Testimony of

# James Dempsey

Executive Director
Center for Democracy & Technology
April 13, 2005

Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology
before the
Senate Committee on the Judiciary

Securing Electronic Personal Data:
Striking a Balance Between Privacy and Commercial and Governmental Use

April 13, 2005

Chairman Specter, Senator Leahy, and Members of the Committee, thank you for the opportunity to testify today. Recent security breaches at a range of companies and institutions resulting in the loss of sensitive personal information have highlighted the need for a more substantial legal framework at the national level for entities collecting, using and selling personal data. A range of harms, including identity theft, can flow from the failure to protect electronic personal data and from governmental or corporate misuse of data or reliance on inaccurate data. We offer here today an overview of the policy landscape and suggest some approaches that Congress should consider to ensure the appropriate level of security and privacy protection. We look forward to working with you and interested stakeholders to achieve balanced solutions.

## THE NEW MARKETPLACE FOR PERSONAL DATA

In the past decade, the commercial collection and sale of personal information has changed dramatically, driven by a combination of factors, facilitated by the Internet, and resulting in an ever more rapid flow of sensitive personal information in ways that most consumers barely understand. The implications for commerce, national security and personal privacy have been detailed in recent books such as Robert O'Harrow's "No Place to Hide."

The private sector and the federal government have many legitimate needs for personal information, and the sharing of data offers benefits to consumers in the form of readily available credit. Businesses and non-profit entities, ranging from landlords to retailers to lawyers to universities, obtain and share personal information to provide services and facilitate economic transactions. Indeed, an important use of commercial data services is for anti-fraud purposes, including the prevention of identity theft. The federal government uses personal information to determine eligibility for government benefits, to support law enforcement, and to fight the war on terror.

An important category of this information is drawn from public records at courthouses and other government agencies. Data brokers (we use the term throughout our testimony for lack of a better one, without intending to be derogatory and recognizing that it is not well-defined) add considerable value by aggregating and categorizing this information to provide a more complete picture of the individuals to whom it pertains.

While data brokers provide important services to the government and the private sector, they also raise a host of privacy issues and concerns about the security of this information. The recent security breaches at ChoicePoint and LexisNexis have prompted calls for examination of this new industry. Already-regulated entities, such as Bank of America, have also lost control of sensitive personal information. So have merchants whose primary business is not data aggregation. DSW Shoe Warehouse, a chain of shoe retailers, announced recently that someone had stolen customers' credit card information from its database. And the New York Times reported that already this year nine universities have reported the loss or compromise of sensitive personal information. Precisely because databases of electronic personal data have tremendous value, they are attracting identity thieves.

Even legitimate uses of personal data can result in harm to individuals. For instance, individuals can suffer adverse consequences when data brokers sell inaccurate or incomplete information that results in the loss of employment opportunities. In the context of government use of personal information, adverse consequences could include being suspected of criminal or terrorist activity.

Congress has addressed privacy and security issues with respect to credit reporting agencies in the Fair Credit Reporting Act (FCRA), financial institutions in Gramm-Leach-Bliley (GLB), and health care providers in the Health Insurance Portability and Accountability Act (HIPAA). But Congress's sectoral approach to information privacy has left gaps in the coverage of the law.

## OVERVIEW OF POLICY RESPONSES

We see at least five sets of issues facing Congress at this time:

1. As a first step towards preventing identity theft, entities, including government entities, holding personal data should be required to notify individuals in the event of a security breach.

2. Since notice only kicks in after a breach has occurred, Congress should require entities that electronically store personal information to implement security safeguards, similar to those required by California AB 1950 and the regulations under Gramm-Leach-Bliley.

3. Congress should impose tighter controls on the sale, disclosure and use of Social Security numbers and should seek to break the habit of using the SSN as an authenticator.

4. Congress should address the federal government's growing use of commercial databases, especially in the law enforcement and national security contexts.

5. Finally, Congress should examinee the "Fair Information Practices" that have helped define privacy in the credit and financial sectors and adapt them as appropriate to the data flows of this new technological and economic landscape.

## WHAT IS PRIVACY?

Information privacy is not merely about keeping personal information confidential. Rather, it is well established by United States Supreme Court cases, the federal Privacy Act, and privacy laws like the FCRA and HIPAA that the concept of privacy extends to information that an individual has disclosed to another in the course of a commercial or governmental transaction and even to data that is publicly available. Information privacy is about control, fairness, and consequences. Data privacy laws limit the use of widely available, and even public, information because it is recognized that individuals should retain some control over the use of information about themselves and should have redress to the consequences that result from others' use of that information. A set of commonly accepted "Fair Information Practices" captures this broader conception of privacy and is reflected, albeit in piecemeal fashion, in the various privacy laws and in the practices of commercial entities and government agencies. These principles govern not just the initial collection of data, but also the use of information collected and shared in the course of governmental and commercial transactions.

The "Fair Information Practices" were first articulated in the 1970s and have been embodied in varying degrees in the Privacy Act, the FCRA, and the other "sectoral" federal privacy laws that govern commercial uses of information. The concept of Fair Information Practices (FIPs) has remained remarkably relevant despite the dramatic changes in information technology that have occurred since they were first developed. While mapping these principles to the current data landscape poses challenges, and while some of the principles may be inapplicable to public record data, they provide a remarkably sound basis for analyzing the issues associated with creating a policy framework for the privacy of commercial databases.

The FIPs principles are variously enumerated, but we see eight: (1) notice to individuals of the collection of personally identifiable information, (2) limits on use and disclosure of data for purposes other than those for which the data was collected in the first place, (3) limitations on the retention of data, (4) a requirement to ensure the accuracy, completeness and timeliness of information, (5) the right of individuals to access information about themselves, (6) the opportunity to correct information or to challenge decisions made on the basis of incorrect data, (7) appropriate security measures to protect the information against abuse or unauthorized disclosure, and (8) the establishment of redress mechanisms for individuals wrongly and adversely affected by the use of personally identifiable information. A lot more work would be needed to develop a regulatory framework imposing all of these principles on all entities that hold or use personally identifiable data. Nevertheless, these principles do provide a framework for analyzing the current situation. They suggest certain immediate steps that Congress could take.

## NOTICE OF BREACH

As a first step, there should be a national requirement that individuals be notified when their information held by a third party is obtained by an unauthorized user. CDT would support appropriate federal legislation modeled on the California disclosure law that would require holders of sensitive personal information to notify people whose

information might have been stolen or otherwise obtained by unauthorized persons. Some industry leaders have also supported federal notice legislation, as did the Chairman of the Federal Trade Commission at earlier congressional hearings.

The California law worked well after the ChoicePoint security breach. As a result of the California law, ChoicePoint was required to notify individuals so they could take protective action. And public pressure led ChoicePoint to give nationwide notice. California is currently the only state with such a law on the books, but other states are currently considering similar legislation. Congress should enact federal legislation that is as protective as the California statute.

There as been some debate about when entities should be required to give notice of a breach. Some have argued that the holder of the information should be allowed to exercise discretion in determining whether the breach is one that poses a significant risk of harm to individuals. Concern has been expressed that if consumers are notified of every security breach, they would receive too many notices and become immune to them. While the risk of over-notification is real, guidance issued by the State of California on its disclosure law seems to address concerns about over-notification. An appropriate standard might be to require entities that discover a breach of security of a system containing unencrypted personally identifiable data in electronic form to notify any U.S. resident whose data was, or is reasonably believed to have been, acquired by an unauthorized person. If the entity is not certain whether the breach warrants notification, it should be able to consult with the Federal Trade Commission. This would allow the entities to avoid giving notice in the case of accidental unauthorized access that does not pose a risk of harm to the public, while ensuring that the public is adequately protected in those cases where data has been acquired unlawfully. Additionally, it may be desirable to have a two-tiered system, with notice to the FTC of all breaches of personal data and notice to consumers where there is a potential risk of identity theft. Broader notice to the FTC would help with oversight and would allow for adjustment in reporting thresholds.

Notice alone, however, is not enough. Consideration needs to be given to the question of what options a consumer has after receiving notice of a breach. Consumers can require a fraud alert on their credit reports, but under current law that has to be renewed every 90 days unless the individual is actually the victim of identity theft, in which case he is entitled to a 7 year notice. Another approach is to give consumers the ability to "freeze" their credit reports, blocking their release and thus preventing the issuance of credit. Texas and California currently allow credit report freezes, and Vermont and Louisiana freeze legislation is supposed to take effect this summer. At least 15 other states are considering similar legislation. Another way to allocate risk may be to create a "Do Not Issue Credit without Verification List," allowing consumers to post a warning to creditors to obtain additional identity verification before issuing credit. This would not be a freeze, but would put creditors on alert that they need to be careful.

SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

While notice legislation would be helpful in mitigating the damage from a security breach and might prod companies to improve security proactively, Congress should enact legislation requiring commercial entities that hold personal information to implement information security programs. Already there is a patchwork of requirements. Financial institutions are already subject to information security requirements under Gramm-Leach-Bliley, and the Health Insurance Portability and Accountability Act imposes similar requirements on health care providers and insurers, The Sarbanes-Oxley legislation also has a provision that is interpreted as imposing some kind of data security obligation. The Federal Trade Commission has exercised its Section 5 authority and obtained consent agreements with a number of companies that are looked to as models. And the California law known as AB 1950 has imposed a general data security obligation on companies doing business there.

It is probably time to bring some uniformity to these requirements. The Federal Trade Commission regulations implementing Gramm-Leach-Bliley provide a good framework and probably have about the right level of detail for security programs for data brokers and other commercial entities. They require an entity to develop, implement and maintain a comprehensive information security program that contains administrative, technical and physical safeguards that are tailored to the size and nature of the entity. Among other elements of a security program, they require entities that hold personal information to conduct a risk assessment to identify and develop systems to protect against anticipated threats and unauthorized access to information, to train employees, to audit their systems to identify unauthorized access, and to periodically reassess the program's effectiveness. Otherwise, the FTC approach gives entities that collect and store personal information the flexibility to develop security programs that fit their business models.

SOCIAL SECURITY NUMBER PROTECTION

Personal privacy is not just threatened by ineffective or nonexistent information security systems, however. Another threat to personal privacy is the proliferation and misuse of Social Security numbers. When the federal government first issued Social Security numbers in 1936, it limited their use to identifying accounts for workers with earnings from jobs covered by the Social Security Act of 1935. Social Security numbers were not supposed to serve as the universal identifiers that they have become. In fact, they were initially called Social Security Account Numbers and for

many years the words "Not For Identification" appeared on Social Security cards. Over time, however, Social Security numbers have become de facto national identifiers, serving as the key that unlocks many databases containing medical records, university records, employee files and bank records, just to name a few.

Worse, the SSN is used as an authenticator. That is, it is used like a PIN number - even though SSNs are widely available, entities treat them as if they were a secret and that therefore someone is you if he knows your SSN. This is very poor security practice. As a result, Social Security numbers are a major factor in identity theft.

CDT supports legislation that would tighten controls on the sale, purchase and display of Social Security numbers. Given the ubiquity of Social Security numbers in the public domain, it might not be possible to prevent criminals from acquiring them, but that does not mean we should give up trying to curtail the SSN's overuse and misuse. We believe that this can be done without prohibiting the use of the SSN as an identifier or disambiguator in large databases. Certainly, the SSN should be phased out as a student or employee ID number reflected on ID cards, transcripts and other records disclosed outside an institution. Congress should also, where feasible, limit the use of Social Security numbers by government entities. In particular, states should be prohibited from using Social Security numbers on drivers' licenses.

These changes will have limited effect, however, unless it is also recognized that it is poor security practice to use the SSN as an authenticator - treating it like a password or an obscure bit of information likely to be known only to the one person to whom it was issued. The habit of relying on the SSN for verification of identity needs to be broken.

GOVERNMENT USE OF COMMERCIAL DATABASES

An often overlooked but very important issue is the federal government's use of commercial databases. As discussed earlier, the government uses commercial data for law enforcement and national security purposes. The Privacy Act of 1974 was supposed to subject government agencies that collect personally identifiable information to the Fair Information Practices, but the Act's protections only apply to federal "systems of records." That means that the government can bypass the Privacy Act by accessing existing private sector databases, rather than collecting the information itself. Thus, although the Privacy Act requires notice to and consent from individuals when the government collects and shares information about them, gives citizens the right to see whatever information the government has about them, and holds government databases to certain accuracy standards, none of those rules applies when the government accesses commercial information without pulling that data into a government database. Currently, the government need not ensure (or even evaluate) the accuracy of the data; it need not allow individuals to review and correct the data; and the government is not limited in how it interprets or characterizes the data.

Commercial information can and should play a key role in law enforcement and national security investigations. But agencies relying on that data should have clear guidelines for its use--guidelines that both protect individual rights and ensure the information is useful for investigative purposes.

One option would be to make it clear that the Privacy Act applies whether the government is creating its own database or acquiring access to a database from a commercial entity. Also, Congress could apply the concept of Privacy Impact Assessments to the acquisition of commercial databases. Section 208 of the E-Government Act of 2002 already requires a PIA if the government initiates a new "collection" of information. The same process should apply when the government acquires access to a commercial database containing the same type of information that would be covered if the government itself were collecting it.

Another approach, based on a bill that Senator Wyden introduced in the last Congress, would be to require the government to perform an accounting of private sector databases before using them. Under the Wyden proposal, a government agency that acquired access to databases containing personally identifiable information concerning U.S. citizens would be required to publish in the Federal Register a description of the database, the name of the entity from which the agency obtained the database and the amount of the contract for use of the database. In addition, the agency would be required to adopt regulations that establish

? the personnel permitted to access, analyze or otherwise use the database;
? standards that govern the access to and analysis and use of such information;
? standards to ensure that personal information accessed, analyzed and used is the minimum necessary to accomplish the government's goals;
? standards to limit the retention and re-disclosure of information obtained from the database;
? procedures to ensure that such data is accurate, relevant, complete and timely;
? auditing and security measures to protect against unauthorized access to or analysis, use or modification of data in the database;
? applicable mechanisms that individuals may use to secure timely redress for any adverse consequences wrongly experienced due to the access, analysis or use of such database;
? mechanisms, if any, for the enforcement and independent oversight of existing or planned procedures, policies or guidelines; and
? an outline of enforcement mechanisms for accountability to protect individuals and the public against unlawful or

unauthorized access to or use of the database.
Agencies might also incorporate into their contract with commercial entities provisions that provide for penalties when the commercial entity sells information to the agency that the commercial entity knows or should know is inaccurate or when the commercial entity fails to inform the agency of corrections or changes to data in the database.
The Intelligence Reform Act that Congress passed last December established guidelines for the government's evaluation of Secure Flight plans that suggest a broader framework for use of data. Congress could adopt similar guidelines for government agencies to follow before implementing any screening program that uses commercially available data. As an initial matter, all government screening programs should be congressionally authorized. This would ensure some degree of public accountability and congressional oversight. In addition, all screening programs should be subject to regulations that include, at a minimum, the following elements:
? procedures to enable individuals, who suffer an adverse consequence because the system determined that they might pose a security threat, to appeal the determination and correct any inaccurate data;
? procedures to ensure that the databases the government uses to establish the identity of individuals or otherwise make assessments about individuals will not produce a large number of false positives or unjustified adverse consequences;
? procedures to ensure that the search tools that the department or agency will use are accurate and effective and will allow the department or agency to make an accurate prediction of who may pose a security threat;
? sufficient operational safeguards to reduce the chance for abuse of the system;
? substantial security measures to protect the system against unauthorized access;
? policies that establish effective oversight of the use and operation of the system; and
? procedures to ensure that the technological architecture of the system does not pose any privacy concerns.
These approaches, all of which Congress has previously approved in similar contexts, strike a balance between the government's need for information and the privacy interests of individuals. Adapting the Privacy Act and Fair Information Principles to government uses of commercial databases would go a long way toward closing the unintended gap in privacy protection that exists under the current law.

REGULATION OF DATA BROKERS

Finally, Congress should consider whether there are gaps in the current sectoral laws that protect privacy and focus on the harms that can flow from use of inaccurate or misleading information. This is not about use of marketing data to send catalogues or sales offers. Rather, in the context where adverse consequences can result, Congress should apply to data brokers the Fair Information Practices that are the framework of the Fair Credit Reporting Act and other privacy laws.
As the law stands now, these Fair Information Practices apply only when data brokers collect and use information in a way that is governed by the Fair Credit Reporting Act. For instance, if a data broker sells personal information to a third party that uses the information to determine eligibility for insurance, the Fair Credit Reporting Act would apply and certain rights would attach to the individual to whom the information pertains. The individual would be able to obtain a copy of the report, challenge the accuracy of the data and correct any inaccurate information. The ability to do this is particularly important when a person can suffer adverse consequences--such as the denial of insurance--from the use of the personal information. But if the data broker sold that same information to an insurance company for use in claims processing - in which case the individual might be denied reimbursement under her insurance policy - the individual would not have any of those same rights.
We note that Derek Smith, the Chairman and CEO of ChoicePoint, last year called for a national dialogue on privacy, to develop a policy framework for his companies and others. Specifically, Smith called for expanding the principles reflected in the FCRA:
"We should agree that the consensual model is best to the maximum degree possible, understanding that law enforcement and national security uses may outweigh getting prior consent for certain information. By this I mean that individuals should give permission (or not) at the time information is gathered and should agree to its use. Data should not be used for a different purpose unless new permission is obtained. However, we must recognize that public record data is, fundamentally, just that - public - and does not fit within the consensual model because of the current local, state, and federal freedom of information acts.

Everyone should have a right of access to data that is used to make decisions about them - subject to the same caveats about law enforcement and national security uses. In other words, expand the principles of the Fair Credit Reporting Act to all types of information: right to access, right to question the accuracy and prompt a review, and right to comment if a negative record is found to be accurate."

CONCLUSION

Resolving these issues will require a broad-based and inclusive dialogue. We must strike a balance, but the current absence of a comprehensive legal framework for the collection, sale and use of sensitive personal information is yielding harms that are made clear every day. The Center for Democracy and Technology looks forward to working with the Committee, with all of today's witnesses, and with all stakeholders. We are not helpless in the face of the ongoing revolution in information technology. Through the policy process, we can decide whether there is "No Place to Hide."