Chapter 8
E-privacy Protection—Centering on Global Main Legal Instruments and Prospects

Yimeei Guo and Ying Luo

Abstract The Internet also creates many threats to our personal privacy. Unless we know the "rules of the road," our online activity may lead to significant privacy problems. For convenience, this article uses the term "e-privacy" to stand for our personal privacy in the Internet. To avoid an off-limit discussion, after discussing the definition of privacy and e-privacy, this paper analyzes the e-privacy issue and some legal instruments at international and national level with the concern on the collection of personally identifiable information (PII) by Web site operators from visitors to government and commercial Web sites, or by software that is surreptitiously installed on a user's computer ("spyware") and transmits the information to someone else, then discusses the captioned problems including a case study in China. Finally, as there is not any complete e-privacy rule for the Internet in China, this paper wants to make some suggestions to Chinese legislature for further specific regulations based on the analysis of the e-privacy in the conclusion.

Keywords E-privacy · Spyware · Legal instruments

8.1 Introduction

The Internet has created an entirely new legal dynamic as well as a new social and business one. From advertising to intellectual property to privacy and electronic-commerce (e-commerce), the online environment has generated novel legal issues and challenges. At the forefront is the subject of privacy.

Published by "Proceedings of 9th Academic Research Conference on Cross-Straits Chinese Culture and Operation Management", July 8, 2006. pp. 300–308.

Y. Guo (✉) · Y. Luo
Management Science Department, Xiamen University, Xiamen 361005, China
e-mail: yimei_guo@necmail.xmu.edu.cn

Y. Luo
e-mail: yuhe_ly@sina.com

Y. Guo (ed.), *Research on Selected China's Legal Issues of E-Business*,
DOI 10.1007/978-3-662-44542-6_8

Generally speaking, the Internet offers many benefits to netizens. Web sites provide a vast world of information, entertainment, and shopping at our fingertips. E-mail, instant message (IE), chat rooms, and ICQ enable us to communicate with friends, family, and strangers in ways we never dreamed of a decade ago.

But the Internet also creates many threats to our personal privacy. Unless we know the "rules of the road," our online activity may lead to significant privacy problems. For convenience, this article uses the term "e-privacy" to stand for our personal privacy in the Internet.

E-privacy issues generally encompass two types of concerns. One is the collection of personally identifiable information (PII) by Web site operators from visitors to government and commercial Web sites, or by software that is surreptitiously installed on a user's computer ("spyware"[1]) and transmits the information to someone else. The other is the monitoring of electronic mail and Web usage by the government or law enforcement officials, employers, or internet service providers (ISPs).

To avoid an off-limit discussion, after discussing the definition of privacy and e-privacy, this paper analyzes the e-privacy issue and some legal instruments at international and national level with the former type concern and discusses the captioned problems including a case study in China. Finally, as there is not any complete e-privacy rule for the Internet in China, this paper wants to makes some suggestions to Chinese legislature for further specific regulations based on the analysis of the e-privacy in the conclusion.

8.2 What is Privacy/E-privacy?

8.2.1 The Right of Privacy

The notion of privacy was first postulated in a Harvard Law Review article by Louis D. Brandeis, later to become a Justice of the Supreme Court of the USA, and Samuel D. Warren of the Harvard Law School, in 1890.[2] They described privacy as "the right to be let alone"[3] when they were offended by press coverage of their families, and by "recent inventions and business methods."[4] It took almost 20 years before the American courts issued judgments which adopted that principle.[5]

---

[1] Spyware, a catch-all phrase for software that enables a person's online movements to be tracked, has quietly become the latest threat to cyber security, affecting eight out of 10 computers. See Anita Kumar, "Can Congress get arms around spyware problem?", http://www.sptimes.com/2005/05/02/Technology/Can_Congress_get_arms.shtml.

[2] Brandeis and Warren (1890).

[3] Ibid.

[4] Id, at 195.

[5] Boufford (1998).

Later on, in another article by William Prosser, four different types of invasions of privacy were pointed out, including:

1. appropriating an individual's name or likeness for commercial benefit;
2. unreasonable intrusion or interference with an individual's interest in solitude or seclusion;
3. publicly disclosing private facts;
4. publicly placing an individual in a false light.[6]

8.2.2 E-privacy and "Fair Information Practices"

From an information technology (IT) perspective, a much better definition of privacy has been that of Alan Westin, where he described privacy as:

> the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[7]

This definition embodies the concept of "*fair information practices*" which forms the basis for many of the regulatory and voluntary data-protection schemes.[8]

In short, "privacy" is not just a matter of what is kept secret. In the context of e-commerce and e-government, the right to privacy, i.e., e-privacy is really "*the right to control the use of personal information*" that is disclosed to others.[9]

Throughout the world, the privacy of information about individuals is guided by the principles of "*fair information practices.*" These principles, which were authoritatively detailed by the Organization for Economic Co-Operation and Development (OECD),[10] represent basic guidelines for responsible information practices that respect the interests of individuals. They form the foundation of many national and local privacy laws, international agreements on data protection, and various industry codes of best practices.[11] It is these principles that provide the framework for privacy impact assessments and the reference point for the work of privacy commissioners.

---

[6] Prosser (1960). See also Zacchini v. Scripps-Howard Broadcasting Co., 433 U.S. 562,571(1977), Note 7.

[7] Westin (1967) at 7.

[8] See supra note 4.

[9] See Privacy and E-Government (2003).

[10] See "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*", 1980, http://www.oecd.org/EN/document/0,,EN-document-0-nodirectorate-no-24-10255-0,00.html.

[11] See supra note 8.

As expressed by the OECD and other international bodies, fair information practices include:

- **Collection limitation**: No more information should be collected than is necessary to complete the transaction, and any such data collected should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data quality**: Personal data should be relevant to the purposes for which they are to be used, should be accurate and complete, and should be kept up-to-date.
- **Purpose specification**: When personal data are collected, the purpose for the collection should be specified and the subsequent use limited to the fulfillment of that purpose or such others as are not incompatible with the original purpose.
- **Use limitation**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.
- **Security**: Personal data should be protected by reasonable security safeguards against loss or unauthorized access, destruction, use, modification or disclosure.
- **Openness**: In general, there should be no secret collections of data. As a matter of general policy, there should be openness about data practices and policies. Means should be readily available to individuals to establish the existence and nature of databases, the main purposes of their use, and the identity of the entity responsible for the database.
- **Individual participation**: An individual should have the right to obtain access to any data about him held by a data controller. This includes: (a) confirmation of whether or not an entity has data relating to him; (b) to obtain copies of data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, or corrected or completed.
- **Accountability**: Entities collecting data should be subject to enforcement measures that give effect to the principles stated above.

There are obvious exceptions to some of these principles in specific applications. For example, in the context of law enforcement investigations, it is not always possible to give notice to a suspect or to give him access to the information that the police are collecting. Nevertheless, these principles provide a framework for thinking through the privacy issues raised by any government collection of personal information.[12]

[12] "Personal (or personally identifiable) information" is data that can be associated with an individual. Notably, a person's name need not be attached to the information for it to qualify as "personal information." For example, data categorized by a unique numeric identifier is considered personal information even where no name is attached to it, since the numeric identifier can be used to determine the name.

8.3 Main Legal Instruments Dealing with Data Privacy

8.3.1 International Instruments

8.3.1.1 The 1980 OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data

The Guidelines contain a set of data privacy principles similar to those stipulated in "*the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.*"[13] The Guidelines have been very influential on the drafting of data privacy laws and standards in non-European jurisdictions, such as Australia, New Zealand, and Canada.[14] They have also been formally endorsed—though not necessarily implemented—by numerous companies and trade associations in the USA.[15] Further, they constitute an important point of departure for ongoing efforts by the Asia-Pacific Economic Cooperation (APEC) to draft a set of common data privacy principles for jurisdictions in the Asia-Pacific region.[16]

8.3.1.2 The Montreux Declaration

In terms of other international legal instruments, there does not exist a truly global convention or treaty dealing specifically with data privacy. The call to the United Nation (UN) was made in a declaration adopted at the 27th International Conference of Data Protection and Privacy Commissioners in Montreux in early September of 2005.

In what they have called "the Montreux Declaration," the commissioners also call for governments to encourage the adoption of legislation in line with recognized data protection principles and to extend it to their mutual relations; and for the Council of Europe to invite non-member states of the organization to ratify the Convention for the protection of individuals with regard to automatic processing of personal data and its additional protocol.

International organizations have been asked to commit themselves to complying with data protection rules; international non-governmental organizations

---

[13] European Treaty Series No. 108; adopted Jan 28, 1981; in force Oct 1, 1985. Further on the Convention, see, e.g., Henke (1986), Bygrave (2002), especially p. 32.

[14] Reference to the Guidelines is made in the preambles to both Australia's federal "*Privacy Act of 1988*" and New Zealand's "*Privacy Act of 1993*". Further on the Guidelines' importance for Australian policy, see Ford (2003). In Canada, the Guidelines formed the basis for the Canadian Standards Association's "*Model Code for the Protection of Personal Information*" (CAN/CSA-Q830-96), adopted in March 1996. The Model Code has been incorporated into Canadian legislation as Schedule 1 to "*the Personal Information Protection and Electronic Documents Act of 2000*".

[15] See, e.g., Gellman (1993).

[16] See generally the documentation collated at http://www.apecsec.org.sg/apec/documents_reports/electronic_commerce_steering_group/2004.html.

(NGOs) have been asked to draw up data protection standards; and hardware and software manufacturers have been asked to develop products and systems that integrate privacy-enhancing technologies.

The nature of the legally binding instrument to be adopted by the UN is not prescribed; but Swiss data-protection commissioner Hanspeter Thür told SwissInfo.org that it could be a text adopted by the UN in the same way as human-rights provisions.

Progress in implementing the objectives will be subject to a regular assessment. The first such assessment will be carried out at the 28th International Conference, due to take place in September 2006 in Argentina.

The commissioners also adopted a resolution presented by Germany on the use of biometric data in passports, ID cards, and travel documents. In it, the commissioners call for effective safeguards to be built in so as to limit the risks inherent in biometrics. They also adopted a resolution from Italy on the use of personal data for political communication purposes.[17]

8.3.1.3 The European Union

Within the European Union (EU), several Directives on data privacy have been adopted, the first and most important of which is "*Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*" (hereinafter "*EU Directive*").[18] This instrument is binding on EU member states. It is also binding on non-member states (Norway, Iceland and Liechtenstein) that are party to the 1992 Agreement on the European Economic Area (EEA). While the Directive is primarily a European instrument for European states, it exercises considerable influence over other countries not least because it prohibits (with some qualifications) transfer of personal data to those countries unless they provide "adequate" levels of data privacy (see Articles 25–26).[19] Many non-European countries are passing legislation in order, at least partly, to meet this adequacy criterion.[20]

Furthermore, the Directive stipulates that the data privacy law of an EU state may apply outside the EU in certain circumstances, most notably if a data

---

[17] See "Global data protection law needed, say regulators," OUT-LAW News, 19/09/2005, http://www.out-law.com/page-6132.

[18] Adopted Oct. 24, 1995, O.J. L 281, Nov. 23, 1995, p. 31 et seq. Two sectoral Directives on data privacy have also been adopted. The first of these was "*Directive 97/66/EC of Dec.15, 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector*", O.J. L 24, Jan. 30, 1998, p.1 et seq. This has now been replaced by "*Directive 2002/58/EC of July 12, 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*", O.J. L 201, July 31, 2002, p. 37 et seq.

[19] See e.g., Kuner (2003), Chap. 4.

[20] Further on this influence, see Swire and Litan (1998), Shaffer (2000), Waters (2003).

controller,[21] based outside the EU, utilizes "equipment" located in the state to process personal data for purposes other than merely transmitting the data through that state (see Article 4 <1> <c>).[22] All of these provisions give an impression that the EU, in effect, is legislating for the world.[23]

Although the Directive establishes what a company can and cannot do with the data they hold, yet it does not make any specific provisions with regard to e-mail or more specifically, e-mail marketing. Unsolicited e-mail, i.e., "spam" is becoming a growing problem that is costing business worldwide a staggering £6bn per year in online connection costs.[24] As the European Parliament and the Council of the European Union conceive: the Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services, publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy. So-called spyware, Web bugs, hidden identifiers, and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.[25]

Therefore, a new EU anti-spam law—*Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*[26] came into force on December 11, 2003, and is already having a dramatic effect on the amount of spam sent to computer users. Under the Directive, spyware becomes illegal software.[27] This Directive's implementation glorifies the formal stepping in the global anti-spam war of EU and is an important weapon to enhance the consumer's confidence on Internet and e-communication as well.[28]

---

[21] A "data controller" is a person or organization who/which determines the purposes and means of processing personal data: see E.U. Directive, Article 2(d).

[22] See further Bygrave (2000); Kuner, *supra* note 14, Chap. 3.

[23] See further Bygrave (2000); Kuner, *supra* note 17, Chap. 3.

[24] See "*EU Directive on e-mail marketing*", http://www.extravision.com/eudirective.cfm.

[25] "Preamble, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", O.J.L 201, 31/07/2002, pp. 0037–0047.

[26] Ibid.

[27] Article 13 provides that: the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

[28] See "EU implements Anti-spam Act, spyware becomes illegal software," Dec. 3, 2003, http://news.ccidnet.com/pub/article/c951_a69660_p1.html.

8.3.2 National Instruments

8.3.2.1 The USA

By contrast, the US legal regime for data privacy is much more atomized. While there is fairly comprehensive legislation dealing with federal government agencies,[29] omnibus legislative solutions are eschewed with respect to the private sector. Legal protection of data privacy in relation to the latter takes the form of ad hoc, narrowly circumscribed, sector-specific legislation, combined with recourse to litigation based on the tort of invasion of privacy and/or breach of trade practices legislation.[30] European-style data privacy agencies do not exist.

At the same time, though, a "safe harbor" agreement has been concluded between the USA and EU allowing for the flow of personal data from the EU- to US-based companies that voluntarily agree to abide by a set of "fair information" principles based loosely on the EU Directive. The scheme, which so far has attracted over 500 companies,[31] has been held by the European Commission to satisfy the Directive's adequacy test in Article 25.[32]

Today, much of the privacy regulation in the USA occurs at the state level, where many of the 50 states have enacted privacy laws that govern specific industries, issues, or practices. Often, these laws are inconsistent, so that a set of business practices that is legal and commonplace in one state may be prohibited just across the state line. In addition, the *number* of state privacy laws is increasing quickly—for example, more than 20 states have passed separate financial privacy laws just since the beginning of 2004.

At the same time, Congress has enacted federal privacy legislation specific to certain industries. For instance:

- *The Gramm-Leach-Bliley Act* applies to financial institutions;
- The Health Insurance Portability and Accountability Act (HIPAA)of 1996[33] applies to health care providers;
- The privacy provisions of *the Cable Act* apply to cable operators;

---

[29] Most notably *the Privacy Act of 1974* and *Computer Matching and Privacy Protection Act of 1988*. Note also the limited protection of data privacy afforded under the Constitution as construed by the Supreme Court: see especially *Whalen v. Roe*, 429 U.S. 589 (1977). See further Schwartz and Reidenberg (1996), Chap. 4.

[30] See generally the overview in Schwartz and Reidenberg, *supra* note 13, especially Chaps. 9–14.

[31] See "http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list" (accessed July 6, 2004).

[32] Decision 2000/520/EC of July 26, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (O.J. L 215, 25th Aug. 2000, p. 7 et seq.). However, the scheme is presently under review by the Commission.

[33] 42 USC § 201 et seq. (42 USC 1320d-2).

- The privacy provisions of *the Communications Act* apply to telecommunications carriers[34];
- Specific privacy laws address children's online privacy,[35] spam, telemarketing, and junk faxes[36];
- *The Identity Theft Penalty Enhancement Act (ITPEA)* increases criminal penalties for phishing and other forms of identity fraud. This measure, signed by the President in July 2004, establishes punishment guidelines for anyone who possesses someone else's personal information with intent to commit a crime.[37]
- And concerns over spyware are now prompting an array of federal legislative proposals.[38]

Finally, a bill announced on February 8, 2006, in Congress would require every Web site operator to delete information about visitors, including e-mail addresses, if the data is no longer required for a "legitimate" business purpose.[39]

While all of these are well-intended efforts, this ad hoc approach to privacy legislation has many drawbacks. It has led to an overlapping, inconsistent, and incomplete patchwork of state and federal laws that creates compliance chaos for businesses and uncertainty for consumers.

Consumers and businesses alike are often faced with the daunting task of determining whether one or more of the existing laws applies. The answer may depend on the type of data involved, the kind of company that collects it, where and how it is collected, and how it might be used.

For example, personal information collected by a bank is covered by one privacy standard, but that same information collected by a hospital is covered by a different standard. If that information is from a child under the age of 13, it is protected by yet another standard if it is collected online, but it may not be protected at all if it is collected offline. And each of those standards may be affected by state law, but in a different way from state to state. Yet, despite all of these legal

[34] Part I of title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended by adding at the end the new section 231: (d) Privacy Protection Requirements.

[35] "*Child Online Privacy Protection Act* (*COPPA*)", 15 USC 6501-6506.

[36] *The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act)*, 18 USC 1037.

[37] On Sept. 30, 2005, California Governor Arnold Schwarzenegger signed the Anti-Phishing Act of 2005 into law. The first-of-its-kind bill makes Internet phishing a punishable offense. The new law will permit victims to seek recovery of actual damages or up to $500,000 for each violation, whichever is greater. See Walaika K. Haskins, "California Passes Nation's First Antiphishing Law", Oct. 4, 2005, http://www.newsfactor.com/story.xhtml?story_id=38456.

[38] So far, the anti-spyware legislation has been enacted in twelve states. For example, in 2004, California has enacted "*the Consumer Protection Against Spyware Act*", to "protect California consumers from the use of spyware and malware that is deceptively or surreptitiously installed on their computers." See "Schwarzenegger Signs California Anti-Spyware Bill", Sept 28, 2004, http://www.reuters.com/newsArticle.jhtml?storyID=6359582.

[39] Declan McCullagh, "Bill would force Web sites to delete personal info", February 8, 2006 http://news.com.com/2100-1028_3-6036951.html.

distinctions, the consequences of misuse of that information could be exactly the same in each scenario.[40]

8.3.2.2 Canada

Across the Atlantic, Canada comes closest of the North American countries to embracing the European approach. There is now federal legislation in place to ensure comprehensive protection of data privacy in relation to both the public and private sectors, such as *Privacy Act of 1982*, *Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000*.

The PIPEDA came into full effect on January 1, 2004, which would apply to all businesses in Canada that use direct marketing and/or data mining, that collect, store and communicate personal information respecting employees and/or customers, and businesses with partners and business allies, or outsource company functions of this nature. The Act specifically requires that businesses disclose the purposes for the collection of personal information and that they obtaining consent for such use. The Act also contains restrictions against repurposing or publishing/sharing that information.[41]

Some provinces have already enacted data privacy legislation in relation to provincial and local government agencies and/or the private sector.[42] Data privacy agencies exist at both federal and provincial levels. The Commission of the European Communities has formally ruled that, in general, Canada offers "adequate" protection for data privacy pursuant to Article 25 of the EU Directive.[43]

8.3.2.3 The Asia-Pacific Region

In this region, there exist a handful of relatively comprehensive legislative regimes on data privacy—most notably those in Australia, New Zealand, Hong Kong, Korea, and Japan.[44] The bulk of these jurisdictions—but not Japan—has also

---

[40] Brad Smith, "*Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation*", Nov. 2005, http://www.cdt.org/privacy/20051103microsoftprivacy.pdf.

[41] Brent Krause, "*An Overview of the Canadian Personal Information Protection and Electronic Documents Act*", Feb. 2001, http://www.gigalaw.com/articles/2001-all/krause-2001-02-all.html.

[42] See, e.g., Quebec's Act on Protection of Personal Information in the Private Sector of 1993.

[43] Decision 2002/2/EC of Dec. 20, 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (O.J. L 2, Jan. 4, 2002, p. 13 et seq.).

[44] Further on Australian law, see, e .g., Hughes and Jackson (2001); on New Zealand law, see Longworth and McBride (1994) and Roth (1994)—(looseleaf, regularly updated); on Hong Kong law, see Berthold and Wacks (2003); on Korean law, see Yi and Ok (2003) and Chung (2003); on Japanese law, see Case and Ogiwara (2003).

established data privacy agencies. New Zealand has been the fastest and perhaps most ambitious of these jurisdictions in the data privacy field; it was the first to enact data privacy legislation applying right across the public and private sectors.[45]

Australian, Korean, and Japanese legislation in the field was initially limited largely to regulating the data-processing activities of government agencies,[46] but has recently been extended to cover the private sector as well.[47] However, some of these extensions still leave large gaps in private sector coverage.[48] Other aspects of the laws in question also diverge from the EU model(s).[49] Not surprisingly, none of the countries concerned has yet been formally recognized by the European Commission as offering adequate protection pursuant to the EU Directive. By contrast, India is reported to be considering enactment of a data privacy law modeled on the EU Directive largely due to a fear that its burgeoning outsourcing industry will flounder without such legislation in place.[50]

Data privacy regimes in other Asia-Pacific jurisdictions tend to be rather patchy in coverage and enforcement levels. Thailand, for instance, has inserted data privacy rules covering the government sector, in legislation dealing primarily with freedom of government information.[51] Singapore has so far decided to establish a data privacy regime based on voluntary, self-regulatory schemes that are linked with its national trust mark programmer.[52] The primary catalyst for the schemes appears to be commercial concerns.[53]

---

[45] See Privacy Act of 1993.

[46] For Australia, see Privacy Act of 1988; for Japan, see Act for Protection of Computer-Processed Personal Data Held by Administrative Organs of 1988; for Korea, see Act on Protection of Personal Information Maintained by Public Agencies of 1994.

[47] For Australia, see Privacy Amendment (Private Sector) Act of 2000; for Japan, see *Privacy Law of 2003*; for Korea, see *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. of 1999*. Note too that several of the Australian States have enacted data privacy laws covering their respective government agencies and, to a lesser extent, the health sector. See, e.g., *Victoria's Information Privacy Act of 2000 and Health Records Act of 2001*.

[48] For example, with a few exceptions, the Australian legislation does not apply to "small business operators"; i.e., businesses with an annual turnover of AUD$3 million or less [see federal Privacy Act, sections 6C(1), 6D, 6DA & 6E)]. Another major gap is that the legislation does not cover the processing of data by employers about their present and past employees (as long as the processing is directly related to the employment relationship) [Section 7B(3)].

[49] The Japanese laws, for example, do not formally operate with a distinction between sensitive and non-sensitive data, and they make relatively extensive use of "opt-out" consent mechanisms.

[50] See Pedersen (2003).

[51] See Official Information Act of 1997, described in Opassiriwit (2002).

[52] See "Model Data Protection Code for the Private Sector of 2002"; Industry Content Code of 2002.

[53] For criticism of the schemes, see Greenleaf (2002).

8.4 E-privacy Protection in China

8.4.1 Current Situation and Development

China's laws and regulations do not generally provide comprehensive rights and protections to Internet users. There is often tension between formal legal rights and those recognized in actual cases. Considering a right to privacy, Article 38 of China's Constitution refers to a fundamental right of personal dignity, believed by most Chinese legal scholars to incorporate a right of privacy.[54] Article 40 provides for the freedom and privacy of citizens' communications, and bars other organizations and individuals from infringing on those rights. The same Article, though, contains restrictions on or permits deprivation of a citizen's privacy or correspondence rights by public authorities to "meet the needs of state security" or "investigate criminal offenses"—broad, ambiguous exceptions. Some of China's legislation alludes to a similar right of privacy. However, Chinese constitutional jurisprudence does not recognize a fundamental right of privacy in action.

Legislation governing Internet users contains the same dichotomy. Certain regulations partially recognize a right to privacy. For example, Internet users' personal information is protected against unauthorized public disclosure by electronic messaging service providers.[55] Users whose personal information is disclosed, in violation of this provision, can sue for damages and injunctive relief.[56] Similarly, it is illegal to use computer information systems to steal or disrupt others' information or jeopardize the lawful interests of citizens; violators risk civil penalties.[57]

User communications also enjoy protection, at least in theory. Regulations affirm the freedom and privacy of users' e-mails and ban others from infringing upon their privacy. Violators who illegally intercept, modify, or delete others' e-mails face criminal liability.[58] Even compulsory seizure of e-mails and other private telecommunications by the state is limited, according to the laws, to instances where the public security authority, public procurator authority, or the national security authority must do so to investigate a national security threat or criminal

---

[54] Art.101 of the China's "*General Principles of Civil Law*" protect both personal dignity and the "right of reputation" and have been construed by the Supreme People's Court to include the right to privacy. Most likely, Chinese legal scholars extrapolate this conclusion from the relevant SPC decisions. See *Privacy Protection in China's Cyberspace*, China Law and Practice, February 2003.

[55] Art.12, *Administration of Internet Electronic Messaging Service Provisions*.

[56] Art.19, Id.

[57] Art.25, *Protection of the Safety of Computer Data Systems Regulations*; Article 58(2), *Telecommunications Regulations.*

[58] Art.4.2, *Internet Security Decision*.

conduct.[59] Such seizures are formally governed by specific criminal procedure requirements.[60]

However, the state possesses the power to regulate Internet content and to demand that ISPs and Internet Content Providers (ICPs) turn over personal information of Internet users who violate the laws or post prohibited content (a term defined broadly). Upon official request, an ISP or ICP must provide the user's name, IP address, e-mail address, user name, information on any changes in IP address and use, and all data saved by the service provider's computer when the prohibited content or illegal conduct took place, including time, content, originating source, and system logs.[61]

Thus, while China ostensibly provides some protection to users in the form of legally guaranteed rights, these safeguards rarely function in practice.

Nevertheless, South China's Guangxi Zhuang Autonomous Region has already banned unauthorized publication or forwarding of the applicants' personal information by administrative permit authorities in a set of regulations that took effect on February 1, 2005.

Recently, in Chinese booming market economy, many people leave their personal data when filling out applications. But some data holders—hospitals, realtors, telecom, and ISPs—sell the information to others who will later come up with unwelcome phone calls or visits.

New mothers in Beijing, for example, find they have to answer many unexpected calls shortly after they are home with the babies—infant formula suppliers, baby haircutters, and insurance agents have already got a long list of potential customers from the delivery room. Also, a gang in Shanghai was recently found to have stolen other people's personal information, applied for credit cards in their names and made vicious overdraft amounting to RMB ¥ 470,000 (US$56,600).[62]

Therefore, it should be noted that the draft of *the Law for Personal Information Protection of the People's Republic of China*, completed in January 2005, after 2 years' deliberation, has been submitted to the Information Office of the State Council for processing. With a definition of personal information that is broader than just including privacy, the drafted law places a wide range of information under protection, including cell-phone numbers, family addresses, medical records, and occupation. Once the law is proclaimed, violators of personal information will be charged with administrative, civil, and even criminal responsibility.[63]

---

[59] Art.66, *Telecommunications Regulations*.

[60] Art.116, *Criminal Procedure Law*.

[61] Ministry of Public Security, *Questions Relevant to the Implementation of the Circular*.

[62] See "Lawmaker Urges Legislation to Curb Rampant Privacy Infringement", Xinhua News Agency March 6, 2005. It is also available at http://www.china.org.cn/english/2005lh/121920.htm.

[63] "Do We Need Legislation to Protect Personal Information?", Beijing Review, March 24, 2005, Vol. 48, No. 12, at Col. 44.

8.4.2 Ucloo.com Case Study

8.4.2.1 The Fact

Since early December 2005, Ucloo.com—an Internet portal that is said to hold personal files on 90 million people—has provided a service nicknamed "souren," meaning searching for a specific person. By paying RMB 1 (12 US cents) through one's mobile phone, it is possible to find personal information such as telephone numbers, addresses, and even details of marital status and credit ratings. A student was surprised that someone he had never met called him and knew what he had written in his schoolmate address book. Later on, he was told the man obtained his contact details from Ucloo.com.

Another portal called 5460.net has been accused of leaking its pool of 90 million data files on users to Ucloo.com. But those concerned from 5460.net said the company had never authorized Ucloo.com to use its data and it had no idea how the portal had obtained the files.

5460.net, which has a collection of schoolmate address information covering 90 million people, has said it may take Ucloo.com to court.

Under pressure, Ucloo.com has canceled the charged service and said netizens can use the service through e-mail and apply for corrections of the personal information kept by the portal.[64]

8.4.2.2 A Brief Comment

The primary concern is how the portal obtained the data in the first place. Those in charge of Ucloo.com said they had obtained the data through legal channels and all of the personal information they held had appeared somewhere on public Web sites. They admitted only a portion of their data came from 5460.net.

If what they said is true, we have reason to remind ourselves that we must use caution whenever we are required to fill in forms on the Internet, such as providing an e-mail address, because that is how personal information enters the public domain.

Personal information is often required if surfers wish to view certain documents or apply for an e-mail address, but Web sites should have an obligation to keep personal information secret.

Another concern is whether the portal has the right to use the data at all, even if it has obtained contact details by legal means. Apparently, when such information as a person's phone number, address, or even his or her family background or

[64] Zhu Yuan, "Web users worry about ease of obtaining personal data", China Daily Jan. 16, 2006 at p. 4. It is also available at http://www.chinadaily.com.cn/english/doc/2006-01/16/content_512461.htm.

marital status is involved, the person should be contacted for consent before the information is used.

As many reports in China have revealed, it is obvious those whose personal information has been put on the Web site have never given consent. If anyone gets into trouble because of the information provided on the Web site, the portal will be liable for legal penalties.

Although a notice on the Ucloo.com Web site says the firm is registered in the USA, yet, this does not mean it has the right to provide the service. This incident indicates that more detailed rules are urgently needed for the management of information on the Internet. The rise of the Internet has made life and work more convenient, but the risk of invasion of privacy has also increased because of the free flow of information.[65]

8.5 Conclusion and Suggestions

Internet privacy, without doubt, presents significant issues for consumers, industry, and the government. It is also without doubt that these issues have increasingly become the subject of private and governmental attention in the form of lawsuits and proposed legislation.

There are serious questions, however, whether such attention is, in fact, effectively addressing the risks of abuse that exist in connection with the use of personal information obtained from Internet activity, and what the costs may be for such attention.

As to China, the Internet development is still in the initial stage, regulations need posit the suitable stand to both promote the Internet evolvement and guarantee the user's interests. Regulations shall consider difference between countries while taking foreign laws as reference. Regulations shall also differentiate various Internet services while taking responsive measures.

Finally and overall, as the government has to ensure a better awareness among the citizens about the privacy risk of Internet and the adequate solutions the technical tools and the interactivity of the network provide. It is quite clear that the Internet's user is himself his own better identity protector. He might decide to prevent the arrival of cookies, to erase them, or block their sending; he might through techniques of encryption of anonymous protect the confidentiality of his message or its anonymity; he might reveal or not certain data, decide to communicate only with rated Web sites and use his access right to control their activities.[66]

---

[65] Ibid.

[66] Yves Poullet, Internet and privacy: any conclusions, http://www.droit.fundp.ac.be/textes/conclusions.pdf.

References

Berthold, M., and Wacks, R. 2003. *Hong Kong data privacy law: Territorial regulation in a borderless world*, 2nd ed. Hong Kong: Sweet & Maxwell Asia.

Boufford, John G. 1998. Privacy on the information highway. *U.N.B.L.J.* 47: 219.

Brandeis, L.D., and S.D. Warren. 1890. The right to privacy. *Harvard law review* 4: 193.

Bygrave, L.A. 2000. Determining applicable law pursuant to european data protection legislation. *Computer Law and Security Report* 16: 252–257.

Bygrave, L.A. 2002. *Data protection law: Approaching its rationale, logic and limits*. The Hague/London/New York: Kluwer Law International.

Bygrave, Lee A. 2004. Privacy protection in a global context—a comparative overview. *Scandinavian Studies in Law* 47: 319–348. privacy%20in%20global%20context.pdf.

Case, D., and Y. Ogiwara. 2003. Japan's new personal information protection law. *Privacy Law & Policy Reporter* 10: 77–79.

Chung, H.-B. 2003. Anti-spam regulations in Korea. *Privacy Law & Policy Reporter* 10: 15–19.

Ford, P. 2003. Implementing the EC directive on data protection—an outside perspective. *Privacy Law & Policy Reporter* 9: 141–149.

Gellman, R.M. 1993. Fragmented, incomplete, and discontinuous: the failure of federal privacy regulatory proposals and institutions. *Software L. J.* 6: 199, 230.

Greenleaf, G. 2002. Singapore takes the softest privacy options. *Privacy Law & Policy Reporter* 8: 169–173.

Henke, F. 1986. *Die Datenschutzkonvention des Europarates*. Frankfurt am Main/Bern/New York: Peter Lang.

Hughes., and Jackson, M. 2001. *Hughes on data protection in Australiam*, 2nd ed. Sydney: Law Book Co. Ltd.

Kuner, C. 2003. *European data privacy law and online business*. Oxford: Oxford University Press.

Longworth, E., and T. McBride. 1994. *The privacy act: a guide*. Wellington: GP Publications.

Opassiriwit, C. 2002. Thailand: a case study in the interrelationship between freedom of information and privacy. *Privacy Law & Policy Reporter* 9: 91–95.

Pedersen, A. 2003. India plans EU-style data law. *Privacy Laws & Business* (68): 1, 3.

Privacy and E-Government. Privacy impact assessments and privacy commissioners –two mechanisms for protecting privacy to promote citizen trust online. 1 May 2003, http://www.internetpolicy.net/practices/030501pia.pdf.

Prosser, William. 1960. Privacy. *Cal. L. Rev.* 48: 383.

Roth, P. 1994. *Privacy law and practice*. Wellington: Butterworths/LexisNexis.

Schwartz, P.M., and J.R. Reidenberg. 1996. *Data privacy law: a study of united states data protection*. Charlottesville: Michie Law Publishers.

Shaffer, G. 2000. Globalization and social protection: the impact of e.u. and international rules in ratcheting up of U.S. privacy standards. *Yale J. of Int'l Law* 25: 1–88.

Smith, Brad. Protecting consumers and the marketplace: The need for federal privacy legislation. http://www.cdt.org/privacy/20051103microsoftprivacy.pdf.

Smith, Marcia S. 2004. Internet privacy: Overview and pending legislation. Updated 6 July 2004, CRS Report for Congress. http://fpc.state.gov/documents/organization/35133.pdf.

Swire, P.P., and R.E. Litan. 1998. *None of your business: world data flows, electronic commerce, and the european privacy directive*. Washington, DC: Brookings Institution Press.

Waters, N. 2003. The European influence on privacy law and practice. *Privacy Law & Policy Reporter* 9: 150–155.

Westin, A.F. 1967. *Privacy and freedom*. New York: Atheneum.

Rice, Denis T. Privacy in cyberspace: A primer. http://www.howardrice.com/uploads/content/privacy_cyber.pdf.

Yi, C.-B., and K.-J. Ok. 2003. Korea's personal information protection laws. *Privacy Law & Policy Reporter* 9: 172–179.