Consumers Union

Publisher of Consumer Reports

**TESTIMONY OF**
**FRANK TORRES**
**LEGISLATIVE COUNSEL FOR CONSUMERS UNION**

**BEFORE THE**
**SENATE COMMITTEE ON COMMERCE,**
**SCIENCE, AND TRANSPORTATION**

**S. 2201**
**ONLINE PERSONAL PRIVACY ACT**

**APRIL 25, 2002**

Consumers Union[1] appreciates the opportunity to present this testimony on the ***Online Personal Privacy Act, S. 2201*.** This hearing provides a forum to discuss why American consumers need meaningful and comprehensive online privacy protections, how S. 2201 accomplishes those goals, and Consumers Union's support for the bill.

## INTRODUCTION

Consumers Union has long been an advocate for strong privacy protections. Along with other consumer and privacy advocates we pushed for amendments to the Gramm-Leach-Bliley Act to try to provide consumers control over how their personal financial information is collected and whether it could be shared. We fought for strong medical privacy regulations and continue to push for privacy related to health like genetic information. Consumers Union is also part of a broad privacy coalition that has supported online privacy protections.

Stronger laws are needed to give consumers control over their personal information. Legislative efforts such as S. 2201 will help ensure that consumers are told about how and why information is collected and used, provided access to that data, and given the ability to choose who gets access to their most intimate personal data.

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports*, its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with approximately 4.5 million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

S. 2201 represents a balanced and reasonable approach to online privacy. The bill reflects where there could be some agreement on the substantive privacy protections of notice, access and consent.

Consumers Union believes that basing the protection trigger on the type of information collected, rather than on any specific industry sector is a right way to ensure consumer data is safeguarded. This is a logical way to consider the privacy issue. Consumers should not have to keep track of all the businesses entities that may be collecting information about them, especially in light of the growing number of cross-industry mergers and the passage of the Gramm-Leach-Bliley Act. S. 2201 provide clear guidance for businesses as well. If you collect and use consumer data covered by the bill, you know what you have to do.

**BACKGROUND**

The right to be left alone appears to have been trumped by the pressure exerted by businesses to protect and expand their ability to gather personally identifiable information from consumers. No part of life is left untouched by data collection activities. Financial and medical records, what you buy, where you shop, your genetic code, are all exposed in a privacy free-for all. Complete strangers can, for a price, have access to your most intimate secrets. Often, consumers have no choice in whether or not information is collected and no choice in how it is used.

Do consumers care about their privacy? You bet they do.

- According to a survey commissioned by STAR, a subsidiary of Powell Tate, conducted by SWR Worldwide, many consumers report they have informed their primary financial institution of their desire to opt out (31 percent) of information sharing. And 40 percent plan to opt out in the next 12 months. This opt out rate is significantly higher than that reported by financial institutions.

- The survey, conducted after September 11, also found that more than half of the respondents (57 percent) expressed concern that their primary financial institution may be sharing personal or financial information with its affiliates or third parties. The majority (59 percent) also reported that their level of concern is about the same as it was a year ago.

- A recent report by KPMG, entitled A New Covenant With Stakeholders: Managing Privacy as a Competitive Advantage, cites a survey of U.S. voters by the Public Opinion Strategies firm last year indicating that strengthening privacy laws to assure that computerized medical, financial or personal records are kept private is the highest-rated issue of concern to voters nationwide.

- KPMG also noted that increasingly, individuals want to choose who does and does not have access to their medical, financial, purchasing, and other personal information. And, if access is needed, individuals would like to be able to specify for what purposes and to what extent access will be granted. They also want specific

assurances that the information they consider private is, in fact, kept private by the organizations with which they do business.

- Forrester Research found that 72 percent of consumers participating in a survey last year considered it a violation of privacy for businesses to collect and then supply personal data to other companies. 94 percent of Internet users want privacy violators to be disciplined. 70 percent said that Congress should pass legislation protecting privacy on the Internet. In December, Forrester found 69 percent of Americans worried about their financial privacy.

- Other surveys have estimated that concerns about privacy and lack of trust cost U.S. companies $12.4 billion in 2000 because consumers were reluctant to share their personal information over the Internet.

- A 2001 study by the Markle Foundation found that by more than a 3 to 1 margin (63-19 percent) the public says it is more concerned about companies collecting personal information online than offline.

- Nearly two-thirds of the public, 64 percent, say that the government should develop rules to protect people when they are on the Internet, even if it requires some regulation of the Internet.

- The study also found that the public is looking not only for protection by others, but they want an ability to control their own on-line experience, and the uses that others might make of what they do on-line. By a strong 58-37 percent margin, the public prefers an opt-in regime.

- Finally, the survey concluded that the public perceives that the Internet, although useful, is not yet a medium that enables them to hold others accountable when they go on-line.

All these surveys lead to the same conclusion: the majority of consumers are concerned about the threats to their privacy while online. An Ernst and Young report *Privacy Promises Are Not Enough*, noted that "at the core of this trust issue is the fact that consumers do not trust businesses to protect their privacy or follow their stated privacy policies."

Increasingly, consumers want to choose who does and does not have access to their medical, financial and other personal information. Consumers want to be able to specify for what purposes and to what extent access to their information will be granted. Consumers want assurances that the information they consider sensitive will be kept private by the businesses they use. Often, consumers have no choice in whether or not information is collected and no choice in how it is used. Today, any information provided by a consumer for one reason, such as getting a loan at a bank, can be used for any other purposes with virtually no restrictions.

**COMMENTS ON S. 2201**

There are a number of elements of privacy protection that have become clearer over the course of our involvement in the privacy debate which are reflected in S. 2201:

- A distinction can be made between sensitive and non-sensitive information. **S. 2201 advances the privacy debate by recognizing the distinction between sensitive and non-sensitive data.** We have commented that more sensitive personal data, like financial and medical information, warrant the strongest possible protections. For this type of data we favor an approach that requires a business to obtain the consumer's consent prior to sharing that data.

  For other data collected, a lessor standard may be appropriate. We support this approach only if clear notice is given to the consumer prior to the collection of the data and that the consumer is given the opportunity up front to choose not to have his or her information shared with others. We encourage providing specific and uniform mechanisms for exercising an opt-out.

  For telephone marketing several states are implementing "do-not-call" lists. Even the Direct Marketing Association maintains such a list. A one-stop universal opt-out would be a useful tool for consumers. We anticipate that the Federal Trade Commission will move forward soon on a final rule for a national do-not-call list. Perhaps a similar mechanism for the online world should be encouraged.

- Consumers need a stronger law to protect their personal financial information. **S. 2201 offers a substantial improvement over the privacy provision of the Gramm-Leach-Bliley Act by providing that sensitive financial information cannot be shared with affiliates or third parties without the express consent of the consumers.** S. 2201 would allow financial institutions to share less sensitive data with their affiliates under the opt-out standard.

  The Gramm-Leach-Bliley Act falls far short of providing meaningful privacy protections in the financial setting. Loopholes in the law and in this draft rule allow personal financial information to be shared among affiliated companies without the consumer's consent. In many instances, personal information can also be shared between financial institutions and unaffiliated third parties, including marketers, without the consumers consent.

  Consumers across the country are receiving privacy notices from their financial institutions. Unfortunately these opt outs, in reality, will do little or nothing to prevent the sharing of personal information with others. Other loopholes allow institutions to avoid having to disclose all of their information sharing practices to consumers. In addition, the GLB does not allow consumers to access to the information about them that an institution collects. While states were given the ability to enact stronger protections, those efforts have met fierce resistance by the financial services industry.

Reports and surveys conducted by the Privacy Rights Clearinghouse show how poorly written and difficult to understand the financial privacy notices are. Despite those obstacles, a recent survey indicates that consumers are choosing to opt-out.

- Consumers' health information should not be shared without their express consent. **S. 2201 protects personal health information across the board—under the bill health information cannot be shared without the prior consent of the consumer.** There appears to be widespread agreement on this principle.

  Consumers should not be put in the position of privacy intrusions when they go online to seek medical advice or information about prescription drugs, for example. Those seeking medical treatment are most vulnerable and should be allowed to focus on their treatment or the treatment of their loved ones, rather than on trying to maintain their privacy. It is unfair that those citizens must be concerned that information about their medical condition could be provided to others who have no legitimate need to see that information.

- **S. 2201 requires notice and consent prior to the sharing of personal information with others.** Online entities that collect personal information should be responsible for providing notice to consumers if they intend to share personal data with others and allow consumers to opt-out of such data collection and sharing third parties.

- **S. 2201 will allow consumers to opt-out of sharing their less sensitive data.** This requirement should be easy to implement, in most cases consumer choice can be provided at the point where the information is collected. The opt-out for less sensitive information is distinguishable from the stricter regime that would apply to more sensitive financial and medical data. An opt-out may be adequate for such information provided that the notice and choice is given up-front, prior to the collection, and is clear and in plain English. Consumers Union believes that the "robust" notice called for in S. 2201 will provide consumers with the type of notice to get the job done and avoid the pitfalls of the financial privacy notices.

  This is a reasonable step. Consider the position of the former Vice President of Yahoo!, Seth Godin, who has written about "permission marketing. He says that about 38 percent of the people that are given a chance to tell his company their interests to get information about things that match their profile do, in fact, opt-in. He goes on to call opt-out a sham.

- **Businesses should be responsible for safeguarding the sensitive data of Internet users if they choose to collect and use that data.** Businesses that collect and share sensitive personal information should be held accountable if that information is shared after a consumer has said no to such sharing of information. For example, if disclosure of sensitive financial data without the consumer's consent is the cause of that consumer's identity being stolen, shouldn't the businesses that sold the information be held accountable and be responsible for that consumer's loss?

The approach in S. 2201 is reasonable on this issue. It provides a private right of action only related to the misuse of sensitive personal data. Even the, the standard is high – a consumer can only recover upon a showing of actual harm. Actions cannot be brought if a systems failure or an event beyond the control of the business caused the disclosure.

We have not seen evidence of an onerous litigation burden despite a number of prior privacy statutes that allow such action. Most of these laws have been on the books for years:

- Section 616 of the Fair Credit Reporting Act – up to $1,000 for knowing or willful noncompliance plus punitive damages and actual damages for negligent noncompliance;
- 47 U.S.C. Section 551 Cable Communications Policy Act – $1,000 or actual damages plus punitive damages;
- Section 2520 of the Electronic Communication Privacy Act – between $500 and $10,000 and actual damages;
- 18 U.S.C. Section 2710 Video Privacy Protection Act --$2,500 in actual damages plus punitive damages;
- 47 U.S.C. Section 227 Telephone Consumer Protection Act – up to $500 for each violation.

- **The strength of S. 2201 must be balanced against any preemption of state law.** In response to consumer concerns about privacy several states are poised to act on these issues. We consider the work of the states vital. Consumers Union believes that it is critical to seek the input from the states, including state attorneys general and legislators, before deciding to preempt state privacy efforts. As long as the underlying privacy standards remain strong, S. 2201 will set a strong national privacy standard. Should S. 2201 be weakened Consumers Union would reconsider its continued support for the bill and urge that states be allowed to pass tougher privacy laws. Let us be clear, should the other provisions in the bill change, we would reconsider our position on preemption. Preempting state law is predicated on getting the strongest possible consumer protection in the underlying legislation.

**THE ONLINE MARKETPLACE**

The ability to collect, share and use data in all sorts of ways boggles the mind. Consumers, in many cases, aren't even aware that data is being collected, much less how profiles about them are created. The information collection overload is particularly troublesome when it becomes the basis for decisions made about an individual -- like how much a product or service will cost.

Cross industry mergers and consolidations have given financial institutions unprecedented access to consumers' personal data. Technology has made it possible and profitable to mine that data. No law prevents businesses from using data to choose between desirable borrowers and less profitable consumers the institutions may want to

avoid. Special software helps guide sales staff through scripted pitches that draw on a customer[1]s profile to persuade the account holder to buy extra, and in some cases junk products.

Some web-based businesses already seem to be willing to move beyond the privacy wasteland where GLB left consumers. There no longer appears to be a question, for some, of whether consumers should get notice, access, and control over their information. The challenge is how to effectively put these principles into practice.

A May 2000 *Consumer Reports* survey of web sites, *Consumer Reports Privacy Special Report, Big Browser is Watching You*, shows that consumers' privacy is not being protected online. The report also shows that privacy notices at several popular sites are inadequate and vague. This data, as do other recent web surveys, shows the state of consumer privacy online continues to hit or miss.

Privacy policies are not a substitute for privacy protections, especially when some companies don't even follow what is in their policies. Just because a company has a privacy policy does not mean that they follow Fair Information Practices. And consumers are skeptical about self-regulation.

The marketplace is changing daily. The Wall Street Journal reports that Time Warner has the names, addresses and information on the reading and listening habits of 65 million households. USA Today says Time Warner has access to information about its 13 million cable subscribers and from its other businesses, like Time and People magazine. With so much information, how will the competitiveness of the marketplace be impacted by this merger? Will companies who seek to operate under a higher privacy standard be at a competitive disadvantage and unable to compete against a larger entity that is able to make unrestricted use of the personal information it obtains?

**DO CONSUMERS BENEFIT FROM DATA SHARING?**

Financial institutions promised that in exchange for a virtually unfettered ability to collect and share consumers' personal information, that consumers would get better quality products and services and lower prices. This is why, they claimed, consumers shouldn't have strong privacy protections like the ability to stop the sharing of their information among affiliates, or access to that information to make sure its accurate. Let's look at reality.

Bank fees for many consumers continue to rise. Information about financial health may actually be used to the consumer's determent if it is perceived that the consumer will not be as profitable as other customers. Both Freddie Mac and Fannie Mae say between 30 and 50% of consumers who get subprime loans, actually qualify for more conventional products, despite all the information that is available to lenders today. Credit card issuers continue to issue credit cards to imposters, thus perpetuating identity theft, even when it seems like a simple verification of the victim's last known address should be a warning. Instead of offering affordable loans, banks are partnering with payday lenders. And when do some lenders choose not to share information? When sharing that

information will benefit the consumer -- like good credit histories that would likely mean less costly loans.

Chase Manhattan Bank, one of the largest financial institutions in the United States, settled charges brought by the New York attorney general for sharing sensitive financial information with out-side marketers in violation of its own privacy policy. In Minnesota, U.S. Bancorp ended its sales of information about its customers' checking and credit card information to outside marketing firms. Both of these were of questionable benefit for the bank's customers. Other institutions sold data to felons or got caught charging consumers for products that were never ordered.

Maybe the right approach is to let institutions that want a consumer's information to be put in a position to convince that consumer that some benefit will be derived from a willingness to give that information up to the institution. Such an approach may increase trust in financial institutions and let consumers have control and choice over their own personal information. The same technology that enables vast amounts of data to be collected can be used to give consumers access to that data. It is a simple thing to tell consumers what is collected and how it is used.

**CONCLUSION**

Consumers face aggressive intrusions on their private lives. Often a consumer is forced to provide personal information to obtain products or services. Many times information that has been provided for one purpose is then used for another reason, unbeknownst to the consumer. Financial institutions, Internet companies health providers and marketers have been caught crossing that line. Meanwhile, identity theft is at an all time high.

Sound and comprehensive privacy laws will help increase consumer trust and confidence in the marketplace and also serve to level the playing field. These laws do not have to ban the collection and use of personal data, merely give the consumer control over their own information.

Consumers should have the right to be fully and meaningfully informed about an institution's practices. Consumers should be able to choose to say "no" to the sharing or use of their information for purposes other than for what the information was originally provided. Consumers should have access to the information collected about them and be given a reasonable opportunity to correct it if it is wrong. In addition to full notice, access, and control, a strong enforcement provision is needed to ensure that privacy protections are provided.

S. 2201 provides the privacy protections consumers deserve.