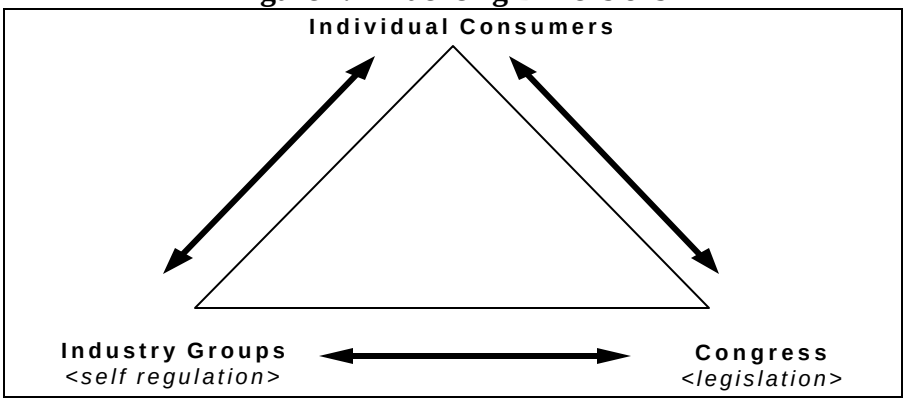
ANALYZING THE BALANCE BETWEEN CONSUMER, BUSINESS AND GOVERNMENT: THE EMERGENT INTERNET PRIVACY LEGAL FRAMEWORK

Richard V. McCarthy, Quinnipiac University, richard.mccarthy@quinnipiac.edu
Jay E. Aronson, University of Georgia, jaronson@terry.uga.edu

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 addressed 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 (Figure 1) (government, individual consumer needs and business as represented by industry groups) that are influencing the development of a legislated Internet privacy model.

Figure 1. Influencing Dimensions



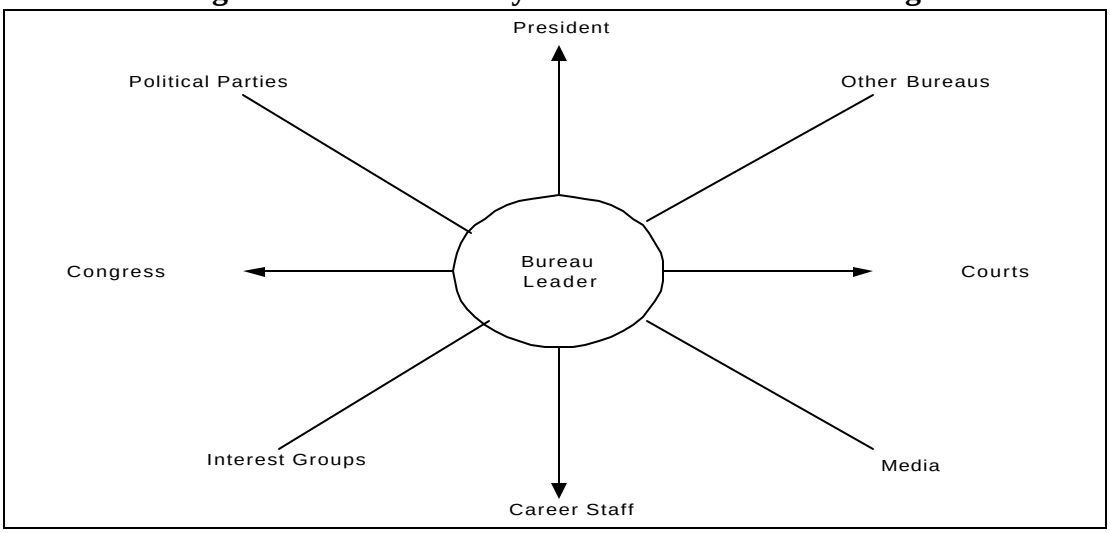
Keywords: Internet privacy, Sayre Model

FEDERAL GOVERNMENT DECISION MAKING MODEL

The Wallace Sayre Model of decision-making in the Federal Government (Figure 2) 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 [9]. 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 2 – Wallace S. Sayre Model of Decision Making



The Sayre Model suggests that interactions among the 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 as the central spoke. One of the reasons for this adaptation is the intricacy that has developed within the federal government whereby most policies require the coordination and cooperation of several bureaus to be successfully implemented. Additionally, the role of career staff has changed over time. More recently, political appointees hold senior level staff positions.

The Need for a Legal Framework

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 [2] 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 [12] 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." They 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 [11] 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
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.

Has Cyberspace become evasive? Clarke [5] points out that profile data can easily be combined with push driven technologies to send out personal information about customers to constituents that 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.

Privacy and Self-Regulation

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 to easily accessible across the Internet, and the theft thereof can lead to significant problems such as the disruption of personal credit history [3].

Goldberg, Wagner and Brewer [8] 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 therefore is an important issue in the protection of privacy on the Internet. Goldberg, Wagner and Brewer [8] 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.

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 then 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 [13].

Internet Privacy Legislation – The Federal Government Response

There are several inter-related bills that, if 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.

During the 107th Congress, Robert Frelinghuysen (D-NJ) introduced H.R. 89 Online Privacy Protection Act of 2001 into the House of 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 that will all privacy protection to be regulated. 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 [7]. 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 [10].

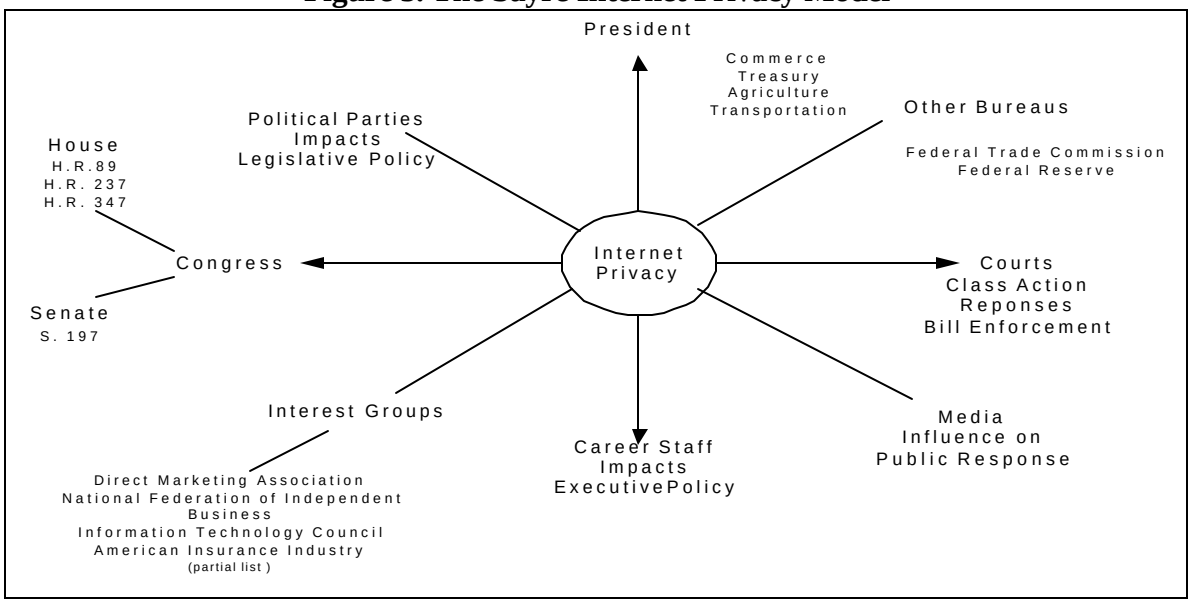
Two other bills have been introduced into the House that addresses the privacy issue. H.R. 237, sponsored by representatives Eschoo and Cannon echo the intent of H.R. 89 however; it is more specific in its identification of the bureaus responsible for the enforcement of this responsibility. In addition 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 by 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. This act also prohibits the sale of consumer information in the event that a company becomes insolvent.

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 Dreier (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" [6]. It was drafted in response to the expansion of liability for Internet service providers as stated in the Draft Convention on Cyber-Crime by the Council of Europe.

The Sayre Internet Privacy Model

The Sayre Model of decision making in government can be extended to include the implementation of an Internet Privacy Model that will require 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 that 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 (Figure 3) 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.

Figure 3. The Sayre Internet Privacy Model



Industry groups recognize that the Internet privacy issue is likely to have legislation enacted. Brian Adkins [1], from the Information Technology Industry Council, 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 companies 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 [4]. DMA membership requires compliance with the privacy promise.

CONCLUSION

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 polices the companies who have adopted privacy standards but does not adequately address companies who ignore or violate those standards.

In a report to Congress [4], 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:

1. *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.
2. *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.
3. *Access* – Consumers would be provided reasonable access to review and correct inaccuracies in information collected about them.
4. *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 companies 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

Available by request from the authors.