THE INEFFICIENCY OF LEGISLATION AND GLOBAL STANDARDS ON INFORMATION PRIVACY: A PROPOSED SOLUTION

Garry L. White, C.C.P., C.D.P., C.N.E., C.C.N.A., PhD., Department of Computer Information Systems & Quantitative Methods , Texas State University, 600 University Drive, San Marcos, TX 78666. (512) 254-9103, gw06@business.swt.edu

James R. Cook, C.C.P., C.D.P., PhD. Department of Computer Information Systems & Quantitative Methods , Texas State University, 600 University Drive, San Marcos, TX 78666. (512) 245-3181, jc09@swt.edu

ABSTRACT

Privacy laws are of little value since the Internet does not recognize national jurisdictions. What is legal in one country, is illegal in another. Due to different cultures and values and government types, it is impossible to establish global standards and legislation to ensure privacy. This paper argues two possible solutions: 1) the user has the burden of ensuring his/her maximum privacy. This is done via client software and browsers. 2) Instead of a "one size fits all" global standard, international companies implement different company policies that meet the privacy regulations of different countries and expectations of those citizens.

INTRODUCTION

Computer technology has created a global community. No longer is commerce limited to geographical boundaries. Such changes in technologies and market structures have shifted competition from a national to a global scope [13]. Multinational companies have developed a global integration of information infrastructures that cross national borders and time zones [28]. In other words, global information infrastructures ignore jurisdictions. Two such infrastructures are the Internet and transborder data flows (TBDF).

The Internet provides global communication of web pages across judicial/government boundaries. TBDF is defined as international personal data circulation [26]. The United Nations Center on Transnational Corporations (UNCTC) defines TBDF as the movement of data across geographical boundaries. This may involve delivery of data through different countries and international organizations [26].

These two infrastructures allow direct interaction between a business and a customer anywhere in the world. There are no immigration or customs checks. Data flows across the globe just as it flows across a local area network. New ways of global e-commerce have been created. However, these technologies have created a new problem with privacy. Existing laws on privacy were never written to deal with such new technologies.

THREATS TO PRIVACY

The Internet and electronic commerce have created potential threats to consumers' privacy [20]. These privacy threats are invisible to most users [6]. Although many believe the Internet is anonymous, the reality is to the contrary. Client sources can be traced via the IP address. The operating system of the

client can be identified, and the date and time are recorded. The application can be identified, and the web site can place a "cookie" on the client's PC. A "cookie" keeps track of what the user is doing and sends it back to the web site. When the user enters personal information, more privacy issues come into play, especially if accessing a web server in another country. Only well educated users are aware of these issues and are able to deal with them.

Few web sites have explicit privacy policies and many fail to meet basic standards for privacy protection [11] [32]. Many federal agency web sites track users despite rules banning the practice [15]. Only a small percentage of web sites approach the type of privacy protection that would be provided by most rudimentary privacy laws in the U.S. [25].

The Internet is shifting away from the assumptions of anonymity upon which the Internet was originally designed [3]. Decisions about privacy are being driven by market forces and technology rather than by ethical or legal reasoning [6]. Laws, especially international laws, were never written to deal with such new technologies.

The privacy problem with TBDF revolves around what data or information can be collected, and how it is used. Since data flow crosses international boundaries, the use and collection of personal data will have different restrictions. What an international company can collect and do in one country, may be illegal in another country.

U.S. LEGISLATION

Some believe that legislation by Congress will provide the most effective way to provide information privacy [21] [25] [2] [10]. An example of such legislation was the Consumer Online Privacy and Disclosure Act (H.R. 347). This legislation would require Web sites to obtain consumer consent before tracking visitors [7]. However, such laws only apply to Web sites located in the U.S. What about the Web sites in foreign countries?

There is also the issue of the enforcement of such legislation. The FTC currently has this responsibility. A case in point is Hershey's operations of several web sites directed toward children. The FTC alleged that the company took no steps to ensure that a parent or guardian saw or filled out the consent forms [1]. Hershey is a U.S. company. What about web sites outside the U.S. that are directed to children?

The problem is that information privacy has emerged as an international issue. Privacy is a basic right in a democratic society [2]. However, other countries may view this differently. Hence, their privacy laws might be different.

EFFECTS OF DIFFERENT CULTURES

The architecture of the Internet is based on the principle of geographic indeterminacy. The information processing capabilities of the network were designed to make distance and geographic location irrelevant [23]. This leads to conflicts in data protection/privacy regulation differences among different countries. In other words, protection of personal data varies from nation to nation, as does the regulatory agencies governing them [26] [8].

Cultural and political differences contribute to this problem. Perception or the definition of privacy differs across cultures [16]. Some nations may or may not be overly concerned about the need for data protection to protect their citizens or corporations [26]. Some countries are democratic; privacy of

citizens is valued. Other authoritarian countries are less concerned about privacy of their citizens. This lack of harmonization poses a fundamental challenge to international data flows and the Internet [23]. Global international laws on privacy may not be the answer.

For example, the regulatory approach to privacy protection by many foreign jurisdictions is different from the U.S. [4] [31] [19]. The U.S. and Europe use very different approaches to information privacy. These differences have lead to regulatory and managerial conflicts [28].

Europeans have stricter protections than the U.S. [27] [22]. A European standard is that a business cannot pass personal information to a third party without the consent of the individual concerned [8]. The European Parliament rejected the "Safe Harbor" data transport privacy regulations approved after two years of negotiations between the European Commission and the U.S. [18] [17]. Safe Harbor finally did go into effect November 1, 2000. However, how will American customers and employees respond when a company is providing a higher level of protection to European residents than they are to American residents [30]? "Safe Harbor" essentially requires U.S. companies, when dealing with European consumers, to observe stringent European Union rules for disclosing consumer data. The European Parliament questions America's willingness to protect confidential data of European citizens [5].

"Privacy" has been on the agenda of the United Nations since the late 1970's [3]. Yet, today there is no global standard to ensure privacy with e-commerce and the Internet. Although e-commerce has forced nations to enact legislation to protect the information privacy of their citizens and corporations [26], these laws only apply to the legislation jurisdiction. When companies or customers deal with e-commerce or the Internet on an international level, these laws produce privacy conflicts. "One size does not fit all" with respect to regulatory implementations [16].

Reidenberg (2000) suggests that these privacy conflicts will be resolved by finding compatibility points, or by bringing together enacted legislation from the different countries [23]. This probably will never happen since cultural values on privacy are different.

Another alternative to legislation from different countries, is for companies to adopt standards of the strictest privacy regime as a company policy [8]. However, this can only be voluntary since laws vary across nations, and such strict policies could limit company operations in marketing and business transactions. Thus, one standard does not fit all.

ISSUES OF VOLUNTARY SELF-REGULATIONS

In 1980, the organization for Economic Cooperation and Development (OECD) published voluntary guidelines on privacy protection and transborder data flow [31]. However, such pursuits have not been successful. A problem with voluntary standards is consistency across international boundaries. The voluntary standard accepted in one country may be different in another country. For example, The European Union rejected voluntary standards, known as P3P, in January 1998. P3P proposed the protection of personal data with the use of cookies on the Web. The standards were too low, and the burden of enforcing privacy was placed on the users rather than on data controllers [14]. P3P was not legally enforceable, and thus there was no mechanism to ensure that organizations followed through with P3P [14].

Current efforts to promote self-regulation will not adequately address privacy on the Internet. Values and standards vary across international boundaries. Industry policies are incomplete, incoherent, and unenforceable. Thus, there is no effective means of enforcement [25]. Self-regulation is not an option; some things are just too important to be left to the free market [8].

BURDEN ON USERS

Privacy advocates argue that companies should ask permission before tracking users' online activities [24]. Users should have the right to prevent some transfers of personal information [12]. This leads to more user control of privacy. The user becomes more active in protecting his/her privacy.

The most recent versions of the two main browsers, Navigator and Internet Explorer, allow users a choice between receiving cookies from websites, or blocking them completely [9]. However, blocking is not the default setting. Blocking requires computer skills/knowledge that many consumers lack.

To resist threats to privacy, it has been proposed that legislation action control the information in government and business. Legislation action is also proposed to develop standards by the computer industry to safeguard computerized data. However, as pointed out in an earlier section of this paper, legislation is not an option. Individual vigilance is required [2].

These privacy threats are invisible to the user, but privacy protections are not. However, the use of privacy-protecting technology/software again requires time and skills/knowledge that many users of the Web lack [6].

CONCLUSIONS

Legislation, nationally or internationally, will never establish a common, global standard to ensure privacy. Cultures and values are too different. Both the user and international companies must carry this burden of privacy. Client software and web browsers must be designed to ensure that the user has control over his/her privacy. Even then, the user must be vigilant when accessing web sites, especially if they are in foreign countries. The user must also be skilled and knowledgeable with regard to computer security technology.

Although a theoretical model by Rudraswamy & Vance (2001) hypothesizes that, as the number of nations with adequate privacy laws attains a critical mass, remaining nations will adopt privacy regulations in order to effectively participate in the e-commerce area. Nations and their cultures are too different [26]. Some will not adopt privacy regulations that would effectively participate in e-commerce as defined by other nations. Companies and businesses are the ones that participate in e-commerce, not governments. Instead, it is hypothesized that:

1) International companies will implement different company policies that meet the privacy regulations of different countries and expectations of those citizens.
2) Users will become more educated and skilled with regard to computer privacy technology.

REFERENCES

[1] Anonymous (2003). Mrs. Field's Cookies and Hershey's Foods assessed largest penalties to date for COPPA violations. *Computer and Internet Lawyer*, 20(5), 30-31.

[2] Auerbach, I. (1985). Professional responsibility for information privacy. *Computers & Security,* 4(2), 103-107.

[3] Bennett, C. (2001). Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. *Ethics and Information Technology,* 3, 197-210.

[4] Cain, R. (2002). Global privacy concerns and regulation – Is the United States a world apart? *International Review of Law, Computers & Technology,* 16(1), 23.

[5] Cambanis, T. (2000). Data-privacy accord with U.S. faces renegotiation in Europe. *Wall Street Journal*, July 6, A.23.

[6] Camp, L. (1999). Web security and privacy: An American perspective. *Information Society,* 15(4), 249-256.

[7] Cantos, L., Porcelli, N. & Selby, S. (2001). House introduces legislation requiring consumer "opt-in" for Internet cookies. *Intellectual Property & Technology Law Journal,* 13(4), 22-23.

[8] Connolly, P. (2000). Privacy as global policy. *InfoWorld*, 22(37), 49-50.

[9] Craig, A. (1998). Cookie worries are unfounded, U.S. Government says. *TechWeb News*, March 16. Accessed from www.techweb.com/wire/story/TWB19980316S0015 on July 16, 2003.

[10] Dreazen, Y. (2002). The best way to… …guard your privacy. *Wall Street Journal*, Nov 18, R.4.

[11] Electronic privacy information center (1997). Surfer Beware: Personal Privacy and the Interent. Accessed from www.epic.org/reports/surfer-beware.html on 7/16/2003.

[12] Graham, J. (1987). Privacy, computers, and the commercial dissemination of personal information. *Texas Law Review,* 65(7), 1395-1439.

[13] Karimi, J. & Knsynski, B. (1991). Globalization and information management strategies. *Journal of Management Information Systems*, 7(4), 7-26.

[14] Matlis, J. (2002). P3P. *Computerworld*, 36(44), 28.

[15] Mearian, L. (2001). Report: Many federal Web sites use cookies. *Computerworld*, 35(17), 21.

[16] Milberg, S., Smith, J. & Burke, S. (2000). Information privacy: Corporate management and national regulation. *Organization Science,* 11(1), 35-57.

[17] Neeley, D. (2000). Privacy agreement reached. *Security Management,* 44(6), 34.

[18] Oriez, C. (2000). Safe harbor agreement reached. *Information Executive,* 4(10), 4.

[19] Oz, E. (1994). Barriers to international data transfer. *Journal of Global Information Management,* 2(2), 22-29.

[20] Pedley, P. (2002). Data protection for intranets and Web sites. *Business Information Review,* 19(3), 41.

[21] Petersen, S. (1995). Your life as open book: Has technology rendered personal privacy virtually obsolete? *Federal Communications Law Journal,* 48(1), 163-186.

[22] Rasmusson, E. (2000). The perils of international direct mail. *Sales and Marketing Management,* 152(4), 107.

[23] Reidenberg (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, 52(5), 1315-1367.

[24] Roha, R. (2000). Prying eyes. *Kiplinger's Personal Finance,* 54(8), 118-124.

[25] Rotenberg, M. (1999). Oversight Hearing on Electronic Communications Privacy Policy Disclosures. Subcommittee on Courts and Intellectual Property Committee on the Judiciary, U.S. House of Representatives, Rayburn House Office Building, May 27, 1999. Accessed on7/16/2003 from www.epic.org/privacy/internet/ EPIC_testimony_599.html.

[26] Rudraswamy, V. and Vance, D. (2001). Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment. *Logistics Information Management*, 14(1/2), 127.

[27] Simpson, G. (2000). Businesses criticize U.S.-EU privacy pact as hurdle to global e-commerce efforts. *Wall Street Journal*, April 6, A.24.

[28] Smith, H. (2001). Information privacy and marketing: What the U.S. should (and shouldn't) learn from Europe. *California Management Review,* 43(2), 8-33.

[29] Stephens, D. (1999). The globalization of information technology in multinational corporations. *Information Management Journal,* 33(3), 66-71.

[30] Thibodeau, P. (2000). Privacy legislation raises questions: Will Americans envy strong EU protections? *Computerworld*, 34(45), 1-2.

[31] Waples, E. & Norris, D. (1992). Information systems and transborder data flow. *Journal of Systems Management*, 43(1), 28-30.

[32] Yang, H. and Chiu, H. (2002). Privacy disclosures of Web sites in Taiwan. *Journal of Information Technology Theory and Application*, 4(3), 15.