Journal of International Information Management

Volume 11 | Issue 1 Article 3

2002

Using the Sayre Model to analyze Internet privacy

Richard V. McCarthy
Quinnipiac University

Jay E. Aronson
University of Georgia

Using the Sayre Model to analyze Internet privacy

Richard V. McCarthy
Quinnipiac University

Jay E. Aronson
University of Georgia

ABSTRACT

The Internet continues to evolve as a transportal of electronic commerce. It has penetrated into every facet of organizational life, from the ordering of commodity goods to providing a means to speed the recording and payment of federal income taxes. Internet usage continues to expand rapidly, surfacing issues in its wake that must be managed in order for it to ensure that it is viable as a long-term strategic tool for government and industry. To bridge the legal gap that has emerged as a result of the dynamic growth of the Internet, the United States Congress has acted to begin to address issues such as access to information and the unauthorized use of personal data. Though the issues themselves are not new, the amount of information and the rapidity of transfer of the information have been greatly expanded by the use of the Internet. This paper explores the relationship between the three dimensions (government, individual consumer needs and business as represented by industry groups) that are influencing the development of a legislated Internet privacy model.

INTRODUCTION

The rapid infusion of new technology frequently results in technological development that exceeds the pace in which management issues are identified and addressed. The development of the Internet has uncovered privacy and security issues that have resulted in the need to develop a combination of a technological and legal framework to address these issues. This paper explores the developing legal framework that is emerging to address the need to protect information that is collected and transmitted via the Internet.

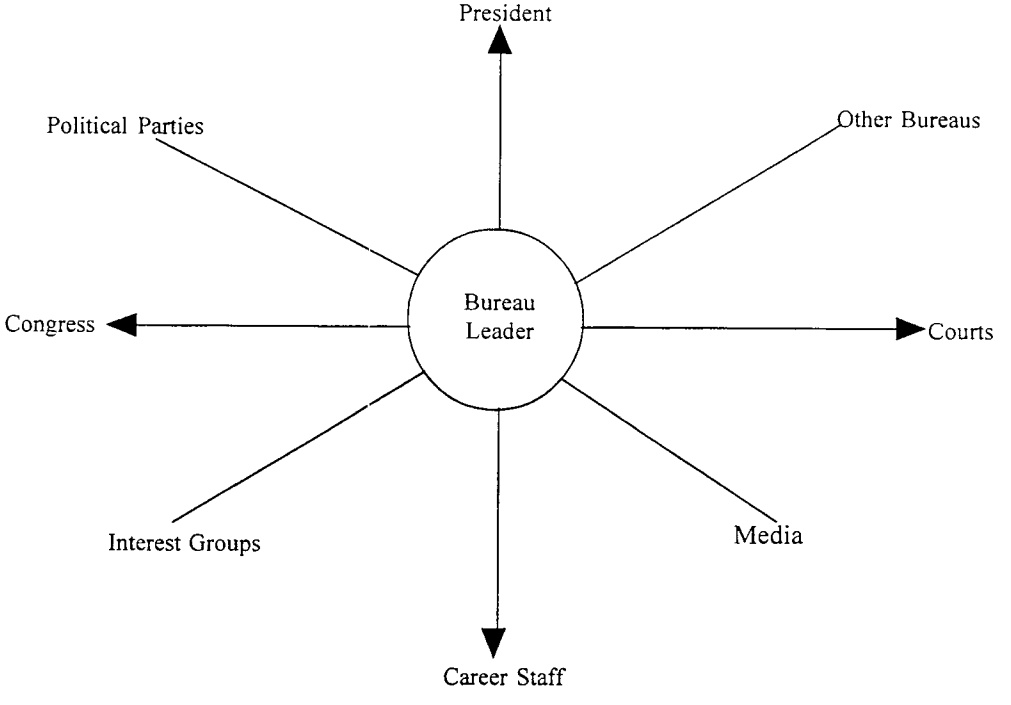
The Sayre Model of government decision-making was used to analyze the differing constituents perspectives that affect how to manage privacy and the Internet. It defines a framework for analyzing the legal framework that must be developed to safeguard personal information that is collected and utilized by organizations that have implemented e-commerce business models.

REVIEW OF THE LITERATURE

Federal Government Decision Making Model

The Wallace Sayre Model of decision in the Federal Government (see Figure 1) presents a set of nine action points that identify the critical power structures and interplay needed in order to implement programs and policies within the government (Held, 1979). The model is a useful representation to explain how domestic issues get transformed into policy within the United States. The nine action points comprise a wheel. Depending on the issue, each spoke on the wheel can be sub-defined to identify the key agents that influence the particular issue. For example, within the Congress, this can be split into the House and the Senate. Further, it can be split into the individual committees that comprise the House and Senate.

Figure 1. Wallace S. Sayre Model of Decision Making in Government



The Sayre Model suggests that interactions among these nine points are required to successfully implement a program or policy. Power structure spanning is required to make a program successful. The model provides a basis for critical analysis of each participant. This theoretical model describes the bureau leader as the focal point of a policy issue. This is based upon the premise that it is the bureau leader who is ultimately responsible for the implementation of policy. More recent adaptations of this model define the issue ad the central spoke. One of the reasons for this adaptation is the intricacy that has developed within the federal government whereby most policies require a coordination and cooperation of several bureaus in order to be successfully implemented. Additionally, the role of career staff has changed over time. More recently, senior level staff positions are held by political appointees.

The Need for Legal Framework

> "We are all at a critical juncture, a point where industry is asked to self-regulate at the behest of government and public trust. This choice, while daunting, presents an exciting and unprecedented opportunity for industry to take the lead in shaping public policy for this important new medium. Consumers are expecting that industry and government will work together to find new and better ways to make the Internet safe, inspire consumer confidence, and preserve the innovative spirit of e-commerce. But, the failure of industry to meet this challenge will not only have a negative effect on the future of e-commerce, but also on the public's confidence in industry's ability to take the lead in solving important public policy problems." (Thompson, 1998)

Widespread use of the Internet has brought to the forefront privacy issues such as confidentiality, authentication, and the integrity of personal information. It has created new security mechanisms, such as digital certificates, in an attempt to provide safeguarded controls over the information assets maintained by organizations. The extent to which organizations will self-govern the need to maintain confidentiality over information varies and therefore regulatory bodies have begun to immerse themselves in the Internet privacy issue. That is not to say that organizations have not recognized or even ignored the safeguarding of information received from customers. Akdeniz (2000) points out that the Cyber-Rights & Cyber-Liberties organization within the United Kingdom authored a privacy letter from a customer's perspective to be sent to Internet service providers to raise issues in relation to Internet Service Providers (ISP) privacy policies. The letter stated that, "it should be the duty of the ISPs to safeguard the fundamental rights and freedoms of Internet users to private communications, and in particular their right to privacy with respect in the processing of personal data which is explicitly protected by international agreements such as the European Convention on Human Rights."

Wang, Lee and Wang (1998) define the electronic invasion of privacy as the "unauthorized collection, disclosure, and other use of personal information as a direct result of electronic commerce transactions." The subsequently classify personal information into two categories. *Static private information* is defined as information that is not expected to change significantly over

time. This includes historical, medical and financial data, personal beliefs, and family relations. *Dynamic personal information* includes personal information that can be used to develop a personal profile, but is subject to frequent changes.

Tavani (1999) defines *informational privacy* as the set of issues related to the intrusion and inference of privacy. Technology can raise concerns in two important ways:

1. Technology that is used to collect information without the awareness of an individual and
2. Technology that is used to collect information but the individual has no say in the distribution of the information.

Data mining technologies utilized on Web-based databases present informational privacy concerns. Information about individuals can be excavated from their online activities to create profiles about the individual. Data mining inference software can then be used to analyze the profiles. Who assesses the validity of these inferences? In many cases, the individual has no knowledge that this has even taken place, so an incorrect inference can go undetected by the individual to whom it applies.

Consumer Internet privacy concerns can be classified into seven categories (Wang, Lee, & Wang, 1998):

1. Improper Access -- consists of accessing an individual's computer without their knowledge or consent. This is not limited to computer hacking, but also includes the unauthorized collection of information for marketing purposes.
2. Improper Collection -- consists of the collection of personal information such as name, address and e-mail address without the consent of the individual. This usually leads to an analysis and transfer of the information without the knowledge and consent of the individual.
3. Improper Monitoring -- consists of surveillance of an individual Internet usage without their knowledge and consent. This can consist of tracking which websites a person visits, how long they stay there, or whether they opted out after the home page.
4. Improper Analysis -- consists of analyzing and drawing conclusions from an individual's personal information without their knowledge and consent.
5. Improper Transfer -- consists of the transfer of an individual's personal information from one business to another without their knowledge and consent.
6. Unwanted Solicitation -- consists of the transmittal of material (such as junk e-mail) to an individual without their request.
7. Improper Storage -- consists of the capture and maintenance of personal information by a business in an insecure manner.

Has Cyberspace become evasive? Clarke (1999) points out that the profile data can easily be combined with push driven technologies to send out personal information about customers to constituents who were not intended to receive that information. Storage technology has continued

to increase in capacity allowing for almost limitless amounts of data to be obtained and transformed into corporate assets.

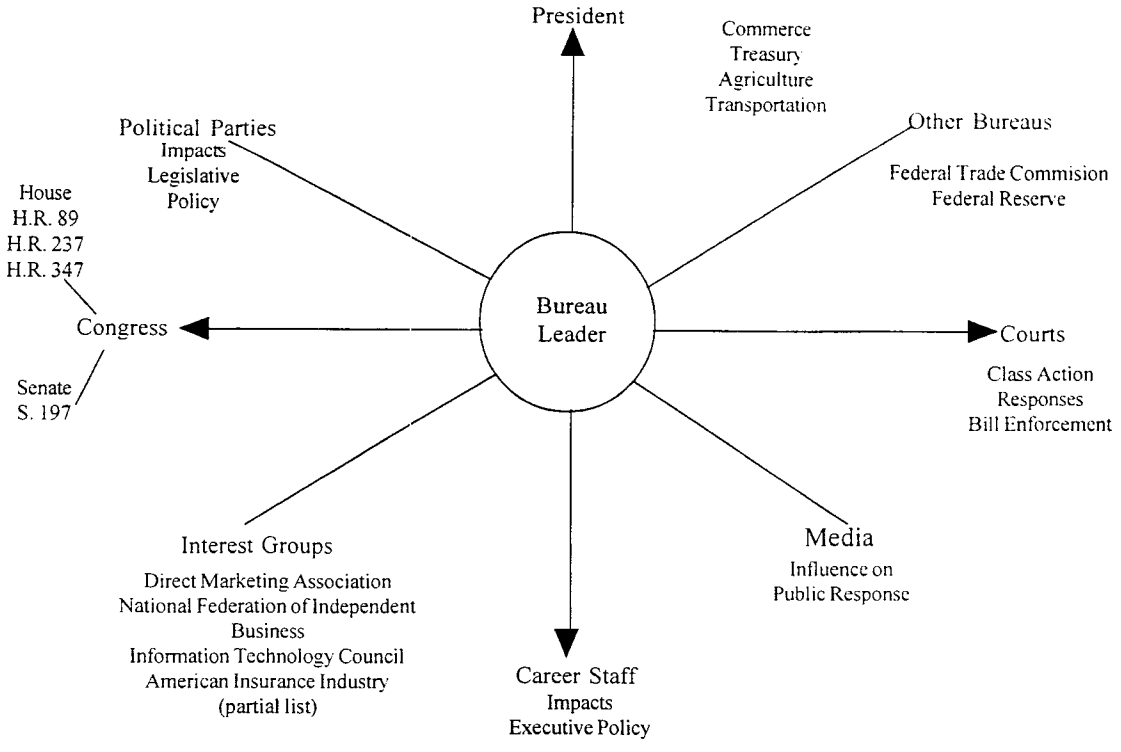
THE SAYRE INTERNET PRIVACY MODEL

The Sayre model of decision-making provides a framework to analyze privacy and the Internet from the perspectives of the multiple constituents that impact the issue. There are significantly differing perspectives as to how this issue should be addressed. The interest groups represent the industry perspective that centers on the implementation of a self-regulated technological solution. The implementation of an Internet Privacy Model will require that the self-regulation and legislative components coexist to achieve the balance between privacy of information and the continued use of the Internet as a cost effective method of transacting business. There are several important criteria to consider. The technological solutions proposed by businesses will help to ensure that personal information collected via the Internet is safeguarded; with the expectation that this will increase consumer trust and therefore usage of the Internet. The legislative proposals begin to develop a framework to provide legal protection for the privacy of information. The role of the political parties in the Sayre Model for Internet Privacy (see Figure 2) is crucial because one of the driving forces that keeps this issue alive in the Congress is that it polls well amongst consumers. The economic criteria should consider the ultimate cost to business in order to be in compliance. Thus far, the proposals themselves do not appear to be costly to implement.

Industry groups recognize that the Internet privacy issue is likely to have legislation enacted. The Information Technology Industry Council (Adkins, 2001), pointed out the two issues that are key to their constituents are the development of a single standard that would be applied at the federal level and clear resolution of the Opt In-Opt Out issue. Federal standards should supplant the states developing their own privacy standards in order to have one uniform process. Opt In-Opt Out refers to the manner in which consumers would decide if they agree with a company's privacy policy. An Opt-Out approach requires that a consumer specify that they do not consent to the use of personal information for purposes other than the intended business transaction; if the consumer does not Opt Out then they give permission by default. An Opt-In approach would require that a consumer must specifically give permission to use personal information for other than an intended business transaction. Industry group positions have greater opposition to Opt-In policies because of the tendency for people to not Opt-In. Many industry groups have already adopted self-regulatory standards. For example, the Direct Marketing Association (DMA) Privacy Promise commits its members to provide customers with the ability to opt out of information exchanges (Bureau of Consumer Protection, 2000). DMA membership requires compliance with the privacy promise.

One of the critical incidents that have caused consumers to voice concerns over privacy of information on the Internet is the case of Toysmart.com. Although Toysmart.com stated that they would never share personal information regarding their customers with anyone, when the company went into bankruptcy they attempted to sell their customer database. Their argument was that the personal information they collected was a corporate asset and as such they had a right to

Figure 2. The Sayre Internet Privacy Model



sell it. The Federal Trade Commission filed suit against them alleging a violation of the recently enacted Children's Online Privacy Protection Act (COPPA). COPPA requires that parental consent be obtained by any operator of a commercial web site directed to children under the age of 13 (Federal Trade Commission, 2000). Though Disney Corporation has recently settled this case by purchasing the customer database and agreeing to destroy it, it points to the need to augment self-regulated efforts with a legal framework designed to protect the privacy rights if individuals (Stoughton, 2001).

There have been several privacy related cases that have been adjudicated recently, forming the initial basis for case law precedent for Internet privacy issues. Universal Image, Inc. vs. Yahoo! Inc. (No 99-13839-B, Texas, December 22, 1999) alleged that Yahoo deliberately breached an information-sharing contract when Yahoo withheld information on subscribers to their recently acquired Broadcast.com. Universal contended that Broadcast was obligated to provide registration and address information as well as provide links on Broadcast's Web pages. Universal also accused Yahoo of violating Texas' anti-stalking laws by tracking Internet users without their consent through the use of cookies. In two class action suits, consumers accused RealNetworks'

collection of personal information as a violation of their posted privacy policy (Orange County Superior Court, November 4, 1999 and Pennsylvania, November 10, 1999). RealNetworks offered a patch to individual consumers that would prevent them from tracking individual consumer Internet activity. In Judnick vs. DoubleClick, Inc. it was alleged that DoubleClick unlawfully obtained and sold private personal information as part of the acquisition of Abacus Direct Corp. Judnick accused DoubleClick of using technology to profile Internet users financial and confidential information without their prior written consent. This complaint has also caused the Electronic Privacy Information Center (EPIC) to lodge a complaint with the Federal Trade Commission against DoubleClick (Warner, 2000).

Privacy and Self-Regulation

Privacy of information has been an issue long before a computer ever transmitted the first byte of data. However, the need to safeguard and protect information has emerged as an explosive business issue over the past five years as a result of the multitude of Internet users. Privacy protection is an issue raised by consumers in part because of the fear of *identity theft.* The collection of personal information across the Internet did not create the issue of identity fraud. However, it has brought the issue to national attention due to the volume of personal information and ease of access that it offers. Social Security numbers have been made easily accessible across the Internet, and the theft thereof can lead to significant problems such as the disruption of personal credit history (Berghel, 2000).

Goldberg, Wagner, and Brewer (1997) point out the potential long-term privacy issues that the Internet presents. The multitude of long-term data storage that is capable of being maintained on the Internet makes it possible to collect personal information and store it for many years. This has the potential to create a *dossier effect,* whereby a single query can result in an extensive compilation of information regarding an individual. Candidates for political office have experienced the results of this effect by having minute details of their life that occurred thirty or more years ago broadcast by the media as part of the public record. Anonymity there is an important issue in the protection of privacy on the Internet. Goldberg, Wagner, and Brewer (1997) define anonymity into two categories: *persistent anonymity* in which the user maintains an online persona that is disconnected from their personal identity over a long period of time and *one-time anonymity* in which the user has a single session persona that is disconnected from their personal identity. Anonymity on the Internet, however, has also been used for illicit purposes, such as the illegal distribution of copyrighted material or the misrepresentation of an individual and their qualifications.

Some Web sites include privacy statements that specify how and why information that is being collected will be used. It may also specify whether the information is shared with or sold to third parties (Flammia, 2000). For example, the Web site of California Senator Barbara Boxer includes a privacy statement that states, "My Web site only collects the personal information you authorize and uses it only for purposes you have approved. I promise you that any information you provide will never be sold, rented, or otherwise distributed for commercial or political

purposes." It also includes links based upon privacy related questions that address:

- What information is gathered and how it is used
- With whom is the information shared
- What safeguards are in place to protect your information
- How you can update or correct personal information.

Detailed descriptions for each of the preceding are described within the links (Boxer, 2001). Senator Boxer's privacy policy is an example of the implementation of the requirements for Senate bill 2928 (described below) that constitutes a portion of the emerging legal framework to manage privacy on the Internet.

Technological safeguards have begun to emerge in response to the need to safeguard information. It is still too soon to tell if this is *too little too late.* Carnor (1999), points out that anonymity agents and pseudonym agents have been created to mask the identity of a user who does not wish to be specifically recognized. However, when a user wishes to transact business, such as an on-line purchase resulting in a merchandise delivery, they must identify themselves in order for the transaction to be completed.

The World Wide Web Consortium (W3C) has taken a lead role in the development of technological standards to address privacy practice disclosure for personal data that is collected over the Web. The Platform for Privacy Preferences Project (P3P) was initiated to develop a standard mechanism to enable users to be informed of the privacy practices of Web sites. It would than be left to the user to decide if they wish to proceed. This will be accomplished through the users Web browser by interpreting XML based privacy practices that will be established at the Web site. Microsoft Internet Explorer 6.0 is expected to support the P3P standard, and Netscape is also planning on adding this support in a subsequent release. A Web site server setting will inform the user that it supports the P3P standard. Future enhancements to this standard will include an ability for the user and Web site to negotiate privacy policy through the software. The P3P specification will support digital certificates and digital signature capabilities to authenticate that the user's P3P privacy requirements. The goals of the P3P standard are to:

1. Enable privacy practice disclosure on the Web
2. Ensure that any data that is exchanged conforms to the disclosure identified by the privacy practice statement (though the W3C indicates that they are not an enforcement mechanism)
3. Specify the necessary grammar and vocabulary to support this standard through XML
4. Develop protocols for the exchange of privacy disclosures (World Wide Consortium, 2001).

On September 1, 2000, Amazon.com drew attention to the effectiveness of self-regulated privacy policies by disclosing that it reserves the right to sell data that it holds on twenty-three million customers should it ever be acquired (Rosen, 2000). In a survey of 2,000 Americans conducted by Pew Internet & American Life, as reported on by *Information Week* (Rosen, 2000) of online privacy concerns by consumers, five concerns were identified, including:

1. Unknown businesses or individuals obtaining personal information
2. Computer hackers obtaining credit card information
3. People lying about their identities
4. Someone tracking sites where individuals go to
5. E-mail being read by persons other than the intended recipient.

Hochheiser (2000) identified five factors that influence the development of self-regulated standards to increase the legitimacy and effectiveness of privacy protection tools. These include:

1. Transparency--Standards must be developed through an open and public process.
2. Notice--Information on standards must be publicly accessible and provided with sufficient lead time to all interested individuals.
3. Inclusion--Standards mechanisms need to be created for inclusion of perspectives from representation of members, both technical and non-technical.
4. Evaluation--Independent assessment of the impact of proposals needs to be evaluated prior to acceptance.
5. Education--Internet users must be educated about the efforts and products to standardize usage and safeguarding of information. This will also serve to build trust in standards.

The Federal Government Perspective

There are several interrelated bills that, is passed will begin to establish a legal framework at the federal level that all businesses must comply with in order to safeguard information that is collected and maintained across the Internet. These bills will be analyzed individually and collectively to evaluate their potential impact on the business to consumer relationship that is supported through electronic commerce across the Internet. In 1974, Congress passed the Privacy Act. The Act, which applies to federal agencies, restricts the collection, use and dissemination of personal information. The Computer Matching and Privacy Act of 1988 extended this protection for the exchange of information contained in databases. These acts are an example of recognition of the privacy issue by the Congress.

On May 19, 2000 the Federal Trade Commission proposed legislation that would require online companies to give consumers three basic choices designed to protect information they collected. These consists of either providing notice of any corporate privacy protection policy, the ability to correct any errors on personal information or a choice to opt out of participation on any information sharing program. The FTC conducted a survey of 335 Internet sites, and found that only 20 percent of the sites divulge plans for the sharing of personal information and allow the consumer to opt out. Congress supported these principles, but there is debate over what the role of the FTC should be in the regulation of privacy of information across the Internet (Ota, 2000). One of the most significant bills before the Congress dealing with this issue is Senate Bill 2928,

The Consumer Privacy Act, introduced in the 106th Congress by Senators McCain, Kerry, Abraham, and Boxer. The bill is designed specifically to protect the privacy of individuals who use the Internet. It states, "it is unlawful for a commercial Website operator to collect personally identifiable information online from a user of that Website unless the operator provides--(1) notice to the user on the Website in accordance with the requirements of subsection (b) and (2) an opportunity to that user to limit the use for marketing purposes, or, disclosures to third parties of personally identifiable information collected that is (A) not related to provision of the products or services provided by the website, or (B) not required to be disclosed by law" (McCain, Kerry, Abraham & Boxer, 2000). This bill provides a more specific definition to the right to have information that is gathered by organizations be used for its intended purpose. This bill extends the protection offered by Senate bill 2606, the Consumer Privacy Protection Act that was sponsored by Senators Hollings, Rockefeller, Bryan, Breaux, Inouye, Feingold, Edwards, Kerry, Cleclan, Durbin and Byrd and passed by the 106th Congress.

During the 107th Congress, Robert Frelinghuysen (D-NJ) introduced H.R. 89 Online Privacy Protection Act of 2001 into the House or Representatives. The bill calls for "the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet." Its purpose is to increase the protection of personal information that is gathered across the Internet and to begin to prescribe a framework for regulating privacy protection. The bill requires that within one year of enactment, Web sites will be required to provide clear notice as to what personal information is collected, how it is used and with what other companies the data are shared. It also requires that the Web site provide a simple process for individuals to consent to or limit the disclosure of personal information that is used for purposes that are unrelated to the purpose in which the information was originally collected. It also requires that Web site operators maintain reasonable procedures to protect the security and confidentiality of personal information. Failure to be in compliance could result in a civil action being brought against the party who does not provide the protection of personal information. This would provide for a means on the part of consumers to bring class action lawsuits against organizations that did not safeguard individual information. The Federal Trade Commission has taken the position that failure to comply with a stated privacy policy is a violation of the Federal Trade Commission Act (Peden, 2000).

Two other bills have been introduced into the House that addresses the privacy issue. H.R. 237, sponsored by representatives Eschoo and Cannon echo the intent of H.R. 89. However, it is more specific in its identification of the bureaus responsible for the enforcement of this responsibility. In addition to empowering the Federal Trade Commission with the responsibility for the enforcement of the safeguarding of personal information on the internet, this bill requires compliance under the Federal Deposit Insurance Act, the Federal Credit Union Act, the Packers and Stockyards Act, and the Farm Credit Act. In effect, it defines the coordination of responsibility between the Department of Commerce, Transportation, Treasury and Agriculture to ensure that the issue is dealt with effectively. H. R. 347, introduced by representative Gene Green, extends H. R. 237 but further stipulating that Internet profiling is prohibited. This would require that Web

site operators may not allow a third party to attach a cookie to an individual, as a means of creating a profile without the knowledge and consent of the individual. As a direct response to the Toysmart.com case, this act also prohibits the sale of consumer information in the event that a company becomes insolvent. The Spyware Control and Privacy Protection Act of 2001 (S. 197) represents an initial response by the Senate to also address the issue of privacy of information. It broadens the scope of privacy of information to include any computer software made available to the public, without limitation to the Internet as the channel of communication.

The emerging legal framework for Internet privacy must also take into account third party liability issues that arise from the use of an Internet service provider. Though not specifically proposed in response to the issue of Internet privacy, Rep. David Dreir (D-CA), has drafted H.R. 12 which opposes "the imposition of criminal liability on Internet service providers based upon the actions of their users" (Dreir, 2001). This act was drafted in response to the expansion of liability for Internet providers as stated in the Draft Convention on Cyber-Crime by the Council of Europe.

DISCUSSION

The Sayre Model provides a basis to analyze the complex legal framework that emerges when rapid technological advancement is not met a corresponding management structure to ensure that information is safeguarded in a secure environment. The Internet is beginning to mature as a commerce, collaboration and communication tool. Its explosive growth has led to a myriad of issues that were left unchecked until now, including the important need to ensure that personal information is safeguarded only with those with whom it is entrusted and only used for its intended purpose. Self-regulation has worked to some degree, in that while privacy is a concern for consumers, few people have suffered actual losses as a result of privacy related issues. Self-regulation in effect policies the companies who have adopted privacy standards but does not adequately address companies who ignore or violate those standards.

In a report to Congress (Bureau of Consumer Protection, 2000), the Federal Trade Commission reversed their position from 1998 and recommended that consumer-oriented commercial Web sites be required to comply with four information practices designed to promote privacy standards that could meet the needs of businesses and consumers. These standards include:

a. *Notice*--A clear notice of information practices must be posted on all Web sites describing what information is collected, how it is used, and how it is disseminated.

b. *Choice*--Consumers should be provided the choice for how their information is used for both external and internal secondary uses. It is implied, though not specifically stated, that businesses that report personal data to regulatory agencies (e.g., insurance and financial services) would be exempt from this stipulation for that purpose.

c. *Access*--Consumers would be provided reasonable access to review and correct inaccuracies in information collected about them.

d. *Security*--Web sites would be required to take reasonable steps to ensure the security of information collected about consumers, though the report does not attempt to define what are considered reasonable steps.

A uniform federal privacy of information program for the exchange of information across the Internet should not have a significant impact on many companies utilizing e-commerce. It should help to boost consumer confidence and trust in the use of the Internet.

FUTURE WORK

Validation of the Internet privacy model will be tested using a survey designed to assess the strength of the relationship between a company's Internet privacy policy and its affect on the consumers willingness to use the Internet as a means of electronic commerce. Future work will include a follow-up study on the effectiveness of the Internet privacy legislation and its effect on both businesses and consumers. A survey of the Fortune 500 companies is planned to determine their current Internet privacy policy and how they link to industry practices. Two follow-up studies will be performed. The first will investigate the status of the House and Senate bills and what new initiatives arise to react to the implementation of the bills. The second study will survey how Internet privacy policies and their implementation have changed as a result of a defined legislative framework.

REFERENCES

Adkins, B. (2001, February 20). Information Technology Industry, personal interview.

Akdeniz, Y. (2000). New privacy concerns: ISPs, crime prevention and consumers' rights. *International Review of Law Computers & Technology, 14*(1), 55-61.

Berghel, H. (2000, February). Identity theft, social security number, and the web. *Communications of the ACM, 43*(2), 17-21.

Boxer, B. (2001, February). Privacy policy, boxer.senate.gov/privacy/privacy.htm

Bureau of Consumer Protection, Federal Trade Commission. (2000, May). *Privacy online: Fair Information practices in the electronic marketplace, a report to congress.*

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

Cranor, L. (1999, February). Internet privacy. *Communications of the ACM, 42*(2), 29-31.

Dreir, D. (2001). Opposing the imposition of criminal liability on Internet service providers based on the actions of their users. H. R. 12, thomas.loc.gov

Federal Trade Commission. (2000, July). FTC announces settlement with bankrupt website, Toysmart.com, regarding alleged privacy policy violations. www.ftc.gov

Flammia, G. (2000, May). Privacy versus convenience. *IEEE Intelligent Systems,* 12-13.

Frelinghuysen, R. (2001). Online privacy protection act of 2001, H.R. 89, thomas.loc.gov

Goldberg, I., Wagner, D., & Brewer, E. (1997). Privacy-enhancing technologies for the Internet. *Proceedings of COMPCOM '97,* 103-109.

Held, W. (1979). Decision making in the federal government: The Wallace S. Sayre model. The Brookings Institution, White Paper, 1-22.

Hochheiser, H. (2000, April). Indirect threats to freedom and privacy: Governance of the internet and the WWW. *Proceedings of the Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions,* 249-254.

Kaiser, J. (1999, June 18). OMB mandates U. S. Web privacy notices, forms steering panel. *Privacy Times.*

McCain, Kerry, Abraham, & Boxer. (2000). Consumer Internet privacy enhancement act, S. 2928, thomas.loc.gov

Ota, A. (2000, May 27). FTC asks lawmakers for expanded authority to protect Internet privacy. *CQ Weekly,* 1273.

Peden, S. (2000, June 5). Clicking 'yes' for merger raises dicey web issues. *The National Law Journal,* 15-17.

Rosen, C. (2000, October 9). Internet legislation. *Information Week,* 95-96.

Stoughton, S. (2001, January 30). Toysmart.com list to be destroyed. *Boston Globe,* D7.

Tavani, H. (1999). Informational privacy, data mining, and the Internet. *Ethics and Information Technology,* 137-145.

Thompson, J. (1998, December 1). Managing the privacy revolution '98. *Remarks Before the 4th Annual National Conference on Privacy & American Business.*

Wang, H., Lee, M., & Wang, C. (1998, March). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63-70.

Warner, M. (2000, September 26). Recent legislation impacting technology. Presentation to the American Insurance Association Claims Officer Committee.

World Wide Consortium (2001, February). P3P 1.0 A new standard in online privacy, www.w3c.org