NEW ENGLAND COLLEGE

Establishing a Consumer Privacy Registry

Date: February 28, 2008
To: United States Senate
From: John Doucette and Lianna French
Student Leader for Proposal: John Doucette

Problem: The protection of citizens' privacy is a vital concern in the 21st century. New and readily available technology has simplified the processes of information collection and aggregation by business and government institutions. Internet use is particularly on the rise, with roughly 71% of the United States' population having accessed the internet regularly in 2007[1] for social, commercial and political purposes. Users are now able to instantly communicate, make purchases, file taxes, support political candidates, or apply for credit cards from the relative security of their own homes or any location where the internet is readily available. The US Census Bureau accordingly placed 4th quarter E-commerce sales for last year at $36.2 billion, up from about 4.2% in the 3rd quarter of 2007, indicating that a sizable portion of sales in the United States are taking place entirely online.[2] Accompanying these impressive opportunities, however, are certain risks which require federal consideration.

A major issue of contention is that many internet companies in particular have included a process for collecting personal information from consumers when making purchases and that such aggregated records are not strictly used for the purposes of the rendered product or service. Instead, they are often assembled into profiles which are used to determine if the consumer is a likely candidate for a third-party product. Even if the website or vendor is considered secure, it is not uncommon for businesses and organizations to collect and distribute this information to third parties interested in connecting with potential consumers. Though it is typical for these profiles to contain only the most basic of materials, such as a name or email address, they may also include sensitive information, like a home address, telephone number, purchasing records, or even a social security number. Such practices, even when adhering to the rules and regulations already in place, are a violation of privacy unless they are conducted with the affirmative consent and reasonable awareness of the consumer.

While the debate about consumer consent and choice may be generalized in terms of opt-in and opt-out, this distinction does not take into consideration the wide range of confusing mechanisms that supposedly offer consumers the opportunity to consent to secondary use of their information. The lack of an effective and comprehensive legal tool enabling consumers to specify how their information can be used provokes several undesirable results. An innocuous but irritating outcome is the receipt of spam email from advertisers. Current provisions to limit such advertising methods are unsuccessful

---

[1] U.S Census Bureau. Department of Commerce. *Computer Use and Statistics*. 2007.
[2] Department of Commerce. *U.S Census Bureau News*. February 15 2008.
< http://www.census.gov/mrts/www/data/html/07Q4.html>.

because they merely prohibit communication between the sender and recipient, rather than addressing the root of the problem, which is unreasonable access to personal information. More serious repercussions include criminal activity, such as fraud, identity theft, and the potential violation of privacy rights through the collection, sale, and exchange of personal information without the reasonable awareness of consumers. Not only is this a threat to consumers, but it is also damaging to businesses whose operational models depend on consumer confidence in the security of their collected information.[3] A widespread loss of confidence on the part of consumers could cause serious financial losses and a steadily worsening economic environment for businesses that depend on the willingness of consumers to share their private information.

Solution: Comprehensive legislation addressing the means by which businesses can collect, aggregate, and distribute personal information is necessary in order to protect the privacy of citizens. To accomplish this objective without placing an unnecessary burden on businesses, compromising valuable products and services, or violating the rights of free speech and expression, we propose the establishment of a national database modeled on the Do Not Call registry, which would record the preferences of each participating citizen, and specify how their personal information may be used, aggregated or shared with third parties. This database would be public and accessible by businesses and non-profit organizations and would be a fair and cost-effective alternative to current methods.

Business interests currently favor weaker opt-out privacy laws. Under these guidelines, businesses are free to collect, aggregate and share information unless the consumer deliberately opts out. This usually requires calling a phone number, being forced into compliance in order to complete a transaction, or sending an e-mail to an obscure address which is buried in the fine print of an associated contract. This system of opt out consent imposes minimum financial burden on internet companies, but does little to ensure that consumers are made aware that their information will be further circulated. In contrast, privacy advocates have typically favored mandatory opt-in rules, imposing the burden on companies to obtain the affirmative consent of each consumer when his/her information is shared with a third party. Many businesses oppose these policies because they impose such a steep financial burden that their business model becomes unsustainable. According to these methods, companies seeking to use personal information to enter new markets, target their marketing efforts, and improve customer service, would need to either contact one customer at a time to gain their individual permission to use information, or obtain this consent through obscure opt-out methods. An opt-in system, requiring the explicit consent of individual consumers, is always more expensive than an opt-out system., but provides consumers with a greater level of privacy. In contrast, an opt-out system, which infers permission if consumers do not explicitly object, is less costly , but is also a very inefficient means of preserving consumer privacy interests.

A national database would combine the low cost of opt out systems with the affirmative consent of opt in systems. Individuals would gain greater control over how their personal information is used, while businesses would be aided in retaining the full confidence of their consumers without the costs imposed by a requirement for contacting and obtaining

[3] Projecting the Economic Impact of the Internet: *The American Economic Review*, Vol. 91 (2001)

consent when information is circulated to third parties. The national database will be inexpensive to establish, maintain, and update as new technology develops and will end the legislative deadlock created by the current zero sum paradigm of privacy vs. cost.

Sources: In conducting research for this project, I discussed the legal issue with NH State Representative Jim Ryan and Associate Professor of Political Science Wayne Lesperance. Statistics were collected from the US Census Bureau of the Dept. of Commerce. Articles include: *The Impact of Privacy Rules on Retail Credit Markets*, Duke Law Journal (2008), *Social Implications of the Internet Paul DiMaggio*: Annual Review of Sociology, Vol. 27. (2001), pp. 307-336, Projecting the Economic Impact of the Internet: *The American Economic Review*, Vol. 91, No. 2, Papers and Proceedings of the Hundred Thirteenth Annual Meeting of the American Economic Association, (May, 2001) pp. 313-317.