TECHNOLOGY POLICY INSTITUTE

Studying the Global Information Economy

Statement of Thomas M. Lenard, PhD
President and Senior Fellow, Technology Policy Institute

Privacy and Data Security: Protecting Consumers in the Modern World

Before the Committee on Commerce, Science, and Transportation
United States Senate

June 29, 2011

Statement of Thomas M. Lenard, PhD[*]
President and Senior Fellow, Technology Policy Institute

Privacy and Data Security: Protecting Consumers in the Modern World

Before the Committee on Commerce, Science, and Transportation
United States Senate

June 29, 2011

Chairman Rockefeller, Ranking Member Hutchison and Members of the Committee: My name is Thomas Lenard and I am president and senior fellow at the Technology Policy Institute, a non-profit, non-partisan think tank that focuses on the economics of innovation, technological change, and related regulation in the United States and around the world. I appreciate the opportunity to testify before you today on privacy and data security. These issues are critically important for innovation in the digital economy, which relies on the flow of large amounts of information.

I would like to stress two points in my testimony: first, the importance of having reliable data and analysis for good policymaking in this area; and, second, that privacy and security are different and therefore should be dealt with separately.

[*] The views expressed here are my own and do not necessarily reflect the views of TPI, its board, or its staff.

Privacy

The privacy debate has engendered strong opinions, but relatively little data or analysis. In some respects, we had better data for policy making 10 years ago than we do now. In 2001, when the last of a series of four studies by researchers at the FTC and elsewhere was completed, we at least had baseline data on the privacy practices of commercial websites. During the period covered by the studies, the privacy practices of commercial websites generally improved. However, to my knowledge there has been no systematic study since 2001, so no one knows what commercial website practices are today and whether they are better or worse than they were a decade ago. Policymakers can't make informed policy decisions without facts about the practices prevalent in the marketplace.

In addition to basic data, the benefits and costs of alternative privacy regimes (including the status quo) need to be carefully analyzed in order to identify the policies that will best serve the interests of consumers. The commercial use of information online produces a range of benefits, including advertising targeted to consumers' interests; advertising-supported services and content, such as free email and search engines; and fraud detection and reduction in other threats, such as malware and phishing. More privacy means less information available for the marketplace and, therefore, potentially fewer benefits for consumers. Indeed, most privacy proposals are designed to make it easier for consumers to limit the amount of information firms collect and retain. The principal purpose of cost-benefit analysis is to make the tradeoffs inherent in greater privacy protection explicit and evaluate them.

On the cost side, a recent study found that the European Privacy Directive reduced the effectiveness of online advertising by about 65 percent. In other words, privacy protections make advertising less useful to consumers and, therefore, less valuable to advertisers. Advertisers will pay less for less-effective ads, which reduces the resources available to support online content. The authors found this was particularly so for more general (less product-specific) websites, such as newspapers.

Although only a few empirical studies of the costs of privacy regulation exist, even less information is available on the benefits. The benefits of privacy are the reduced harms associated with information being available or misused. If it is difficult to show harm from current practices—and thus far it has been—then it is also difficult to demonstrate that increased privacy regulation will produce benefits. We do know that people routinely give up some information about themselves in return for access to content and other services, such as email and online news subscriptions, and more useful advertising. This suggests that consumers are willing to give up some privacy for the value they receive.

The benefits and costs of specific proposals, such as a Do-Not-Track mechanism should be evaluated to make sure they improve consumer welfare. Some people may use a Do-Not-Track mechanism because they derive utility simply from knowing they are not being tracked. These potential benefits need to be weighed against the costs, which include the direct costs of implementation as well as the indirect costs in terms of the quantity and quality of services and content on the Internet. Many of these costs would be borne not only by Do-Not-Track participants but by other users as well. A Do-Not-Track mechanism (depending on how many people used it) could reduce the value of the Internet as an advertising medium, and therefore the

revenues available to support content for all Internet users. A Do-Not-Track mechanism could also affect the quality of major Internet services, such as search engines, which use data on search histories to update and improve their algorithms, and to protect against threats such as search spam, click-fraud, malware and phishing. The fewer data available to search engines, the less well they will perform. In sum, the information generated by online tracking generates positive externalities that support the services that everyone uses. Consumers who opted for a Do-Not-Track mechanism might be free-riding off those consumers who allowed their data to be used.[1]

The idea for a Do-Not-Track mechanism comes from the telemarketing Do-Not-Call List, which has been very popular. But the similarities between the two end at their names. People sign up for the Do-Not-Call List in order to reduce unwanted marketing solicitations. A Do-Not-Track mechanism would likely have the opposite effect. Consumers might receive a greater number of ads that are less-well targeted to their interests. This cost should also be taken into account. Several easily available tools let consumers block ads on the Internet, but a Do-Not-Track mechanism is unlikely to be one of them.

The three major browser providers—Google, Microsoft, and Mozilla—have announced that their products will include Do-Not-Track mechanisms. It is unclear whether this is a response to demands from consumers or to the specter of regulatory intervention. In any event,

[1] This is in contrast to the Do-Not-Call List. Signing up for the Do-Not-Call List would not appear to impose costs on other consumers.

these “market” solutions should be permitted to develop without any additional pressure or requirements from the government.

Data Security

With respect to data security, the most recent survey from Javelin Strategy and Research found that total identity fraud in 2010 was at its lowest level in eight years. While all types of fraud declined, and average costs per victim declined, mean consumer out-of-pocket costs increased, in part due to an increase in “friendly fraud”—fraud perpetrated by people known to the victim, such as a relative or a roommate.

Security presents a different set of issues than privacy. People may be comfortable with the intended uses of their data, but are worried about unintended uses and want their data to be secure. Identity theft—which involves the loss of personal data that poses a financial threat (such as a credit card number)—is perhaps the primary security concern of individuals. Regulating the collection and use of information by legitimate firms does not appear to make it more difficult for criminals to access information such as credit card numbers and, therefore, does little or nothing to deter identity theft. In fact, excessive control of information may increase the risk of identity theft by making it more difficult for sellers to determine if a potential buyer is fraudulent or not. Moreover, anything that encourages individuals to shift transactions offline is likely to be counter-productive.

There are two general responses to data breaches and related fraud—improved security to reduce the likelihood that such events will happen, and notification of the victims in the event

that they do happen. Both of these are addressed in the data security bills being considered by Congress.

Substantial evidence suggests that data breaches, identity theft and related frauds are very costly to the firms involved. The FTC, in a 2003 study, found that the costs of identity theft to businesses were about 10 times the costs to individuals. Credit card issuers and merchants are typically liable for the costs of fraudulent charges—a form of insurance provided to credit card holders. The costs to firms are reflected in the significant stock market losses they suffer when victimized by security breaches. Thus, companies have a strong incentive to spend money on data security and it is unclear that government action in this area is warranted.

Incentives for notification may be less strong. However, whether a regulatory notification requirement would make people better off is an empirical question. Are the expected benefits greater than the expected costs? This is a complicated question but several factors affect how we should view notification requirements:

First, even when consumers receive notice of a security breach, most of them do nothing about it. This lack of action is probably a rational response because even when data are compromised, the probability of identity theft is extremely small and actions like placing fraud alerts or closing accounts are not costless. Moreover, the costs of most instances of identity theft—i.e., credit card fraud—are incurred by firms and not individuals.

Second, we don't have good information about the range of consumer responses to notification. If consumers receive more notices, they may simply become indifferent to them. Or, they may become afraid to do business online. This would be a costly over-reaction because

online commerce is safer than offline commerce. Indeed, one of Javelin's principal recommendations in its annual reports is that consumers should move their transactions online.

Because of these factors, a notification mandate should carefully target those individuals most at risk of identity fraud in order to increase its potential benefits.

Perhaps the most significant benefit of federal data security and breach notification legislation would be preempting the patchwork of state laws. Since most companies operate nationally, a state-by-state approach is unlikely to work well. For that reason, enacting a carefully crafted federal bill could yield savings for firms and consumers.

Conclusion

The privacy and data security debates are extremely important to the future of the digital economy and of innovation in the United States. Unfortunately, they are taking place largely in an empirical vacuum. Without substantially better data and analysis, there is no way of knowing with any confidence whether proposals currently under consideration will improve consumer welfare.