Fall 2004

Terrorism, Technology, and Information Privacy: Finding the Balance

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Terrorism, Technology, and Information Privacy: Finding the Balance

by Fred H. Cate

I want to describe briefly one example of the research that the generosity of alumni supports. Because this is truly a work in progress, I will pose questions rather than attempt any answers, but the questions address a subject that is timely, controversial, important, and, I hope you will agree, interesting. — FHC

Government data mining

The nation is confronted with many examples of vexing questions about how to regulate the government's access to personal information maintained by or in the private sector:

• The Defense Department announced that it was working on "Total Information Awareness" — later renamed "Terrorism Information Awareness" — a research and development program that included technologies to search personally identifiable transaction records and recognize patterns across separate databases for the purpose of combating terrorism.

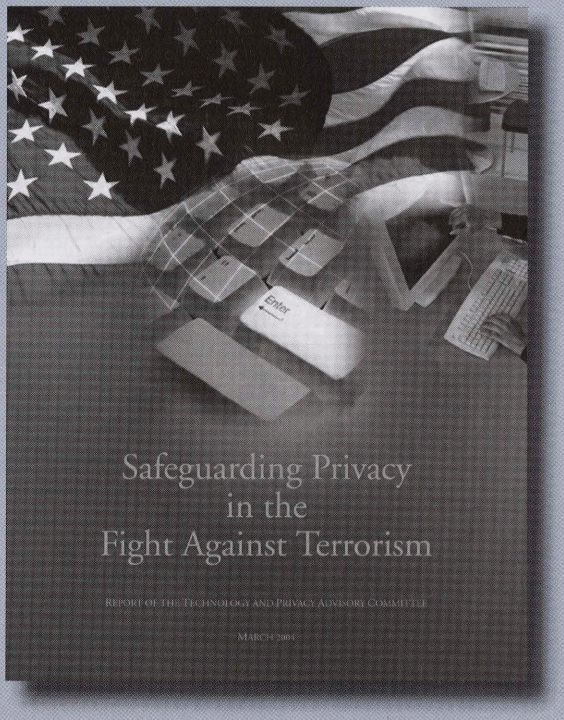
• The Advanced Research and Development Activity center, based in the National Security Agency, has a project — Novel Intelligence from Massive Data — to develop tools to examine large quantities of data to "[r]eveal new indicators, issues, and/or threats that would not otherwise have been found due to the massiveness of the data."

• Section 201 of the Homeland Security Act, signed into law in November 2002, requires the Department of Homeland Security to "establish and utilize … data-mining and other advanced analytical tools" to "access, receive, and analyze data" in order to "detect and identify threats of terrorism against the United States."

• Army defense contractor Torch Concepts, with the assistance of the Department of Defense and the Transportation Security Administration, obtains millions of passenger records from JetBlue Airways and Northwest Airlines to study how data profiling can be used to identify high-risk passengers. For many of the passengers, Torch Concepts was able to buy demographic information including data on gender, occupation, income, Social Security Number, home ownership, years at current residence, number of children and adults in the household, and vehicles.

• The TSA has announced that it is in the process of deploying the second generation of the Computer-Assisted Passenger Prescreening System, which compares airline passenger names with private- and public-sector databases to assess the level of risk a passenger might pose.

• The USA PATRIOT Act, adopted in the aftermath of the Sept. 11, 2001, terrorist attacks, expands the power of the Treasury Department's Financial Crimes Enforcement Network (FinCEN) to require financial institutions to report suspected money laundering or terrorist activities by their customers. The act also mandates new "Know Your Customer" rules, which require financial institutions to verify the identity of any person seeking to open an account, maintain records of the information used to verify the person's identity, and determine whether the person appears on any list of known or suspected terrorists or terrorist organizations.



• Florida police have created a new database called MATRIX (Multistate Anti-Terrorism Information Exchange) to link law enforcement records with other government and private-sector databases. The new system is designed to "find patterns and links among people and events faster than ever before." Eight states and the DHS are now participating in MATRIX, which is funded by the Justice Department and the DHS.

All of these and similar government programs present variations on the same question: To what extent should the government be able to conduct sophisticated computerized searches of transactional records and other private sector databases of U.S. citizens and permanent residents in an effort to detect and prevent terrorist attacks, for national security, and for law enforcement purposes?

(*continued on page 6*)

Technology Privacy and Advisory Committee

Faced with this difficult and critical question, the federal government did what it often does: appoint a committee. In February 2003, Secretary of Defense Donald Rumsfeld appointed the Technology and Privacy Advisory Committee to advise him on whether anti-terrorist data-mining technologies should be developed, and, if so, what safeguards should be developed to ensure those technologies are used "in accordance with U.S. law and American values related to privacy." The committee consists of eight members:

- **Newton N. Minow**, chair, is senior counsel to the law firm of Sidley Austin Brown & Wood; he served as chair of the Federal Communications Commission under President Kennedy.
- **Floyd Abrams** is a partner in the New York law firm of Cahill Gordon & Reindel and the William J. Brennan Jr. Visiting Professor of First Amendment Law at the Columbia Graduate School of Journalism.
- **Zoë Baird** is president of the Markle Foundation and previously was senior vice president and general counsel of Aetna and an attorney in the White House and in the Justice Department.
- **Griffin Bell** was managing partner of King & Spalding, a judge on the U.S. Court of Appeals for the 5th Circuit, and attorney general of the United States.
- **Gerhard Casper** is president emeritus of Stanford University and the Peter and Helen Bing Professor in Undergraduate Education at Stanford.
- **William T. Coleman Jr.** is a senior partner and the senior counselor in O'Melveny & Myers; he served as secretary of transportation during the Ford administration.
- **Lloyd N. Cutler** is a founding partner of the law firm of Wilmer Cutler & Pickering; he served as counsel to Presidents Clinton and Carter.
- **John O. Marsh Jr.** is a distinguished professor of law at George Mason University; previously he was a member of Congress, assistant secretary of defense for legislative affairs, counselor to the president, and the longest-serving secretary of the Army.

The eight members read like a *Who's Who* of government, law, industry, and higher education. Between them, they have earned 10 JDs or doctorates and more than 100 honorary doctorates. They represent all three branches of government, including one federal appellate court judge, one member of Congress, two cabinet secretaries, an attorney general, three White House lawyers (including one who worked as White House counsel for two presidents), and one chair of the FCC.

They serve on the boards of an impressive cross section of Fortune 500 companies, including AMAX, Aon Corp., CBS, Chase Manhattan Bank, Chubb Corp., CIGNA Corp., IBM, Pan American, Sara Lee Corp., Foote Cone & Belding, Manpower Inc., PepsiCo., and the Tribune Company.

They are an enviable model of public service, including the chairs of the Carnegie Corp., the Commission on President Debates, the Rand Corp., and PBS — and that is just Mr. Minow. Six of the eight are members of the American Law Institute; three were Supreme Court clerks; and three are name or managing partners of the nation's 50 largest law firms.

In short, if anyone could figure out the proper balance between privacy and government data mining, these people could. However, they — and certainly I, as their counsel — have found it more difficult than I think any of us would have expected. With hindsight, there seem to be four reasons, all of them related in varying degrees to technological changes.

Technology of data mining

The government has always used personally identifiable data about individual U.S. persons as part of its law enforcement and national security efforts. Current law is already appropriate to address such inquiries (requiring in most cases a warrant or wiretap order before a U.S. person can be the subject of search, seizure, or surveillance).

Dramatic advances in information technology, however, have greatly increased the government's ability to access data from diverse sources, including commercial databases. New technologies also allow the government to engage in data mining to search vast quantities of data for the purpose of identifying people who meet specific criteria or otherwise present unusual patterns of activities. Such data mining is arguably one 21st-century equivalent of general searches, because its key characteristic is that it involves scrutiny of data about individuals who have done nothing to warrant government suspicion.

The volume of data

Those technologies have also exponentially increased the volume of data available about individuals and greatly reduced the financial and other obstacles to retaining, sharing, and exploiting those data in both the public and

private sector. We leave data trails behind us every day as we make purchases, browse the Internet, travel, commute, make phone calls, send e-mail, go to school, punch time clocks, use electronic keys, watch television, or engage in thousands of other ordinary activities. Digital technologies make those easy to capture — in fact, difficult to avoid capturing — and the high value of that information creates a powerful incentive to do so.

In addition, the government is collecting vast storehouses of information through its everyday activities and through its national security efforts. One of the most immediate challenges facing U.S. anti-terrorist activities is separating out the "signal" of useful information from the "noise" of all of those data. Technological tools are essential to help analyze data and focus human analysts' attention on critical relationships and patterns of conduct. Their use, however, necessarily raises significant privacy and other civil liberties issues.

New terrorist threats

As the attacks of Sept. 11, 2001, made clear, the United States faces a new and deadly terrorist threat. That threat is qualitatively different from anything the nation has faced before because of the power of terrorists to strike from within, their willingness to sacrifice their own lives in the relentless pursuit of the devastation of our nation, their demonstrated ability to turn technologies into weapons than can cause mass destruction, and their use of advanced information technologies to launch highly coordinated, well-financed, and painstakingly rehearsed attacks against the United States. This combination threatens not only American lives, but our way of life and our ability to defend ourselves.

Inadequacy of the distinctions on which current law is based

Current law is too fractured and outdated to ensure either that the government can access the data it really needs to protect national security and fight crime effectively or that individual privacy is protected in the process. For example, the Supreme Court's application of its determination that the Fourth Amendment protects only "reasonable" expectation of privacy has yielded uneven and often incomprehensible results. The court has found "reasonable" expectations of privacy in homes, businesses, sealed luggage and packages, and even drums of chemicals, but no "reasonable" expectations of privacy in voice or writing samples, phone numbers, conversations recorded by concealed microphones, and automobile passenger compartments, trunks, and glove boxes.

Current law is too fractured and outdated to ensure either that the government can access the data it really needs to protect national security and fight crime effectively or that individual privacy is protected in the process.

Most relevant to government projects that could involve accessing data about U.S. persons from commercial databases, the Supreme Court held in 1976 in *United States v. Miller* that there can be no reasonable expectation of privacy in objects or information held by a third party. The case involved bank records, to which, the court noted, "respondent can assert neither ownership nor possession." Such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," and therefore the court found that the Fourth Amendment is not implicated when the government sought access to them, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." The Fourth Amendment just doesn't offer much protection in the data mining context, since all of the data involved are held by a third party.

Moreover, the Supreme Court's application depends significantly on the nationality of the individual(s) involved, the country in which the search takes place, and whether the motivation for the search is "national security" and "law enforcement." Statutes designed to help fill some of the constitutional gaps reflect this same approach.

This "line at the border" approach has never been easy to apply. Multiple inquiries into the events of Sept. 11 suggest that it contributed to the government's inability to detect or prevent those attacks. These distinctions are made even more difficult — if not entirely meaningless — by global information technologies and the nature of the new terrorist threat. The threats are not so easy to divide into home and abroad; government anti-terrorism

(*continued on page 8*)

Terrorism

(*continued from page 7*)

initiatives don't fit neatly into artificial "national security" or "law enforcement" categories; data mining searches don't distinguished very readily between U.S. person data and non–U.S. person data; and global networks like the Internet ignore national borders and greatly reduce the relevance of geography and nationality.

The current political climate is contributing to making the laws applicable to data mining even more fractured. Less than three months after Congress adopted the Homeland Security Act, in which it required the DHS to "establish and utilize … data-mining and other advanced analytical tools" to "access, receive, and analyze data" in order to "detect and identify threats of terrorism against the United States," it adopted an amendment to the Omnibus Appropriations Act restricting the DOD from developing or deploying data-mining technologies in the war on terrorism. Such inconsistency offers little guidance to government officials or to the public about either how to fight terrorism or how to protect privacy.

The challenge ahead

Updating the law to respond to these new challenges is a daunting, but urgent, challenge. On one side is the risk of failing to identify and deter terrorist attacks. On the other are the civil liberties put at risk by data mining. The original motto of the Total Information Awareness program was *Scientia Est Potentia* — "Knowledge Is Power." Awareness that the government may, without probable cause or other specific authorization, obtain access to myriad distributed stores of information about an individual is likely to alter his or her behavior.

This is not always a bad outcome. However, knowledge of that power can cause people to change their behavior to be more consistent with a perceived social norm, to mask their behavior, and/or to reduce their activities or participation in society to avoid the surveillance. Vice President Hubert Humphrey observed almost 40 years ago, "We act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered, and our very character will change."

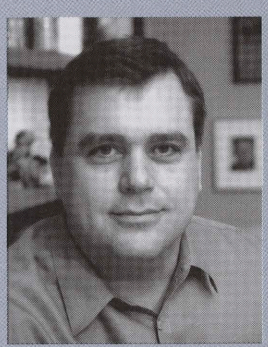
The risk is not only that commercial and social activities are chilled, but that protected rights of expression, protest, association, and political participation are affected as well. In the context of government data monitoring in a democracy, the risk of the power to access data from disparate sources is not merely to information privacy, but to other civil liberties, including freedom of expression, association, and religion.

Benjamin Franklin warned more than two centuries ago, "They that can give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety." This is not merely a theoretical issue. Franklin might well have added that those who would trade liberty for safety all too often achieve neither.

The resolution of the tension between security and liberty is not as easy as Franklin's oft-quoted phrase makes it sound. But it is a tension as old as our country. In fact, it is embodied in our Constitution, which links the commitments to "establish Justice, insure domestic Tranquility, [and] provide for the common defense" with "secure[ing] the Blessings of Liberty."

Alexander Hamilton wrote in Federalist Paper 8 in 1787, exhorting the people of New York to ratify the Constitution, that "[s]afety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates."

Faced with a new and dangerous threat from international terrorism, we too must guard against this natural tendency. "The violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger," Hamilton warned, "will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free."



Tyagan Miller

Fred H. Cate

Fred H. Cate is a Distinguished Professor at the Indiana University School of Law—Bloomington and director of the Indiana University Center for Applied Cybersecurity Research. This essay is based on remarks he made on Oct. 17, 2003, at the 21st Century Society Dinner, honoring those who gave $1,000 or more to the Law School's annual Fund for Excellence.

The advisory committee presented its final report, "Safeguarding Privacy in the Fight Against Terrorism," to Secretary Rumsfeld in May 2004. The report is available online at www.sainc.com/tapac or www.defenselink.mil.