Does government regulation offer any better protection to market participants than private assurance?

Regulation and the Marketplace

By Karim Jamal
University of Alberta
Michael Maier
University of Iowa
***and* Shyam Sunder**
Yale University

Adam Smith laid the foundation for modern economic theory by positing that the self-interest of the merchant is the major force leading to good business practice. That fundamental idea has been elaborated to understand better how merchants develop reputation, and seek to signal their good character to consumers and differentiate themselves from less scrupulous merchants. While economists generally find those ideas to be quite persuasive, many others are not convinced. Demands for government regulation are often motivated by the belief that unscrupulous merchants drive a market "to the bottom." As we ponder the demand for regulation in a post-Enron world, a basic question arises: Under what conditions is government regulation better at protecting market participants than private, evolving, market-driven protections?

An intriguing answer to that question emerges if we examine a relatively unregulated area of market participant protection: e-commerce privacy. In the United States, the privacy of participants engaged in e-commerce is largely unregulated by government; instead, many commercial Web sites contract with third parties like TRUSTe and BBB Online to establish privacy protection codes and certify to Web surfers that the sites adhere to those codes. In the United Kingdom, on the other hand, e-commerce privacy is a matter of government regulation and enforcement by an agency created for that purpose. That difference provides us an excellent laboratory in which to compare the results of government-enforced protections to protections that evolve through market forces. Which type of protection best serves market participants?

Karim Jamal is the Alexander Hamilton Professor of Business at the University of Alberta. He can be contacted by e-mail at karim.jamal@ualberta.ca.
Michael Maier is a doctoral candidate in the Henry B. Tippie School of Business at the University of Iowa. He can be contacted by e-mail at michael-maier@uiowa.edu.
Shyam Sunder is the James L. Frank Professor of Accounting, Economics, and Finance at the Yale School of Management. He can be contacted at shyam.sunder@yale.edu.

PRIVACY PROTECTION

New e-commerce technologies have substantially increased the ability of online merchants to collect, monitor, target, profile, and even sell personal information about customers to third parties. In response to broad societal concerns about privacy, the Organization for Economic Cooperation and Development (OECD), the U.S. government, and the European Union (and its predecessors) began extensive discussions in the 1970s about developing a regulatory framework for privacy. Those discussions were guided by five privacy principles enumerated by the OECD:

Notice/Awareness: Participants should receive notice of an entity's information practices before they divulge any personal information.

Choice/Consent: Participants should be given options as to the uses of any personal information collected from them, especially for secondary uses that are unrelated to the original transaction.

Access/Participation: A participant should have access to the information recorded about him and be able to modify any information that is deemed incorrect.

Integrity/Security: Collectors must take reasonable

steps to ensure data integrity, convert it into anonymous form before using it for secondary purposes, and destroy untimely data.

Enforcement/Redress: There must be a mechanism in place to enforce the privacy policies.

In 1995, the EU parliament formalized its privacy law by passing the European Directive on Data Protection. The directive adopted the five principles and required the member countries to bring their national laws into compliance. The directive also requires each member government to create an independent government body to monitor the development, implementation, and enforcement of national data protection law.

In the UK, the monitoring and enforcement of the privacy law is carried out by a government body called the Information Commission. The commission has been active in publicizing the law, its role, and in taking enforcement actions. Its budget increased on average by over 50 percent each year during 1997–2002. The number of complaints it received about privacy violations rose from 4,178 to 12,479 during the same period. More information about the Information Commission can be obtained from a UK government Web site at *www.dataprotection.gov.uk*.

THE UNREGULATED U.S. MARKET

In our recent *Journal of Accounting Research* paper "Privacy in E-Commerce," we examined several aspects of privacy policies in Web commerce in the United States, where there is a general absence of government regulation. First, we examined the development of privacy standards by vendors of assurance services. Four privacy assurance providers (Truste, BBB Online, PWC, and WebTrust) offer competing privacy standards and associated Web-seals. We conducted an analysis of the standards of each of those organizations and found that organizations with the more demanding privacy disclosure standards (Truste and BBB Online) dominate the market for selling privacy seals. Lower quality standards (like WebTrust) find very few customers. There is a race to the top, not a race to the bottom.

Next, we examined the privacy policies of 100 high-traffic Web sites. In this part of the study, we conducted a field study to assess the quality of the sites' posted privacy policies. We used a "Web crawler" — a computer program — to identify which sites use their own or third-party "cookies" to track the actions of their visitors. The actual cookie usage is compared to the posted privacy policy and usage disclosure for each site. The first two columns of Figure 1 show that most Web sites post their privacy policies, disclose their cookie usage, and describe how they use the data they gather. Further, the Truste and BBB Online clients disclose such information more often than the other sites do. Since all Web sites do not use cookies (or allow third parties to use cookies from their sites), the percentage disclosure rates of cookie (and third-party cookie) usage in Figure 1 are relative to the sites who do use cookies (and third-party cookies) to track visitors.

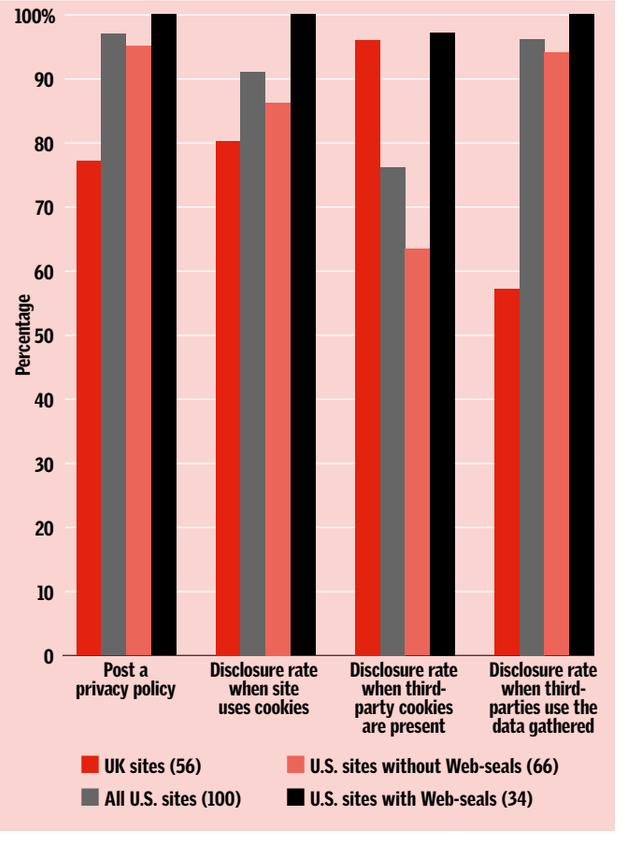
Next, we compared the stated policies and actual practices along a second dimension of privacy — effective implementation of "opt-out" choices by registrants. We gathered data by conducting a field experiment in which we register under two different names at each Web site. In one registration, we "opted-in," authorizing the site to send us commercial messages and share our data with third parties. In the second registration, we "opted-out" by telling the Web site not to allow the use of our "personal" data for secondary purposes by internal or external affiliates, partners, or contractors working with a site. We found that the opt-out choices made by the registrants were respected by all but a few Web sites. Out of 43 opt-out registrations, 12 generated no messages, 18 generated no messages after one confirmatory message immediately following the registration, and 13 generated multiple messages. Over a 26-week period, the average volume was 0.45 messages per registration per week. A single site generated 48 percent of those messages, and five sites generated 92 percent of all messages. When registrants are careful to opt-out at the time of registration, most Web sites do not violate their privacy. However, all registrants may not be as careful as we were in conducting this experiment, and 57 of the 100 sites did not even allow us to opt-out.

Out of 69 sites where we could opt-in at registration, 13 did not send us any mail, seven sent us one initial confirmatory message, and 49 sites sent us multiple messages. Over a 26-week period following registration, the average volume at 8.44

FIGURE 1

Notifying visitors

Disclosure of privacy policies on U.S. and UK Web sites.



messages per registrant per week was significantly higher than what the opt-out registrants received. Again, the messages came predominantly from a handful of Web sites; a single site generated 56 percent of all messages.

Whether registrants opt-in or opt-out, most sites follow good privacy practices and do not leak personal information about their customers to others. Unfortunately, it does not take many leaks to create consumer nuisance, and under both opt-in and opt-out registrations, a few sites do leak consumer data. None of the leaking Web sites carried a privacy certification by a Web-seal; watching out for a Web-seal is therefore an effective way of identifying and avoiding such Web sites.

U.S. privacy standards, policies, and disclosure practices of e-commerce sites have developed under a competitive regime in the absence of regulation backed by threat of sanctions. Our examination of the industry does not support the concern about chaos in the absence of regulation. Many sites do target their registrants with a large amount of message traffic in the opt-in condition, and a few even target registrants who exercise an opt-out option. The flood of junk e-mail annoys consumers, who may demand that the government restrict such commercial activity as the European Union did.

THE REGULATED UK MARKET

To test whether government regulation in the UK protects e-commerce privacy more effectively than the competitive approach in United States, we repeated our study by examining 56 high-traffic Web sites in the UK to address three key questions about regulation:

- Does legal regulation of privacy practices create demand for privacy certification (Web-seals)?
- Does a privacy law improve disclosure of privacy policies?
- Does a privacy law improve privacy practices and reduce commercial e-mail "spam"?

Web-seals In the U.S. sample of 100 high-traffic Web sites, 34 paid for a privacy assurance Web-seal from an independent party. None of the 56 sites in the UK sample displayed a Web-seal. It appears that legislated privacy standards and their enforcement by a government agency have not been accompanied by the development of a market for private Web assurance services. In the United States, Web sites can signal their good intentions to consumers by subjecting themselves to an examination by a Web-seal vendor. The signal helps consumers make informed decisions on which sites to visit or register at. This signaling system does not develop in the regulated UK environment, depriving consumers of the ability to avoid the scofflaw sites.

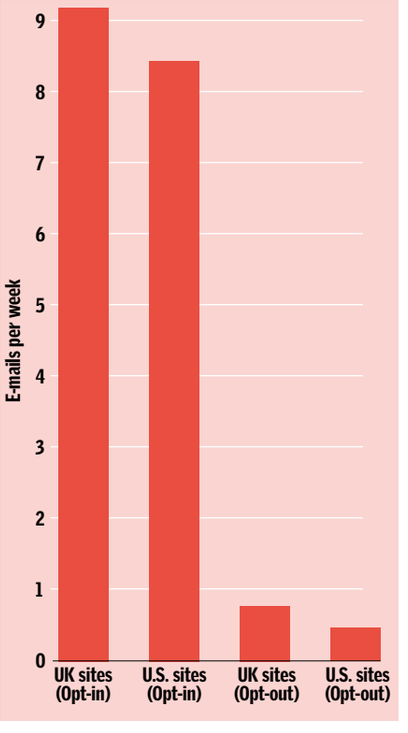
Privacy disclosure It is easy to locate the privacy policies of 97 percent of the U.S. Web sites. In most cases, a link to the policy is located at the home page. The UK law not only requires Web sites to provide their privacy policy before collecting any personal data, it also requires that the privacy policy be prominent, be easy to find, and easy to read. Yet, links to the privacy policy are more difficult to locate on the UK Web sites. After extensive search, we located the privacy policies of only 77 percent of the sites in the UK sample. Hence, the disclosure rates in the UK are lower than in United States. Overall, the privacy disclosures in the UK are no better than in the United States. Instead of trying to communicate their privacy policies to their customers, UK sites seem to focus on barely fulfilling the legal requirements. Still, a significant number of Web sites fail to comply with the law. If improving the ability of consumers to give their informed consent with respect to the use of their personal data is the intent behind the UK law, it does not seem to have been fulfilled.

Spam Compared to 0.45 messages per week from each U.S. opt-out registration, each opt-out registration in the UK generated 0.75 messages per week on average. The corresponding volumes from opt-in registrations at 8.44 and 9.20 per week, respectively, are higher by an order of magnitude. In both countries, a single site generated more than half of the total spam received (56 percent in the United States and 66 percent in the UK). As depicted in Figure 2, the UK privacy law overall is no better than the United States competitive regime in protecting the consumers from spam, either on average or in the worst-case scenario.

FIGURE 2

Spam attack

Average number of e-mail messages generated per week.



Fewer Web sites in the UK use cookies to track the behavior of their visitors (88 versus 98 percent in the United States). The use of third-party (Internet advertisers') cookies in the United States is more common (50 percent of the sites in the UK sample and 79 percent in the U.S. sample allow third parties to use cookies to track visitor activity). The UK law has successfully responded to the late-1990s concerns about cookie usage; however, spam became a concern later and the UK law has not been effective in reducing it.

CONCLUSION

The UK (and the EU) chose to protect the e-commerce privacy of its citizens through legislation and its enforcement by government. The United States, for the most part, allows the privacy policies

in e-commerce to evolve as norms of e-commerce without legislated standards or a punitive enforcement mechanism.

We compared the performance of the two regimes on two dimensions of privacy. With respect to choice/consent (i.e., participants controlling any secondary uses of their personal information), the two regimes do about equally well. The number of e-mail messages received by those who give their consent to receive such messages (opt-in) is about the same under the two regimes. Nor do the two regimes differ significantly as to the messages received by those who opt-out. Only a few e-commerce sites fail to honor the choices exercised by the registrants, and the number and spamming behavior of such firms does not vary significantly between the two regimes.

With respect to notice/awareness (i.e., participants receiving timely notice of a Web site's information and privacy policies), the statutory enforcement regime of the UK performs no better, and in some respects even less effective, than the competitive U.S. regime. For example, fewer UK sites post their privacy policies, and the posted policies are more difficult to find. UK Web sites that use cookies disclose such usage less often than their U.S. counterparts and are less forthcoming on how they use the data collected for secondary purposes.

In the absence of legislated standards and government enforcement, the United States has experienced the development of a market for Web assurance services, including privacy assurance. The U.S. Web sites that display the service providers' assurance seals perform at least as well as, and on average better than, the UK sites in protecting the privacy of their users. Our comparative study of the UK and the United States reveals that privacy has fared no better in the regulated UK market than in the unregulated U.S. environment.

Contrary to the claims made in the 1990s, the laws of economics remain unchanged in the dotcom world; the self-interest of Internet merchants still seems to drive most of them to respect the privacy of their customers. Attempts to use regulation to control the behavior of a few outliers in a market characterized by fast-changing technology are unlikely to be effective. Internet service providers with spam-weary customers of their own (e.g., AOL) are better able to adapt rapidly to spammers' changing technology and tactics. Those service providers, again pursuing their own interests, will be more effective than the government in reining in spam. R

READINGS

- "Enforced Standards versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Practices in the U.S. and the U.K.," by Karim Jamal, Michael Maier, and Shyam Sunder. Working paper, 2003.
- "Privacy in E-Commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market," by Karim Jamal, Michael Maier, and Shyam Sunder. *Journal of Accounting Research*, Vol. 41, No. 2 (May 2003).