Statement of Thomas M. Lenard, Ph.D.
Senior Fellow and Senior Vice President for Research
The Progress & Freedom Foundation

Privacy in the Commercial World II

Before the
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives

June 20, 2006

Statement of Thomas M. Lenard, Ph.D.
Senior Fellow and Senior Vice President for Research
The Progress & Freedom Foundation*

Privacy in the Commercial World II

Before the
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives

June 20, 2006

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Thomas Lenard. I am senior fellow and senior vice president for research at The Progress & Freedom Foundation, a non-partisan, non-profit "think tank" that focuses on public policy issues that affect the digital revolution and the information economy generally. Privacy and data security are clearly among the most important of these issues.

The advances in information technology that define the digital revolution have reduced the costs of gathering, storing, manipulating and transmitting information of all kinds. While the economic and social impacts of these advances have been overwhelmingly positive, they also have raised concerns on the part of individuals about what information is being collected, how it is being used, who has access to it and how secure it is. These concerns have been exacerbated by a series of high-profile data-security breaches that have exposed millions of individuals to potential fraud and convinced much of the public that we face an epidemic of identity theft.

* This testimony represents the views of the author and not necessarily those of the Foundation, its staff or its board of directors.

When considering whether and how to regulate, however, we need to be mindful that we truly do live in an information economy and that the personal information utilized by firms produces great value for consumers and the economy. It is the reason, for example, why any individual with a decent credit rating can get a loan approved virtually instantaneously. It also facilitates competition generally, making it easier for new firms to enter markets that require customer data. It is an area where the United States has a significant advantage over other countries that have more restrictive data and privacy laws and where consumer credit markets and other markets that rely on personal information don't work as smoothly.

Moreover, regulation will inevitably have unpredictable and unintended consequences, especially when imposed on a medium like the Internet that is changing so rapidly. Perhaps the most serious potential cost is a loss of innovation—new uses of information and of the Internet itself that would be frustrated by a new regulatory regime. There are many examples of ways in which information is now being used that were not contemplated when the information was collected, and which would be precluded by some of the measures that have been proposed.

In deciding whether additional regulation is desirable, and, if so, in what form, the following basic public policy questions need to be addressed:[1]

- Are there "failures" in the market for personal information?
- If market failures exist, how do they adversely affect consumers?
- Can such failures be remedied by government action?
- Will the benefits of government regulation exceed the costs?

The Market for Personal Information

Although privacy and data security are obviously inextricably intertwined, it is useful to think of them separately for the purposes of regulatory analysis. So, the first question is whether there are failures in the market for information and, in particular, whether consumers are being harmed by the legal use of personal information for commercial purposes. The answer is that, despite widespread perceptions that personal information is subject to misuse, there does not appear to be much in the way of evidence, even anecdotal evidence, of such harm.

Implicit in the proposals to regulate the market for personal information is that there is a market failure resulting in "too much" information being produced, disseminated and used. As a general matter, however, markets work better with more information. As the cost of information goes down, market participants obtain more of it and, consequently, make better decisions. For example, consumers benefit from receiving information that is better targeted to their

[1] For an elaboration of many of the points made in this testimony, see Paul H. Rubin and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, Kluwer Academic Publishers and The Progress & Freedom Foundation, 2002.

interests, as well as from not receiving information that is not of interest to them. Similarly, legitimate marketers have an interest in not sending messages to consumers who aren't interested in them. Merchants with more information can better estimate demand, reducing inventory costs and even lessening swings in overall economic activity. They can also use geographic computer-based information to put their new stores in locations that best serve consumers, and to stock the most useful merchandise for those consumers.

Information can correct market failures that would otherwise exist. For example, asymmetric information is a form of market failure that occurs when one party to a transaction has more information than the other. Both credit markets and insurance markets are potentially subject to problems of this sort, because lenders and insurers may have less information than applicants about the applicants' risk characteristics. Asymmetric information problems of this sort may cause lenders and insurers to be unwilling to offer transactions that consumers would want and that would benefit them. In general, increased use of personal information alleviates, rather than exacerbates, this type of market failure.

Moreover, the "public good" nature of information—once produced, it can be reused multiple times—means that advertisers, credit institutions and insurance companies all may use the same information. The ability to sell for advertising or marketing purposes information initially collected for credit or insurance rating purposes increases the value of that information. Thus, the

markets for advertising and marketing information generate increased information in markets that might truly be susceptible to asymmetric information market failures—e.g., credit and insurance markets.

The market also appears to provide incentives for firms to respond to consumers' privacy concerns in a variety of ways. Firms that violate consumer expectations about privacy face a loss of "reputation" that translates into losses in the marketplace. When a firm does something that is perceived as harming its reputation with consumers, the firm suffers a substantial loss in value. Firms, therefore, have a strong incentive to avoid undertaking policies that risk offending their customers. The Internet speeds the collection of information about consumers, but it also enables consumers to more easily obtain information about firms' activities on the Web. In addition, voluntary standards, defined and enforced by third parties or consortia of Web operators, are an important mechanism for providing information to consumers about Web sites' information policies. Finally, new technologies, such as spam filters, are available to consumers who are concerned about privacy.

Data Security

Data security presents a slightly different issue. While there may be no evidence of market failure or consumer harm from the legal use of personal information in commercial markets, that does not necessarily imply that firms have the appropriate incentives to safeguard the information under their control or take appropriate steps, whatever these may be, if the data are compromised.

The most recent data on identity theft and its costs (from a 2006 report from Javelin Strategy and Research) do not support the public perception that identity theft is a growing problem. They show that the costs of identity fraud have been essentially constant over the last several years for which data are available (which would indicate that, in a growing economy, they have been declining relative to total transactions). Since 2003, the number of victims of identity fraud has declined by almost 12 percent—to 8.9 million annually—while the average cost per victim has increased by over 20 percent. However, since most victims don't incur the costs related to their fraud cases, the average consumer costs have declined by 24 percent, although the time it takes consumers to resolve fraud cases has increased from 33 to 40 hours.

Other data suggest that costs have been decreasing over time. Estimates by Nilson show that over a longer period—1992 to 2004—the costs of credit card frauds decreased from $0.157 to $0.047 per $100 in credit card sales.[2] Similarly, Visa recently indicated that its fraud costs are at an all-time low of five cents per $100 of transactions. This is a reflection of the fact that credit card firms are continually updating and improving levels of security. The Nilson Report also indicates that fraudulent charges are lower as a percentage of credit card use in the U.S. than in the rest of the world; for example, credit card payments in the U.S. are three times the U.K. level, as compared with fraudulent charges, which are only about 1.2 times the U.K. level.

[2] These figures are for costs to card issuers.

It shouldn't be surprising that fraud costs per dollar of transaction are declining. About 90 percent of the costs of identity theft and related frauds are borne directly by businesses, including banks, credit card issuers and merchants. In addition, studies show that firms suffer large losses in stock value when security is breached. Interestingly, these studies are from a period before any consumer notification was required. Despite the perception that information about security breaches was unavailable prior to enactment of the California notification requirement, information about breaches did become public before that time—perhaps as a result of securities regulatory requirements—and markets reacted accordingly. Thus, even without any laws mandating notice to consumers, firms have had a very strong incentive to avoid data security breaches because the market penalizes them severely.

It is unclear whether firms also have adequate incentives to notify compromised consumers, so the issue is an empirical one: do the benefits of notification outweigh the costs? This issue was addressed in an economic analysis of notification requirements for data security breaches I recently did with Paul Rubin, who is a professor of law and economics at Emory University as well as an adjunct PFF fellow.[3]

We found that a notification requirement is dubious on benefit-cost grounds. The expected benefits to consumers of such a requirement are extremely small—probably under $10 per individual whose data have been

[3] Thomas M. Lenard and Paul H. Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches," The Progress & Freedom Foundation, *Progress on Point*, Release 12.12, July 2005.

compromised. There are several reasons for this. First, most cases of identity theft involve offline security breaches, which are not affected by notification requirements. Second, the probability of an individual compromised by a security breach becoming an identity-theft victim is extremely small. Third, most of these are victims of fraudulent charges on their existing credit accounts, for which they have very limited liability, rather than victims of true identity theft. Finally, even a well-designed notification program is likely to eliminate only a small fraction of the expected costs.

While the direct costs of notification may not be large, the indirect costs both to consumers and to sectors of the economy that depend on the free flow of information are likely to be substantial, primarily because of the likelihood that both consumers and firms suffering a security breach will overreact to notification. Firms in the information business may start limiting access to their information in an effort to reduce their risk exposure. Of particular concern is the prospect that the publicity associated with multiple notifications may induce consumers to shift their credit transactions offline, which the data show would actually increase their exposure to identity theft.

Effect on Competition

Many of the costs of privacy and data security regulations are likely to be relatively invariant with the size of the firm and therefore higher per unit of output for small than for large firms. Many of the costs are also what economists call “sunk” costs, which means they are not recoverable if, for example, the business

fails. This is an added burden that will deter start-ups and could have an adverse effect on competition.

Most importantly, any regulation of the information sector that raises the costs of targeted advertising and obtaining accurate customer lists has a greater adverse effect on new entrants and small firms than it does on large, established firms. This is particularly true for Internet advertising, where established firms have lists of their own customers and visitors to their web sites, but new firms must purchase such lists. As long as there is a market for customer lists and other such information, entrants can begin competing relatively easily. However, if regulation should reduce the size of the market and increase costs, competition from new entrants would be reduced.

Federal vs. State Regulation

Given the nature of the Internet, regulation at the state level has the potential to produce additional costs and impede interstate commerce due to inconsistencies. A true federalist approach is not possible with markets and firms that are national, and even international, in scope. Firms will tend to comply with a single set of rules. In the absence of a preemptive federal statute, they will comply with the most stringent set of state regulations, which will in effect "preempt" other state regulations.

Without federal preemption, companies are still faced with the prospect of familiarizing themselves with numerous different state laws to make sure they are

in compliance. The costs associated with this, which do not vary much with firm size, constitute a particular burden for smaller firms. Federal preemption of state privacy and data-security laws will reduce compliance costs and improve the benefit-cost balance.

Conclusion

The privacy debate represents some of the most complex policy-making challenges we have seen. This requires careful analysis of the actual proposals and their likely consequences to assure that, if adopted, their benefits are sufficient to justify their costs.

Thus far, and despite perceptions to the contrary, the evidence suggests that the market for personal information is working well and producing large benefits for consumers. Regulating in this rapidly changing technological environment, without evidence of significant market failure, runs the risk of adversely affecting innovation and slowing the progress of the IT revolution, with potentially adverse implications for growth and productivity.