Commercial Data and National Security

James X. Dempsey & Lara M. Flint*

Introduction

In an effort to make better use of information technology in combating terrorism, the federal government is researching, and in some cases already implementing, new ways to use the vast databases of personal information collected commercially by companies in almost every line of business and by the data warehouses and aggregators that have become an important part of the information-based economy. The information available in private databases ranges from insurance, travel, and financial data, to records of retail purchases, to information compiled from disparate governmental records such as court papers, licenses, and property records. Reflecting trends that began before September 11, 2001, but that have accelerated since then, the new data environment has two unprecedented features: the depth and breadth of personally identifiable information available from private sources, and the capacity to analyze such data and draw from it patterns, inferences, and knowledge. Even proponents of the use of private databases for purposes of counterterrorism acknowledge that the combination of these two factors has grave privacy and due process implications.[1] Yet, the development and implementation of data analysis techniques for counterterrorism purposes is proceeding without a suitable legal framework. While there are some legal constraints on the government's use of commercial data for counterterrorism purposes, they are fragmentary, incomplete, and unresponsive to the kinds of uses that are associated with the current emphasis on the prevention of terrorism through intelligence collection and analysis.[2]

---

* James X. Dempsey is Executive Director and Lara M. Flint is Staff Counsel at the Center for Democracy and Technology, Washington, D.C. Research for this article was supported by grants from the Open Society Institute, the Markle Foundation, and the John D. and Catherine T. MacArthur Foundation.

1 *See* SEC'Y OF DEF., ATTORNEY GEN. & DIR. OF CENT. INTELLIGENCE, REPORT TO CONGRESS REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM: IN RESPONSE TO CONSOLIDATED APPROPRIATIONS RESOLUTION, 2003, PUB. L. NO. 108-7, DIVISION M, § 111(B) 27–35 (2003) (analyzing the impact of the Terrorism Information Awareness program on privacy and civil liberties at the request of Congress); PAUL ROSENZWEIG & MICHAEL SCARDAVILLE, CTR. FOR LEGAL & JUDICIAL STUDIES, HERITAGE FOUND., LEGAL MEMORANDUM NO. 6: THE NEED TO PROTECT CIVIL LIBERTIES WHILE COMBATING TERRORISM: LEGAL PRINCIPLES AND THE TOTAL INFORMATION AWARENESS PROGRAM 4 (2003) (arguing that increased intrusions on privacy caused by new counterterrorism technologies need to be justified by the "particular nature, significance, and severity of the threat being addressed by the program"); PAUL ROSENZWEIG, CTR. FOR LEGAL & JUDICIAL STUDIES, HERITAGE FOUND., LEGAL MEMORANDUM NO. 8: PROPOSALS FOR IMPLEMENTING THE TERRORISM INFORMATION AWARENESS SYSTEM 7–23 (2003) (proposing mechanisms to ensure that data mining technology is implemented with minimal risk to civil liberties); K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1, 50–74 (2003) (examining the privacy concerns associated with use of new data mining technologies).

2 Among the few in-depth analyses of the legal and policy issues raised by the prospect of using commercial data for counterterrorism purposes are the reports of the Technology and Pri-

Some of the issues surrounding governmental use of commercial databases were brought to the fore in late 2002 and early 2003, thanks to news reports and commentary about the Total Information Awareness program, renamed the Terrorism Information Awareness ("TIA") program, conducted under the auspices of the Pentagon's Defense Advanced Research Projects Agency ("DARPA").[3] In the fall of 2003, Congress cut off funding for TIA research, giving rise to the impression that the government had retreated from the use of commercial data.[4] To the contrary, various other government agencies continue to explore the use of commercial sector data for counterterrorism and other law enforcement and intelligence purposes, and the private sector continues to develop and offer the government services and systems based upon the aggregation and analysis of personally identifiable information available to the private sector.[5]

---

vacy Advisory Committee established by the Secretary of Defense and of a private sector task force organized by the Markle Foundation. *See* TECH. & PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM (2004), *available at* http://www.sainc.com/tapac/finalreport.htm; MARKLE FOUND. TASK FORCE ON NAT'L SECURITY IN THE INFO. AGE, CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY (2003); MARKLE FOUND. TASK FORCE ON NAT'L SECURITY IN THE INFO. AGE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE (2002). Both Markle reports are available at http://www.markle.org. *See also* MARY DEROSA, CTR. FOR STRATEGIC & INT'L STUDIES, DATA MINING AND DATA ANALYSIS FOR COUNTERTERRORISM (2004); GINA MARIE STEVENS, CONG. RESEARCH SERV., PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS (2003).

3 *See*, *e.g.*, Robert O'Harrow, Jr., *U.S. Hopes to Check Computers Globally; System Would Be Used to Hunt Terrorists*, WASH. POST, Nov. 12, 2002, at A4; William Safire, *You Are a Suspect*, N.Y. TIMES, Nov. 14, 2002, at A35.

4 The Defense Department appropriations bill for fiscal year 2004 eliminated funding for TIA. *See* Department of Defense Appropriations Act, Pub. Law No. 108-87, § 8131(a)–(b), 117 Stat. 1054, 1102 (2004). Specifically, the law stated:

> (a) Notwithstanding any other provision of law, none of the funds appropriated or otherwise made available in this or any other Act may be obligated for the Terrorism Information Awareness Program: *Provided*, That this limitation shall not apply to the program hereby authorized for Processing, analysis, and collaboration tools for counterterrorism foreign intelligence, as described in the Classified Annex accompanying the Department of Defense Appropriations Act, 2004, for which funds are expressly provided in the National Foreign Intelligence Program for counterterrorism foreign intelligence purposes.
>
> (b) None of the funds provided for Processing, analysis, and collaboration tools for counterterrorism foreign intelligence shall be available for deployment or implementation except for:
>
> (1) lawful military operations of the United States conducted outside the United States; or
>
> (2) lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States citizens.

Id. The accompanying conference report specified that four specific research programs of the Information Awareness Office could continue, but none of those is related to "pattern analysis" or "data mining" as discussed in this article. *See* H.R. REP. NO. 108-283, at 327 (2003), *reprinted in* 2003 U.S.C.C.A.N. 1168, 1189.

5 GENERAL ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES, GAO -04-548 (2004), *available at* http://www.gao.gov/new.items/d04548.pdf.

It is beyond the scope of this article to examine the questions of effectiveness.[6] In general, however, it seems indubitable that there are uses of commercial data, and combinations of government and commercial data, that could aid in the fight against terrorism. Without presuming to answer the effectiveness issues, and without underestimating the importance of those questions as a threshold matter, this article focuses on the privacy issues posed by uses of private sector databases for national security: what are the risks to privacy, why are the current privacy laws insufficient, and what should be the rules for this new capability? While government, corporate, and academic researchers are assessing the effectiveness of specific applications, policymakers need to consider simultaneously the privacy and civil liberties issues associated with uses of private sector data for counterterrorism, before moving forward on implementation. If those developing information systems take privacy into account in the research and development phase, they can build privacy protections into the design of applications, which is

6 In considering the application of information technologies to counterterrorism, efficacy should be a threshold issue, for if we cannot show that a particular use of commercial databases will yield improvements in national security, then we should not deploy the capability, and we need not reach civil liberties questions. Some uses of commercially compiled data, such as quickly determining where a suspect may be residing, are clearly effective. The efficacy of others, including some of the pattern-based searches sometimes referred to as "data mining," remain speculative and unproven. Assessments of efficacy—including questions of reliability, error rates (false positives and false negatives), and cost—can only be made reliably in the context of specific applications and based on objective research. The examination of efficacy must also include a consideration of alternatives, given that the government has limited resources to allocate to anti-terrorism efforts. Analysis of commercial data must be shown to be more effective than other techniques not yet fully implemented, notably, techniques that would improve the government's ability to use the information that it has already collected by traditional means for the express purpose of identifying terrorists. If efforts are lagging to better analyze and share information about individuals already suspected of terrorist ties, and their associates, it makes little sense to divert resources to the examination of data not initially collected for the purpose of identifying terrorists—data that primarily relates to persons with no suspected ties to terrorism. And within the context of uses of commercial data, it would seem to be more effective to use commercial data to augment suspicions or leads generated by traditional law enforcement or intelligence methods, rather than engaging in pattern-based queries on the lawful transactions of millions of innocent persons. Congress should focus its oversight on questions like whether the FBI is analyzing all the communications it intercepts and whether it is tracking down all of the leads emerging, for example, from information seized from terrorist training camps in Afghanistan. *See generally Securing Freedom and the Nation: Collection Intelligence Under the Law: Hearing Before the House Perm. Select Comm. on Intelligence*, 108th Cong. (2003) (statement of Kate Martin, Dir., Ctr. for Nat'l Sec. Studies), *available at* http://intelligence.house.gov/PDF/martin040903.pdf, 2003 WL 1890887. To advance the assessment of efficacy, government agencies should be much more explicit publicly about what commercial information they really want and how they intend to use it. Congress should insist upon public review of the specifics of how government proposes to use information. This can occur without compromising the methods themselves. In this regard, the congressional decision in 2003 to cut funding entirely for DARPA research into "data mining" for counterterrorism purposes may make it harder to assess effectiveness, for it pushed the research, and therefore the consideration of efficacy questions, into classified programs and proprietary contexts. The approach of the earlier "Wyden Amendment" was preferable—it allowed TIA research to go forward, but prohibited domestic deployment until the government addressed both efficacy and privacy. *See* Consolidated Appropriations Resolution, Pub. L. No. 108-7, Div. M, § 111, 117 Stat. 11, 534–36 (2003).

easier and more effective than trying to add on privacy protections after a project is launched.

This article focuses on agencies operating primarily in the United States that can collect information on citizens and non-citizens alike. We do not examine the difficult set of issues arising from the "line at the border," which distinguishes between the foreign intelligence agencies operating primarily overseas and the law enforcement and counterintelligence agencies operating primarily in the United States. Specifically, we do not consider whether intelligence agencies operating primarily overseas may be subject to limits in collecting or accessing data on U.S. citizens.[7]

I. Introduction to Privacy Issues Posed by Use of Commercial Data for Purposes of Counterterrorism

A. Definitions and Framework

1. What Do We Mean by "Privacy"?

With respect to personally identifiable information provided to the government or generated in the context of commercial transactions, privacy is not just about keeping information confidential or secret. Rather, as is well established by United States Supreme Court cases, the Privacy Act, and privacy laws governing the private sector, 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.[8] In these various contexts, privacy is about control, fairness, and consequences, rather than simply keeping information confidential. Data privacy laws thus 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 be able to manage the consequences of 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 fact that data is sold or exchanged commercially or that it is "publicly available" does not mean that the information can be used without privacy constraints. Much of the data compiled by the private sector is subject

7 "U.S. person" is a term of art that refers to U.S. citizens, permanent resident aliens, and U.S. corporations. *See* 50 U.S.C. § 1801(i) (2000).

8 In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court rejected the "cramped notion of personal privacy" that "because events . . . have been previously disclosed to the public, . . . [the] privacy interest in avoiding disclosure of a . . . compilation of these events approaches zero." U.S. Dep't of Justice v. Reporters Comm. for the Freedom of the Press, 489 U.S. 749, 762–63 (1989); *see also* Reno v. Condon, 528 U.S. 141, 148 (2000) (upholding federal regulatory scheme restricting states' sale of driver's license information to commercial entities). The Privacy Act and federal privacy legislation governing various kinds of commercial data are described in Part II.

to statutory rules intended to protect the values of fair information use. Arrest records, for example, are publicly available governmental records, but they cannot be used for employment purposes unless they include disposition data.[9] Driver's license data is available for some purposes and not for others.[10] Bankruptcy records are publicly available, but cannot be included in credit reports if they are more than ten years old.[11] Private compilations of publicly available data used for certain commercial purposes are subject to data quality requirements.[12] Individuals are legally entitled to access their credit reports and insist upon corrections, even though none of the data in the reports is confidential and some of it is publicly available.[13]

Moreover, the compilation of publicly available data into computerized form can change the privacy equation in terms of its use and disclosure. For example, the Supreme Court has held that the government can withhold from public disclosure databases composed entirely of publicly available data because there is a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information . . . and revelation of the [information] as a whole."[14] The Court further noted: "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[15]

For these reasons, while the phrase "publicly available" may be used to mean that data was obtained from a source available to anyone, it says little about how information can be used when compiled and sold for commercial

---

9 A series of cases arising under Title VII prohibited the use of arrest records without convictions as the basis for denying employment. *See*, *e.g.*, Reynolds v. Sheet Metal Workers Local 102, 498 F. Supp. 952, 973 (D.D.C. 1980), *aff'd*, 702 F.2d 221 (D.C. Cir. 1981) (noting disparate racial impact of arrest record inquiry and holding that because "defendants have made no attempt to validate the arrest inquiry as job related . . . it must be eliminated"); Gregory v. Litton Sys., 316 F. Supp. 401, 403 (C.D. Cal. 1970), *modified on other grounds*, 472 F.2d 631 (9th Cir. 1972) (holding employer's policy of denying employment to persons arrested a certain number of times but not convicted "unlawful because it has the foreseeable effect of denying black applicants an equal opportunity for employment"). Government employers and licensing authorities are subject to constitutional standards in making decisions, and the Supreme Court has held that it is a due process violation to exclude a person from the practice of law or other occupations, based solely on an arrest that did not result in a conviction. *See* Schware v. Bd. of Bar Exam'rs, 353 U.S. 232, 238–43 (1957); *see also* Fair Credit Reporting Act § 605, 15 U.S.C.A. § 1681c(a)(2), (5) (West 1998 & Supp. 2003).

10 *See* Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725, § 2721(b) (2000) (specifying permissible purposes for disclosing driver's license information).

11 *See* Fair Credit Reporting Act § 605, 15 U.S.C.A. § 1681c(a)(1).

12 *See id*. § 1681e(b) (requiring consumer reporting agencies preparing consumer reports to follow "reasonable procedures to assure maximum possible accuracy"); *see also* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, §§ 311–318, 117 Stat. 1952, 1988–99 (amending the Fair Credit Reporting Act to enhance accuracy requirements).

13 *See* Fair Credit Reporting Act §§ 609–611, 15 U.S.C.A. § 1681g–1681i.

14 U.S. Dep't of Justice v. Reporters Comm., 489 U.S 749, 764 (1989).

15 *Id*. The Court thus rejected the notion that an individual has no privacy interest in data that is publicly available somewhere. *See id*. at 770 ("In sum, the fact that an event is not wholly 'private' does not mean that an individual has no interests in limiting disclosure or dissemination of the information." (quotation omitted)).

purposes, or how it should be used by the government in law enforcement, intelligence, or homeland security efforts.

2. What Is Data Mining?

Policy discussions about counterterrorism uses of commercial data often lack clarity because terms such as "data mining," "pattern analysis," "knowledge extraction," "dataveillance," and other ambiguous and sometimes loaded terms mean different things to different people.[16] In this article, we try to be more specific. Primarily, we distinguish between uses of data that are "pattern based" and those that are "subject based." We use the term "pattern-based" searches to refer to searches of large databases when the query does not name a specific individual, address, identification number, or other personally identifiable data element, but instead seeks information that matches or departs from a pattern. Proposed uses of pattern-based searches in the counterterrorism context are based on the premise that the planning of terrorist activity creates a pattern or "signature" that can be found in the ocean of transactional data created in the course of everyday life.[17] In contrast to pattern-based searches, "subject-based" queries are data searches that seek information about a particular subject already under suspicion based on information derived from traditional investigative means, whether that subject is represented by a name, a telephone number, or a bank account number. Another use of data is "link analysis," the process of finding linkages or relationships among individuals in a data set or across data sets (e.g., finding that two people with different last names live at the same address). Link analysis may be either subject based or pattern based. "Risk assessment" refers to the use of data to determine whether a particular individual (or transaction) poses a risk or threat based upon predictors drawn from past experience or expert speculation as to what characteristics or behaviors are indicative of a fraudulent or otherwise malevolent intent. Risk assessment may involve use of subject-based queries to draw together information about a person from disparate databases, which may then be compared to a profile or pattern developed to identify unusual behavior or characteristics correlated with risk. "Screening" is an approval process—it may involve a physical search (such as walking through a metal detector), comparing the name of a person with names on a watch list of suspects, or conducting a risk assessment based on multiple factors. "Identity resolution" is the process of determining whether various pieces of information pertain to the same individual. At its simplest, identity resolution determines whether "Bob Jones" and

16 For example, while critics of the TIA projects routinely referred to them as "data mining," DARPA officials rejected use of the term. *See* Dr. Tony Tether, Director, DARPA, Written Statement Submitted to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census of the House Committee on Government Reform 2 (May 6, 2003), http://reform.house.gov/UploadedFiles/DARPA%20testimony.pdf (last visited June 26, 2004).

17 For example, according to Dr. John Poindexter, head of TIA, the technological capabilities being developed by TIA were intended to search "for indications of terrorist activities in vast quantities of transaction data." *See* John Poindexter, Director, Information Awareness Office, DARPA, Remarks as Prepared for Delivery at DARPATech 2002 Conference (Aug. 2, 2002), http://www.fas.org/irp/agency/dod/poindexter.html (last visited June 26, 2004).

"Robert Jones" are the same person. It is the basis of much data aggregation and is often a crucial first step in risk assessment and link analysis. As we explain below, the privacy implications of these various uses of data are quite different and therefore deserve different rules.

Further distinctions may clarify consideration of the civil liberties implications of the use of commercial data for national security purposes. To begin to understand how rules could be crafted to promote fair and effective use of such information, it may be beneficial to consider a series of axes that define various ways of using personally identifiable information.

One axis contrasts the use of data collected by the government for the purposes of counterterrorism with the use for counterterrorism purposes of data collected by the private sector for business reasons. At one end of this axis, improved analysis of data collected by the government specifically for counterterrorism purposes offers obvious benefits and should be a priority of national security information technology efforts.[18] At the other end of the axis is the government's access to, and analysis of, commercial data generated in the course of ordinary business transactions. We focus on the government's use of commercial data for counterterrorism because it poses unique, and so far unresolved, concerns. In the middle of this axis, although closer to the commercial data end, is the counterterrorism use of the vast array of personally identifiable information collected by the government for non-terrorism purposes—for example, tax and Social Security records. Use of such data in counterterrorism investigations poses issues similar to those associated with the use of commercial data.[19] Also in the middle of this axis is data collected by the government for purposes unrelated to terrorism, which is copied by commercial entities from various open records systems such as court records and sold back to the government in compiled electronic formats.

---

18 This is not to suggest that we have no concerns about the legal authorities under which government agencies initiate the collection of information for counterterrorism purposes. For example, we have argued elsewhere that certain standards in the statutes for interception of communications and associated transactional information are inadequate. *See*, *e.g.*, *Freedom After Sept. 11: Hearing Before the Senate Comm. on the Judiciary*, 108th Cong. (2003) (statement of James X. Dempsey, Executive Dir., Ctr. for Democracy and Tech.); *Terrorism Investigations and the Constitution: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 108th Cong. (2003) (statement of James X. Dempsey, Executive Dir., Ctr. for Democracy and Tech.). We accept the basic premise, however, that the government should have, subject to appropriate controls, the authority to obtain relevant information from almost every source about individuals suspected with particularity of participating in or planning terrorism. We also have concerns about the absence of meaningful standards and oversight for the transfer of data between intelligence agencies and law enforcement agencies, but again we agree that, subject to safeguards, counterterrorism information should be shared among government agencies.

19 The government's use for counterterrorism of information collected for non-terrorism purposes also poses risks to the integrity and efficiency of the program for which the information was originally collected. For example, using tax records to try to predict patterns of terrorism may seem appealing but could further erode trust in the tax system, exacerbating hesitancies to accurately self-report earnings information. To protect the tax system, as well as personal privacy, federal law prohibits use of tax records for purposes unrelated to administration of the tax system. *See* 26 U.S.C.A. § 6103 (West 1998 & Supp. 2003), *amended by* Pub. L. No. 108-173, 117 Stat. 2066 (2003); Pub. L. No. 108-89, 117 Stat. 113 (2003).

A second axis distinguishes between data that is "publicly available" and data that is normally shared only among users within a closed network (such as financial records shared only within the financial services industry). People often use the terms relating to this axis ambiguously, clouding the policy analysis. In reference to data, "public" can mean either "governmental" or "publicly available." "Private" can mean either "held by a private sector entity (including data copied from a government source by a private sector aggregator)" or "confidential." Moreover, "publicly available" is used in several different ways. It can refer to information that is widely available for free, such as information in telephone directories, available on the Internet with a Google search, or published in newspapers. "Publicly available" can also mean information that is available for free, but with effort, such as arrest records, bankruptcy filings, land ownership records, and other governmental records that are publicly available to anyone willing to go down to the courthouse or other government office and transcribe them. Private companies collect much of this "publicly available" government data and sell it. When this data is collected and compiled, it may be referred to as "public source" or "publicly available" by virtue of the fact that it is drawn from public records, but this does not mean that any member of the public can afford to access it. In its compiled form, this data, while "publicly available," is proprietary, and its use is controlled by contractual and other protections intended to preserve its value. "Publicly available" also sometimes refers to data held by non-governmental entities, even if that data is rarely disclosed or is shared only within closed networks. We prefer to use the term "publicly available" rather narrowly to refer to data drawn from any public source, such as newspapers, the Internet, and government records open to public inspection. We refer to other data that may be commercially sold by more specific terms, such as "credit reports."

Another axis expresses the distinction between subject-based and pattern-based searches. Subject-based searches, which involve querying governmental or private sector data to find out more about an individual already under suspicion—address, assets, financial activities, travel, linkages to others—are an investigative method that law enforcement agencies have used for years. In contrast, pattern-based searches involve queries in the absence of particularized suspicion for data patterns believed to be associated with terrorism. The pattern may be based on some specific intelligence (e.g., a tip that unknown terrorists are planning an act through certain means) or it may be purely hypothetical (based on informed speculation of how terrorists might act). Pattern-based searches may be performed on data acquired by the government for counterterrorism purposes or on governmental or commercial data collected for nonterrorism purposes. As a general matter, there are fewer privacy concerns associated with the use of commercial data for subject-based searches intended to locate or learn more about a specific suspected terrorist than there are with the use of commercial data for pattern-based searches. Pattern analysis raises the most serious privacy and civil liberties concerns because it involves examination of the lawful daily activities of millions of people. Pattern analysis poses concerns under both the constitutional presumption of innocence and the Fourth Amendment principle that

the government must have individualized suspicion before it can conduct a search. As one commentator has argued:

> [W]hen the government engages in mass dataveillance to conduct general searches of millions of citizens without cause to believe that a crime has been committed, the searches arguably raise the same dangers in the twenty-first century as the general warrants that the Framers of the Fourth Amendment feared in the eighteenth century.[20]

A fourth axis concerns the sensitivity of the data. Discerning the sensitivity of data can require subtle distinctions. Medical records are generally seen as more sensitive than travel records, but within a medical record the name and address of a patient is far less sensitive than information about diagnosis and treatment. Therefore, accessing only an address in medical records in order to locate a person is far less troublesome than using travel records to draw inferences about a person's intentions. Another distinction that pertains to sensitivity is whether data is identified with a particular person, or "de-identified." De-identified data is generally less sensitive. For example, collecting diagnosis data from emergency rooms without patients' names and using that data to spot trends in symptoms poses very different concerns than accessing the symptom data with names or other personal identifiers attached.

A fifth axis distinguishes among various uses or consequences. At one end is the use of commercial data to locate a person already determined through traditional investigative means to be a possible terrorist. Link analysis techniques to determine who has associated with a known or suspected terrorist lie further along the axis. Further along the axis is the use of data to trigger suspicion, as the predicate for further investigation. A trigger might be as simple as the fact that a person on an expired visa has applied for pilot's training. Finally, at the far end of the spectrum is the use of data as the basis for some adverse action, which might range from subjecting someone to more intensive screening at an airport to denying someone a job.

These axes are not perfectly descriptive of the complex informational landscape. Indeed, analysis of the issues is complicated by the fact that the distinctions we have drawn are blurring. For example, if a counterterrorism analyst has the name of a specific suspected terrorist and queries various databases looking for other information associated with that name (bank account numbers, addresses, vehicle registrations, phone numbers), that is clearly a subject-based query. But what if the analyst has only non-unique physical, ethnic, or occupational descriptors of a specific individual and seeks all records matching that description in an effort to identify the individual? And while we can distinguish between searches of governmental databases compiled for counterterrorism purposes and searches of private sector databases compiled for purposes unrelated to terrorism, what if the govern-

---

20 *Data Mining: Current Applications and Future Possibilities: Hearing Before the House Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, Comm. on Gov't Reform*, 108th Cong. (2003) (statement of Jeffrey Rosen, Assoc. Professor, The George Washington Univ. Law Sch.).

ment uses its coercive powers or its procurement authority to acquire entire databases of privately held data and then searches the data repeatedly? Is that a search of commercial data, or is it a search of governmental data collected for counterterrorism purposes? In the course of a criminal investigation, such as the investigation of the September 11 crimes, the government can issue broad subpoenas for data from commercial entities, such as the companies that process airline reservations. Under traditional investigative techniques, that data could be subject to computer analysis, including link analysis or pattern-based queries. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act allows data to be broadly shared among law enforcement and intelligence agencies.[21] Should policy treat subsequent searches of such data as searches of governmental data acquired specifically for purposes of counterterrorism, or should the rules treat them as searches of commercially provided data?

In sum, the contemporary landscape of personally identifiable information is complex. Of necessity, the rules for accessing and using this data will have to be equally complex, depending on the type of data and the uses of it.

B. Use of Commercial Data by the Government for Counterterrorism Purposes

Although TIA has been defunded, a myriad of law enforcement, intelligence, and homeland security programs rely (or are planning to rely) on commercial data, and some are using forms of pattern-based analysis.[22] For example, through the Secure Flight project, the Transportation Security Administration intends to rely on commercial databases to verify the identity of airline passengers.[23] The Foreign Terrorism Tracking Task Force of the Department of Justice ("DOJ") is employing "risk modeling algorithms, link analysis, historic review of past patterns of behavior, and other factors to distinguish persons who may pose a risk of terrorism from those who do not."[24] Changes to the Attorney General Guidelines in 2002 expressly gave the Federal Bureau of Investigation ("FBI") authority to engage in "data mining,"[25] and the FBI has entered into contracts with at least one data warehousing company.[26] The Information Analysis and Infrastructure Protection

---

21 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 203, 115 Stat. 272, 278–81; *see also infra* Part III.

22 GENERAL ACCOUNTING OFFICE, *supra* note 5.

23 *See* Privacy Impact Assessment; Secure Flight Test Phase, 69 Fed. Reg. 57,352 (Sept. 24, 2004); Privacy Act of 1974: System of Records; Secure Flight Test Records, 69 Fed. Reg. 57,345 (Sept. 24, 2004).

24 STEVENS, *supra* note 2, at CRS-3. **R**

25 DEP'T OF JUSTICE, ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS 21–22 (May 30, 2002), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf (last visited June 26, 2004) [hereinafter ATTORNEY GENERAL GUIDELINES].

26 *See* Memorandum from the National Security Law Unit, Office of the General Counsel, FBI, to National Security Division, FBI, on Guidance Regarding the Use of Choicepoint for Foreign Intelligence Collection or Foreign Counterterrorism Investigations 1 (Sept. 17, 2001)

Directorate at the Department of Homeland Security ("DHS") has congressional authorization to use "data mining" technology.[27] On May 1, 2003, the Terrorist Threat Integration Center commenced operations with the mandate to analyze the full breadth of intelligence information, making it an almost certain candidate for the use of pattern analysis technology. Indeed, the government has been using pattern-based searches for some time. The Financial Crimes Enforcement Network ("FinCEN") relies on pattern-based searches to try to identify from among all large money transfers the few that involve money laundering.[28] The Securities and Exchange Commission uses pattern-based searching to identify insider trading.[29] And numerous state and local governments are joining the antiterrorism crusade by exploring the use of aggregated commercial and governmental data in a DHS- and DOJ-funded system known as the Multistate Antiterrorism Regional Information Exchange System ("MATRIX").[30] In many instances, governmental entities draw on the databanks and expertise of the commercial sector, which has relied on pattern-analysis technology for years to track customer purchases, hone direct marketing techniques, and prevent credit card fraud.[31]

C. Challenges of Using Commercial Data for Government Purposes

While government agencies already rely on commercial data, both existing and potential uses face significant challenges. One serious challenge to effective governmental use of commercial information is the quality of the data.[32] One study indicated that seventy percent of credit reports have some

---

(responding to request from the National Security Division "for advice concerning legal restrictions on the use of ChoicePoint, a data warehousing company, for foreign intelligence collection or foreign counterintelligence investigations"), *available at* http://www.epic.org/privacy/publicrecords/cpfcimemo.pdf (last visited June 26, 2004); *see also* Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint: U.S. Agencies' Growing Use of Outside Data Suppliers Raises Privacy Concerns*, WALL ST. J., Apr. 13, 2001, at A1.

27 *See* Homeland Security Act of 2002, Pub. L. No. 107-296, § 201(d)(14), 116 Stat. 2135, 2145–47.

28 The USA PATRIOT Act specified that FinCEN was to provide government-wide access to information collected under the anti-money laundering laws, records maintained by other government offices, as well as privately and publicly held information. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 361, 115 Stat. 272, 329–32.

29 *See* Taipale, *supra* note 1, at 16 n.43. **R**

30 *See, e.g.*, Robert O'Harrow, Jr., *U.S. Backs Florida's New Counterterrorism Database: 'Matrix' Offers Law Agencies Faster Access to Americans' Personal Records*, WASH. POST, Aug. 6, 2003, at A1. MATRIX has been the subject of considerable controversy, and several states have pulled out of the project citing privacy concerns. *See, e.g.*, Duane D. Stanford & Joey Ledford, *State Can't Give Driver Records to the Matrix*, ATLANTA J.-CONST., Oct. 21, 2003, at A1 (discussing statement of Georgia Attorney General that it would be illegal for the state to turn over driver records, which include personal information, for use in MATRIX system).

31 *See* Jim McGee, *Is Computer Snooping on the Ropes? Not by a Long Shot*, CONG. Q. HOMELAND SEC. 2.0 ¶ 30 (Mar. 5, 2003) (on file with The George Washington Law Review); Simpson, *supra* note 26, at A1. The FBI's use of commercial data includes a contract with one **R**
data aggregator providing access to fourteen billion public records. *See* McGee, *supra*, ¶ 30; Memorandum from the National Security Law Unit, *supra* note 26, at 1. **R**

32 Data quality concerns plague government databases as well. *See* JOAN FRIEDLAND, NAT'L IMMIGRATION LAW CTR., INS DATA: THE TRACK RECORD (2003), *available at* http://www.nilc.org/immlawpolicy/misc/INS%20data%20accuracy.pdf (last visited June 26, 2004) (com-

mistakes, and almost one third have such serious errors that they affect whether the individual is denied credit.[33] Identity theft, for example, adds erroneous data to commercial databases.

Another challenge facing the government is that, in some important ways, the questions being posed by government agencies searching for terrorists in data patterns are harder to answer than the questions usually posed by commercial users of that data. For many applications in the commercial context, the relevant question is simply *what* an individual is doing—with no great concern for that individual's motives. In the terrorist context, the relevant question is *why* an individual took a particular action, such as renting a car or purchasing chemicals. While pattern analysis can objectively identify what a person has done, and even say whether it is within a norm, it is far harder to attribute motivation to actions.

There are commercial uses of data that do assess motive, such as those that analyze seemingly innocent transactions to detect fraud. The government's task of identifying potential terrorists, however, is far more difficult from a statistical perspective than the private sector's task of preventing fraud or identifying risk. In the commercial context, there is a large baseline of known frauds that can be used to develop and constantly refine the risk assessment patterns. In contrast, agencies searching for a terrorist signature have a very small sample set on which to base their predictions. From a statistical perspective, there are few known terrorists whose behavior analysts can study, and the next set of terrorists may very likely display behaviors that do not match prior patterns. It is quite uncertain whether a computer pro-

piling list of General Accounting Office and Office of Inspector General reports detailing accuracy and related problems with U.S. immigration data). As Mark Forman, then-Associate Director of the Office of Management and Budget ("OMB"), told a congressional subcommittee, the quality of agency databases is often "poor," which leads to the inevitable result of "garbage in, garbage out" when the government attempts to rely on those databases. *Davis Dismisses Calls for Data Mining Regulations*, WASH. INTERNET DAILY, Mar. 26, 2003 (on file with The George Washington Law Review). Rather than addressing these data quality problems, however, some agencies are giving less attention to data quality. For example, in March 2003, the FBI issued a notice that it no longer intended to attempt to maintain the accuracy and timeliness of information in the National Crime Information Center ("NCIC"), a key law enforcement information system used daily by virtually every law enforcement entity in the country, because it would no longer comply with subsection (e)(5) of the Privacy Act. *See* Exemption of Records Systems Under the Privacy Act, 68 Fed. Reg. 14,140 (Mar. 24, 2003) (to be codified at 28 C.F.R. pt. 16) (exempting the FBI from subsection (e)(5) of the Privacy Act that requires government agencies to maintain their records "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination," 5 U.S.C. § 552a(e)(5) (2000)). Civil liberties advocates urged the government to reconsider that decision. *See* Joint Letter and Online Petition from the Electronic Privacy Information Center to the OMB 2 (Apr. 7, 2003), http://www.epic.org/privacy/ncic/ (last visited Mar. 4, 2004) (urging the OMB to "exercise its oversight responsibilities" by "reviewing and revising" the rule).

33 *See* JON GOLINGER & EDMUND MIERZWINSKI, U.S. PUBLIC INTEREST RESEARCH GROUP, MISTAKES DO HAPPEN: CREDIT REPORT ERRORS MEAN CONSUMERS LOSE (1998), *available at* http://uspirg.org/uspirg.asp?id2=5970&id3=USPIRG& (last visited June 26, 2004); *see also* CONSUMER FED'N OF AM. & NAT'L CREDIT REPORTING ASS'N, CREDIT SCORE ACCURACY AND IMPLICATIONS FOR CONSUMERS 6–7 (2002), *available at* http://www.consumerfed.org/121702CFA_NCRA_Credit_Score_Report_Final.pdf (last visited June 26, 2004) (citing numerous studies finding high rates of error in credit reports).

gram with little in the way of prior data can accurately pick a small number of unknown terrorists out of the nearly 300 million people living in the United States.[34]

Most significantly, however, the consequences of governmental antiterrorism measures are quite different than the consequences of data analysis in the commercial context. For example, if you do not buy the book Amazon.com recommended to you based on other customers' buying patterns, the negative consequences are slight. If your credit card company puts a hold on the use of your card because it noticed an odd usage pattern and suspected someone might have stolen your card, you can explain and continue to use your card. But the consequences of using data for counterterrorism purposes can be much more serious. They can include arrest, deportation, loss of a job, greater scrutiny at various screening gates, investigation or surveillance, or being added to a watch list.[35]

II. Privacy's Gap: The Lack of an Effective Framework for Governmental Use of Commercial Data

Keeping in mind the many ways in which the government is already using commercial data and the corresponding risks to civil liberties, we turn next to the existing legal regime governing access to, and use of commercial data for counterterrorism purposes. Ironically, while some proponents of governmental use of commercial data have argued that the government should have the same access to consumer data that the private sector has, the private sector is actually subject to clearer and stricter rules for the use of data under current law than government counterterrorism agencies. Governmental officials defending plans to use commercial databases for counterterrorism purposes have argued that all such uses will be in strict compliance with applicable privacy laws.[36] Such assurances are misleading, however, because there are very few privacy laws applicable to the government's acquisition and use of commercially compiled data for counterterrorism purposes.

Congress has regulated the private sector's use of personally identifiable information through so-called "sectoral" legislation: separate laws applicable to different types of data considered to need privacy protection. One of the most important of these laws is the Fair Credit Reporting Act ("FCRA"),[37] intended to protect consumers from the disclosure of inaccurate personal in-

34 Some administration officials have indicated that the number of terrorists in the United States is likely to be around 5,000. *See* Bill Gertz, *5,000 in U.S. Suspected of Ties to Al Qaeda*, WASH. TIMES, July 11, 2002, at A1.

35 Indiscriminately compiled watch lists have been relied on by employers performing background checks on potential employees, *see* Kelli Arena, *U.S. Watch List Has 'Taken on Life of Its Own,' FBI Says*, (Nov. 20, 2002), *at* http://www.cnn.com/2002/LAW/11/19/fbi.watch.list/ (last visited June 26, 2004), and to subject others to intrusive searches and delays at airports, *see* Ann Davis, *Why a 'No Fly List' Aimed at Terrorists Delays Others*, WALL ST. J., Apr. 22, 2003, at A1; Steve Lohr, *Data Expert Is Cautious About Misuse of Information*, N.Y. TIMES, Mar. 25, 2003, at C6.

36 *See, e.g.*, Tether, *supra* note 16, at 9 (DARPA Director claiming that DARPA intended its TIA project to proceed in "full compliance with U.S. constitutional law, U.S. statutory law, and American values related to privacy"). R

37 Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681–1691 (West 1998 & Supp. 2003). Signif-

formation held by consumer reporting agencies. Consumer reporting agencies are the private sector's central source of credit, financial, employment, and criminal history information (although as a result of the Internet they are no longer the exclusive source that they once were). In the FCRA, Congress established rules for when credit reports may be disclosed for important private sector decisions such as employment, insurance, and credit (and for similar decisions by the government). Under the FCRA, credit records must be accurate, and they cannot include certain older information.[38] They can be disclosed and used only for certain permitted purposes.[39] An individual also has the right to review and correct information in his credit report.[40]

Many privacy rules do not apply to governmental use of commercial information to identify possible terrorists, even though the consequences can be just as dire, if not worse. In this section, we analyze existing laws and show that there are, in fact, few legal constraints on government access to commercial databases for counterterrorism purposes.

Briefly summarized, the landscape is this: The federal Privacy Act does not apply to governmental use of commercial databases that were collected for business purposes. The Supreme Court's reading of the Constitution does not offer guidelines for government access to data generated in the course of commercial transactions and held by private companies. Statutorily, the United States has no comprehensive privacy law for commercial data, so a great deal of information is available to law enforcement and intelligence agencies through voluntary disclosure, or for purchase from data aggregators.[41] The sectoral privacy laws that do exist for specific categories of records (credit, medical, financial) are riddled with exceptions of varying breadth, which allow access to and sharing of data for law enforcement or intelligence purposes. All the privacy laws include exceptions for access pursuant to grand jury subpoena, a powerful tool.[42] Under the USA PATRIOT Act, the FBI acquired broad authority to issue "National Security Letters" or obtain court orders compelling the disclosure of data from commercial enti-

---

icant changes to the FCRA were signed into law in December 2003. *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952.

38 *See* 15 U.S.C.A. § 1681e(b) (accuracy); *id.* § 1681e(a) (timeliness).

39 *See id.* § 1681b.

40 *See id.* § 1681g (right to review); *id.* § 1681i (right to correct). The landscape of legal rules governing access of law enforcement and intelligence agencies to some commercially held information is laid out in two charts the Center for Democracy & Technology ("CDT") prepared for the Markle Foundation Task Force. *See* CDT, Commercial Access to Information, http://www.cdt.org/security/guidelines/final_commercial_matrix.shtml (last visited June 13, 2004); CDT, Law Enforcement and Intelligence Access to Information, http://www.cdt.org/security/guidelines/final_government_matrix.shtml (last visited June 13, 2004).

41 Actually, private entities could legally voluntarily disclose much of this information to the government, but it is far more convenient for the government to buy access to compilations, thereby "outsourcing" the compilation and maintenance of the data.

42 *See, e.g.*, 12 U.S.C. § 3407 (2000) (permitting access to financial records with a judicial subpoena under certain circumstances); 20 U.S.C. § 1232g(b)(1)(J)(i) (2000) (providing for access to educational records with a grand jury subpoena); 45 C.F.R. 164.512(f)(1)(ii)(B) (2002) (allowing for disclosure of health records, pursuant to Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033–34).

ties for intelligence investigations of international terrorism.[43] Once the government obtains commercial data for counterterrorism purposes, there are no effective constraints on redisclosure to other agencies for counterterrorism purposes.[44]

The Constitution does, however, impose some constraints on the government's use of data. Those rules are very clear in criminal prosecutions. In employment and other screening contexts, the Due Process and Equal Protection Clauses limit how the government can use information to make decisions. Those limits, though somewhat unclear, could be important in determining the limits of the government's use of data for counterterrorism.

A. Constitutional Limits on Access to Commercial Data

As a threshold matter, under current Supreme Court jurisprudence, the Constitution is not a source of guidelines for government access to data that consumers "reveal" to third parties, such as insurance companies, merchants, banks, or travel agencies. While the First Amendment limits the power of the government to compel disclosure of membership lists of political and religious organizations,[45] and while the *content* of electronic communications is constitutionally protected,[46] the Court held in the 1970s that information acquired by businesses from individuals in the course of ordinary transactions is not protected by the Fourth Amendment.[47] The Court reasoned that consumers do not have a legitimate expectation of privacy in information they divulge to businesses, including financial records and transactional data about telephone calls and other electronic communications.[48]

---

43 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88. These provisions are so broadly drafted that they seem to allow the FBI to access entire databases of information without specifying any particular person as the target.

44 *See, e.g.*, *id*. § 203 (permitting sharing of data acquired with grand jury subpoena).

45 *See* NAACP v. Alabama *ex rel*. Patterson, 357 U.S. 449, 460–67 (1958).

46 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 communications concerning the offense will be obtained. *See* 18 U.S.C. § 2518(3) (2000). 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. *See* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1805(a) (2000).

47 *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that there was no reasonable expectation of privacy in phone numbers dialed because petitioner had voluntarily disclosed them to the phone company and they were recorded by the phone company for legitimate business reasons); United States v. Miller, 425 U.S. 435, 440–46 (1976) (holding that there is no Fourth Amendment interest in checks and deposit slips, since they are not confidential communications and contain only information voluntarily conveyed to the bank).

48 *See Smith*, 442 U.S. at 742; *Miller*, 425 U.S. at 441–43. The exact scope of this "business records" doctrine is unclear. Other articles in this symposium question, persuasively, the broad reading that has been given to cases like *United States v. Miller* and *Smith v. Maryland*. It will take a re-evaluation by the Supreme Court, however, to create a constitutional framework for access to commercial data. For our purposes it is sufficient to note that the Constitution, as now interpreted, does not set limits on government agencies seeking access to data from commercial entities.

B. The Privacy Act

The Privacy Act of 1974 established certain rules for federal governmental records.[49] The act requires notice to, and consent from, individuals when the government collects and shares information about them.[50] It gives citizens the right to see whatever information the government has about them.[51] It also holds governmental databases to certain accuracy standards.[52] But the application of the Privacy Act to governmental use of commercial databases is limited, and there exist major exceptions for law enforcement and intelligence agencies.[53]

Congress passed the Privacy Act in response to concerns about the creation of large, centralized governmental databanks of personal information. The Act's protections apply only where the government is creating a "system of records."[54] Counterterrorism uses of commercial information may not involve the creation of governmental databases covered by the Act because searches and data analysis can be conducted in such a way that the data never leaves 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 governmental database. If the government is simply accessing databases created by commercial entities for their own reasons, there may be no system of records subject to Privacy Act requirements.[55]

The Privacy Act does include a provision that extends its coverage to databases created under government contract, but it seems that the provision does not include governmental searches of private sector databases already compiled and maintained for other purposes. 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."[56] 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 ("OMB") 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."[57] Im-

49 Privacy Act of 1974, 5 U.S.C. § 552a (2000).

50 *Id*. § 552a(b)–(e).

51 *Id*. § 552a(d)(1).

52 *Id*. § 552a(e)(5)–(6).

53 *See id*. § 552a(k).

54 *Id*. § 552a(a)(5).

55 *But see* DOJ, Requisition/Order for Supplies or Services with ChoicePoint, Inc., Statement of Work § 13.2 (June 24, 2002) (suggesting that Choicepoint will be "design[ing], develop[ing] or operat[ing] a system of records" subject to the Privacy Act) (on file with The George Washington Law Review).

56 5 U.S.C. § 552a(m).

57 Privacy Act Guidelines, 40 Fed. Reg. 28,976, 28,976 (July 9, 1975). Longtime OMB official Robert Bedell testified at a 1983 congressional hearing that subsection (m) was added late in the process of drafting the Privacy Act to prevent an agency from entering "a contract by

plementing regulations issued in 1983 also 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."[58] In 1981, the DOJ confirmed this interpretation of subsection (m) when responding to a question about whether a government agency could contract with consumer reporting agencies to provide information to the government for use in debt collection:

> If identifying information is furnished to a consumer reporting agency in order to locate and retrieve information already within its files, it is our view that the identifying information so furnished does not constitute a system of records to which subsection (m) applies. *The system of records being operated is a pre-existing private system to which nothing is being added, and which would continue to exist wholly without regard to the [government] contract.*[59]

Even when information is pulled into governmental databases, law enforcement and intelligence agencies are exempt from many key provisions of the Privacy Act. Simply by publishing a notice in the Federal Register, law enforcement agencies and the Central Intelligence Agency ("CIA") can exempt their records from the Act's requirements that records be maintained accurately and that individuals be permitted to access and correct their records.[60] Any agency can share its records with any other agency if the sharing is a "routine use" and has been noticed in the Federal Register.[61] A "routine use" is any use that is compatible with the purpose for which the information was collected.[62] Certainly, this allows all agencies involved in counterterrorism to share information. The definition of "computer matching" excludes matches performed for foreign counterintelligence purposes.[63] Finally, any agency can disclose records to any other federal, state, or local agency for any law enforcement activity upon written request specifying the particular portion desired and the law enforcement activity for which the record is sought.[64]

---

which an agency simply permits some contractor to operate its systems of records." *Oversight of the Privacy Act of 1974: Hearings Before a Subcomm. of the House Comm. on Gov't Operations*, H.R., 98th Cong. 123 (1983) (statement of Robert Bedell, Deputy Admin., Office of Info. & Regulatory Affairs, OMB).

58 48 C.F.R. § 24.104 (2002) (emphasis added); *see also id.* §§ 52.224-1, 52-224-2 (requiring contractors to comply with the Privacy Act).

59 *Debt Collection Act of 1981: Hearing on H.R. 2811 Before a Subcomm. of the House Comm. on Gov't Operations*, 97th Cong. 235 (1981) (emphasis added).

60 *See* 5 U.S.C. § 552a(j)–(k).

61 *See id.* § 552a(b)(3), (e)(4).

62 *See id.* § 552a(a)(7).

63 *See id.* § 552a(a)(8)(B)(vi). Computer matching is similar to link analysis, 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. *See id.* § 552a(8)(A).

64 *See id.* § 552a(b)(7). This does not, however, authorize disclosures to intelligence agencies. It is unclear whether agencies like the FBI and DHS, which are both intelligence and law enforcement agencies, can claim law enforcement status for purposes of some Privacy Act provisions and intelligence agency status for purposes of other provisions.

The Privacy Act is not entirely irrelevant to the use of data for counterterrorism purposes. The prohibition on disclosure of records for purposes unrelated to their initial collection would almost certainly prohibit a federal social service agency, for example, from disclosing its records to an intelligence agency for counterterrorism purposes; such a disclosure probably would not satisfy even the broadest definition of "routine use." Subsection (m) extends the Act's provisions to databases created under contract with the government. Otherwise, however, the Act imposes few limits on the government's use of commercial databases.

C. The Patchwork of Privacy Statutes Applicable to Commercial Data

1. Unprotected Data: Voluntary Disclosure

Because the United States has no comprehensive privacy law applicable to commercial databases, the analysis of rules concerning commercial data must start with a presumption of access—so long as no law prohibits it, the government can purchase or request voluntary disclosure of any commercially held records. Especially since September 11, the FBI has obtained commercial databases from private entities, from grocery store frequent-shopper records to scuba diving certification records, without having to exercise any compulsory authority.[65] So long as no statute prohibits government access to the information, a voluntary request is entirely legal. Third parties that hold consumer information often comply with such requests because they want to be helpful to the government or because compliance seems to be the path of least resistance. Categories of information for which there is no applicable privacy law include, *inter alia*: travel records, retail purchases—online and offline—of anything ranging from books to groceries, "Easy Pass" toll records, real estate and mortgage information, magazine subscriptions, club memberships, and utility bills.

2. Federal Privacy Legislation

While the United States has no comprehensive privacy statute, a considerable patchwork of privacy laws protects data in corporate hands. These laws, however, are riddled with exceptions for law enforcement and intelligence agencies.

a. Fair Credit Reporting Act

As noted above, the FCRA is one of the most important laws intended to protect consumers from the disclosure and use of inaccurate personal information held by consumer reporting agencies.[66] Its protections are undercut, however, by a number of exceptions that enable broad government access to credit report information.

---

65 Ben Worthen, *What to Do When Uncle Sam Wants Your Data*, CIO MAG., Apr. 15, 2003, at 56, 56–58.

66 Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681–1691 (West 1998 & Supp. 2003), *amended by* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952.

As a threshold matter, it is unclear whether the FCRA would apply at all if a private company collected information solely for law enforcement or intelligence purposes. The FCRA only applies to the disclosure of information that is collected for the purpose of, is expected to be used for, or is used to establish eligibility for credit, insurance, employment, or other specifically enumerated purposes, none of which involve predicting terrorism.[67] So if a company (even one covered by the FCRA as a consumer reporting agency for other purposes) sets up a database expressly for purposes related to law enforcement or intelligence and searches that database for 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.[68] Such activities may, however, be subject to the Privacy Act under subsection (m).[69] Courts have suggested that the FCRA applies to disclosures of information if some of that information was *originally* collected by the disclosing company for credit related or other FCRA purposes.[70]

Second, the FCRA does not cover a significant amount of information contained in credit reports, such as name, address, telephone number, social security number, and other identifying information. This information is found in "credit headers," typically found at the top of a credit report.[71] In addition, the FCRA allows a consumer reporting agency to provide any government agency with consumers' names, current and former addresses, and current and former employers, for any purpose and without any restrictions.[72]

Moreover, the USA PATRIOT Act added a new provision to the FCRA, granting *any* government agency authorized to investigate or engage in intelligence activities related to international terrorism the power to issue "National Security Letters" to compel disclosure of "a consumer report of a consumer and all other information in a consumer's file" if the agency certifies in writing that the consumer report is necessary to that investigation, activity, or analysis.[73] It is unclear whether the agency needs to identify a

67 *See* 15 U.S.C.A. § 1681a(d).

68 *See id*.

69 *See* 5 U.S.C. § 552a(m).

70 *See, e.g.*, Bakker v. McKinnon, 152 F.3d 1007, 1012 (8th Cir. 1998) ("[W]hether a credit report is a consumer report . . . is governed by the purpose for which the information was originally collected in whole or in part by the consumer reporting agency."); Ippolito v. WNS, Inc., 864 F.2d 440, 453 (7th Cir. 1988) ("[E]ven if a report is used or expected to be used for a non-consumer purpose, it may still fall within the definition of a consumer report if it contains information that was originally collected by a consumer reporting agency with the expectation that it would be used for a consumer purpose."). We note that the FBI's National Security Law Unit issued a memorandum on September 17, 2001, stating that the FBI's use of information collected by data warehousing company Choicepoint need not comply with the FCRA because "Choicepoint does not collect 'public record information' for any of the [FCRA-enumerated] purposes." *See* Memorandum from the National Security Law Unit, *supra* note 26, at 13. R

71 *See* Commentary on the Fair Credit Reporting Act, 16 C.F.R. pt. 600 app. 4.F (2004) (commentary on section 603).

72 *See* 15 U.S.C.A. § 1681f.

73 *See id.* § 1681v (corresponding to Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of

specific consumer to exercise this power. Broadly interpreted, the provision would allow any agency conducting an investigation or other intelligence activity or analysis regarding international terrorism to demand access to all the records held by a consumer reporting agency or to any records meeting certain parameters.

Another provision of the FCRA gives the FBI separate authority to issue "National Security Letters" to compel disclosure of certain information by consumer reporting agencies, including the names of the financial institutions where an individual has accounts and identifying information about individuals, based on a claim that the information is "sought for" an authorized investigation to protect against international terrorism or clandestine intelligence activities.[74] As described in more detail below, FBI officials can issue these "National Security Letters" without judicial approval.

This provision also allows the FBI to obtain *ex parte* court orders forcing disclosure of full credit reports, upon a showing that the reports are "sought for" the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activity.[75]

b. Right to Financial Privacy Act

The Right to Financial Privacy Act ("RFPA") protects the privacy of financial records.[76] The act contains a "National Security Letter" provision giving the FBI access to certain bank records and other financial records upon certification that the records in question are "sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities."[77] In December 2003, Congress expanded this authority to cover more than just typical financial records; it now includes all records of certain specified businesses, including jewelers, automobile dealers, pawn shops, travel agencies, and real estate agents.[78]

2001, Pub. L. No. 107-56, § 358(g)(1)(B), 115 Stat. 272, 327–28). Section 626 was redesignated section 627 in more recent legislation. *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, § 214, 116 Stat. 1952, 1980.

74 *See* 15 U.S.C.A. § 1681u(a). This provision, formerly section 625 of the FCRA, was redesignated section 626 in recent legislation. *See* Fair and Accurate Credit Transactions Act of 2003 § 214.

75 *See* 15 U.S.C.A. § 1681u(c).

76 *See* Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2000 & Supp. I 2003).

77 *See id.* § 3414(a)(5)(A).

78 *See* Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, § 374, 117 Stat. 2599, 2628 (2003). The new law amends the definition of "financial institution" for purposes of section 1114 of the RFPA, 12 U.S.C. § 3414, incorporating the far broader definition of "financial institution" used in money laundering laws. *See* 31 U.S.C. § 5312(a)(2) (2000). That definition includes many entities that are not strictly "financial" institutions, such as "a broker or dealer in securities or commodities," *id.* § 5312(a)(2)(G), "a currency exchange," *id.* § 5312(a)(2)(J), "an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments," *id.* § 5312(a)(2)(K), "an insurance company," *id.* § 5312(a)(2)(M), "a dealer in precious metals, stones, or jewels," *id.* § 5312(a)(2)(N), "a pawnbroker," *id.* § 5312(a)(2)(O), "a travel agency," *id.* § 5312(a)(2)(Q), "a telegraph company," *id.* § 5312(a)(2)(S), "a business engaged in vehicle sales, including automobile, airplane, and boat sales," *id.* § 5312(a)(2)(T), "persons involved in real estate closings and settlements," *id.* § 5312(a)(2)(U), "the United States Postal Service," *id.* § 5312(a)(2)(V), "a casino, gambling

c. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act,[79] enacted in 1999, includes privacy provisions requiring financial institutions to inform their customers of their privacy policies[80] and to allow each customer to "opt-out" of sharing information with nonaffiliated third parties.[81] The disclosure of credit header information, although not governed by the FCRA, is subject to Gramm-Leach-Bliley.[82]

Gramm-Leach-Bliley and its implementing regulations include exemptions that allow government access to information for counterterrorism 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."[83] Another exemption to Gramm-Leach-Bliley allows disclosure of financial information "to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities."[84] Either or both of these exemptions would seem to permit disclosure of financial records in response to a "National Security Letter" under the RFPA.[85]

d. Health Insurance Portability and Accountability Act

Congress has also enacted legislation to protect the privacy of medical records—the Health Insurance Portability and Accountability Act of 1996

casino, or gaming establishment with an annual gaming revenue of more than $1,000,000," *id.* § 5312(a)(2)(X), and "any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters," *id.* § 5312(a)(2)(Z). Because of the way the definitions work, the records subject to disclosure are not limited to actual financial records. Under the RFPA, "financial records" are defined as "any record held by a financial institution pertaining to a customer's relationship with the financial institution." 12 U.S.C. § 3401(2). Because a travel agency is considered a financial institution, the new authority thus covers *any* records held by the travel agency, even if the records do not relate to financial matters.

79 Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999), Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12, 15, 16, & 18 U.S.C.).

80 *See* 15 U.S.C. § 6803 (2000).

81 *See id.* § 6802(b).

82 *See* Trans Union LLC v. FTC, 295 F.3d 42, 50–51 (D.C. Cir. 2002) (holding that regulation's broad definition of "financial" information to include such identifying information as would be contained in a credit header was permissible interpretation of Gramm-Leach-Bliley Act, which delegated rulemaking authority to the Federal Trade Commission to implement the Act's privacy provisions).

83 15 U.S.C. § 6802(e)(5); *see also* 16 C.F.R. § 313.15(4) (2002).

84 15 U.S.C. § 6802(e)(8); *see also* 16 C.F.R. § 313.15(7)(ii).

85 Even the provision of the Gramm-Leach-Bliley Act that prohibits the acquisition of consumer data by false pretenses contains what amounts to another law enforcement exception. *See* 15 U.S.C. § 6821. The prohibition is not to "be construed so as to prevent any action by a law enforcement agency . . . to obtain customer information of a financial institution in connection with the performance of the official duties of the agency." *Id.* § 6821(c).

("HIPAA").[86] Again, HIPAA and its implementing regulations provide broad exceptions for law enforcement and national security purposes.

In particular, HIPAA regulations permit disclosure of medical information without limitation "for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act . . . and implementing authority."[87] This 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.[88]

HIPAA regulations also permit disclosure of medical records to federal, state, and local law enforcement officials in response to a court order, judicial or grand jury subpoena, and, under certain circumstances, an administrative request or subpoena.[89] 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.[90]

e. Family Educational Rights and Privacy Act

Congress passed the Family Educational Rights and Privacy Act, which applies to educational institutions that receive federal funding, to protect the confidentiality and accuracy of educational records.[91] But section 507 of the USA PATRIOT Act created a loophole allowing the DOJ to obtain educational records if they are relevant to a terrorism investigation.[92] That provision, however, provides some greater protections than those applicable to other types of records. It requires the DOJ to obtain an *ex parte* court order, based on a showing of specific and articulable facts demonstrating the relevance of the requested records.[93] Nonetheless, there is no requirement that the DOJ identify a specific target of the investigation; a broad reading of the

86 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, & 42 U.S.C.).

87 45 C.F.R. § 164.512(k)(2) (2002) (internal citations omitted).

88 *See* Jim McGee, *New Medical Privacy Law Opens Back Door to Intelligence Agencies*, CONG. Q. HOMELAND SEC. 2.0 (Apr. 23, 2003) (on file with The George Washington Law Review). As Peter Swire, Chief Counselor for Privacy at the OMB during the Clinton Administration stated: "Post 9/11, you can see how the national security exception [to the medical privacy law] could become a back door for law enforcement access to medical records without issuing subpoenas that HIPAA usually requires." *Id.* (quotation omitted).

89 *See* 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).

90 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 215(g)(1)(B), 115 Stat. 272, 287–88.

91 *See* Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2000 & Supp. I 2003).

92 *See id.* § 1232g(j) (corresponding to USA PATRIOT Act § 507).

93 *Id.*

exemption could result in the government accessing entire databases of educational records.

f. Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 ("ECPA")[94] allows the FBI to issue "National Security Letters" ordering disclosure of telephone and electronic communications transactional records if they are relevant to an authorized investigation to protect against "international terrorism" or "clandestine intelligence activities."[95] 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.[96]

3. "National Security Letter" Authority Under the USA PATRIOT Act

As indicated above, the FBI has the power to compel the disclosure of certain commercial information in the absence of a court order by means of "National Security Letters." The FBI can use these letters to obtain credit records under the FCRA,[97] bank, credit card, and other financial records under the RFPA (including, as of December 2003, records of certain businesses like jewelers and car dealerships that would not typically be thought of as "financial"),[98] and communications transactional records under ECPA.[99] FBI officials in field offices can write these letters without authorization from FBI Headquarters and without the approval of a judge. The USA PATRIOT Act expanded "National Security Letter" authority, so now the letters need not identify a suspect or a particular person whose records are sought.[100] As discussed above, if the law is broadly read, "National Security Letters" could require private entities to turn over or provide access to entire databases. An important oversight question for Congress is whether the FBI is using the expanded "National Security Letter" authority to obtain business records without naming individuals to whom the records pertain.

The standard for a "National Security Letter" under ECPA is mere relevance to an intelligence investigation.[101] A request for financial records or credit reports does not even have to assert that the information is relevant. Rather, an FBI official in a field office need only certify that financial information is being "sought for" foreign counterintelligence purposes to protect

94 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

95 18 U.S.C. § 2709(b)(2) (2000 & Supp. I 2003).

96 *See* 18 U.S.C. § 2709(a) (2000).

97 *See* 15 U.S.C.A. § 1681u (West 1998 & Supp. 2003).

98 *See* 12 U.S.C.A. § 3414(a)(5)(A) (West 1998 & Supp. 2003) (as amended by Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, § 374, 117 Stat. 2599, 2628 (2003)).

99 *See* 18 U.S.C. § 2709 (as amended by Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, § 505 (g)(1)(B), 115 Stat. 272, 365–66).

100 *See* USA PATRIOT Act § 505.

101 *See* 18 U.S.C. § 2709(b).

against international terrorism or clandestine intelligence activities.[102] While only the FBI can issue "National Security Letters," the statutes explicitly allow the FBI to share the data it obtains with other agencies for foreign counterintelligence purposes.[103] The USA PATRIOT Act further directs the Attorney General and the heads of other federal agencies with law enforcement responsibilities to share with the CIA all foreign intelligence information in the possession of the FBI or other such agencies.[104]

4. Business Records Authority Under the USA PATRIOT Act

Section 215 of the USA PATRIOT Act gives the FBI another broad source of authority to obtain business records.[105] This authority covers any conceivable business record, from travel records to medical, library, and bookstore records.[106] Section 215 allows the FBI in terrorism and intelligence investigations to obtain a court order for any privately held business record without having to specify the target of the investigation.[107] Broadly read, the provision allows the FBI to access an entire database of privately held information, rather than just the records of a particular suspect. 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.[108] In September 2003, the Attorney General acknowledged publicly that the FBI had not used section 215 since its enactment.[109] It remains an open question whether the DOJ interprets section 215 as permitting it to obtain business records without naming individuals to whom the records pertain.

5. Routinized Disclosure of Records

In addition to the ability to compel disclosure of records compiled by businesses for business purposes, the government's power to require businesses to create and report data regularly is expanding. For example, anti-

102 *See* 12 U.S.C. § 3414(a)(5)(A) (2000 & Supp. I 2003); 15 U.S.C.A. § 1681u(b).

103 *See* 12 U.S.C. § 3412(a) (allowing transfer under the RFPA of records that the transferring agency certifies "there is reason to believe . . . are relevant to a legitimate law enforcement inquiry, or intelligence or counterintelligence activity, investigation . . . related to international terrorism"); 15 U.S.C. § 1681u(f) (2000 & Supp. I 2003) (allowing FBI to share information with other federal agencies under the FCRA "as may be necessary for the approval or conduct of a foreign counterintelligence investigation"); 18 U.S.C. § 2709(d) (allowing the FBI to share records under the ECPA in accordance with guidelines of the Attorney General "for foreign intelligence collection and foreign counterintelligence investigations conducted by the [FBI], and, with respect to [another federal agency] if . . . relevant to the authorized responsibilities of such agency").

104 *See* USA PATRIOT Act § 905(a).

105 *See id*. § 215 (amending 50 U.S.C. § 1862 (2000 & Supp. I 2003)).

106 *See id*. (amending 50 U.S.C. § 1861(a)(1)).

107 *See* 50 U.S.C. § 1861(b).

108 *See id*. § 1861(c)(1).

109 Memorandum from the Attorney General to Robert S. Mueller, Director of the FBI (Sept. 18, 2003), *available at* http://www.cdt.org/security/usapatriot/030918doj.shtml (last visited June 26, 2004).

money laundering laws, including the Bank Secrecy Act[110] (enacted in 1970 and expanded by the USA PATRIOT Act),[111] impose extensive reporting requirements on the financial industry, resulting in the availability of far more financial information to law enforcement entities. The Bank Secrecy Act requires financial institutions to report various types of transactions to the government and also imposes certain recordkeeping and record retention requirements on financial institutions.[112] Similar reporting requirements have been imposed on universities with respect to foreign students,[113] and on airlines with respect to passengers.[114]

D. Once Obtained, Data Can Be Widely Shared

As we have shown, under today's legal regime for counterterrorism use of commercial data, standards for the collection of or access to information are very low or nonexistent. Once the government obtains the data, there are even fewer rules on its disclosure. The USA PATRIOT Act has loosened the rules for information sharing among law enforcement and intelligence agencies. Although information sharing is crucial to an effective antiterrorism effort, the recent changes have left a vacuum in the areas of standards and oversight.

Traditionally, both the criminal justice system and the intelligence framework had fairly strict and well-defined rules for government access to, sharing of, and use of personally identifiable information. Before the information-based economy put so much personal information in the hands of third parties, the government had to obtain what it wanted from the subject of the investigation, with notice and, if it wanted the information immediately, under the fairly high standards for obtaining search warrants. Rules governing use of the information as evidence in a criminal proceeding were clear and offered robust protection to the individual.[115] Sharing was permitted only with other criminal justice agencies.[116] In the intelligence system, the government had only limited ability to compel disclosure of data.[117] Al-

110 Bank Secrecy Act, 12 U.S.C. §§ 1951–1959 (2000 & Supp. I 2003).

111 *See* USA PATRIOT Act §§ 351–366.

112 *See, e.g.*, 12 U.S.C. §§ 1952–1953.

113 *See* USA PATRIOT Act § 416 (requiring the Bureau of Immigration and Customs Enforcement to collect information from schools on nonimmigrant students); Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, § 501(a)(1), 116 Stat. 543, 560–61 (requiring educational institutions to report any failure of an alien to enroll).

114 Manifest Requirements Under Section 231 of the Act, 68 Fed. Reg. 292, 292 (Jan. 3, 2003) (proposed rule to implement section 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002).

115 The Sixth Amendment right to confront one's accusers, for example, protects against the use of secret evidence. *In re* Oliver, 333 U.S. 257 (1948).

116 For example, before the USA PATRIOT Act, the criminal wiretap law allowed intercepted communications to be shared only with law enforcement agencies, *see* 18 U.S.C. § 2517 (2000), *amended by* USA PATRIOT Act § 203(b), and the rules governing grand juries allowed sharing only with other criminal justice agencies, *see* FED. R. CRIM. P. 6(e)(3)(C), *amended by* USA PATRIOT Act § 203(a).

117 The first National Security Letter authority was not enacted until 1986. *See* Electronic Communications Privacy Act of 1986 § 201[a], 18 U.S.C. § 2709(b)(2) (2000), *amended by* USA PATRIOT Act § 505. National Security Letters for financial records and credit records were

though intelligence agencies could always legally share intelligence information with criminal investigators, institutional barriers and the overbearing desire to protect "sources and methods" severely limited the sharing of information outside of the "intelligence community." In addition, aside from the very real chilling effect of the possibility of being under surveillance, there were relatively few adverse actions that intelligence agencies could lawfully take against ordinary citizens.

The new environment changes all that by removing the rules governing the sharing of data between law enforcement and intelligence agencies, and by authorizing or encouraging the use of information for screening purposes outside the criminal justice system. For example, the USA PATRIOT Act allows the sharing of "foreign intelligence," "counterintelligence," or "foreign intelligence information" obtained in criminal investigations with "any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official."[118] While cooperation and exchange of information between law enforcement and intelligence agencies is necessary and desirable, the USA PATRIOT Act contains virtually no safeguards to protect Americans' privacy and First Amendment rights. For example, section 203 permits sharing of a vast array of information that is not related to international terrorism, without regard to whether that information concerns legal or illegal activities.[119] Considering that criminal investigative techniques, especially wiretaps and grand jury subpoenas, often produce substantial amounts of private and sensitive information on persons who are not subjects of an investigation and are not involved in any illegal activity, this provision represents an unprecedented expansion of the authority of intelligence agencies to obtain information on American citizens and permanent residents within the United States.

This new authority is particularly troubling with respect to the sharing of information obtained from grand jury investigations. The grand jury is a

authorized in 1986 and 1996, respectively. Intelligence Authorization Act for Fiscal Year 1987, Pub. L. No. 99-569, § 404, 100 Stat. 3197 (1986); Intelligence Authorization Act for Fiscal Year 1996, Pub. L. No. 104-93, § 601, 109 Stat. 974.

118 *See* USA PATRIOT Act §§ 203(a)(1), (b)(1), (d)(1). Specifically, section 203 allows the sharing of information gathered from grand juries, criminal wiretaps, and criminal investigations in general. *See id.*

119 Section 203 of the USA PATRIOT Act permits sharing of "foreign intelligence" and "counterintelligence" as defined in the National Security Act of 1947 and permits sharing of a new category of "foreign intelligence information." *See id.* Under the National Security Act, "foreign intelligence" is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." *See* National Security Act of 1947, 50 U.S.C. § 401a(2) (2000 & Supp. I 2003). "Counterintelligence" is "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." *Id.* § 401a(3). Under section 203, the newly defined term "foreign intelligence information" includes information, "whether or not concerning a United States person" that concerns an "actual or potential attack," "sabotage or international terrorism," and "clandestine intelligence activities" by a "foreign power or by an agent of a foreign power," as well as information about a "foreign power or foreign territory" that "relates to the national defense or the security of the United States" or "the conduct of the foreign affairs of the United States." *See* USA PATRIOT Act § 203(d)(2); *see also id.* §§ 203(a)(1), (b)(2).

uniquely powerful institution. It can compel anyone to testify before it under oath. A person who refuses to testify may be sent to jail. If the government believes that a person testifying before the grand jury is lying, it can prosecute the witness for perjury. The grand jury can compel any business to turn over any records or databases, again under threat of imprisonment for those who refuse. In the past, these expansive powers were subject to two important controls: anything from the grand jury that the government used in a criminal trial was subject to the full panoply of due process requirements, while everything else the grand jury collected had to be kept secret and could be used for no other purpose. While the first of these protections remains largely in place, section 203 of the USA PATRIOT Act abolished the second, giving intelligence, national defense, and protective agencies the benefit of the grand jury's powers with none of the protections of the criminal justice system.[120] No prior judicial approval is required for disclosure of grand jury information or wiretap intercepts to intelligence agencies.[121] Disclosure is not limited to those intelligence officials directly involved in terrorism investigations.[122] There are no meaningful standards or safeguards to control use of the information other than a vague proviso that "[a]ny Federal official to whom information is disclosed . . . may use that information only as necessary in the conduct of that person's official duties."[123] Section 203 does require the Attorney General to establish procedures governing disclosure of information identifying a United States person when that information is the fruit of a grand jury investigation or criminal wiretap.[124] The guidelines, issued in September 2002, merely require the labeling of grand jury and wiretap information containing information about a U.S. person and leave it to the receiving agency to decide how to handle the information.[125]

While section 203 states that the foreign intelligence and counterintelligence gathered in a criminal investigation *may* be shared with intelligence agencies,[126] section 905 goes one step further and *requires* that the Attorney General and the head of any other law enforcement agency disclose to the Director of the CIA all "foreign intelligence" obtained in any criminal investigation.[127] Like section 203, such disclosures are not limited to information

120 *See* USA PATRIOT Act § 203(a).

121 *See id*. § 203(a)(1). Section 203, which governs disclosure of grand jury information, does require that "[w]ithin a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made." *Id*.

122 *See id*. (authorizing disclosure, in matters involving foreign intelligence or counterintelligence, "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties").

123 *Id*.; *see also id.* §§ 203(b)(1), (d)(1).

124 *See id*. § 203(c).

125 *See* Memorandum from the Attorney General to the Heads of Department Components, Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons 2–3 (Sept. 23, 2002), *available at* http://www.usdoj.gov/olp/section203.pdf (last visited June 26, 2004).

126 *See* USA PATRIOT Act § 203.

127 *See id*. § 905(a)(2) (requiring the "Attorney General, or the head of any other department or agency of the Federal Government with law enforcement responsibilities" to "expedi-

related to international terrorism. To the contrary, section 905 covers all information relating to individuals and organizations that involves any foreign government and organization, even if that information concerns entirely lawful business, political, or personal activities, and the provision itself contains no standards or safeguards for use or redisclosure of the information.[128] The Attorney General has issued guidelines for disclosure of the information, but those guidelines provide few limitations. Indeed, the section on "use restrictions" directs law enforcement agencies to disclose information "free of any originator controls or information use restrictions."[129]

While in the past information collected in criminal investigations could be disclosed only to other criminal justice agencies for law enforcement purposes, where it remained subject to the strict due process protections of the criminal justice system, data collected for criminal justice purposes can now be disclosed to any federal intelligence, protective, immigration, national defense, or national security official, with no prior judicial approval. And while intelligence agencies were never prohibited from sharing with law enforcement agencies information that appeared related to criminal activity, intelligence agencies are now being encouraged to engage in such sharing.

E. Constitutional Limits on Use of Data

Although the Constitution (as currently interpreted) plays little role in limiting government access to and sharing of commercial data, the Bill of Rights does impose some constraints on the government's use of information to make decisions affecting individuals. Some of these constraints arise in the criminal justice context. As noted above, there are strict due process protections on the use of information in criminal trials. But even before the adversarial process begins, the Constitution constrains governmental dependence on incriminating leads generated by computer if the underlying data is of dubious accuracy. The leading case is *Arizona v. Evans*.[130] In that case, a police officer ran an individual's name through his patrol car computer during a routine traffic stop.[131] The computer indicated—incorrectly—that there was an outstanding warrant for the individual's arrest.[132] In fact, the warrant had been quashed weeks before, but the system had not been updated, so the

---

tiously disclose to the Director of Central Intelligence . . . foreign intelligence acquired . . . in the course of a criminal investigation"). Section 905 applies only to "foreign intelligence" as defined in the National Security Act of 1947, while section 203 applies to "foreign intelligence," "counterintelligence," and a new category of "foreign intelligence information." *See id.* § 203(d).

128 *See id* § 905(a)(2).

129 Memorandum from the Attorney General to the Heads of Department of Justice Components and Heads of Federal Departments and Agencies with Law Enforcement Responsibilities, Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation (Sept. 23, 2002), *available at* http://www.usdoj.gov/olp/section905a.pdf (last visited June 26, 2004).

130 Arizona v. Evans, 514 U.S. 1 (1995).

131 *Id.* at 4.

132 *Id.*

police officer placed the individual under arrest.[133] The Supreme Court found that the officer's action was lawful,[134] but Justice O'Connor, in a concurrence joined by Justices Souter and Breyer, argued that arrests can constitutionally be made on the basis of computer matches only if it is reasonable to rely on the information in the database, and whether reliance is reasonable turns on whether information in the database is known to be updated and accurate:

> 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).[135]

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.[136]

Evans thus provides a constitutional basis for the principle that the government should not rely on databases to arrest or detain individuals unless those databases and the method of searching them are accurate. If a detention at an airport for more intensive scrutiny under a passenger screening program is a seizure for Fourth Amendment purposes (a question we do not purport to answer here), then the use of inaccurate or unreliable data to make that detention would not be reasonable.

There are other areas in which the Constitution limits the government's discretion to act on the basis of inaccurate or incomplete information. As noted above, due process constrains the government from denying a license to practice an occupation to someone based on a mere arrest—i.e., on incomplete information.[137] Governmental decisions affecting individuals in the context of the welfare state are also subject to due process protections.[138] In *Greene v. McElroy*,[139] the Supreme Court held that an engineer employed in developing and producing goods for the military involving military secrets could not be deprived of his security clearance, and therefore his job, in a proceeding that lacked the protections of confrontation and cross-examination. The pronouncement of the Court in that case is relevant to the use of information for security screening purposes that can result in adverse action:

---

133 *Id*.

134 *Id*. at 16.

135 *Id*. at 17 (O'Connor, J., concurring).

136 *Id*. at 17–18 (O'Connor, J., concurring).

137 *See supra* note 9 and accompanying text; *see also* Schware v. Bd. of Bar Exam'rs, 353 U.S. 232, 238–43 (1957). **R**

138 *See, e.g.*, Goldberg v. Kelly, 397 U.S. 254 (1970).

139 Greene v. McElroy, 360 U.S. 474 (1959).

> Certain principles have remained relatively immutable in our jurisprudence. One of these is that where governmental action seriously injures an individual, and the reasonableness of the action depends on fact findings, the evidence used to prove the Government's case must be disclosed to the individual so that he has an opportunity to show that it is untrue.[140]

There are, however, other precedents in the area of granting and denying of security clearances where the Court was far more solicitous of the executive branch's discretion to make decisions without due process.[141] While outside the scope of this article, the constitutional law surrounding these and other adverse actions taken by the government could be further explored to develop limits on the government's discretion to take adverse action against individuals in the name of preventing terrorism.

III. Outlines of a Legal Scheme for Use of Commercial Data for Counterterrorism Purposes

To summarize, under existing law the government can ask for, purchase, or demand access to most private sector data subject to few limits. Sharing of data is broadly permitted among agencies with counterterrorism responsibilities. Constraints on how the government can use the data once accessed are fragmentary. Some constitutional limits apply to the use of the data to arrest or detain individuals, and there may be due process limitations on the use of such data to deny government employment or licenses, but otherwise there are few rules governing the use of commercial data for counterterrorism purposes. This has produced a situation of uncertainty not only for a public wary of government overreaching, but also within the government itself and the private sector. The current lack of clarity inhibits efforts to develop potentially useful applications of commercial information. Counterterrorism efforts urgently need rules to fill this gap.

Key questions include: When, and under what circumstances, should the government be able to access entire databases? Should there be different access standards for information of varying sensitivity, such as medical data or location data generated by wireless services? Should there be different standards based on the type of search—one standard for subject-based queries and a different one for pattern-based searches? Does the searching of databases without the disclosure of identity mitigate privacy concerns? If it is possible to search data without disclosing identity, what should the rules be for disclosure to the government of the identity of those whose data fits a pattern? Are some uses of commercially available data of less concern than others? For example, should different rules apply to looking up an address, versus identifying a pattern that will trigger the initiation of an investigation,

---

140 *Id.* at 496.

141 *See, e.g.*, Dep't of Navy v. Egan, 484 U.S. 518, 528 (1988) (citing concerns pertaining to separation of powers, holding that the "grant of a clearance requires an affirmative act of discretion" by an executive official, and denial of such clearance was therefore not subject to the same due process protections required when government takes other adverse actions against its employees).

versus a screening application that will result in the denial or burdening of a right or privilege (such as getting on an airplane)? And who should make various approval decisions about access, about the patterns that are the basis for scans of private databases, and about actions taken on the basis of information? How can data accuracy be improved and enforced? 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? What due process rights should apply when adverse action is taken against a person based on data analysis?

A. The Principles of Fair Information Practices

One starting point for answering these questions is the long-accepted set of principles known as "Fair Information Principles," which were first articulated in the 1970s and which have been embodied in varying degrees in the Privacy Act,[142] the FCRA,[143] and the other "sectoral" federal privacy laws that govern commercial uses of information. As explained above, these laws are riddled with exceptions (including major exceptions adopted without serious consideration in the haste of enacting the USA PATRIOT Act), so that their precise terms do not apply to the new counterterrorism uses of information.[144] Nonetheless, the Fair Information Principles have remained remarkably relevant despite the dramatic changes in information technology that have occurred since they were first developed. While mapping these principles to the models of data analysis currently being pursued for counterterrorism purposes poses challenges, and while some of the principles are clearly inapplicable to the needs of law enforcement and intelligence agencies, they provide a remarkably sound basis for analyzing the issues associated with creating a system of checks and balances for the use of commercial databases in counterterrorism activities. The principles—notice, collection (access) limitation, use and disclosure limitation, retention limitation, data quality, individual access, system security, and accountability and redress—are discussed below in the context of new uses of personal data in counterterrorism activities.

1. Notice

A fundamental principle of fair information practices is that individuals should have notice both of the fact that information is being collected about them and of the purpose for which it is being collected.[145] Notification prior to data collection affords individuals the opportunity to choose not to disclose the information (albeit often at the cost of foregoing the opportunity to engage in the transaction that is made conditional upon disclosure of the in-

142 Privacy Act of 1974, 5 U.S.C. § 552a (2000).

143 Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681–1691 (West 1998 & Supp. 2003), *amended by* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952.

144 *See supra* Part II.

145 This principle is reflected in the Privacy Act. *See* 5 U.S.C. § 552a(b).

formation) and is a precondition to the individual's ability to ensure the collected data is accurate.

Notice is an element of Fourth Amendment searches, but when law enforcement and intelligence agencies are collecting information from third parties in the context of an investigation focused on specific individuals, it may be desirable to delay notice to those individuals that they are the subjects of an investigation. However, it is not automatically apparent that the same constraints must apply when the government seeks to use commercial and governmental databases for the newer screening uses. When the government uses data for screening purposes, all individuals are subject to the same scrutiny. The government can thus give notice of the types of information that it is collecting or accessing and the ways in which it plans to use the information without telling suspected terrorists what is known about them or even that they are suspects. Notice may actually improve the effectiveness of the data collection effort. For example, if an individual is notified when she books a plane ticket that the airline is collecting particular pieces of information to pass along to the government to review for security purposes, she may be more likely to provide accurate responses or volunteer information to explain discrepancies. A terrorist may try to evade the system by giving false information, but that is a problem that the system must be designed to address regardless of whether notice is given.

Even when the government uses commercial data in criminal justice or intelligence investigations, it can give the public general notice of the types of commercial information it uses and the ways it uses them without compromising specific investigations. The notice principle also can be partly implemented by notice to Congress of data analysis practices.

2. Collection (Access) Limitation

The collection limitation principle holds that no more data should be collected or accessed than is necessary to accomplish the legitimate purpose at hand.[146] Whether the government is drawing information into its own databases or looking at data held by others, the principle is the same—the government should not gather or review any personal information not directly relevant to the purpose of the collection or access.

One way to implement the collection limitation principle is by leaving commercial information in the hands of data aggregators and having them respond only to specific queries. Under such an approach, the government would not be acquiring the databases. For any given search, the government would acquire only the data that matches its search terms (the "hits").

The government will be reluctant, for security reasons, to disclose its search terms, such as the names of suspected terrorists, to the commercial holders of data. Researchers are developing anonymizing techniques that allow analysis of otherwise personally identifiable data without disclosing the identifying attributes of the individuals whose information is being searched. Using these techniques, only the identities of those few persons identified by

146 This principle, like the notice principle, is reflected in the Privacy Act. *See* 5 U.S.C. § 552a(e)(1).

the query as matching a watch list entry would be disclosed to the government. The process could have two steps, such that after the analysis determined that there was information matching the search criteria, further authority (judicial or otherwise) could be sought to obtain individual identities and other personally identifiable information regarding only those individuals who matched the query. Under this concept of "selective revelation," the vast majority of data in the commercial database would never be accessible to the government in a personally identifiable format.[147]

The collection or access limitation protects other constitutional interests in addition to privacy. For example, the rules for use of data should include a strong barrier against the use of information disclosing political or religious affiliation.[148] One possible source of appropriate guidelines is the Criminal Intelligence Systems Operating Policies promulgated by the DOJ, which state:

> [Law enforcement] shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is a reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.[149]

3. Use and Disclosure Limitation

Information collected for one purpose should not be used for another purpose without consent.[150] The use of commercial data for counterterrorism purposes necessarily involves using information for a purpose other than the one for which it was initially collected. The use and disclosure limitation, however, should apply to tertiary uses. Any government agency using commercial data for counterterrorism purposes should ensure that its use and redisclosure of that information to other agencies are limited to those counterterrorism purposes. This principle has the added advantage of promoting data quality, by requiring the second government agency seeking the same information for an unrelated purpose to return to the source of the information, where it may have been updated or corrected.

---

147 *See* Don Clark, *Entrepreneur Offers Solution for Security-Privacy Clash*, WALL ST. J., Mar. 11, 2004, at B1.

148 The tendency to use politics as a guide to potential violence remains strong. Recently, the FBI urged local police to collect information on demonstrators protesting the Iraq war, *see* Eric Lichtblau, *FBI Scrutinizes Antiwar Rallies: Officials Say Effort Aims at 'Extremist Elements,'* N.Y. TIMES, Nov. 23, 2003, at A1, and the New York Police Department in the spring of 2003 questioned hundreds of arrested antiwar protesters about their political activities and recorded the information in a database, a project they abandoned after outcry from civil libertarians and constitutional law experts, *see* William K. Rashbaum, *Police Stop Collecting Data on Protesters' Politics*, N.Y. TIMES, Apr. 10, 2003, at D1.

149 Criminal Intelligence Systems Operating Policies, 28 C.F.R. § 23.20(b) (2002).

150 This principle is found in the Privacy Act, *see* 5 U.S.C. § 552a(b), and the Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681–1691 (West 1998 & Supp. 2003), *amended by* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952.

The principle of limited reuse and redisclosure is also a limit on "mission creep," which is one of the major concerns with counterterrorism use of commercial data. The fear is that having developed an effective and justified analytic tool and gained access to commercial sources of information for counterterrorism purposes, an agency or other agencies will then seek to use the information for purposes extending beyond counterterrorism, purposes that on their own would not have supported access to the information, but that seem to offer benefits at a marginal cost once the information is available. This is a very hard dynamic to resist. A federal agency that has access to data because it is attempting to identify suspected terrorists will be easily tempted to report non-terrorism related offenders that it uncovers. There is a risk that such added uses will not be as effective as the purpose for which the system was designed, and may in fact divert resources from the success of the initial mission. There should be a distinct, transparent policy debate and decision for each new proposed governmental use of data.

4. Retention Limitation

As a general rule, data should be retained no longer than is necessary for the purpose for which it was collected. This is a concept inapplicable to some counterterrorism purposes, since the value of some investigative information may become apparent only years after it was collected. The retention limitation principle, however, does have relevance to various screening applications and other counterterrorism uses of information. Purging data significantly reduces the opportunity for abuse. For example, the Transportation Security Administration ("TSA") stated that the proposed airline security screening program would purge its data on passengers who are U.S. persons within a "certain number of days" after the relevant travel is completed.[151] Each agency that uses commercial data should have a policy delineating precisely what data it retains and for how long—and should not retain any data not necessary to the purpose for which it was collected.

5. Data Quality

Data quality will be an essential factor affecting both the efficacy and civil liberties ramifications of any use of personally identifiable information for counterterrorism purposes. As the president of one data mining company said, "the quality of the prediction is directly proportional to the quality" of the data.[152] As noted above, data quality has constitutional implications

151 *See* Notice of Status of System of Records; Interim Final Notice: Request for Further Comments, 68 Fed. Reg. 45,265, 45,267 (Aug. 1, 2003). This is a vast improvement over TSA's initial statement that it would retain data for 50 years. *See* Notice to Amend a System of Records, 68 Fed. Reg. 2,101, 2,102 (Jan. 15, 2003). The purging provision, however, applied only to data regarding U.S. persons, suggesting that TSA would retain data on the travel of non-U.S. persons after a flight had safely been completed and use it for other intelligence purposes. *See* Notice of Status of System of Records, 68 Fed. Reg. at 45,267.

152 *Data Mining: Current Applications and Future Possibilities: Hearing Before the Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, of the House Comm. on Gov't Reform*, 108th Cong. (2003) (statement of Jen Que Louie, President, Nautilus Systems, Inc.).

where information systems are used by law enforcement officials to arrest or detain individuals and in other situations where the government makes decisions adverse to individuals.[153] Especially in the context of pattern-based searches, the procedures the government employs to verify and confirm the relevance of the pattern and the reliability of the "hit" will determine whether it is reasonable for the government to rely on pattern analysis to take adverse action against an individual.

The opportunity and need to address data quality arises whenever the government enters into a contract for access to commercial data. Before entering into a contract for access to a particular commercial database, the government should formally assess the accuracy, completeness, and timeliness of the data. Data quality should be a competitive factor in choosing from among various commercial databases. And those who use the data should be apprised of its reliability so that they may adjust their level of confidence accordingly. In fact, a reliability assessment could accompany the various intelligence products that are based on commercial data (just as other assessments include some indication of reliability). Agencies should set data quality standards for data acquired from commercial providers and insist upon periodic auditing, with negative consequences up to and including contract termination when data fails to meet agreed-upon standards. If agencies are acquiring information and bringing it into their own databases at a particular point in time, they should track the date they acquired the information and make provisions for updating it.

6. Individual Access

A crucial principle found in both the Privacy Act and the laws affecting the commercial world is that individuals should have access to the personally identifiable information held about them. This right is often the key to enforcing other principles. For example, the FCRA gives consumers access to their credit reports and requires credit reporting companies to correct errors.[154] The right to insist that information about oneself be accurate is meaningless without the right to access and review the data. In the intelligence and law enforcement contexts, there are obvious security concerns that preclude allowing terrorist suspects to review what the government knows about them. But giving all individuals access to the commercial data about themselves poses no such risk. Laws should be established or strengthened allowing individuals to review and verify commercial data used by the government for counterterrorism purposes. One way to do this is to amend the FCRA to extend some of its protections to data used by the government for counterterrorism purposes not otherwise covered by the FCRA. This could be done in a way that preserves the exception that prohibits notice to the individual in the case of subject-based queries for law enforcement or intelligence purposes. Even in the absence of legislative action, government agencies entering into contracts for commercial data could require as a condition

153 *See supra* text accompanying notes 130–39.

154 *See supra* text accompanying notes 37–40. **R**

of the contracts that the data aggregators provide FCRA-like rights to individuals.

In cases where individual review is not feasible, the review rights could be vested in an agency privacy officer, an inspector general, or a judge—someone who would have the authority on behalf of an individual to review records held about that person to determine if they are properly acquired, accurate, and maintained pursuant to proper authority.[155] While such a reviewer might be able to disclose little to the individual, he could provide an oversight mechanism. Agencies should also establish complaint procedures that include access to information for individuals who face adverse consequences (such as not being permitted to board an airplane) due to the use of commercial data.

7. System Security

Agencies that create systems that handle sensitive personal information are required to secure their systems against both internal and external threats. An information security strategy should address unauthorized access to and use of the information, as well as unauthorized destruction and modification of the information. Agencies should establish audit trails to monitor how employees use systems.

8. Accountability and Redress

Any system for personally identifiable information must have accountability and redress mechanisms. There is broad agreement that these should include audit trails to protect against unauthorized access, disclosure, or misuse. Technical work is being done on "immutable audits," involving tamper-proof logs that would automatically track and correlate all use of the system, so that any misuse could be identified immediately. Some of the same technical means that facilitate collaboration could also support ongoing, distributed auditing. Accountability mechanisms should also include periodic inspections to ensure that privacy principles are being enforced, with reports to Congress. As suggested above, any agency that uses commercial data for law enforcement or intelligence purposes should have a high-level privacy officer with primary responsibility for establishing, reviewing, and enforcing

155 Section 1001 of the USA PATRIOT Act specifically required the DOJ to designate an official in the Office of the Inspector General to review complaints about intrusions on civil liberties. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 1001(1), 115 Stat. 272, 391. The statute establishing the Department of Homeland Security created a privacy officer, *see* Homeland Security Act of 2002, Pub. L. No. 107-296, § 222, 116 Stat. 2135, 2155, and an officer for civil rights and civil liberties, *see id*. § 103, both of whom would seem to have authority to investigate specific complaints, *see id*. §§ 222, 705. Unfortunately, when the President created the Terrorist Threat Integration Center, he placed it outside of either of these statutory oversight mechanism and created nothing to replace them. *See The Terrorist Threat Integration Center (TTIC) and Its Relationship With the Departments of Justice and Homeland Security: Hearing Before the House Comm. on the Judiciary & the House Select Comm. on Homeland Security*, 108th Cong. (2003) [hereinafter *Terrorist Threat Integration Center Hearing*] (prepared statement of Jerry Berman, President, Ctr. for Democracy & Tech.).

privacy standards, similar to the position created by statute within DHS,[156] and an official with authority to investigate specific complaints of abuse or error.

The accountability process should also include periodic evaluations of cost and effectiveness, including the relative cost and effectiveness of particular applications of commercial data. As explained above, effectiveness is a core civil liberties concern because lack of effectiveness indicates no justification for the use of personally identifiable information.

B. Rules for Government Access and Consequences

Despite changes in information processing technology, the principles of fair information practices provide a good starting point for developing guidelines for governmental use of commercial databases. Even though some of the fair information practices are less relevant than others, they suggest ways to address the issues posed by governmental use of personally identifiable information for counterterrorism purposes. Two issues in particular require further elaboration: standards for government access, and due process protections for dealing with the consequences of governmental use of information.

1. Government Access Standards

As shown above, the Supreme Court's "business records" doctrine and the changes wrought by the USA PATRIOT Act have left many records held by the private sector unprotected against government access or subject to only minimal standards for access.[157] This is dangerous for privacy, for it leaves the flow of sensitive information unchecked, but it is also undesirable from the perspective of governmental efficiency, since it permits an indiscriminate flood of fragmentary, ambiguous information that could drown intelligence agencies that are ill-equipped to handle the information they currently have.

The government needs a more calibrated approach that provides guidelines for counterterrorism access to commercial data. These guidelines should take into account the sensitivity of the information, whether it is widely or publicly available, and how the government plans to use it.[158] The guidelines must specify criteria for the government to obtain data, as well as an appropriate decisionmaker. Obtaining address data to locate a specific person in whom the government has a legitimate interest should be much easier than obtaining detailed personal information that is not widely available. Searches without particularized suspicion pose special risks, requiring special rules. We thus recommend that rules governing government access to commercial data take into account three key questions: What type of data is the government accessing? Does the government have particularized suspicion? How does the government intend to use the data?

156 *See supra* note 155. **R**

157 *See supra* Part II.

158 For a discussion of the five privacy axes, see *supra* Part I.A.2.

Some kinds of data should be available to analysts and investigators on a routine basis, so that they can be searched instantly, without prior approval of each query, while more sensitive data, or data not widely available, should be harder for the government to access. Name, address, and listed telephone number are examples of information in commercial databases that should be available to every law enforcement and intelligence agency with no prior authorization (although only as part of an ongoing investigation, subject to audits and other internal controls). Similarly, criminal history data, driver's license data, and other "publicly available" records should be available for online access. By contrast, medical or financial details should be obtained only with a court order based on an appropriate factual showing of need.

The government's authority to access information should also vary depending on how it plans to use a particular database. If an FBI agent seeks access to a data aggregator's information to obtain additional information on a single suspected terrorist, that subject-based search creates fewer privacy implications than a broad pattern-based search of that same database, because pattern-based searches review information about many people under no suspicion at all.[159] It may be appropriate to require special judicial or senior executive approval before undertaking any pattern-based search, to ensure that there is a sufficient factual basis to design an effective pattern-based search.[160] The sensitivity of the data might be factored into this determination, as well as whether the data can be anonymized for purposes of analysis, so that the government does not learn the identity of any individual until it meets a higher threshold.

One approach for authorizing pattern-based searches of commercial data might be found in a "section 215 with teeth." As explained above, section 215 of the USA PATRIOT Act authorizes the FBI to obtain a court order compelling disclosure of information by commercial entities, based solely on an unsupported assertion that the information is "sought for" an authorized counterintelligence investigation.[161] The provision seems to allow the government to compel disclosure of entire databases.[162] It is one of the most criticized provisions of the USA PATRIOT Act.[163] Section 215 could be amended, however, to require a more appropriate basis for pattern-based queries. An amended section 215 could require a judicial finding, based on facts shown by the government, that there is a reason to believe that terrorist activity is afoot fitting a certain pattern, and that reliable information rele-

159 We remain highly skeptical of the efficacy of pattern-based searches, especially when compared to the many tasks associated with tracking individuals known or suspected on the basis of traditional leads of engaging in terrorism, their associates, and their networks. The question of efficacy must be evaluated by the executive and legislative branches in much greater detail than it has been to date before we even get to the question of judicial or other authorization for specific pattern-based searches on specific databases.

160 TECH. & PRIVACY ADVISORY COMM., *supra* note 2, at 47–48, 51–52. **R**

161 *See supra* text accompanying note 90. **R**

162 *See* USA PATRIOT Act § 215.

163 We have previously argued that section 215 should be amended to require reasonable suspicion for subject-based queries. *See, e.g.*, *Freedom After Sept. 11: Hearing Before the Senate Comm. on the Judiciary*, 108th Cong. (2003) (statement of James X. Dempsey, Executive Dir., Ctr. for Democracy and Tech.).

vant to the interdiction of that activity would likely be obtained from the search of one or more commercial databases. Under this approach, an agency that had intelligence information about a possible future attack and that wanted to run a pattern-based search to identify potential planners would be required to demonstrate to the court: (1) facts giving reason to believe that a threat existed displaying certain characteristics; (2) a description of the databases that the government wants to search, including an assessment of the sensitivity of the data involved and its accuracy and reliability; (3) an explanation of why other methods of investigation were inadequate; and (4) a statement indicating whether the commercial databases would remain under the control of the commercial source or whether they would be acquired by the government. The court would evaluate the application to determine whether the government had shown sufficient specific and articulable facts to give reason to believe that a pattern-based search will turn up information relevant to a counterterrorism investigation, and that the databases to be searched were reliable and accurate enough to produce uniquely relevant information.

The scheme might also require the court to consider the sensitivity of the data being searched. If the court found that the data was sensitive, the court might authorize the search only on an anonymized basis, requiring the government to make a higher showing to obtain the individual identities of those who fit the search criteria. If an agency runs a pattern analysis program against certain databases, the algorithm might turn up, hypothetically, ten people who fit the pattern. To find those individuals' identities, government officials would have to return to court to justify their need for the information based on the likelihood that the pattern demonstrates that the individuals are terrorists. Factors the court might consider include the nature of the databases searched, the intelligence that led authorities to believe a certain pattern was relevant, the quality of the data, and the likelihood of false positives.

2. Consequences

Traditionally, governmental counterterrorism uses of personally identifiable information were fairly narrow. In the case of citizens and permanent resident aliens, the government's only active option was criminal prosecution. In the criminal justice system, the rules for use of information were clear and protective of the individual. If an investigation ended without a criminal prosecution, the information remained within the criminal justice files and could not be used for other purposes. By statute, grand jury information was sealed. If a criminal prosecution ensued, robust due process rules applied. While immigrants were vulnerable,[164] intelligence agencies had no authority to take adverse action against U.S. persons. In the new environment, with its emphasis on prevention outside the criminal justice system, the government is likely to take a range of adverse actions against citizens for which the due process rules are unclear.

164 *See, e.g.*, Reno v. Am.-Arab Anti-Discrimination Comm., 525 U.S. 471 (1999).

A full discussion of consequences and due process is hampered by the lack of specificity in many discussions about how the government will be using commercial information and other data analysis techniques. How will the government use "knowledge" generated by computerized analysis of commercial and governmental data? Could the data analysis trigger a criminal or intelligence investigation? Will it be used to build a criminal case? (Once a criminal investigation proceeds to the stage of search and seizure or arrest, traditional probable cause protections come into play.) Will it be used to place someone on a watch list? Will it be used for screening purposes—to trigger 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? The exact means of preventing terrorism outside of the criminal justice and immigration systems are ill-defined, but it is clear that personally identifiable information will be used to screen individuals at airports and possibly in other transportation contexts, as well as in employment matters.[165]

Given the new emphasis on screening and prevention, criminal due process rules will often be inapplicable. The establishment of access standards for pattern-based searches, the use of anonymization techniques to shield the identity of persons in databases, and the monitoring of usage to identify unauthorized uses only partially resolve the concerns raised by the use of commercial data. Even if the guidelines include all those techniques, the questions remain of how "hits" will be used and what opportunity an individual will have to prove he is not a risk.

The use of commercial databases to create watch list entries presents some significant questions. On what basis can an individual be added to a watch list, and for what purposes? Do watch lists have different designations for different levels of risk that individuals present, such as a "known terrorist" versus a "person of interest"? Can an individual discover and challenge the fact that he is on a watch list? Particularly where the government uses commercial data to augment watch lists, those lists should be subject to minimum data quality requirements, be governed by internal verification procedures, be reviewed and updated on a periodic basis, have a clear standard for adding names, and provide some way for an individual who has been erroneously listed to have his name removed.[166]

---

165 One of the few specific discussions of how information can be used is presented in the second report of the Markle Task Force. *See* MARKLE FOUND. TASK FORCE, CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY, *supra* note 2, at 30–38. R

166 For more on watch list guidelines, *see* MARKLE FOUND. TASK FORCE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE, *supra* note 2, at 27–31. Another possible source of watch list standards can be found in the Criminal Intelligence Systems Operating Policies, which govern Regional Information Sharing Systems, or RISS. Those regulations require reasonable suspicion of criminal activity before information can be collected on an individual, *see* 28 C.F.R. § 28.20(a) (2002), and explain that reasonable suspicion "is established when information exists which establishes sufficient facts to give . . . a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity," *id.* § 23.20(c). A similar standard could be used to decide whether a name goes on a watch list. Those regulations also require periodic review and validation of information that is retained. *Id.* § 23.20(h). R

Perhaps the hardest issue is how to provide due process to those who face adverse consequences. This involves protecting people not only against the consequences of abuse, but also against authorized uses that happen to be mistaken, either because they were based on erroneous information or because the analysis resulted in false positives. Different rules will probably be needed depending on the consequences; a person denied a job may have more rights than a person subject to a baggage search at an airport. For example, one possible rule could require further traditional investigation before any overt action is taken against an individual based solely on a pattern-based query. If the process is of a screening nature, and leads, for example, to denial of a job, the set of procedures applicable to security clearance determinations may serve as a model.

Other uses will need new control and oversight mechanisms. For example, if a pattern-based search leads to criminal or intelligence investigation, prompt resolution of those investigations would be desirable, so that those upon whom the computer mistakenly casts suspicion do not remain under surveillance. Current guidelines for FBI investigations set various time limits beyond which investigative activity cannot proceed without headquarters or DOJ approval.[167] For investigations opened as a result of pattern-based searches, those timelines should be shorter than normal in order to promptly resolve suspicions.

The companies selling the data to the government in the first instance might be the focus of another potential redress mechanism. As discussed above, the FCRA does not appear to apply to information that data aggregators sell to the government for law enforcement or intelligence purposes. Thus, as the government increasingly relies on commercial data aggregators in counterterrorism efforts, it may be necessary to provide individuals with some of the same access and correction rights that they have with their credit reports. This right could be established either through legislation or the government contracting process. Such a reform could have broad benefits: individuals could ensure their information is correct, companies would gain consumer trust and improve their data quality, and government agencies would obtain better data. Also, giving everyone the right to view and correct the data while it remains in the commercial sector would ameliorate concerns about providing direct access to governmental counterterrorism information.

C. Structuring Controls Throughout the Government

Where these guidelines should be developed within the governmental system and what role each branch of government should play in their implementation remain difficult questions. Certainly, we should not leave the guidelines up to individual agencies. The government needs a set of comprehensive guidelines that would apply to the entire federal law enforcement, intelligence, and homeland security community—both to give the American public confidence that the government will use these new technologies responsibly, and to ensure that their use does not migrate toward the agency with the most secrecy and the least restrictive rules. There is a strong argu-

167 *See* ATTORNEY GENERAL GUIDELINES, *supra* note 25, at 9. **R**

ment that the guidelines should be promulgated by the president, subject to some form of notice and comment. If the president fails to act, however, Congress will have to address the issue. Moreover, even if the president fully used the rulemaking and procurement power, the executive branch's authority can only extend so far: in order for judicial controls to become part of the process, Congress will have to act.

1. The Role of the Executive Branch

The executive branch has not made oversight and accountability regarding the use of commercial data and advanced analytic technology easy. In 2002, Congress created DHS and gave it the role of bringing together and analyzing intelligence from all agencies.[168] Congress also created a Privacy Officer and a Civil Rights and Civil Liberties Officer as important checks on that authority.[169] Just a few months later, however, the President created the Terrorist Threat Integration Center by Executive Order and gave *it* the intelligence fusion and analysis role.[170] The Terrorist Threat Integration Center was placed under the Director of Central Intelligence, outside of the oversight mechanisms that Congress specifically created at DHS.[171]

This approach—unilaterally creating information analysis programs outside of a system of checks and balances—does not suggest an executive branch commitment to oversight and control of new information analysis functions. As we have shown here, such rules and guidelines are important not only to protect civil liberties, but also to ensure that governmental counterterrorism activities are focused and effective. Since we need government-wide rules, the most logical place for development of their framework is within the executive branch, where the realities of day-to-day law enforcement needs and intelligence analysis can be taken into account. Especially in light of the executive branch's poor track record on accountability, it is important that the development of those rules should occur through a transparent process involving public notice and comment periods. There are several options. The president might issue a draft Executive Order or Presidential Directive and solicit comments before issuing a final version. Alternatively, DHS could issue regulations on the use of commercial data, again pursuant to notice and comment procedures, and the president could extend the application of those regulations to other agencies to ensure a single government-wide standard.

2. The Role of Congress

Congress's role is crucial. Congress has already conducted oversight of "data mining" and set some constraints on its implementation through the budgetary process.[172] Congress should continue to use both the budget pow-

168 *See supra* note 155. **R**

169 *Id.*

170 *Id.*

171 *See generally Terrorist Threat Integration Center Hearing*, *supra* note 155. **R**

172 Congress deferred implementation of the CAPPS II program until certain questions had been answered, and the original "Wyden Amendment," which became law in February 2003,

ers and its oversight authority, although establishment of substantive guidelines should be the goal, as opposed to the all-or-nothing approach that congress took with regard to TIA.

As a first step, Congress should prohibit domestic use of pattern-based searches by any government agency acting in a law enforcement, intelligence or homeland security capacity until the effectiveness of such searches has been proven—to the satisfaction of the executive branch, Congress, and the American public—and privacy rules have been written. While Congress should continue to authorize research and development, it should take another act of Congress to go beyond development into actual use.

Congress should insist on reports by executive branch agencies as to what commercial data they are already using and for what purposes.[173] Once it has basic information about how commercial data is currently being used, Congress should conduct an in-depth, non-partisan investigation into the efficacy of current and future uses, including an analysis of whether pattern-based searches can work in the national security context. If effectiveness is demonstrated, then we will need a set of privacy protections and checks on governmental power that would apply government-wide. If the president does not adopt adequate guidelines, Congress will have to legislate them. And no matter what guidelines the executive branch issues, Congress will need to legislate the role of the judiciary in approving the use of pattern-based searches and the de-anonymization of search results.

Only if effectiveness is proven, and a privacy framework is established, should Congress consider explicit authorization of pattern-based searching technology using both governmental and commercial data. Any such authorization should include a sunset provision to ensure that Congress has an opportunity to evaluate the effectiveness of the technology once it is put into practice, as well as its civil liberties implications.

3. The Role of the Judiciary

As explained above, under current law, when the government is accessing information in the hands of commercial entities, the judiciary exercises little meaningful control. Given the serious consequences that may flow from counterterrorism uses of data outside the criminal justice context, particularly pattern-based searches, it is appropriate to consider what role the judiciary might play as a check on executive power. There are several ways to structure a judicial role that would provide that check without unduly burdening executive branch efficiency. One mechanism is to require a court order approving the use of pattern-based analysis in the first instance. This is

---

prohibited any domestic deployment of TIA during Fiscal Year 2004, but permitted research and development. *See* Consolidated Appropriations Resolution, Pub. L. No. 108-7, Div. M, § 111, 117 Stat. 11, 534–36 (2003).

173 *See, e.g.*, Citizens' Protection in Federal Databases Act, S. 1484, 108th Cong. § 3(b) (2003) (requiring DHS, FBI, CIA, and other agencies to submit reports to Congress detailing "any use by the department . . . of databases that were obtained from or remain under the control of a non-Federal entity, or that contain information . . . acquired initially by another department . . . for purposes other than national security, intelligence, or law enforcement"); Data-Mining Reporting Act of 2003, S. 1544, 108th Cong. § 3.

the "section 215 with teeth" concept discussed above.[174] But courts also can play a role after the pattern-based analysis has occurred. Although individuals who believe that government use of commercial data has violated their *constitutional* rights can sue after the fact, that is an inefficient and likely ineffective check on government power. On the other hand, a private right of action to sue governmental officials who violate any new statutory standards governing the use of commercial data, as part of a larger redress framework, could help limit abuse.

Conclusion

Civil liberties advocates should take no solace in the government's inefficiency in using information technology. Inefficiency itself poses threats to civil liberties when, as now, the government has broad discretionary authority to acquire or access commercial data, but few guidelines on how to use it, thus creating a high risk of erroneous decisions with no due process mechanisms to correct them. Given the current emphasis on terrorism prevention through screening and other means outside the criminal justice context, rules that guide governmental use of information will also serve civil liberties by making decisions more reliable, transparent, and accountable. Governmental use of commercial data presents new challenges that the current legal structure does not adequately address. We need a new framework, but policymakers need not design it in a vacuum. The new framework can draw upon existing principles of fair information practices. It should address not only the question of access to data, but also those questions relating to the permissible uses of data and the protections individuals have against the consequences of that use.

174 *See supra* Part III.B.1.