CENTER FOR
DEMOCRACY
and
TECHNOLOGY

1634 Eye Street, NW Suite 1100
Washington, DC 20006
(202) 637-9800
http://www.cdt.org

**Privacy's Gap:**
**The Largely Non-Existent Legal Framework**
**for Government Mining of Commercial Data**
May 19, 2003

Government officials defending plans to "mine" private commercial databases looking for suspicious patterns indicative of possible terrorist activity have argued that all such data mining will be conducted in strict compliance with applicable privacy laws. What privacy laws might those be? An analysis of existing law shows that there are, in fact, few legal constraints on government access to commercial databases. The Privacy Act does not apply to private sector databases, laws on specific categories of commercial data are riddled with exceptions for law enforcement or intelligence uses, and the Constitution does not protect consumer data held by private companies.

Data mining technology – like that being researched by the Total Information Awareness ("TIA") project at the Pentagon's Defense Advanced Research Projects Agency ("DARPA") – can 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 and credit card and financial data.[1] According to DARPA, the technological capabilities being developed by TIA will search "for indications of terrorist activities in vast quantities of transaction data."

Government officials have defended this technology in part by arguing that they are relying only on information they can lawfully obtain under existing standards. DARPA Director Anthony Tether recently told a congressional subcommittee that DARPA fully intends its TIA

---

[1] DARPA argues that what it is researching does not actually amount to data mining, at least not data mining as it is practiced by marketers and other commercial entities. We use "data mining" here to refer to searches of large databases looking for data that fit patterns of potential terrorist activity. As thus defined, data mining is the use by intelligence agencies (including domestic intelligence agencies) of data in the "transactional space" where the query does not name a specific individual, location, account or other personally identifiable thing.

project to comply "with U.S. constitutional law [and] U.S. statutory law."[2] As this memo will show, that is an empty assurance. Current laws place few constraints on the government's ability to access commercial information for terrorism-related data mining.

First, since the United States has no comprehensive privacy law for commercial data, a great deal of information is available to law enforcement and intelligence agencies for purchase from data aggregators. Actually, much of this information could be voluntarily disclosed to the government by private entities, but it is far more convenient for the government to buy access to compilations, thereby "outsourcing" the compilation and maintenance of the data. Second, all existing privacy laws include exceptions of varying breadth allowing access to and sharing of data for law enforcement and/or intelligence purposes. Third, under the USA PATRIOT Act,[3] the FBI acquired broad authority for anti-terrorism purposes to issue letters or to obtain court orders compelling the disclosure of data from anyone – authority that is so broadly drafted that it seems to allow access to entire databases of information without specifying any particular person as the target. And fourth, the Supreme Court has found that consumers have no protections under the Constitution for data that businesses gather in the course of day-to-day transactions.

This stands in marked contrast to the constraints placed on private companies that wish to use consumer information, whether it be for checking an individual's credit, deciding whether to extend a job offer, or evaluating whether to issue an insurance policy. The government has argued that it should have the same access to consumer data that the private sector has, but in fact it seeks access on very different terms because the private sector is subject to strict rules when it uses consumer information – rules that do not apply to the government's proposed counter-terrorism uses. For example, under U.S. privacy laws, 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. Those same rules do not apply to government use of that information to identify possible terrorists, even though the consequences can be just as dire, or worse.

Thus, under existing law the government can ask for, purchase or demand access to most private sector data. Constraints on how the government can use the data once accessed are uncertain. Sharing is generally broadly permitted among agencies with counter-terrorism responsibilities. Some constitutional limits do apply to the use of the data to arrest or detain individuals. But to argue that data mining is not a concern because the government is only using information it can access legally under current standards sidesteps the real issue that needs to be addressed: What *should* the rules be governing this new technique? Who should approve the patterns that are the basis for scans of private databases and under what standard? What should be the legal rules limiting disclosure to the government of the identity of those whose data fit a pattern? How can data accuracy be improved and enforced? When the government draws conclusions based on pattern analysis, how should those conclusions be interpreted? How

---

[2] Statement by Dr. Anthony Tether, Director of the Defense Advanced Research Projects Agency, submitted to the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform (May 6, 2003).

[3] Public Law No. 107-56.

should they be disseminated and when can they be acted upon? What due process rights should apply to persons identified as possible terrorists?

## The Government Has Broad Authority to Obtain Commercial Information

### -- Unprotected Data: Voluntary Requests and Purchases

Because the United States has no comprehensive privacy law applicable to commercial databases, the analysis must start with a presumption of access – so long as no law prohibits it, the government can request voluntary disclosure of any commercially held records or simply purchase them. Especially since 9/11, and without having to exercise any compulsory authority, the FBI has obtained commercial databases voluntarily disclosed by private entities, from grocery store frequent-shopper records to scuba diving certification records.[4] So long as no statute prohibits government access to that information (and as will be shown below, few do), a voluntary request is entirely legal. Third parties who hold consumer information often comply with these voluntary requests because they want to be helpful or simply because compliance seems to be the path of least resistance.

Government agencies also can purchase access to private databases outright. The FBI, for example, already has contracts with several data warehousing companies that aggregate vast amounts of personal information to create dossiers on individuals.[5] Government also has access to online research systems, both free and fee-based. Some of these compile government information that is publicly available, such as court records and real estate records.

Examples of records for which there is no privacy law include:

- Travel records;
- Store purchases – online and offline, of anything ranging from books to groceries;
- "Easy Pass" toll records and building access cards;
- Real estate and mortgage information;
- Magazine subscriptions;
- Club memberships;
- Utility bills.

---

[4] 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.

[5] Glenn R. Simpson, *FBI Reliance on the Private Sector Has Raised Some Privacy Concerns*, Wall Street Journal (Apr. 13, 2001).

**-- Privacy Act**

The Privacy Act of 1974 (as modified by the Computer Matching Act of 1988) establishes certain rules for federal government records.[6] It requires notice to and consent from individuals when the government collects and shares information about them. It gives citizens the right to see whatever information the government has about them. It holds government databases to certain accuracy standards. But the Privacy Act provides little restraint on data mining of commercial databases.

First, the Privacy Act does not apply to private sector databases. The Privacy Act was passed in 1974 in response to concerns about the creation and dissemination of large government databanks of personal information, so its protections apply only where the government is creating a "system of records." But the data mining currently being developed does not involve the creation of government databases. Data mining can be conducted in such a way that the data never leave private hands. Government agencies can secure (by contract or otherwise) various scans of data held by private corporations without pulling that data into a centralized government database. If the government is simply accessing external databases created by third parties for their own reasons, it is not creating a system of records subject to Privacy Act requirements.

The Privacy Act does include a provision that extends its coverage to databases created by government contractors, but it seems that the provision does not include contractors merely providing access to their own pre-existing databases. Subsection (m) of the Privacy Act states: "When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of [the Privacy Act] to be applied to such system." Both the implementing regulations and the legislative history indicate that this provision was intended to prevent government agencies from avoiding the Privacy Act by outsourcing their systems of records to private contractors. Guidance issued by the Office of Management and Budget in 1975 and still in effect today explains that Subsection (m) applies only "to those systems actually taking the place of a Federal system which, but for the contract, would have been performed by an agency and covered by the Privacy Act."[7] Longtime OMB official Robert Bedell confirmed this reading in a 1983 congressional hearing, where he testified that Subsection (m) was added late in the process of drafting the Privacy Act to prevent an agency from entering "a contract by which an agency simply permits some contractor to operate its systems of records."[8] Implementing regulations issued in 1983 reflect this understanding, requiring contractors to comply with the Privacy Act only when "the design, development, or operation of a system of records on individuals is *required* to accomplish an agency function."[9] Thus, it

---

[6] 5 U.S.C. § 552a.

[7] 40 Fed. Reg. 28976 (July 9, 1975).

[8] Hearings before a Subcommittee of the House Committee on Government Operations, at 122-123 (June 7 and 8, 1983).

[9] 48 C.F.R. § 24.104 (emphasis added); *id*. §§ 52.224-1, 52-224-2.

appears that Subsection (m) does not cover government searches of private-sector information already collected and maintained for other purposes.

Moreover, once information is pulled into government databases, 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.[10]

- 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.[11] This does not, however, authorize disclosures to intelligence agencies.

  ***Important oversight question: Can agencies like the FBI and the Department of Homeland Security, which are both intelligence and law enforcement agencies, claim law enforcement status for purposes of some Privacy Act provisions and intelligence agency status for purposes of other provisions?***

- 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.[12] After three decades of loose judicial interpretation, this has resulted in wide-ranging claims – perhaps best exemplified by the Transportation Security Administration's January 2003 Federal Register notice indicating that it intended to share broad categories of personal data about airline passengers, which it planned to collect for its passenger pre-screening program, with a vast array of government agencies and private entities.[13]

- The definition of "computer matching" excludes matches performed for foreign counterintelligence purposes.[14]

---

[10] 5 U.S.C. § 552a(j), (k).

[11] 5 U.S.C. § 552a(b)(7).

[12] 5 U.S.C. § 552a(a)(7), (b)(3).

[13] 68 Fed. Reg. 2101 (Jan. 15, 2003). TSA officials have since stated that they intend to issue a new Federal Register notice that will differ substantially from the original notice.

[14] 5 U.S.C. 552a(a)(8)(B)(vi). Computer matching is a little like data mining, but the statutory definition of computer matching in the Privacy Act is limited to computerized comparison of automated systems of records for the purpose of administering cash or in-kind assistance programs or federal benefits programs.

The Privacy Act is not entirely irrelevant to data mining. It does prohibit a federal social service agency, for example, from disclosing its records to an intelligence agency for counter-terrorism purposes; such a disclosure probably would not fit under even the broadest definition of a "routine use." But in terms of limits on government uses of private sector databases, the Privacy Act imposes none.

**-- Fair Credit Reporting Act**

Congress has addressed the privacy of commercial databases through so-called "sectoral" legislation: separate laws for different types of data considered to need privacy protection. One of these laws is the Fair Credit Reporting Act ("FCRA"),[15] intended to protect consumers from the disclosure of inaccurate personal information held by consumer reporting agencies. In the past, consumer reporting agencies were the private sector's central source for credit, financial, employment and criminal history information. Accordingly, Congress established fairly strict rules – including how long information is kept, accuracy of information, how information is used, and rights for consumers – when credit reports are disclosed for important private sector decisions such as employment, insurance and credit (and for similar decisions by the government). However, given the way the statute is designed, those rules may not apply at all to government use of the data for purposes of predicting terrorism. To the extent that the Act does apply to the use of credit information for counterintelligence purposes, it contains a number of exceptions that enable broad government access to credit report information.

- First, the FCRA only applies to the communication of information when the information is to be used to establish eligibility for credit, insurance or employment or for other specifically enumerated purposes, none of which involve predicting terrorism. So if a consumer reporting agency voluntarily searches its database at the request of the government (or conducts the search for a fee) and discloses information about persons who fit a pattern of possible terrorist activity specified by the government, it is possible that neither the search nor any disclosures would be a "consumer report" covered by the Act.

- FCRA does not cover a significant amount of information that is contained in credit reports. Information contained in "credit headers"– certain identifying information about consumers typically found at the top of a credit report such as name, address, telephone number, and social security number – is not covered by FCRA.[16]

- The USA PATRIOT Act added a new Section 626 to the FCRA, stating that *any* government agency can compel the disclosure of "a consumer report of a consumer and all other information in a consumer's file" if the agency is authorized to investigate or engage in intelligence activities related to international terrorism and if the agency certifies in

[15] 15 U.S.C. § 1681 *et seq.*

[16] 16 C.F.R. Part 600 Appendix § 603(d)(4)(F); *In re Trans Union*, Opinion of the Commission at 30, Docket No. 9255 (FTC Feb. 10, 2000). This limitation on FCRA is particularly relevant because TSA officials have stated that their new passenger pre-screening program would rely on credit header information to verify the identity of airline passengers.

writing that the consumer reports are necessary to that investigation, activity or analysis.[17] It is unclear whether the agency needs to identify any specific consumer. Broadly interpreted, the provision would allow any agency conducting an investigation or other intelligence activities or analysis regarding international terrorism to demand access to all the records held by a consumer reporting agency or any records meeting certain parameters.

***Important oversight question: Are any agencies using Section 626 of the FCRA to obtain credit reports without naming the individuals to whom the records pertain?***

Thus, while the consumer agency could probably voluntarily disclose the information for counter-terrorism purposes because it is not a consumer report covered by the law, Section 626 authorizes the government to force disclosure.

- Another compulsory disclosure provision of the FCRA, Section 625, specifically gives the *FBI* the authority to issue National Security Letters to compel certain information from consumer reporting agencies, including the names of the financial institutions where an individual has accounts as well as identifying information about individuals, based on a showing that the information is "sought for" an authorized investigation to protect against international terrorism or clandestine intelligence activities.[18] As described in more detail below, these National Security Letters can be issued by FBI officials in field offices without judicial approval.

- Also under Section 625, the FBI can obtain an *ex parte* court order forcing disclosure of full credit reports, upon a showing that the consumer report is "sought for" the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activity.

- Section 608 of FCRA allows a consumer reporting agency to provide any government agencies with consumers' names, current and former addresses, and current and former employers, for any purpose and without any restrictions.[19]

**-- Right to Financial Privacy Act**

The Right to Financial Privacy Act ("RFPA") includes a "National Security Letter" provision giving the FBI access to bank records and other financial records for authorized foreign intelligence and international terrorism investigations and analyses.[20] The FBI must certify

---

[17] 15 U.S.C. § 1681v.

[18] 15 U.S.C. § 1681u.

[19] 15 U.S.C. § 1681f.

[20] 12 U.S.C. § 3414(a).

simply that the records in question are "sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities."[21]

**-- Graham-Leach-Bliley**

The Graham-Leach-Bliley Act,[22] enacted in 1999, includes privacy provisions requiring financial institutions to inform consumers of their privacy policies and to allow each consumer to "opt-out" of sharing information with nonaffiliated third parties. The disclosure of credit header information, although not governed by the FCRA, is subject to Graham-Leach-Bliley.[23]

Graham-Leach-Bliley and its implementing regulations include exemptions that allow government access to information for data mining purposes without notice and consent. One exemption allows disclosure of financial information, without notice or opt-out rights for the consumer, "to law enforcement agencies" or "for an investigation on a matter related to public safety" so long as "permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act."[24] Another exemption to Graham-Leach-Bliley allows disclosure of financial information "to comply with properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities."[25] Either or both of these exemptions would seem to permit disclosure or financial records in response to a National Security Letter under the RFPA or a court order obtained pursuant to Section 215 of the USA PATRIOT Act. (See below for a discussion of Section 215.)

**-- Health Insurance Portability and Accountability Act**

Congress also has enacted legislation to protect the privacy of medical records: the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[26] HIPAA and its implementing regulations provide broad law enforcement and national security exceptions.

In particular, the HIPAA regulations permit disclosure of medical information without limitation "for the conduct of lawful intelligence, counter-intelligence, and other national security activities as authorized by the National Security Act . . . and implementing authority."[27] This

---

[21] 12 U.S.C. § 3414(a)(5)(A).

[22] Public Law No. 106-102.

[23] *Trans Union LLC v. FTC*, 295 F.3d 42, 50-51 (D.C. Cir. 2002).

[24] 15 U.S.C. § 6802(e)(5); *see also* 16 C.F.R § 313.15(4).

[25] 15 U.S.C. 6802(e)(8); *see also* 16 C.F.R § 313.15(7).

[26] Public Law No. 104-191.

[27] 45 C.F.R. § 164.512(k)(2).

remarkably broad loophole could conceivably permit the government to obtain bulk collections of medical records for data mining purposes with no subpoena or court order.[28]

The HIPAA regulations also permit disclosure of medical records to federal, state and local law enforcement officials in response to a court order, judicial subpoena or grand jury subpoena, as well as an administrative request or subpoena under certain circumstances.[29] That would include a court order under Section 215 of the USA PATRIOT Act, which allows the FBI to obtain any business records, including medical records, "sought for" a terrorism or intelligence investigation.

**-- Family Educational Rights and Privacy Act**

Congress passed the Family Educational Rights and Privacy Act to protect the confidentiality and accuracy of educational records. It applies to educational institutions that receive federal funding. But Section 507 of the USA PATRIOT Act created a loophole allowing the Department of Justice to obtain educational records if the records are relevant to a terrorism investigation.[30] That provision, however, provides some greater protections than those applicable to other types of records. To obtain these records, the Justice Department must obtain an *ex parte* court order and must set out specific and articulable facts demonstrating the relevance of the requested records. Nonetheless, there is no requirement that a specific target of the investigation be identified; a broad reading of the exemption could result in the government accessing entire databases of educational records.

**-- Electronic Communications Privacy Act**

The Electronic Communications Privacy Act of 1986 (ECPA) allows the FBI to issue National Security Letters ordering disclosure of telephone and electronic communications transactional records if the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.[31] This authority covers telephone billing records, telephone and Internet customer subscriber records, and a variety of Internet and email transactional information such as date and time, the server being used or accessed, and the author and recipient of email.

---

[28] Jim McGee, *New Medical Privacy Law Opens Back Door to Intelligence Agencies*, CQ Homeland Security (Apr. 23, 2003), quoting Peter Swire, chief privacy counselor in the Clinton Administration.

[29] 45 C.F.R. § 164.512(f)(1). Health information may be disclosed pursuant to a mere administrative request or subpoena only if the information sought is "relevant and material to a legitimate law enforcement inquiry," if the request "is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought," and if de-identified information cannot reasonably be used. *Id.* § 164.512(f)(1)(ii)(C).

[30] 20 U.S.C. 1232g(j).

[31] 18 U.S.C. § 2709(b).

**-- National Security Letter Authority Under the USA PATRIOT Act**

As indicated above, the FBI has powers to compel the disclosure of certain commercial information without having to get a court order. So-called "National Security Letters" are authorized under the FCRA for credit records, under the RFPA for bank, credit card and other financial records, and under ECPA for communications transactional records. These letters can be written by FBI officials in field offices, without authorization from FBI Headquarters and without the approval of a judge. Section 505 of the USA PATRIOT Act expanded the National Security Letter authority, so now these letters need not identify a suspect or a particular person whose records are being sought; rather, if the law is broadly read, National Security Letters can require that private entities turn over or provide access to entire databases.

***Important oversight question: Is the FBI using the expanded National Security letter authority to obtain business records without naming individuals to whom the records pertain?***

Companies that receive National Security Letters are prohibited from disclosing to anyone that the FBI has requested or obtained the information.

The standard for a National Security Letter under ECPA is mere relevance to an intelligence investigation. A request for financial records does not even have to assert that the information is relevant. When an FBI official in a field office certifies that financial information is being "sought for" foreign counterintelligence purposes to protect against international terrorism or clandestine intelligence activities, financial institutions are required to comply.[32] While only the FBI can issue National Security Letters for telephone, electronic communications and financial records, the National Security Letter statutes explicitly allow the FBI to share the data it obtains with other agencies for foreign counterintelligence purposes.[33] And the Attorney General has directed the FBI to share all information in its possession with all other intelligence agencies and agencies involved with counter-terrorism activities.

**-- Business Records Authority Under the USA PATRIOT Act**

As indicated above, Section 215 of the USA PATRIOT Act gave the FBI another broad source of authority to obtain business records. This authority covers any conceivable business records, from travel records to medical records to library and bookstore records. Section 215 allows the FBI in terrorism and intelligence investigations to obtain a court order for any privately held business records without having to specify the target of the investigation.[34] Broadly read, that means the FBI can access an entire database of privately held information, rather than just the records of a particular suspect.

---

[32] 12 U.S.C. § 3414(a)(5)(A).

[33] 15 U.S.C. § 1681u(f) (FCRA); 18 U.S.C. §2709(d) (ECPA); 12 U.S.C. § 3412(a) (RFPA).

[34] 50 U.S.C. § 1861.

***Important oversight question: Is the FBI using Section 215 to obtain business records without naming individuals to whom the records pertain?***

Although the FBI must obtain an order from the Foreign Intelligence Surveillance Court to use this authority, that court is *required* to grant the request so long as the business record database is "sought for" an authorized intelligence investigation – a remarkably low standard that essentially mandates a judicial rubber stamp.

**-- Routinized Records Disclosure**

In addition to the ability to compel disclosure of records compiled by businesses for business purposes, the government has expanding power to require businesses to report data regularly to the government. For example, the anti-money laundering laws, including the Bank Secrecy Act (enacted in 1970 and expanded by the USA PATRIOT Act), impose vast reporting requirements on the financial industry, resulting in far more financial information being made available to law enforcement entities. The Bank Secrecy Act requires financial institutions to report various types of transactions to the government, and imposes certain recordkeeping and record retention requirements on the financial institutions as well. Similar reporting requirement have been imposed on universities for foreign students, and on airlines for passengers.

**What about the Constitution?**

**-- Data Held by Third Parties Is Not Protected**

Under Supreme Court decisions issued in the 1970s, data held by businesses that collect it from individuals in the course of ordinary transactions is not protected by the Fourth Amendment. In two decisions in the 1970s, the Supreme Court reasoned that consumers do not have a legitimate expectation of privacy in information they divulge to businesses. However bizarre that conclusion may be, so long as it stands the government has the power to obtain large quantities of consumer information without violating constitutional constraints.[35]

**-- Can a Computer Provide Probable Cause for a Search or Seizure?**

The Constitution's Fourth Amendment and the Due Process Clause may impose some limits on the extent to which the government can rely on "incriminating" leads generated by computer, especially where the underlying data are of dubious accuracy. The leading case is

---

[35] The *content* of electronic communications is constitutionally protected, and the government must obtain a court order by specifying the target of the wiretap and meeting an appropriately stringent standard of review. To get a court order in criminal investigations under the federal wiretap statute, the government must show that it has probable cause to believe that the individual being targeted committed, is committing or will commit a crime, and probable cause that the communications concerning the offense will be obtained. 18 U.S.C. § 2518(3). To get a court order in intelligence investigations (conducted under the Foreign Intelligence Surveillance Act), the government must show that it has probable cause to believe the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a).

*Arizona v. Evans*, 514 U.S. 1 (1995), in which a police officer ran an individual's name through his patrol car computer during a routine traffic stop. The computer indicated – incorrectly – that there was an outstanding warrant for the individual's arrest; in fact, that warrant had been quashed weeks before. The police officer nonetheless placed the individual under arrest. Justice O'Connor, in a concurrence joined by Justices Souter and Breyer, said that arrests can constitutionally be made on the basis of computer matches only if the police are relying reasonably on police databases based on the knowledge that they are updated and accurate:

> While [here] the police were innocent of the court employee's mistake [in not noting that the arrest warrant had been quashed], they may or may not have acted reasonably in their reliance on the recordkeeping system itself. Surely it would not be reasonable for the police to rely, say, on a recordkeeping system, their own or some other agency's, that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests, even years after the probable cause for any such arrest has ceased to exist (if it ever existed).

Justice O'Connor went on:

> In recent years, we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.

The same principles should apply to use of commercial databases – the government should not rely on commercial databases to develop probable cause to arrest or detain unless those databases and the method of searching them are subject to data quality and reliability standards. The fact that there are many other actions that might be taken in response to leads generated by data mining does not change that principle. To the contrary, verifying and confirming the relevance of the pattern and the reliability of the "hit" before action is taken are what will determine whether it is reasonable for the government to rely on pattern analysis to build a case.

**New Legal Protections Are Needed**

Current law provides government agencies with awesome power to obtain, access and mine commercially held data in the name of fighting terrorism. As Executive Branch agencies head into these uncharted waters, Congress must guide the way. This technology is uniquely powerful and intrusive, and should not go forward without explicit congressional authorization, limitations and oversight.

As a first step, Congress has prohibited domestic deployment of the TIA program (while permitting research and development to go forward) and required the Secretary of Defense, Attorney General and Director of Central Intelligence to issue a report due on or around May 20 detailing the efficacy, costs and privacy implications of the Total Information Awareness data

mining program, as well as their recommendations for minimizing the effects of the program on civil liberties. CDT hopes that report will spark an informed discussion among members of Congress, federal officials, industry leaders, and privacy advocates about the effectiveness of the TIA approach and the appropriate legal limits on data mining. Indeed, the threshold question of whether data mining is an effective way to identify terrorists must be answered before we turn to the civil liberties implications of the technology.

But let us be clear: It is no answer to concerns about government access to commercial databases to assert that agencies will comply with all existing privacy laws. Existing standards are outmoded. They do not contemplate the networked world and the capability to "ping" or scan huge databases without actually acquiring them. The USA PATRIOT Act changes, while never justified in the name of data mining, seem to provide compulsory power should the government want to obtain the data and bring it into their systems. If the new technology is proven effective and the decision is made to go forward, new standards are needed.

The development of those standards needs to be carried out through a consultative approach. CDT is just beginning its own thinking. At this point, we believe that a logical starting point for those guidelines is the long-standing model of "Fair Information Practices" – principles that have been agreed upon by the federal government, privacy experts and some industry groups. These principles include, for example, the notice concept – that, to the extent possible, individuals should be notified when information about them is being collected and how it will be used; the retention limitation – that information should be retained for no longer than is necessary to serve the purpose for which it was collected; and the data quality principle – that those collecting and holding information have a duty to keep it accurate and up-to-date. These principles are reflected in the Privacy Act, and elements of them appear in the "sectoral" federal privacy laws for commercial databases, albeit in weakened form due to the many broad exceptions discussed above. The challenge is to map those principles to the decentralized models of data mining currently being pursued.

Adapting the Privacy Act to government uses of commercial databases is one way to look at setting guidelines for data mining. But some of the Privacy Act provisions are simply inapplicable and others would need to have much greater emphasis. For example, perhaps one of the most important elements of a set of data mining guidelines 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, to arrest a person? This needs to be spelled out. Then procedures need to be adopted that provide due process to persons identified as possible terrorists when adverse actions are taken against them. These procedures may differ depending on the type of action taken; a person denied a job may have more rights than a person subject to a search at an airport. Other rules could include:

- Judicial or senior Executive Branch approval for the patterns that are the basis for scans of private databases.

- Judicial approval for the disclosure to the government of the identity of those whose data fit a pattern.

- Ongoing auditing and evaluation, to assess the effectiveness of particular applications of the technology.

As members of Congress consider future action on the Total Information Awareness program, CDT urges them to evaluate the lack of legal constraints on government data mining efforts, and critically assess the need for new rules.

For more information, contact Jim Dempsey at jdempsey@cdt.org, (202) 637-9800 ext. 112, or Lara Flint at lflint@cdt.org, (202) 637-9800 ext. 113.