TECHNOLOGY POLICY INSTITUTE
Studying the Global Information Economy

# Privacy and the Commercial Use of Personal Information: The Case of Customer Proprietary Network Information

**Thomas M. Lenard and Paul H. Rubin**

**August 15, 2007**

1747 PENNSYLVANIA AVENUE NW ▫ SUITE 850 ▫ WASHINGTON, D.C. 20006
PHONE: 202.828.4405 ▫ E-MAIL: info@techpolicyinstitute.org ▫ WEBSITE: www.techpolicyinstitute.org

THE PROGRESS & FREEDOM FOUNDATION

**Progress on Point**

**Release 14.15 August 2007** **Periodic Commentaries on the Policy Debate**

# Privacy and the Commercial Use of Personal Information: The Case of Customer Proprietary Network Information

**by Thomas M. Lenard and Paul H. Rubin***

## I. INTRODUCTION: PRIVACY AND INFORMATION

The expansion of the Internet has greatly increased our ability to collect, process, and use all kinds of information. Economists are interested in information, because economic theory teaches that, in general, better information leads to markets functioning more efficiently. This benefits all participants—buyers as well as sellers.

Better information improves the functioning of markets in several ways. First, better information produces more competitive markets, which drive prices closer to costs. Second, when consumers are better informed about their options, they are able to purchase products that better satisfy their preferences. Finally, when producers know more about their customers' preferences, they are able to sell products that are more likely to satisfy those preferences. Thus, the increase in information associated with the Internet would be expected to produce significant benefits for all market participants.

In addition to the benefits of increased information, however, there are potential costs in terms of lost privacy. There is a common concern that the increased flow of information is harmful, and that regulation should limit the amount of information available for use in commercial transactions, either by limiting the amount that can be collected in the first place or by limiting how it can subsequently be used. This concern takes two forms. First, there is a view that legitimate firms have too much information about their customers or potential customers, and that this somehow will harm those customers. The other fear is that more information will result in more illegal behavior, including various types of identity fraud—specifically, that collecting and using more personal information increases the risk of that information falling into the hands of criminals who will use it fraudulently.

* Thomas Lenard is senior fellow and acting president at The Progress & Freedom Foundation. Paul Rubin is Samuel Candler Dobbs Professor of Law and Economics at Emory University and adjunct fellow at PFF. This paper reflects the views of the authors and not their respective institutions.

Fears of the first sort do not seem to be warranted (Rubin and Lenard, 2002). There is little evidence—even anecdotal evidence—of any harm to consumers from the legitimate commercial use of personal information. On the contrary, the evidence indicates that the use of personal information for commercial purposes benefits both buyers and sellers, as economic theory would predict. For example, sellers are able to more precisely target ads at consumers with an interest in the product being advertised, so that buyers are able to learn about the prices and characteristics of products in which they have an interest. Conversely, sellers are better able to avoid sending ads to consumers who are not interested in particular items, saving time and resources for both buyers and sellers. Part of the reason for the discomfort with this sort of information use may be that humans do not fully understand that something can be "known" and used by a computer, without any human "knowing" the information.

Fears of illegal use of information are more justified—some information is obtained fraudulently and used for illegitimate purposes. However, even here, fears of misuse seem disproportionate to the actual risk. For example, in a study of laws requiring notice to consumers in the event of security breaches that could potentially compromise personal information, we found that the costs of such notice greatly outweighed any plausible estimate of the benefits (Lenard and Rubin, 2006). A recent study by the GAO (2007) reached a similar conclusion, although this study did not perform a cost-benefit analysis.

A variety of regulations, both in place and proposed, are aimed at countering these privacy concerns. For example, the European Union has strong rules in place that limit the use of information and the ability of parties to retain information. Other proposals require opt-in for various uses of information. Many states have adopted rules requiring notice to consumers when there is a possibility that their information has been compromised.

Studies of these rules have generally indicated that the costs are greater than the benefits. For example, in the EU it is more difficult to obtain credit quickly because privacy regulations make it more difficult for sellers to quickly identify buyers and check their credit (Ernst & Young, 2000). There is even evidence of greater fraud because it is more difficult to use information to validate the identity of borrowers or buyers (Staten and Cate, 2003). As indicated above, our study of notice requirements found that costs are much larger than benefits. It is important to subject any proposed regulations to a rigorous cost-benefit test because, in many cases, costs of existing regulation have been greater than benefits.

It is not surprising that many regulations are not cost-effective. Private parties in these markets often have strong incentives to provide optimal levels of security. For example, the value of credit cards is increased if they are secure, and credit card issuers are central in these markets, so they can and do perform a policing function to reduce undesirable behavior by various sorts of licensees or agents. In the case of identity fraud involving credit cards, consumers bear only a small part of any potential cost, since liability for a lost or misused card is limited to $50. Businesses bear most of

the costs. Therefore, credit card companies have issued internal regulations and rules and made substantial investments in order to increase security. Since costs are privately borne, it is unlikely that there is a market failure, and regulations are unlikely to provide net benefits.

## II. CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)

In the U.S., we have privacy laws directed at specific sensitive classes of information—e.g., medical and financial information—but we do not have a general privacy regime in place (as, for example, in the EU) that limits the collection and use of information for general commercial purposes. One class of commercial information that is regulated is CPNI, which is regulated by the Federal Communications Commission. A recently adopted rule (FCC, 2007) limits the use of CPNI data that telecom companies collect in the course of providing voice services. Moreover, there are legislative proposals for more stringent limitations on CPNI. Thus, CPNI provides a useful case study.

CPNI consists of detailed information about subscribers' use of telephones. It includes call detail records—phone numbers called by subscribers and the frequency and duration of calls—as well as information about telephony services purchased. The FCC regulations apply equally to all CPNI, regardless of its sensitivity. An individual's call detail records and the fact he may subscribe to call forwarding are accorded the same protections.

CPNI has both legitimate and illegitimate uses. For example, there is evidence that data brokers and others have obtained call detail information through "pretexting"—i.e., making false statements in order to obtain confidential personal information they are not entitled to have. Such information might then be offered for sale or used for other purposes.

There are also many legitimate uses of CPNI. For example, consumers might want this information themselves to verify charges on a phone bill. Such information can also be used for marketing purposes. It would be natural for telecom companies to use data from voice or dialup-Internet-service subscribers to identify those most likely to also subscribe to broadband service and to market to those individuals. This benefits not only the companies, but also the potential customers, since the marketing can provide them with useful information. It also furthers our social goal of increasing broadband deployment. However, CPNI regulations limit the telecom providers' ability to use customer information for this purpose.

Regulations should aim at restricting illegitimate uses of customer data without overly burdening the legitimate uses. Existing and proposed regulations fail this test. The recent FCC rulemaking on CPNI (FCC, 2007), and a proposed House of Representatives bill (H. R. 936, "To prohibit fraudulent access to telephone records")

both contain provisions to reduce dangers of pretexting, identity theft and other harmful outcomes by restricting the ability of entities to obtain this information fraudulently. But they also restrict legitimate uses in ways that probably do not provide measurable offsetting benefits.

While there are differences in detail between the two documents, they have some relevant provisions in common. They require, for example, that consumers create a password that must be used to obtain call detail information over the phone, and present photo identification to obtain such information in person. These provisions are aimed at reducing pretexting. They seem relatively harmless and perhaps useful in preventing various forms of fraud, although it is not clear that they improve on methods the telecom companies themselves already are using to prevent customer data from being illegitimately obtained.

Other provisions severely limit the ability of the telecom companies to use CPNI for activities such as marketing research and actual marketing, particularly when those activities are performed by outside entities. There are several problems with this approach to regulating information. First, and most fundamentally, as we discuss below, the FCC presents no evidence that reducing the sharing of information increases data security; in fact, the FCC presents some evidence suggesting that less sharing may reduce security.

Second, if information sharing is not allowed, then firms have two options, depending on how the rules are written. They can simply reduce the use of information for various purposes. This would be the only outcome possible if the regulations prohibit the use of information for purposes other than that for which it was originally collected, which sometimes is the case (and appears to be the case in the House bill). As we discuss below, using less information reduces consumer welfare.

If the rules are written to limit information sharing with outside entities—affiliates, contractors or joint venture partners—then the firm could possibly respond by restructuring itself in order to continue to use the information, by bringing the activities in-house, e.g., by increasing vertical integration or by purchasing related entities. This has costs but no benefits and, in fact, may reduce security.

## III. EVIDENCE ON DATA SECURITY

The basic question with respect to the FCC rule is whether sharing CPNI with outside affiliates poses a security risk. Somewhat surprisingly, given the rule it has promulgated, the FCC itself indicates that there is absolutely no evidence (or at least the Commission doesn't have any) of privacy problems resulting from sharing data with associated firms or joint venture partners:

> While the record does not include specific examples of unauthorized disclosure of CPNI by a joint venture partner or independent contractor, that does not mean unauthorized disclosure has not occurred or will not occur in the future. We see no reason why joint venture partners and independent contractors would be immune from this widespread problem (FCC, p. 26).

That the FCC itself acknowledges that there is no evidence of unauthorized disclosures by the very entities it is regulating should be enough to indicate that there is no justification for this provision of the rulemaking. In the absence of any evidence of harm, the rule will yield no benefits. Since there are costs (as we show below), then, by definition, the costs of the rule must be greater than the benefits.

How does the FCC attempt to justify its policy? In addition to the flawed logic above ("…we see no reason why joint venture partners and independent contractors would be immune…") it adds similar fallacious reasoning: "It is axiomatic that the more companies have access to CPNI, the greater the risk of unauthorized disclosure through disclosure by insiders or computer intrusion" (FCC, p. 26). From this set of ad hoc and unjustified inferences, the FCC apparently believes that its rulemaking passes the *Central Hudson* test, based on the empirically unjustified assertion that "(3) the more independent entities that possess CPNI, the greater the danger of unauthorized disclosure" (FCC, p. 25). But since there is no basis for this assertion, it cannot be used to justify a rule that otherwise violates the First Amendment by unduly restricting commercial speech.

Moreover, even if evidence did exist regarding misappropriation of information in the control of third parties, that would not be enough to justify the FCC rule. If firms are forbidden from sharing information, there are two possible responses. One is to simply use less information, as we discuss below. Another response is to undertake the marketing uses of information in-house. To show that the rule would be beneficial, it is necessary to show that breaches of security are more likely if information is shared than if it is used internally. The FCC does not even attempt to show this. Moreover, it would be impossible to make such a determination from the FCC record (FCC, p. 8 and elsewhere), which indicates that there is evidence of improper use of data from the carriers through pretexting and other methods, and no evidence of such misuse from data controlled by third parties. Thus, ironically, it is consistent with the existing FCC record to conclude that enforcement of the rule might lead to increased risk of data misuse.

Moreover, this analysis ignores the cost side of the issue. In fact, either response—increased in-house use of data or less use of data overall— involves significant costs to consumers. We now discuss these costs.

## IV. COSTS OF LOST INFORMATION

### A. Opt-in vs. Opt-out

Both the FCC rule and proposed legislative measures place significant restrictions on the sharing of CPNI—with joint venture partners or independent contractors and perhaps others—for marketing purposes. As with other privacy measures, they do this not by prohibiting outright the sharing of the data or the use for specific purposes, but rather by requiring the company to obtain the consumer's explicit consent for the use of his or her data. That is, the consumer must explicitly "opt-in" to the uses of the data. The other alternative—"opt-out"—would allow the company to use the data unless the customer requests that they not be used.

Somewhat surprisingly, the FCC suggests that the change from an opt-out to and opt-in requirement is a "minor modification" (FCC, p. 24). However, the evidence suggests that requiring opt-in is tantamount to an outright prohibition on the use of the data. For one thing, the FCC itself indicates that many consumers do not understand the options given to them, so that many would not understand what opt-in means (FCC, p. 23). Moreover, there is substantial evidence that consumers rarely change the default, so that under opt-in much less information would be used (see Rubin and Lenard, pp. 71-74). For example, in testimony before the FTC on the experience of one firm, a witness indicated that, when the default was opt-in, 85 percent of consumers chose not to provide their data. In contrast, 95 percent chose to provide their data when the default was opt-out.

Similarly, a US West telemarketing campaign was only able to obtain an opt-in rate of 29 percent among residential subscribers, and at a cost of $20.66 per positive response. These transactions costs are ultimately paid by consumers. Consumers also incur direct nuisance costs if they are at the receiving end of such campaigns.

Why do consumers accept the default? It may be because they don't consider the issue very important one way or the other. But it is more likely that the transactions costs associated with making a decision, which include reading a detailed notice and understanding the nature of the choice, are not trivial. That is, the costs associated with the process of opting-in or opting-out are not insignificant.

We, along with other economists—e.g., Eli Noam and Hal Varian—have argued that, in the presence of significant transactions costs, the correct policy is opt-out. If the default is opt-in, transactions cost prevent information from going to its highest-valued uses. The FCC asserts that the benefits of its "minor modification" outweigh the costs, but has done no analysis to back this up (FCC, p. 24).

Because the evidence suggests that only a very small percent of consumers would in fact opt-in, we treat opt-in as equivalent for all practical purposes to eliminating that use of information.

### B. The Value of Information

There is a view that information used in marketing is valuable only to sellers because it increases sales. Nothing could be further from the truth. Information is valuable to sellers because it does lead to increased sales. But it is valuable to buyers for the same reason. Since Adam Smith, economists have known that markets provide mutual benefits to buyers and sellers. Information is essential to this process, as buyers must learn what is available before they can make a purchase. Moreover, targeted information is particularly valuable since it can provide consumers with exactly the most useful information about products.

One of the most important economic characteristics of information is that the same information can be used in different ways, by the same party or by different parties. Once the initial costs of gathering and "producing" the information are incurred, additional uses can be undertaken at a relatively low marginal cost. This is an important source of value. It is sometimes argued that information should be used only for the purpose for which it was initially collected. This is part of the European Union Directive on the Protection of Personal Data, and is advocated by some as appropriate policy for the U.S. as well, including for CPNI. Such restrictions are particularly costly because of the multiple-use characteristic of information, and may preclude low-cost, high-valued uses of information that could otherwise occur.

### C. The Valuable Uses of CPNI

CPNI is valuable for all these reasons. It enables sellers to learn about the habits of particular consumers and tailor marketing and advertising to these consumers. Companies have used this information in designing Internet plans and for other marketing purposes. Here are some examples:

1. CPNI has been used to identify candidates for single billing services. For example, telecom companies have targeted customers who are already subscribing to more than one affiliate service and would benefit from seeing all their charges on one bill. This is a clear benefit to consumers, and informing them that they must now, because of CPNI rules, receive several bills instead of one would not be viewed favorably.

2. Telecom companies have used CPNI information for marketing campaigns. These data have been used to develop and offer various bundles of services including local, long distance and broadband services. They have also been used for marketing stand-alone Internet services and various small business services. Companies have created marketing campaigns for bundles of services targeted at customers who, based on their spending and usage levels, might save money by subscribing to these bundles.

Companies have also had programs to identify customers with certain calling patterns or types of services who might be better served by subscribing to particular plans. This use of data may have particularly large social benefits if it enables consumers to subscribe to faster Internet services and leads to increased benefits of the Internet.

3. CPNI data have been used for customer retention initiatives. Telecom companies have undertaken campaigns identifying customers whose contracts would soon be expiring to make sure they are aware of new plans that might be of interest to them. Companies have used CPNI data to make existing customers aware of new services and bundles of services based on the type of customer they are (residential or small business), and the types of services they have subscribed to and their past usage of these services.

4. CPNI has been used to research, innovate and create new types of service and packages of services. Data have been used to conduct customer surveys, research existing and potential new services, and conduct focus groups with regard to those services. Firms have used consultants to assist them in doing research and conducting focus groups, and identifying customers to participate in those focus groups using CPNI, to gauge receptivity to various products and services. This process has been used to design bundles that are today becoming increasingly popular with consumers.

5. Companies have conducted research to determine whether customers who subscribe to certain types of services would be viable leads for other services.

6. CPNI data have been used not only to identify customers that would be candidates for marketing campaigns, but also to eliminate some customers from some campaigns. This reduces the number of useless messages customers receive from marketers. Research might identify customers whose spending is below a certain level and would not be good targets for particular high-end services. Those customers would not be targeted for particular campaigns. Further, companies might want to exclude customers from campaigns for particular services, bundles and packages if they are already subscribing to that family of services or bundles. This exclusion is valuable to both consumers and firms. It is valuable to consumers because they are less likely to waste time reading useless messages. It is valuable to firms because they do not annoy their customers or waste resources on useless messages, and because consumers are more likely to read relevant messages if they do not receive as many useless messages.

7. Additionally, when aggregated, this information can be used in designing calling plans. For example, T-Mobile is currently advertising a "Favorite 5" plan. A company cannot offer such a plan without knowing a good deal about the particular calling patterns of its customers. Companies also offer plans that allow free calling at different times of day; again, such plans cannot be offered without the use of detailed call level information. While this information may be used in an aggregated form, someone must do the aggregating and the regulations as currently written are

sufficiently ambiguous that companies might be unwilling to undertake the needed analyses.

It is important to note that all of these uses of data benefit customers as well as companies. For example, if telecom companies design plans based on usage by customers, then those customers who purchase these plans are benefiting. If customers are offered a particular bundle and find it worthwhile to purchase this bundle, then they must find it better than their previous arrangement, and so again they benefit. Conversely, if a customer is not interested in a particular plan and companies can determine this and not market to that customer, then the customer also benefits by not receiving useless information. Moreover, this customer may pay more attention to other messages from the company if useless messages are weeded out, and will therefore be in a better position to learn about useful programs.

## V. COSTS OF INCREASED IN-HOUSE MARKETING

Firms always face the issue of whether to "make or buy" the inputs into their production processes. There are a variety of factors that go into these decisions related to the goal of minimizing costs and performing the activity efficiently. When these decisions are dictated by regulatory imperatives, efficiency is sacrificed and consumers end up paying the costs.

Moreover, it is important to note that there is an additional element at play here, because the structure of companies in the telecom market varies for historical reasons related to the regulatory regimes under which these companies operated in the past. As a result, CPNI regulations as now written or contemplated will affect different companies differently, for no economic or policy reason.

Telecom companies currently outsource a significant amount of their marketing to outside firms that specialize in marketing, reflecting the cost and quality advantages such firms have. If the costs of doing business increase because firms undertake these activities less efficiently in reaction to regulatory requirements, this will ultimately have a negative impact on consumers. The industry exhibits much competition over terms of service, prices, and other dimensions, so that if costs increase, competitive forces will dictate that this cost increase is passed on to consumers. Indeed, economic theory indicates that even in the case of a monopoly, if costs increase, then profit-maximizing prices charged to consumers will also increase. Conversely, cost decreases will also be fully or partly passed through to consumers. Thus, consumers and producers both benefit from reduced costs.

### A. Benefits of Out-Sourcing: Economies of Scale

A major source of the efficiencies associated with outside contracting is the potential for economies of scale in some activity, so that the optimal (i.e., cost-minimizing) level of the activity is larger than the amount of the output that is used by any one firm. This is pervasive in our economy and explains why firms purchase most products they use. For example, no firm (except for those in the industry itself) produces its own computers. The scale of production for computers is so large that it would not pay for a user of computers to produce them; costs would be too high. Rather, there are large benefits from "outsourcing" this activity and purchasing computers from firms that can make a sufficient number to realize economies of scale in production.

Marketing services are like this. Firms can and do specialize in telemarketing of various types. These firms have capital equipment and a trained staff that can be applied to many activities. They also have specialized knowledge that can be used in marketing campaigns. If telecom companies were forced to undertake this activity themselves, they would create inefficiently small in-house telemarketing departments with none of the benefits of the large specialized firms. Moreover, they would lack much of the specialized human capital of the specialized firms, including perhaps capital devoted to security. They may also lack some specialized data that the marketing firms use (and whose costs can be spread out over a larger number of customers) to market more efficiently.

Moreover, as indicated above, there is no evidence (at least according to the FCC) of telemarketing firms having suffered a security breach. It this activity were in-sourced, it is plausible that risks would increase rather than decrease. It is important to remember that shifting the locus of the activity from outside to inside does not necessarily change the scope of the activity, so the FCC's claim that it is "axiomatic that the more companies have access to CPNI, the greater the risk of unauthorized disclosure through disclosure by insiders or computer intrusion" is, in fact, not axiomatic. If the data exist in two places within a company, they may be just as much at risk as if they exist in two separate companies. If one of the internal users does not have as much skill at data protection as does the outside firm, then risks increase.

### B. Informational Benefits of Out-Sourcing

A second major advantage of outsourcing is that firms can learn more about the costs of the activities they outsource. Outsourcing provides a benchmark. If an activity is conducted in-house, then the firm may have more difficulty in learning about the true cost of the activity. It may be that the in-house division is inefficient or is not using up-to-date technology. If an activity is out-sourced, it is easy to determine the lowest cost for the activity; bids are let and the lowest-cost producer will win the bid. Use of outsourcing creates what are called "high-powered incentives." That is, the market creates the most powerful incentives for cost minimization. The informational benefits provided by the market are lost when an activity is undertaken inside the firm.

### C. Inequities

The CPNI rules prohibit various forms of data sharing among companies. However, it is important to note that different telecom companies operate under different legal structures, so that uses of information that may appear identical to an outsider (for example, transferring data between subsidiaries) may be acceptable in one case and violate the rules in another.

It would not be easy or cost-effective to eliminate these legal differences. For example, AT&T and Verizon, the "legacy" companies, are remnants of the old AT&T. As such, they are subject to various requirements that emanate from the antitrust settlement that broke up the company. These requirements do not affect Sprint and T-Mobile (or the cable companies, who are now providing the same set of services). If the internal subsidiaries of the two legacy companies tried to legally merge to eliminate the differences, they might find that the less-regulated subsidiaries would now be subject to the increased regulation associated with the more regulated divisions. Additionally, the benefits of increased information sharing might not be sufficient to justify the potentially large costs associated with restructuring.

This means that regulations and rules that seem on their face to be neutral with respect to different companies providing similar services are in fact discriminatory. This creates unfair and inefficient competitive and cost advantages for some companies relative to others. Such differentiation serves no economic or policy purpose, and is a result of arbitrary regulation with no benefits. That is, there may be no economic difference between the structure of the various companies, but because of various legal arrangements, the law and the regulations may treat them differently.

The FCC does indicate that there are differences in behavior between carriers (FCC, p. 22, note 117). However, it does not acknowledge that these differences may be rooted in legal and regulatory differences between companies. The FCC states that "We do not believe that this minor change to our rules will have a major impact on carriers because many carriers already do not disclose CPNI to third parties." This statement ignores differences between legal structures and business models of different companies. There are costs to forcing all companies to follow the same business model that may not be immediately visible to a regulatory agency but that may be very real nonetheless to the actual parties involved.

## VI. SUMMARY

Regulation of CPNI collected by telecom companies will limit their ability to share and use information. There can be no benefits from these proposals if the FCC is correct in its assessment that there is no consumer harm from use of CPNI data by outside contractors or partners. On the other hand, there will be substantial costs.

First, companies may do some restructuring or reduce the level of outsourcing in order to comply with these regulations. There are costs to in-sourcing. Moreover, since we can assume companies are now organized to do things as efficiently as they know how, any reorganization would be costly. In addition, some companies are restricted in their organization because they are remnants of the old AT&T and so are still restricted by the antitrust agreement that broke up the company. Thus, any attempts at restructuring would have asymmetric implications for different companies.

The other approach to complying with the regulations is to simply use less information. This would also be costly. Consumers benefit from the existence of new plans offered by the providers, from receiving information about these plans, from receiving other marketing information tailored to their needs, and from not receiving information they find irrelevant. CPNI data are used for all these purposes. If the data could not be so used, consumers would lose these benefits.

## References

Ernst & Young/The Financial Services Roundtable. 2000. Customer Benefits from Current Information Sharing by financial Services Companies.

Federal Communications Commission. 2007. Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information.

Government Accountability Office. 2007. Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown.

Lenard, Thomas and Paul H. Rubin. 2006. "Much Ado About Notification." Regulation.

Noam, Eli. 1997. "Privacy and Self-Regulation: Markets for Electronic Privacy" in Privacy and Self-Regulation in the Information Age. U.S. Department of Commerce. http://www.ntia.doc.gov/reports/privacy/selfreg1htm

Rubin, Paul H. and Thomas M. Lenard. 2002. Privacy and Commercial Use of Personal Information. Kluwer Academic Publishers and The Progress & Freedom Foundation.

Staten, Michael E. and Fred H. Cate. "The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Study of MBNA." Duke Law Journal, vol. 52, p. 745.

Varian, Hal. 1997. "Economic Aspects of Personal Privacy" in Privacy and Self Regulation in the Information Age. U.S. Department of Commerce. http://www.ntia.doc.gov/reports/privacy/selfreg1htm

## Of Related Interest

Thomas M. Lenard, "Privacy in the Commerical World II," Testimony before the Subcommittee on Commerce, Trade, and Consumer Protection, June 20, 2006.

Thomas M. Lenard and Paul H. Rubin, "Slow Down on Data Security Legislation," *Progress Snapshot 1.9.* The Progress & Freedom Foundation, August 2005.

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

Thomas M. Lenard, "S.2201 The Online Personal Privacy Act," Testimony before the Senate Committee on Commerce, Science and Transportation, April 25, 2002.

Howard Beales, "Privacy Notices and the Federal Trade Commission's 2002 Privacy Agenda." *Progress on Point 9.10.* The Progress & Freedom Foundation, March 2002.

William F. Adkinson, Jr., Jeffrey A. Eisenach, and Thomas M. Lenard, "Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites," The Progress & Freedom Foundation, March 2002.

Paul H. Rubin and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information,* Kluwer Academic Publishers and The Progress & Freedom Foundation, 2002.

Alan C. Raul, *Privacy and the Digital State: Balancing Public Information and Personal Privacy,* Kluwer Academic Publishers and The Progress & Freedom Foundation, November 2001.

Jeffrey A. Eisenach, Thomas M. Lenard and James Harper, "Comments to the Federal Communications Commission in the matter of Telecommunications Carriers' Use of Customer Proprietary Network Information and other Consumer Information," The Progress & Freedom Foundation, November 16, 2001.



The Progress & Freedom Foundation ④ 1444 Eye Street, NW ④ Suite 500 ④ Washington, DC 20005
voice: 202/289-8928 ④ fax: 202/289-6079 ④ e-mail: mail@pff.org ④ web: www.pff.org