Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology[1]

before the
House Committee on the Judiciary
Subcommittee on Commercial and Administrative Law
and
Subcommittee on the Constitution

The Defense of Privacy Act and Privacy in the Hands of the Government

July 22, 2003

Chairman Cannon, Chairman Chabot, Members of these two Subcommittees, thank you for the opportunity to testify today on H.R. 338, the Defense of Privacy Act. We commend you for your attention to the important privacy issues surrounding the government's collection and use of personal information. We offer here today our strong support for the Defense of Privacy Act. In addition, we suggest some further steps Congress should take to ensure fairness in the government's collection or use of personal information, particularly with regard to government access to commercial databases and the possible use of "data mining" techniques. We look forward to ongoing work with you on these issues.

I. SUMMARY

The federal government has many legitimate needs for personal information, ranging from administration of benefits programs to tax collection to winning the war on terrorism. Especially in light of the digital revolution, this government demand for information brings with

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Our core goals include enhancing privacy protections and preserving the open architecture of the Internet. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

it heightened risk to privacy and the associated values of Fair Information Practices. The Defense of Privacy Act would put in place an important process to protect Americans' privacy against unnecessary or unwise government intrusions. The Act requires government agencies to closely examine the privacy impact of their rules and regulations and to consider alternative ways to accomplish their objectives while minimizing any adverse privacy impact. The Act focuses on the point when careful consideration of privacy could do the most good: at the beginning of the regulatory process.

The Defense of Privacy Act serves as a sound complement to Section 208 of the E-Government Act of 2002, which requires that federal agencies conduct privacy impact assessments whenever they purchase a new information technology or initiate a new collection of personally identifiable information. However, we note with dismay that the Office of Management and Budget (OMB) has failed to issue guidance to agencies on performing the privacy impact assessments under the E-Gov Act. We urge the Subcommittees to send a strong message to OMB that it should promptly issue guidance to the agencies on the E-Gov Act privacy impact assessment process.

While adoption of the Defense of Privacy Act and full implementation of the E-Gov Act would be important steps, further congressional action is needed to address a new problem: the growing use by federal law enforcement and intelligence agencies of sensitive, personal data about Americans held by the private sector or collected by government agencies for purposes other than law enforcement or intelligence. With growing frequency, the government does not compel disclosure of private sector data but rather purchases access to it. Since this information is not collected under a regulation, it would not be subject to the Defense of Privacy Act. Agencies are developing new "data mining" technologies that would seek evidence of possible

terrorist preparations by scanning billions of everyday transactions, potentially including a vast array of information about Americans' personal lives, such as medical information, travel records, credit card and financial data, and government data initially collected for non-law enforcement purposes. Contrary to some reports, research on data mining continues under the auspices of the Total (now Terrorism) Information Awareness (TIA) project at the Pentagon's Defense Advanced Research Projects Agency. And even if TIA funding were zeroed out, the development of data mining would go on commercially or at other agencies. Government implementations of this uniquely intrusive technology should not go forward without explicit congressional authorization based on (i) a finding of effectiveness, (ii) guidance for implementation, and (iii) oversight. CDT urges the Congress to develop, first, a structure or criteria for evaluating the effectiveness of particular uses of data analytics technology and then, for specific situations where the use of such techniques are found to be effective, guidelines and an oversight process for protecting privacy and due process. CDT offers its assistance in that process.

II. THE DEFENSE OF PRIVACY ACT AND PRIVACY IMPACT ASSESSMENTS

A. The Defense of Privacy Act

CDT strongly supports enactment of H.R. 338, the Defense of Privacy Act, introduced this Congress by Chairman Chabot and cosponsored by Representatives Boucher and Nadler. The bill would require agencies to conduct privacy impact analyses for both new and existing agency rules and regulations. Importantly, it would provide a judicial review mechanism to ensure enforcement. For the same reasons that we supported former Representative Barr's Federal Agency Protection of Privacy Act, which passed the House of Representatives in the last Congress but was never taken up by the Senate, we believe that H.R. 338 provides a sound

approach for enhancing privacy protections for the federal government's collection and use of personally identifiable information.[2]

The privacy impact analyses required by the Defense of Privacy Act will greatly improve the regulatory process. They will force agencies to consider issues they have often overlooked in issuing regulations, namely the privacy implications. Agencies would have to consider ways to reduce the privacy impact of regulations. And they would have to systematically justify their decisions to collect personally identifiable information.

Specifically, the bill requires agencies to address up front some of the basic "Fair Information Practices" that are reflected in the federal Privacy Act of 1974, such as notice to individuals of the collection of personally identifiable information, the right of individuals to access information about themselves, the opportunity to correct information, limits on use and disclosure of data for purposes other than those for which the data was collected in the first place, and appropriate security measures to protect the information against abuse or unauthorized disclosure.

These "Fair Information Practices" form part of the foundation of the Privacy Act, which was enacted in response to the creation of government computer databanks filled with personally identifiable information. (As will be discussed below, the Privacy Act has a number of exemptions and loopholes that render it less effective today than intended.) Other Fair Information Practices, which are also reflected in the Privacy Act, include limitations on the retention of data, a requirement to ensure the accuracy, completeness and timeliness of information, and the establishment of redress mechanisms for individuals wrongly and adversely

---

[2] In the past, CDT has urged the Office of Management and Budget (OMB) to adopt administratively a requirement that agencies undertake privacy impact assessments as part of the regulatory process, even though it is not currently required by statute. OMB has declined to do so.

affected by the use of personally identifiable information. We recommend that those additional principles be included in the Defense of Privacy Act's list of considerations that agencies must review when issuing regulations, so that the Defense of Privacy Act fully tracks the Privacy Act of 1974.

A key element of the Defense of Privacy Act is that it would require policy makers to identify and address privacy issues at the initial stages of a new project or policy – at the conceptual or design stage, before regulations are promulgated. This represents a vast improvement over current practice. It also means that the Act should not adversely interfere with agency operations. Instead, it will reduce the likelihood that any given regulatory scheme will be found to have a negative impact on privacy after it has been implemented, when it may be difficult to mitigate the impact without substantial expense, delay in the program or even litigation. The requirement that agencies periodically review existing regulations that have serious privacy implications could also benefit agency operations by identifying information collection practices that have become outdated or unnecessary and that can be dispensed with altogether.

The privacy impact analyses will not force agencies to adopt any one privacy standard. Indeed, different standards may well be appropriate for different programs dealing with information of varying sensitivity. However, having to work through a privacy impact analysis should guide an agency in acting more responsibly, and as a result this bill should lead to better regulations and fewer unnecessary privacy intrusions.

B. Failure to Fully Implement the E-Government Act

Enactment of H.R. 338 would not be the first time that Congress has directed federal agencies to analyze the privacy impact of their programs. Just last year, the E-Government Act

of 2002 included a provision, Section 208, requiring federal government agencies to conduct privacy impact assessments before developing or procuring information technology or initiating any new collections of personally identifiable information. Under that legislation, a privacy impact assessment must address what information is to be collected, why it is being collected, the intended uses of the information, with whom the information will be shared, what notice would be provided to individuals, and how the information will be secured. The privacy impact assessments required under the Defense of Privacy Act complement the requirements under the E-Gov Act. We urge the Subcommittees to ensure that the two Acts are congruent. Our initial thoughts are that this should be done by making the list of factors to be considered the same in both, and by making it clear that when a new collection of information is initiated by rule, the notice and comment provisions of the Defense of Privacy Act apply to the privacy impact assessment process.

The privacy impact assessments under the E-Gov Act should bring greater transparency to the IT development and procurement process, allowing Congress, citizens and advocacy groups to better scrutinize the privacy decisions of the government. And using the massive purchasing power of the U.S. government, the assessments could help to increase the marketplace for technologies that incorporate privacy "by design."

Unfortunately, privacy impact assessments for information technology procurements have only been implemented by a few agencies, despite the fact that the E-Government Act set an April 2003 deadline for implementation. The Director of OMB was supposed to issue guidelines in April for agencies on how to draft the assessments, but has failed to do so. As a result, the implementation of this important new privacy protection has been significantly pushed back. CDT is very concerned about this delay. These Subcommittees should encourage the

Executive Branch to get on with implementation of the E-Gov Act. Guidance issued for privacy impact assessments under the E-Gov Act could also help agencies perform similar assessments of regulatory actions under the Defense of Privacy Act.

It is worth noting that privacy impact assessment requirements like those in the Defense of Privacy Act and the E-Government Act are not a new or uniquely American concept. Privacy impact assessments already are used in several other countries. Indeed, privacy commissioners in Canada and New Zealand have issued excellent guides or handbooks on conducting privacy impact assessments, which may assist OMB in issuing its guidance. For more information about the international experience, see *Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners – Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online*, a report of the Global Internet Policy Initiative, which can be found at http://www.gipiproject.org/practices/030501pia.pdf.

C. Privacy Officers

We briefly mention one other important privacy protection mechanism, the Privacy Officer, now being implemented at the Department of Homeland Security. In Section 222 of the Homeland Security Act of 2002, Congress established a Privacy Officer for the Department. The Privacy Officer's statutory responsibilities include "evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government" and "conducting a privacy impact assessment of proposed rules of the Department .□□including the type of personal information collected and the number of people affected." CDT believes that every federal agency should have a statutory Privacy Officer with authorities similar to those provided under the Homeland Security Act. This officer would have the stature and expertise to effectively conduct privacy impact assessments of the kind required under the

Defense of Privacy Act, and the Defense of Privacy Act would give these officers specific requirements and an enforcement mechanism to draw on in fulfilling their duties. Attempts by the Clinton Administration to create privacy officers by Executive memorandum were unsuccessful. The position needs and deserves statutory footing.

III. THE NEED FOR FURTHER CONGRESSIONAL ACTION REGARDING THE PRIVACY IMPLICATIONS OF DATA MINING AND OTHER GOVERNMENT USES OF COMMERCIAL INFORMATION

The E-Government Act's requirement that agencies issue privacy impact assessments each time they procure new information technology systems was a vital step toward making privacy a significant part of government decision-making processes. The Defense of Privacy Act addresses another major concern by requiring agencies to consider the privacy implications of their proposed and existing regulations. But there is a third set of issues not necessarily addressed by either of those provisions: "data mining" and other law enforcement and intelligence uses of commercial data and other information that was not initially collected for law enforcement and intelligence purposes. Law enforcement and intelligence agencies are increasingly buying commercial data or developing new uses of government data originally collected for non-law enforcement or intelligence purposes. A new theory of pattern-based analysis is being developed that claims the ability to review the ocean of data we generate in everyday life, potentially including a vast array of information about Americans' personal lives such as medical information, travel records and credit card and financial data. Such techniques turn the presumption of innocence upside down. They seem to assume government access to personal information about everyone from any source. Yet this is an area where few laws, regulations or guidelines constrain the government or provide any meaningful oversight or accountability. CDT urges Congress to address this significant gap in privacy protection.

Before going into further detail, let me be clear on one point: The threat terrorism poses to our nation is imminent and grave. Our nation critically needs a more effective intelligence effort to thwart terrorism, and this effort must include new technologies for collecting and analyzing information from public and private sources. But advanced information technology, by its power to search decentralized databases, has new, grave privacy implications. Such technology must be used only if effective; it must be subject to checks and balances; it must be implemented with a focus on actual suspects, guided by the particularized suspicion principle of the Fourth Amendment; and it must be subject to executive, legislative and judicial controls. At this time, those checks and balances do not exist.

A. Access to Information Initially Collected for Purposes Other Than Law Enforcement and Intelligence

Increasingly, U.S. law enforcement and intelligence agencies are seeking access to commercial data and other personally identifiable information that was not initially collected for law enforcement and intelligence purposes. Agencies can obtain this information via subscription, through voluntarily disclosures, or under new Patriot Act authorities that authorize access under very weak standards.[3] The Constitution as currently interpreted provides no limits on government collection of this information because courts in the pre-Internet era – not envisioning a technology that could link vast public and private databases to present a composite image of any individual – held that individuals do not have Fourth Amendment rights in personal information disclosed to third parties like banks and credit card companies in the course of business transactions.

---

[3] For more details about the government's broad authority to obtain and use commercial information, see *Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data*, available at http://www.cdt.org/security/usapatriot/030528cdt.pdf.

The result is that the government faces few constraints on its ability to obtain and use this information. For years the FBI has had contracts with major companies that aggregate commercial data about individuals. According to an undated FBI presentation obtained by the Electronic Privacy Information Center, the FBI's use of "public source" information (including those proprietary commercial databases) has grown 9,600% since 1992.[4] Other entities that collect commercial information have voluntarily provided the FBI with their databases, from grocery store frequent-shopper records to scuba diving certification records.[5] But it is entirely unclear what, if any, guidelines apply to the FBI's use of this information.

Ironically, when private companies wish to use and share consumer information to assess an individual's credit, decide whether to extend a job offer, or evaluate whether to issue an insurance policy, they must comply with fairly strict rules. For example, under the Fair Credit Reporting Act, private companies cannot use consumer information to deny an individual a job, credit or insurance unless that person has the opportunity to review and correct that information.

Yet the government is subject to none of those rules when it uses that same information to identify possible terrorists, even though the consequences of mistake or abuse can be very serious. The Privacy Act 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," so the government can bypass the Privacy Act simply 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

---

[4] http://www.epic.org/privacy/publicrecords/cpfbippt.pdf.

[5] Ben Worth, *What to Do When Uncle Sam Wants Your Data*, CIO Magazine (Apr. 15, 2003), *available at* http://www.cio.com/archive/041503/data_content.html.

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.[6] Currently, the government need not ensure (or even evaluate) the accuracy of the data; it need not provide individuals with the ability to review and correct the data; and there are no limits on how the government might interpret or characterize the data. Meanwhile, plans are being discussed to promote broader sharing of data with state and local authorities, and the line between domestic intelligence and foreign intelligence has blurred.

CDT recognizes that commercial information can and should play a key role in law enforcement 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.

The accuracy of the information, for example, is essential both to the effectiveness of counter-terrorism efforts and to individuals to ensure they are not mistakenly caught up in an investigation. Marketing data and other information collected for commercial purposes are often

---

[6] Moreover, the Privacy Act exempts law enforcement and intelligence information from many key provisions. Law enforcement agencies and the CIA can exempt their own records from various provisions of the Privacy Act, including the requirement to maintain accurate records and to permit individuals to access and correct their records, simply by publishing a notice in the Federal Register. 5 U.S.C. §!52a(j), (k). The FBI just this year exempted a key national law enforcement database, the National Criminal Information Center, from the accuracy requirements of the Privacy Act. 68 Fed. Reg. 14140 (Mar. 24, 2003). Any agency can disclose records to any other agency (federal, state or local) for any civil or criminal law enforcement activity if the requesting agency makes a written request specifying the particular portion desired and the law enforcement activity for which the record is sought. 5 U.S.C. §!52a(b)(7). (This does not, however, authorize disclosures to intelligence agencies.) An agency can share its records with any other agency if the sharing is a "routine use" and has been noticed in the Federal Register. A "routine use" is any use that is compatible with the purpose for which the information was collected. 5 U.S.C. §!52a(a)(7), (b)(3). This exception has received some very broad interpretations. Finally, the definition of "computer matching" excludes matches performed for foreign counterintelligence purposes. 5 U.S.C. 552a(a)(8)(B)(vi).

inaccurate.[7] Rampant identity theft threatens to pollute credit reports and other commercial databases with false information. Accordingly, a way needs to be found to build data quality standards into government uses of consumer data. Another problem is security. It is important to protect against abuse by rogue agents within law enforcement agencies. There have been recurrent news accounts of police officers using access to police computers to obtain information about celebrities or to track their ex-girlfriends; agencies should establish auditing mechanisms and other safeguards to protect against that type of unauthorized access when agencies query commercial databases. Redress is a third issue: what will be the rights of an individual if adverse action is incorrectly taken on the basis of erroneous or misinterpreted commercial data?

B. Data Mining Technology

A related but even more complicated set of issues concerns so-called "data mining" or "pattern analysis" technology. This set of techniques purports to be able to find evidence of possible terrorist preparations by scanning billions of everyday transactions, potentially including a vast array of information about Americans' personal lives. This type of "pattern-based" analysis is to be distinguished from more traditional "suspect-based" searches, where a law enforcement agency has identified a suspect and is attempting to locate additional information about the suspect (or his associate) through the use of commercial databases. Pattern-based searches heighten civil liberties concerns because they require government access to *everyone's* information, not just that of individuals already under suspicious as a result of traditional investigative means. For that reason, our concerns about the use of private sector information (and government data originally collected for non-law enforcement or intelligence

---

[7] Individuals have won significant damages awards and settlements against companies that aggregate and disseminate consumer information. *See, e.g., Boris v. Choicepoint Services, Inc.*, No. 3:01CV-342-H (W.D. Ky.); *Thomas v. Trans Union LLC*, No. 00-1150 (D. Ore.).

purposes) grow exponentially when the government seeks to use that information as part of a data mining program.

Congress has put a temporary hold on domestic deployment of data mining technology originating from the Pentagon's "Total Information Awareness" (recently renamed "Terrorism Information Awareness") program, and it appears likely that the hold will continue through FY2004. This is a positive step, but data mining of Americans' bank, credit, medical, commercial and other records can continue unhampered at the FBI, CIA, the Terrorist Threat Integration Center (TTIC), and the various components of the Department of Homeland Security. Yet there is a host of unanswered questions regarding this technology that should be answered before it goes forward.

These questions fall into two categories. First, is the technique likely to be effective? If not, there is no reason to pursue it, particularly when we have limited resources for counter-terrorism. No government agency has yet demonstrated that this type of technology will work, and there are serious questions about whether it will generate so much information – including false positives – that it will be impossible to investigate all of the leads. Our intelligence agencies are already overloaded with information they do not have the resources to analyze; adding to that load will serve no purpose.

Second, if data mining is shown to be effective, what should be the rules governing it? Who should approve the patterns that are the basis for scans of private databases and under what standard? What should be the rules limiting disclosure to the government of the identity of those whose data fits a pattern? When the government draws conclusions based on pattern analysis, how should those conclusions be interpreted? How should they be disseminated and when can they be acted upon?

Adapting the Privacy Act and other Fair Information Practices to government uses of commercial databases is one way to look at setting guidelines for data mining. But some of those principles seem inapplicable to the intelligence context, while others need to be further augmented. Perhaps one of the most important elements of guidelines for data mining would be rules on the interpretation and dissemination of hits and on how information generated by computerized scans can be used. Can it be used to conduct a more intensive search of someone seeking to board an airplane, to keep a person off an airplane, to deny a person access to a government building, to deny a person a job? What due process rights should be afforded when adverse actions are taken against individuals based on some pattern identified by a computer program? Can ongoing audits and evaluation mechanisms assess the effectiveness of particular applications of the technology and prevent abuse?

All of these questions must be answered before moving forward with implementation. Meanwhile, Congress should insist on a full reporting from all agencies as to their uses of commercial databases. The privacy impact assessment concept in the Defense of Privacy Act may be an excellent framework for this kind of reporting. Then Congress should limit the implementation of data mining until effectiveness has been shown and guidelines on collection, use, disclosure and retention have been adopted following appropriate consultation and comment. It is time for Congress to create this framework, working with the intelligence agencies, privacy experts, and the industries that hold this data and build the technology to analyze it.

IV. CONCLUSION

CDT commends the Subcommittees for holding this important hearing. Enactment of the Defense of Privacy Act is an important step toward ensuring that federal agencies consider and

address the privacy implications of their programs. Further steps must be taken, however, to ensure that our law enforcement and intelligence agencies operate under a set of privacy-protective polices and guidelines when they access commercial information and seek to "mine" it in search of terrorists. Such guidelines would not merely to protect individual rights; they would focus government activity and make it more effective.

For more information, contact:

Jim Dempsey
(202) 637-9800 x112
jdempsey@cdt.org
http://www.cdt.org