A Commentary on the State of Online Privacy and the Efficacy of Self-regulation

Bill Luther

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr

Recommended Citation
Available at: http://open.mitchellhamline.edu/wmlr/vol27/iss4/13
A COMMENTARY ON THE STATE OF ONLINE PRIVACY
AND THE EFFICACY OF SELF-REGULATION

Representative Bill Luther†

I. INTRODUCTION .................................................................... 2125
II. THE COLLECTION OF INFORMATION ................................... 2127
III. THE FEDERAL TRADE COMMISSION STUDIES ...................... 2128
IV. THE PRIVATE SECTOR'S PERSPECTIVE .................................. 2130
V. CURRENT LAW ...................................................................... 2131
VI. THE CASE FOR STRONG INTERNET PRIVACY
    PROTECTIONS ....................................................................... 2131
VII. CONCLUSION ........................................................................ 2135

I. INTRODUCTION

The issue of privacy has arguably become the most pressing consumer protection issue in the American polity today. Indeed, in our so-called “information age,” the American economy puts a higher premium on the efficient accumulation and distribution of valuable information; in contrast to more traditional business paradigms of the industrial era that valued the efficient manufacturing and distribution of goods. As a result, the personal information of an American consumer is, literally, a valuable commodity to be cultivated, refined and traded. With the rapid consolidation of major sectors of the American economy—most recently and markedly in the financial services industry—this trend towards information gathering and distribution will only accelerate. As such, the personal privacy of American consumers is constantly under assault, and it is incumbent upon policy makers to deal with the issue of consumer privacy in a new, bold manner.

† Rep. Bill Luther is the United States Congressman for Minnesota’s Sixth District. He graduated from University of Minnesota Law School in 1970, cum laude. Rep. Luther was first elected as a Representative in 1995. He currently serves on the Energy and Commerce Committee including its subcommittee on Telecommunications and the Internet.
Nowhere is the rapid deterioration of consumer privacy more apparent than on the Internet and, in particular, on the World Wide Web. Two aspects of the Internet pose particularly daunting challenges with regard to consumer privacy and further highlight the pressing need for political action. First, the commercial dimension of the Internet uniquely drives the need to gather, analyze, and distribute consumers' personal information. As online advertising is often the chief revenue source for many Web sites, there is tremendous pressure to utilize germane consumer information for tailor-made marketing efforts. Second, the very technological nature of the Internet provides the means for commercial interests to (often surreptitiously) accumulate, analyze and distribute personal information with unparalleled, astounding efficiency. Together, these two aspects of the Internet create an informational black hole, wherein personal consumer information whizzes around cyberspace for commercial purposes, never again to be recaptured or controlled by the consumer from whom it originated.

As a member of Congress and the Energy and Commerce Committee's subcommittee on Telecommunications and the Internet, I have consistently argued that the federal government must put a stop to this wholesale erosion of consumer rights. 1 This argument is in direct contrast to those from the private sector that posit that the Internet and the free market should function un-fettered—that in time, Web site operators and businesses will "solve" the privacy problem of their own volition without government mandates. Conversely, I have consistently argued that the American consumer has a right to control the integrity of his or her personal information, and only government intervention can ensure the consumer is so protected. In this article, I intend to continue this argument. Specifically, I will argue that the threat the Internet poses to consumer privacy is real, and the private sector cannot be left to its own means to rectify the problem. Consequently, the federal government must act on behalf of American consumers to pass legislation that will adequately empower consumers to control the accumulation and distribution of their personal information.

1. As the moniker implies, the subcommittee on Telecommunications and the Internet has primary jurisdiction over issues affecting telecommunications—including both voice and data transportation. Moreover, the Energy and Commerce Committee's subcommittee on Commerce, Trade and Consumer Protection has jurisdiction over consumer protection issues—including those involving the Federal Trade Commission, which has taken a lead role on the issue of online privacy.
when they conduct their personal or commercial affairs online.

II. THE COLLECTION OF INFORMATION

The most basic and common method of collecting information in cyberspace uses a technological innovation known as “cookies.” Cookies are small text files placed on a computer from a Web site that was visited by the user or a third party. Cookies may be either “session” cookies or “persistent” cookies, depending on the duration they are allowed to reside on the consumer’s computer. Session cookies expire when the visitor leaves the Web site, while persistent cookies remain on the visitor’s computer for varying lengths of time (hours, days, weeks, months, or years).

Utilizing the placement of session or persistent cookies, Web sites and/or third parties (e.g., Internet marketing firms) collect two “types” of information with regard to consumers who surf the Web. The first type is relatively innocuous: a site can obtain non-personal information about visitors’ computers in order to understand how frequently and in what manner, they interact with the site itself. Thus, by placing a session cookie on each visitor’s computer, a site can determine the number of consumers who have visited the site. When the visitor leaves the site, the cookie terminates and is eliminated from the visitor’s computer.

The other type of information collected is known as “personally identifiable information” (“PII”). Web sites and third parties often compile PII about a particular visitor and use that information for targeted advertising. This process is known as “online profiling.” By placing a persistent cookie on a visitor’s Web site, the Web site operator or third party is able to recognize a repeat visitor and collect information about other sites the user has previously visited. Armed with such information, the Web site or third party, can (1) send a specialized, unsolicited email to the consumer, (2) instantly post tailor-made advertisements on the computer screen when the consumer visits the site and/or (3) sell the information.

In essence, persistent cookies transform the Internet consumer surfer into a mobile bulletin board. Every time a consumer visits a Web site, a cookie is placed on his or her computer; and when the consumer visits other Web sites, those sites know every site that consumer has visited and the type of activity conducted on those sites. For example, a Web site can learn the titles of books perused by a consumer who has visited an online bookstore. The equivalent in a brick-and-mortar shopping mall would be a consumer tacking
a Post-It™ note to a consumer's back for each store visited and for each product examined. This information is a valuable commodity for Web sites and marketers that enables them to advertise in ways heretofore unimaginable.

III. THE FEDERAL TRADE COMMISSION STUDIES

The Federal Trade Commission has been studying online privacy issues since 1995. Since 1998, the Commission has sent three reports to Congress examining the state of online privacy and the private sector's ability to self-regulate and adopt consumer privacy protections. Beginning in 1998, the FTC has evolved in its position on the efficacy of industry self-regulation. In 1998 and 1999, the FTC reported that, while the percentage of Web sites with adequate consumer privacy protections was low, the private sector should still be left to its own fruition to self-regulate on behalf of the consumer. However, the Commission's 2000 Report to Congress now posits that federal legislative intervention is warranted.

In examining the state of online privacy, the Commission used its four pronged “fair information practices” (“FIP”) as its basic, evaluative framework. That is, a consumer-oriented Web site must meet four criteria to be “qualified” as a site that provides sufficient privacy protection to visitors. According to the FTC, these four “widely-accepted” fair information practices are:

1. NOTICE—Web sites should notify consumers in a clear and conspicuous manner that they are collecting personal information about the consumer. Moreover, Web sites should inform consumers as to what information they collect, how they collect it (e.g., directly or surreptitiously by such means as cookies), how they use it, whether they disclose the collected information to other entities, and whether other entities are collecting information through the site.

2. CHOICE—Web sites should allow consumers to prohibit or “opt-out” of such information transfers if the transfers are not necessary to complete the online transaction or if the transfers go beyond the original use for which the information was provided.

3. ACCESS—Web sites should allow consumers reasonable access to the information the site is collecting and distributing.

Moreover, Web sites should allow consumers a reasonable opportunity to correct any mistakes in the information gathered.

(4) SECURITY—Web sites should take reasonable steps to protect the security of the consumer information they collect.

In its first report to Congress in 1998, the FTC reported that ninety-two percent of a comprehensive, random sample of Web sites were collecting a great amount of personal information from consumers who visited their sites. However, only fourteen percent of these sites disclosed *anything* with regard to their FIPs. In 1999, the Commission narrowed the parameters of its report by randomly sampling the most heavily-trafficked sites on the World Wide Web and by surveying the 100 busiest sites. The survey found that only ten percent of the randomly sampled sites even touched on all four of the FIP principles; and only twenty-two percent of the 100 busiest sites did so. Nonetheless, a majority of commissioners recommended that the industry be given more time to self-regulate.

The FTC's May 2000 Report to Congress largely utilized the same sampling techniques as the 1999 study. As a result, the Commission found that only twenty percent of randomly sampled Web sites partially complied with all four of the FIP principles. For the 100 busiest sites, forty-two percent of web operators met the criteria. While these figures represent continued improvement from previous years, the FTC acknowledged that Congressional intervention was now needed to ameliorate the problem of chronically low FIP-compliance rates.

The Commission recommended a legislative response that would require Web sites to abide by the fair information practice principles articulated above. However, the Commission also recommended that any legislative solution be flexible and foster self-regulation in recognition of the constantly-evolving nature of the Internet. As such, a wise piece of legislation would grant rulemak-

---

3. *Id.* at 23.
4. *Id.* at 27.
5. MARY J. CULNAN, GEORGETOWN U., GEORGETOWN INTERNET PRIVACY POLICY SURVEY REPORT TO THE FED. TRADE COMM. 6 (1999), available at http://www.msbe.edu/faculty/culnanm/gippshome.html. The Commission’s 1999 Report was based upon a Georgetown University study known as the Georgetown Internet Privacy Policy Survey. *Id.*
6. *Id.* at 12-14.
7. FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS, at ii (May 2000) [hereinafter 2000 REPORT].
8. *Id.*
ing authority to a qualified government agency (presumably the FTC) with general, as opposed to strict and specific, mandates.

IV. THE PRIVATE SECTOR'S PERSPECTIVE

Industry leaders in the private sector (and indeed, dissenting commissioners in the FTC Report) argue that such legislative action, at this particular time, is rash and potentially harmful. First, they agree that legislation is unnecessary given the progress illustrated by the FTC reports themselves. Since the Commission's initial findings in 1998, there has been a steady and discernible increase in Web site FIP-compliance rates—indeed as noted above, forty-two percent of the 100 busiest sites were FIP compliant in 2000 compared to twenty-two percent in 1999. This represents an almost one hundred percent increase. Similar trends can be extrapolated from the random sample of the most heavily-trafficked Web sites. As such, the industry argues, progress is indeed taking place at a rapid pace, and legislative intervention is unwarranted. The market will naturally "force" Web sites to adopt strong consumer privacy practices in an attempt to attract visitors and business.

Second, industry leaders point out that the ever changing, ever evolving nature of the Internet makes such legislative intervention potentially harmful. The World Wide Web looks quite different today than it did even two years ago. Indeed, even the number of consumers who surf the Web is far greater than it was years ago. In this volatile, competitive environment, the private sector is constantly innovating Internet technology to better serve American consumers in terms of substantive content and logistical efficiency. Legislative mandates could potentially stifle future innovation by inadvertently precluding beneficial Internet activities that have privacy implications.

Third, the industry argues that legislative privacy mandates would significantly diminish the chief source of revenue for most Web sites, viz., advertising revenue. SPAM operations, which send unsolicited e-mail usually to many people, would be unable to effectively send email to targeted consumers. More significantly, many argue the reason most Web sites are freely accessible is because advertisers are willing to pay Web site operators sufficient amounts of money for personalized marketing. That is, a Web site's unique ability to identify germane information about a consumer-visitor—and instantaneously present that consumer with a
tailor-made advertisement—is a powerful marketing tool heretofore unavailable in the private sector. Consequently, if privacy mandates were to restrict a Web site’s ability to gather crucial information about consumers, site-operators would lose a key technological advantage that generates advertising revenue and, consequently, helps keep the Internet relatively free.

V. CURRENT LAW

While consumers are afforded few online privacy protections under current law, the federal cupboard is not quite empty. Under the Federal Trade Commission Act, the FTC has broad authority to ensure general fair trade practices. That is, the Commission can level civil penalties against parties that are engaged in unfair and deceptive practices in and affecting commerce. Thus, if a Web site posts a privacy policy that does not conform with the actual informational practice of the site, the FTC can seek remedies for violations under the FTC act. Furthermore, the Children’s Online Privacy Protection Act (“COPPA”), which took effect last year, governs the collection of information from children under the age of thirteen. Under COPPA, commercial Web sites and online services must inform parents and obtain their verifiable consent before Web sites and online services may collect, use or disclose personally identifiable information obtained from children under the age of thirteen.\(^9\)

VI. THE CASE FOR STRONG INTERNET PRIVACY PROTECTIONS

The Internet offers opportunities to consumers never dreamt of ten to twenty years ago, and this statement is not hyperbole. To be sure, when legislating on matters affecting the Internet, Congress must be very cautious and deliberative to avoid inadvertently harming what is still a relatively nascent technology with enormous, unfulfilled potential. Thus, the issue of online privacy is a thorny one, for it does indeed affect the relationship between consumers and the Internet; and the nature of this relationship has a substantial impact on the manner in which the Internet will continue to develop and grow.

Nonetheless, Congress cannot simply remain inert in the face

---

10. *Id.*
of a disturbing trend whereby the personal, private information of consumers is wholly extracted, condensed, analyzed, and distributed for commercial purposes—all without the knowledge or consent of consumers. While Congress may recognize the enormous potential and the singularity of the Internet, in no way should Congress simply ignore the dignities of personal privacy in the name of technological advancement. There is simply no reason why Congress cannot effectively pass legislation that protects the privacy interests of American consumers while concomitantly fostering the Internet’s growth and development. Congress can and should strike a common sense, rational balance.

Last year, Rep. Edward Markey and I introduced the Electronic Privacy Bill of Rights Act of 1999, a comprehensive legislative mandate that deals with the issue of online privacy. This bill requires Web sites to adhere to the widely-accepted fair information practices to effectively protect consumer online privacy. Only by mandating Notice, Access, Choice, and Security will consumers be assured that they have reasonable control over their personal information. Without such legal requirements, the privacy protections afforded to consumers who surf the Web are largely illusory.

The requirements of Notice, Choice and Access are particularly crucial. There is no compelling reason why consumers should not have control over and a choice about their personal information. Quite simply, if people do not wish to share with marketers and/or businesses information about where they shop or which Web sites they visit, they ought to be able to conduct their personal or commercial affairs in anonymity. Consumers would not likely acquiesce to being monitored while shopping in a brick-and-mortar mall. They would not allow a party to know every store they visited, every product they looked at, every book they perused. Yet such monitoring is precisely what occurs on the Internet. Consumers cannot surf the Web with anonymity. When they conduct their personal or commercial affairs online, they are constantly tagged and analyzed from Web site to Web site. Their personal information is gathered and condensed only to be sold to third parties for marketing purposes. All of this happens in the blink of an eye, with astounding efficiency, and without consumers’ knowledge. There is simply no compelling reason to empower consumers in brick-and-mortar malls, but leave them helpless in cyberspace.

Moreover, in the traditional commercial-retail context, it is conceivable that consumers would often agree to divulge certain
personal information to take advantage of commercial opportunities. Indeed, if the collection and distribution of information is as beneficial as the industry opines, consumers will often allow commercial interests to know about their shopping habits or personal interests. Similarly, in the online context, it is conceivable consumer-surfers will not mind if certain personal information is collected and distributed. If Web sites provide clear and lucid notice to consumers on the nature of the Web sites collection efforts, consumers would conceivably appreciate the unique opportunities such efforts may afford. But the salient point is this: consumers must be given notice and choice. Just as they can in malls, consumers must be able to remain anonymous if they so wish.

Because of the potential business utility in providing consumers with privacy protections, many argue the Internet community and the free market will eventually provide consumers with such protections. Indeed, the evidence shows that an increasing number of Web sites are adopting all four of the fair information practices. However, this argument is problematic. First, the World Wide Web consists of millions of Web sites and billions of individual web pages—and those figures continue to grow in exponential fashion. As such, it is simply not reasonable to expect that a sufficient number of Web sites will naturally adopt consumer privacy protections. Even if, arguendo, a vast majority of site operators eventually and voluntarily impose privacy protections, millions (even billions) of Web sites will not. Thus, it is important to create a legal mandate that forces all sites to comply with FIP principles. Additionally, it is important to establish a private right of action whereby consumers can individually sue Web sites that do not comply. That way, the FTC will not have to be in a position to monitor the millions of potential sites in violation.

Moreover, certain businesses are in operation solely to collect information and sell it at a profit. Such businesses, whether they are online or not, are not affected by the utilitarian impetus towards self-regulation. Thus, in order to affect these types of businesses, a legislative mandate must require all Web sites to comply

with the FIP principles.

Nonetheless, a good legislative proposal must allow enough regulatory flexibility to capture the nuances and complexity of Internet technology. An effective way to achieve this is to delegate broad authority to a government agency—as does the Markey-Luther bill to the FTC. By granting the FTC rulemaking authority to promulgate the standards for FIP compliance, Congress would allow the government agency of expertise to account for the evolving nature of the Internet. Congress would not be "micro-legislating." Instead, it would allow the FTC to draw from its experience and expertise to work out the details. Moreover, any FTC rule is an inherently deliberative final product, because of the requirements of the Administrative Procedures Act. Due to the open nature of rulemaking, industry leaders and experts, (as well as consumer advocates, academics, and other interested parties,) have the right to publicly comment on and contribute to a proposed rule. After such a lengthy, open and deliberative process, the FTC can strike the appropriate balance that effectively protects consumer privacy while concomitantly fostering the growth of the Internet.

Lastly, periodic review of the effects of such legislation (such as required by the Markey-Luther bill) is essential to preserve flexibility. By requiring the FTC to report to Congress on the effects of such legislation five years after enactment, Congress or the FTC could subsequently amend the online privacy rule if the Internet evolves in an unanticipated manner or if the rule imposes unintended, harmful consequences.

The argument that privacy requirements will dry up crucial revenue for Web sites is a dubious one at best. First, it is not clear that a vast majority of consumers will choose to opt-out of information sharing arrangements. Second, many studies have shown that one of the biggest impediments to the growth of e-commerce is the widespread fear that one’s personal information is being used for the wrong purposes. If the federal government ensures the security and integrity of consumers' private information, it is logical to expect that consumers would subsequently increase their online

12. For instance, the FTC sites a study that estimates that privacy concerns may have resulted in as much as $2.8 billion in lost online retail sales in 1999, while another study suggests potential losses of up to $18 billion by 2002 if nothing is done to allay consumer concerns. 2000 REPORT, supra note 7. "This makes sense given that [re]cent survey data demonstrate that 92% of consumers are concerned (67% are "very concerned") about the misuse of their personal information online." Id.
commercial activity. As such, strong privacy protections can only help Web sites gain the trust of consumers, which will bolster their online businesses. Third, as the Internet continues to grow, it is unclear whether more, businesses and marketers will cease paying Web sites sizable amounts of money, because the sites are unable to effectively tailor their advertisements. Just as the explosion of television spawned a new age of advertising revenue (without the benefits of tailor-made marketing), the Internet's continued growth will offer businesses unique opportunities to advertise their products and services. To be sure, SPAM operations may be substantially harmed by strong privacy protections. However, this is probably a reasonable sacrifice given the overwhelming unpopularity of unsolicited email. SPAM, just as conventional telemarketing, can be severely restricted without jeopardizing the overall commercial viability of the Internet.

VII. CONCLUSION

While the Internet promises to be one of the most significant and positive technological innovations in human history, it also poses unique dangers on an equally unprecedented level. Because of the commercial and technological nature of the Internet, the personal privacy of consumers in the United States and around the world is in serious jeopardy. We conduct our online affairs in a fishbowl. When individuals surf the Web, their personal information is immediately collected, condensed, analyzed, and distributed at an astonishing rate. The result is a world in which individuals no longer have control over their own identity.

In response to this consumer crisis, it is incumbent upon Congress to act in a deliberative, yet decisive, manner. Because the private sector will not, and indeed cannot, effectively self-regulate on behalf of the American consumer, the federal government must require Web site operators to provide adequate privacy protections for those who visit their sites. At the same time, such a legislative mandate must be flexible enough to capture the complexity and nuances of the Internet. As such, Congress should pass legislation that delegates discretionary authority to the agency of expertise, authority based upon a mandate that Web sites comply with the fair information practices of Notice, Choice, Access and Security. Such an approach will ensure that consumers are afforded substantive and effective online privacy protections while concomitantly foster
ing the development and growth of this wonderful, revolutionary technology known as the Internet.