Testimony of

Mr. Frank Torres

February 14, 2002

Consumers Union appreciates the opportunity to present this testimony on the Privacy Act of 2001, S. 1055. This hearing provides a forum to discuss why American consumers need meaningful and comprehensive privacy protections.

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 the collection and use of their personal information. Legislative efforts, such as S. 1055 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.

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. 1055:

A comprehensive approach to privacy protection, like S. 1055, is warranted. For consumers, the comprehensive approach of S. 1055 has advantages - clear expectations of how their information will be treated, when it can be shared and how the flow of information can be controlled. The distinctions between privacy intrusions are sometimes lost on consumers. Whether privacy is lost because of a cookie placed on a personal computer after visiting a website or because information obtained from a warranty card is collected and sold it really does not make a difference. Applying privacy protections in both online and offline settings is a fresh approach that has merit considering how the privacy debate has developed. Up to now the approach to privacy has been sector by sector. There are bills on financial privacy, medical privacy and online privacy. Often we hear complaints that one sector is being treated differently than another. S. 1055's comprehensive approach addresses those concerns. If industry wants fair and clear rules that treats everyone the same, they should be supportive of S. 1055's comprehensive approach.

A distinction can be made between sensitive and non-sensitive information. S. 1055 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.

Provided other data collected is used solely for marketing purposes 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. 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. The Federal Trade Commission has recently published a proposed rule for a national do-not-call list.

Consumers need a stronger law to protect their personal financial information. S. 1055 offers a substantial improvement over the privacy provision of the Gramm-Leach-Bliley Act by providing that financial information cannot be shared with third parties without the express consent of the consumers. 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.

Consumers' health information should not be shared without their express consent. S. 1055 protects personal health information across the board--under the bill health information cannot be shared without the prior consent of the consumer.

The sale of social security numbers to the public should be banned. Public disclosure of social security numbers should be limited. Businesses should be prohibited from denying services if a consumer does not wish to provide a social security number in certain circumstances. S. 1055 shuts down many avenues that lead to the release of social security numbers.

Commercial 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. 1055 requires notice and consent prior to the sharing of personal information with a non-affiliated entity.

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.

The remainder of these comments provide greater detail on privacy issues related to marketing, financial data, health data, and identity theft.

Marketing

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.

Increasingly, consumers want to choose who does and does not have access to their medical, financial and other personal information. If access is needed consumers want to be able to specify for what purposes and to what extent access 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.

S. 1055 will allow consumers to opt-out of sharing of information with third parties for marketing purposes. This requirement should be easy to implement, in most cases consumer choice can be provided at the point where the information is collected. Consumers are sometimes given that choice today in both online and offline settings.

The opt-out for marketing purposes is distinguishable from a stricter regime for the collection and use of sensitive financial and health information. So long as the information collected is used solely for marketing purposes, an opt-out approach may be adequate provided notice and choice is provided up front, prior to the collection of the data, and that the notice and choice is clear and in plain English. The opt-out must be easy for consumers, unlike the opt-out under the Gramm-Leach Bliley Act. The opt-out provided by most financial institutions have proven difficult for consumers to understand and hard to exercise.

If properly provided the notice and opt-out contemplated in this legislation could result into a system where consumers may indicate that they want no calls, then individually choose, on a case-by-case, merchant -by-merchant basis, to consent to information collection and use by parties they trust or believe will provide some benefit.

Exceptions to the opt-out requirement should be minimal. The exceptions provided in the legislation appear to be reasonable and should not be expanded.

It is appropriate to allow the Federal Trade Commission to have enforcement authority. The FTC has taken a leadership role in protecting consumer privacy. The agency was given specific authority under the GLB to implement those privacy provisions. In addition it has held numerous workshops and convened advisory committees on the issue of privacy.

The use of seal programs to provide for a safe harbor needs strict scrutiny and oversight. Consumers Union, and many other advocacy organizations remain skeptical of the ability of industry groups to self-regulate. Seal programs are often dependent on the very firms they are supposed to scrutinize. If a safe harbor remains in the bill, there should also be a mechanism to

evaluate whether the program is effective and ensure that the requirements of the program are as strict as the protections contained in the bill.

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.

Financial Privacy

Consumers have reason to be concerned about how their private financial information is being collected, used, shared and sold. Under the GLB there are no limits on the ability of a financial institution to share information about consumers' transactions, including account balances, who they write checks to, where they use a credit card and what they purchase, within a financial conglomerate. Because of loopholes in GLB, in most cases sharing a consumer's sensitive information with a third party is allowed too. All the exceptions created by GLB make it difficult to come up with a list of circumstances where personal financial information cannot be shared.

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.

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.

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. 1055 requires that consumers opt-in before financial information can be shared with third parties.

S. 1055 also provides that a consumer cannot be denied service for refusing to consent to the sharing of his or her information.

The exceptions contained in S. 1055 are limited to reasonable expectations related to the primary use of personal data.

Legislative efforts in this body, like S. 1055, send a strong message to those in the states pursuing similar privacy protections. It is clear that states, like California, are on the right tract in pushing forward with bills like California Senate Bill 773, which will provide strong financial privacy protections in that state. While congressional efforts may lag these state initiatives, sponsors of those bills should take note that they are on target with what federal legislators are considering.

Medical Privacy

Medical information has been used for inappropriate purposes. The medial privacy rule promulgated by the Department of Health and Human Services highlighted a number of cases where private medical information was released for profit and marketing purposes - completely unrelated to the treatment of those patients. A USA Today editorial earlier this year highlighted the consequences of a failure to protect medical privacy. The editorial cited various privacy intrusions - an employer firing an employee when they got the results of a genetic test; release of medical records to attack political opponents; and hackers getting access to health records from a major University medical center (USA Today, March 20, 2001).

Patients should not be put in the position of withholding information or even lying about their medical conditions to preserve their privacy. 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. 1055 requires a customer's affirmative consent before individually identifiable health information can be shared across the board. The bill extends the protections of the HHS rules to cover any setting across the board.

Identity Theft

Beth Givens of the Privacy Rights Clearinghouse estimates that there were 500,000 to 700,000 victims of identity theft last year. The number of complaints to the FTC almost doubled from March to December 2001. It is very easy to obtain social security numbers. Non-social security

administration uses of social security numbers have not been prohibited. As a result, social security numbers are used as identification and account numbers by many entities.

The Internet provides an easy and cheap way to get personal information.
Web sites sell individuals' social security numbers, some for as little as $20. Self-regulatory efforts by information brokers has been ineffective in restriction the sale of sensitive personal information to the general public.

Other elements to consider are the practices of the credit and credit reporting industries. They must also work to prevent fraud and help victims recover from identity theft.
Many consumers have no idea how they become victims of identiy theft. Often, they do not find out their personal information has been misused for more than a year, and sometimes as long as five years. Victims must spend significant amounts of time contacting creditors and credit reporting agencies in order to repair the damage done to their credit histories. In the meantime, they are often unable to obtain credit and financial services, telecommunication and utility services, and sometimes employment.

The expanded use of the SSN as a national identifier has given rise to individuals using counterfeit SSNs and SSNs belonging to others for illegal purposes. Stolen SSNs have been used to gain employment, establish credit, obtain benefits and services, and hide identity to commit crimes.

One of the unfortunate results of the events of last September are reports of identity theft scams. Criminals have tried to obtain data from the unsuspecting families of victims of that tragedy. This should remind creditors that they have a responsibility to verify the identity of individuals prior to issuing lines of credit.

The FTC is taking steps to assist the victims of identity theft, but it is also important to focus on preventing the theft in the first place. As an FTC official recently stated, "...in this day of remote transactions and greater access to publicly available information on each of us, identity theft has never been easier to commit."

S. 1055 helps take Social Security numbers out of circulation. It would prohibit the commercial sale of SSNs. The bill would also limit uses of SSN[1]s by private sector entities and stop the display of SSNs by government agencies.

S. 1055 provides civil penalties for misuse of SSNs. We believe a private right of action provides consumers with a meaningful safeguard against businesses who should be held accountable for the misuse of SSNs.

The legislation is a useful step in protecting SSNs and curbing identity theft. Given the severity of identity theft, and the cost to both business and consumers, there remains a need to monitor and assess the effectiveness of any legislation designed to prevent this problem.