that affords the information industry more freedom to develop while overcoming the shortcomings of an evolving technology; this approach seems is in line with the libertarian leanings of a democratic free market system. By contrast, China carries a central regulatory model, relying more on government directives than self-regulation. Chinese users are less aware than Americans of self-help and technological options protecting their privacy. This approach flows logically from the country's overall socio-political system, that of an authoritarian socialist market economy (see, e.g., Anowkwa et al., 2003; Li, 2007).

In comparative terms, the Chinese system could benefit from greater assurances of individual user privacy, such that netizens might feel more comfortable making politically sensitive posts. Empirical work on web adoption (Mou, Fu, & Atkin, 2011) suggests, for instance, that Chinese netizens' embrace of the Internet is a function of trust in the Internet. By implication, the economic value added provided by online commerce in China is only as strong as the confidence that its users have in the security of their online movements. As Dahlberg (2001) suggests, the "blindness" to one's identity in cyberspace allows users to interact equally and enhances the network's value. The Web is not likely to maximize its potential as an economic engine in China until user privacy concerns are minimized. As commentators (e.g., Kong, 2007) observe, China has an interest in building consumer confidence in e-commerce and promoting the free movement of personal data in the information age.

Based on the comparisons offered here, privacy has yet to be governmentally recognized as a universally established individual right, although users the world over see privacy protection as especially appropriate in the information age. As the contrasting media foundations for each nation might suggest, the relatively freer libertarian leanings underpinning American media go hand-in-hand with greater degrees of online privacy protection in all domains. The one area where China might possess a clear advantage—to the extent that it wants to embrace privacy protections—is in the area of enforcement. Here, see those very same authoritarian attributes that undermine privacy and press protections can also serve to enhance enforceability, in cases where privacy violations are so egregious as to run afoul of China's recent privacy legislation.

Given the Internet's emergence as a medium without borders, it's useful to reconsider the character of privacy in the information age. Should policymakers still consider privacy simply as a fundamental human right or a property right, a commodity that can be controlled through free market approaches, or a combination of the two? Do we need a universal personal information *magna-carta* governing online privacy disclosure in the information age? Within a given country, the policymaking process requires government, institutions, and citizens to cooperate in order to reach a sustainable balance.

As comparative models suggest, online privacy protection is an evolving concept that can be defined by nuances in the local media milieu with which policymakers are faced. The United States handles privacy regulation on a piecemeal basis. Although the FTC encourages self-regulation, the government lacks uniform federal legislation on personal data protection. While China has taken recent steps to provide some legal recognition for privacy, she still lags behind the West in developing a comprehensive legal framework for the regulation, use, and disclosure of personal data.[19]

One might regard as axiomatic the notion that an authoritarian state like China exercises a freer hand vis privacy and censorship issues. The fact that domestic and international pressure prompted the government to delay the implementation of its Green Dam software, however, underscores the Communist Party's felt need to consider public opinion in these domains. Because China has further to go in reaching Western standards for privacy protection and government liberalization generally, it's useful to focus study implications and proscriptions in that context.

China's legislation on privacy protection will need to strike a more reasonable balance between those of the state and the individual. And the principle of the neutrality of technology should be adopted in the choice of the legislative mode, combining lawmaking, technological protection, and self-regulation of the trades. Secondly, international cooperation should be pursued. Since this is an era of globalized economies and the Internet is an open world, international coordination is inevitable in the determination of jurisdiction of laws regulating the order of the Internet, in international judicial collaboration etc. In the Internet era, the conflicts and contradictions between different institutions of privacy have become more prominent. For example, hacking has become a global problem; hackers in every country are compromising individual privacy and secrets of organizations—if not governments—when breaching online firewalls across borders.

Clearly, the scarcity of a strong liberal tradition involving traditional media acting as a Fourth Estate in China renders the Internet "the single most important avenue for people to criticize government policies and to participate in politics" (Zheng & Wu, 2005, p. 525). Specifically, the Internet provides an alternative source for less-censored information, even politically sensitive content. To the extent that the government seeks to maintain social stability via close monitoring of online communiqués, user privacy may fall under increasing risk.

Of particular interest in the privacy realm, commentators note the great potential for online discourse for setting public agendas that can affect decision making (Zheng & Wu, 2005), the formation of Chinese cyber nationalism (Wu, 2007), the rise of the transnational Chinese cultural sphere (Yang, 2003), the formation of collective action and social norms (Arsene, 2008), and the setting of public agendas that can affect government decision making (Mou et al., 2011).

In sum, China has improved laws and regulations by passing legislation to protect personal information and reach a reasonable balance among the state, society, and individuals. During this process, international cooperation is advisable. At the same time, self-regulation remains the primary modality by which to protect online privacy in China. As commentators (e.g., Schell & Shambaugh, 1999) observe, the Chinese people will tolerate restraints on their freedoms in return for stable social and economic progress. Parallel experience with Asian "tigers" like Taiwan and South Korea suggests, however, that citizens will seek more rights as they become more affluent.

Given the compelling role that new media (e g., Twitter) have played in facilitating regime change in the Middle East in 2011, the Internet is emerging as a useful public forum—even a revolutionary tool—for citizens to search for information and interact with each other. Despite anecdotal reports of political apathy among Chinese youth, the recent enthusiasm for online discussion uncovered in recent surveys of college users (Mou et al., 2011) suggests that the Internet will be a compelling agent for socio-political change.

So the earlier-reviewed surveys outlining low public awareness of privacy remedies should not be confused with apathy about the Chinese public sphere online. Online privacy will thus fall under increasing stress as governments seek to monitor how online and mobile media are used in orchestrating anti-regime protests. Later work addressing online privacy will need to consider these privacy dynamics as China continues to liberalize, in the social context and cultural context variations across the globe.

[19] For instance, China offers no national, generally applicable data privacy law, even though a right to prevent disclosure of personal data may arise within the context of (1) defamation action for infringement of the Reputational Rights broadly defined under Chinese civil laws or (2) criminal prosecution against persons who misappropriate personal information in the course of performing their professional duties.

On balance, analysis underscores that different social systems and cultures regard privacy to be an emerging right, but offer different understandings and regulations in order to address online privacy. Simply put, privacy is not yet a universally established individual right, although such an approach is in order. As the global village continues to take shape, later work should continue to explore the formation of policymaking bodies that can address online privacy with a more measured, uniform approach that balances the rights of individual users against endogenous cultural imperatives.

References

Allen, A. L. (2001). Is privacy now possible? A brief history of an obsession. *Social Research*, *68*(1), 301–306.

Ang, P. (2001). The role of self-regulation of privacy on the Internet. *Journal of Interactive Advertising*, *1*(2). Retrieved from 〈http://www.jiad.org/vol1/no2/ang/〉.

Anowkwa, K., Lin, C., & Salwen, M. (2003). *International communication: Cases and issues*. Boston: Wadsworth.

Arsene, S. (2008). Web 2.0 in China: The collaborative development of specific norms for individual expression. *Paper Presented at the Politics: Web 2.0: An International Conference, London, UK*. Retrieved from 〈http://www.newpolcom.rhul.ac.uk/politics-web…/arsene_norms_discussion_china.pdf〉.

Bonavia, M., & Morton, L. (1998). Personal information privacy issues relating to consumption in the U.S. marketplace. *Consumer Interests Annual*, *44*, 25–29.

Bucy, E., Gantz, W., & Wang, Z. (2007). Media technology and the 24-h news cycle. In C. Lin, & D. Atkin (Eds.), *Communication technology and social change* (pp. 143–164). Mahwah, NJ: LEA.

Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication yearbook*, Vol. 6 (pp. 206–249). Beverly Hills, CA: Sage.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communication of the ACM*, *42*(2), 60–67.

CNNIC. (2007). *China Internet development report*. China Internet Network Information Center. Retrieved November 1, 2007 from 〈http://www.cnnic.net.cn〉.

CNNIC. (2010). *Statistical report on internet development in china (July 2010)*. China Internet Network Information Center. Retrieved from 〈http://www.cnnic.cn/uploadfiles/pdf/2010/8/24/93145.pdf〉.

Culture.people.com (2010). People. Retreived from 〈http://culture.people.com.cn/GB/8304520.html〉.

Dahlberg, L. (2001). Computer-mediated communication and the public sphere: A Critical analysis. *Journal of Computer-Mediated Communication*, *7*(1). Retrieved from 〈http://jcmc.indiana.edu/vol7/issue1/dahlberg.html〉.

DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.

Delbert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global Internet filtering*. Cambridge: MIT Press.

Delbert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2010). *Access controlled: The shaping of power, rights and rule in cyberspace*. Cambridge: MIT Press.

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, *33*(3), 102–115.

East-West Connect.com/ (2010) Chinese-Internet-usage-report-2010. Retrieved from 〈http://www.east-west-connect.com/Chinese-Internet-Usage-Report-2010〉.

Epanel. (2007). *Chinese Internet audience survey*. Retrieved from 〈http://www.epanel.cn/cn/imus/images/down/yangbao.pdf〉.

FTC. (2004). *Deter, detect, defend, avoid ID theft*. Federal Trade Commission. Retrieved from 〈www.ttc.gov/bcp/edu/…idtheft/media…/press-releases-2004-2005.html〉.

Gates, W. (2000). *Shaping the Internet age*. Retrieved from 〈https://www.microsoft.com/presspass/exec/billg/writing/shapingtheinternet.mspx〉.

Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal*, *89*, 421–461.

Gibson, W. (1995). *Interview with William Gibson*, 1995. Retrieved from 〈http://www.brmovie.com/Articles/Guardian_WG_1995.htm〉.

Grabowski, J. V., & Li, Y. (2010). *Tort liability law in the People's Republic of China*. Retrieved from 〈www.martindale.com/governmental-law/article_Faegre-Benson-LLP_916960.htm〉.

Green, H. (2001, November 6). *A defining moment for info privacy. Business Week Online*. Retrieved from 〈http://www.nocpa.org〉.

NOCPA. (2007), Retrieved from 〈http://www.nocpa.org/privacy/privacyintro.html〉.

Hong, T. (2005). Internet privacy practices of news media and implications for Online journalism. *Journalism Studies*, *6*(1), 15–28.

Hu, J. (2007). *Hu Jintao's report at the 17*th *Party Congress*. Retrieved from 〈http://www.chinadaily.com.cn/30years/2007-10/25/content_7128784_6.htm〉.

Kandra, A., & Brandt, A. (2003, November). *The great American privacy makeover. PC World*. Retrieved from 〈http://www.pcworld.com/howto/article/0,aid,112468,00.asp〉.

Kaysen, R. (2011, March, 22). *Parents of teen suicide: Prosecute on privacy charges*. Retrieved from 〈http://www.msnbc.msn.com/id/42220366/ns/us_news-crime_and_courts/〉.

Kong, L. (2007). *Online privacy in China: A survey on information practices of Chinese websites*. Retrieved from 〈http://chinesejil.oxfordjournals.org/content/6/1/157.full〉.

Krasnow, I., Longley, C., & Terry, H. (1982). *The politics of broadcast regulation*. New York: Macmillan.

Lau, T. Y., Atkin, D. J., & Lin, C. (2008). Cross media ownership: An analysis of regulations and practices in Australia, Hong Kong, and Singapore. In H. F. Ulrich, & E. P. Lehrmann (Eds.), *Telecommunication research trends* (pp. 127–141). Hauppauge, NY: Nova Science Publishers.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional development theory. *Journal of Social Issues*, *33*(3), 22–42.

Lee, L. T. (2000). Privacy, security, and intellectual property. In A. B. Albarran, & D. H. Goff (Eds.), *Understanding the web: Social, political, and economic dimensions of the Internet* (pp. 135–164). Ames, IA: Iowa State University Press.

Lee, L. T. (2007). Digital media technology and individual privacy. In C. Lin, & D. Atkin (Eds.), *Communication technology and social change* (pp. 257–280).

Lee, L. T., & LaRose, R. (1994). Caller ID and the meaning of privacy. *The Information Society: An International Journal*, *10*(4), 247–265.

Li, S. (2004). Internet shopping and its adopters: Factors in the adoption of internet shopping. In P. Lee, L. Leong, & C. So (Eds.), *Impact and Issues in the new media: Toward intelligent societies* (pp. 81–102). Cresskill, NJ: Hampton.

Li, D. (2007). Online privacy protection. *South-eastern Communication Journal (China)*, *32*(4), 22–23.

Lin, C., & Atkin, D. (2007). *Communication technology and social change*. Mahwah, NJ: LEA.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33*(3), 5–21.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*, 243–261.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society*, *27*(3), 27–32.

Mou, Y., Fu, H., & Atkin, D. (2011). Predicting political discussion in a censored virtual environment. *Paper presented at the International Communication Association*, Boston.

OPA mission. (2011). *Privacy alliance mission*. Retrieved from 〈www.privacyalliance.org/mission〉.

Pedersen, D. M. (1979). Dimensions of privacy. *Perceptual and Motor Skills*, *48*, 1291–1297.

PEW. (2007). *Teens, privacy and online social networks*. Pew Research Center. Retrieved from 〈http://pewresearch.org/〉.

Privacy & American Business. (2004). *New national survey on consumer privacy attitudes*. Press Release, Privacy and American Business. Retrieved from 〈http://www.marketwire.com/mw/release_html_b1?release_id=68484〉.

Raab, C. D., & Bennett, C. J. (1998). The distribution of privacy risks: Who needs protection. *The Information Society*, *14*, 263–274.

Rogers, E. (2002). The information society in the new millennium. In C. A. Lin, & D. Atkin (Eds.), *Communication technology and society: Audience adoption and uses* (pp. 43–64). Cresskill, NJ: Hampton.

Schell, O., & Shambaugh, D. (1999). *The China Reader*. New York: Vintage Press.

Survey reveals that Privacy protection is becoming more and more difficult in the information age. (2002, December 2). *Xinhua News Agency*, Received from 〈http://news.xinhuanet.com/newscenter/2002-12/02/content_646092.htm〉.
Survey reveals increased privacy concerns cause consumers to provide false identity data. (2004, February 19). PR Newswire.
Tribe, L. (1988). *American constitutional law* (2nd ed.). New York: Foundation Press.
Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*, 193–220.
Watts, J. & Branigan, T. (2009). *China delays launch of internet filter Green Dam*. Retrieved from 〈http://www.guardian.co.uk/world/2009/jun/30/green-dam-china-delay〉.
Whitman, L. (2001). A study of user attitudes toward persistent cookies. *Journal of Computer Information Systems*, *41*(3), 1–7.
Wu, X. (2007). *Chinese cyber nationalism*. Lanham, MD: Lexington Books.
Yang, G. (2003). The internet and the rise of a transnational Chinese cultural sphere. *Media, Culture & Society*, *25*, 469–490.
Zheng, Y., & Wu, G. (2005). Information technology, public space and collective action in China. *Comparative Political Studies*, *38*(5), 507–536.
Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven, CT: Yale.
Zittrain, J. (2009, July 19). *Lost in the cloud. The New York Times*. Retrieved from 〈www.nytimes.com〉.