

Prepared Statement of Fred H. Cate
Distinguished Professor and Director
Center for Applied Cybersecurity Research
Indiana University

Before the Privacy and Civil Liberties Oversight Board
December 5, 2006

Chairwoman Dinkins, Vice Chairman Raul, and Members of the Board:

My name is Fred Cate and I am a Distinguished Professor and director of the Center for Applied Cybersecurity Research at Indiana University and a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams. For 16 years I have researched and taught about information privacy and security issues, with a special emphasis during the past five on how these issues interact with national security concerns.

I am the reporter for the American Law Institute's project on Principles of the Law of Government Access to and Use of Personal Digital Information and a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals. Previously I served as reporter for the Department of Defense Technology and Privacy Advisory Committee and for the third report of the Markle Foundation Task Force on National Security in the Information Age. My remarks obviously do not reflect the views of any of these organizations, but I have benefited greatly from my involvement with them and the other colleagues, some of whom are here today, that they included.

Thank you for the opportunity to appear before you today. I applaud the Board for holding this public forum and I appreciate the invitation to participate.

The Need for Political Will

You have so many important and timely issues before you—information sharing guidelines, U.S. persons guidelines, watch list redress procedures, surveillance programs, profiling, state and local fusion centers, data processing, governmental use of commercial data, and the USA PATRIOT Act—that I hardly know where to focus these brief remarks.

Certainly, all of these issues have been addressed in detail in books, articles, testimony, and reports. I attach to this statement a book chapter, "Legal Standards for Data Mining," that I wrote for Robert Popp and John Yen's book, *21st Century Enabling Technologies and Policies for Counter-Terrorism* (2006). Several of the chapters in that book, all three of the Markle Task Force reports (which deal extensively with information sharing), and many other sources offer useful and detailed analysis of the issues you are addressing.

Rather than rehash what is already in print, however, I would like to offer some broader insights that come from investigating a number of these topics. None of these insights is new. In fact, what is most striking about them is how frequently they have been identified in the relevant

literature, and how consistently they appear to have been ignored by the Administration and Congress in current data-based national security efforts.

At heart, therefore, my message today is that while the details of these specific topics may be quite complex, the basic policy and legal criteria for how they should be approached are often straightforward. They have been thoroughly addressed by many distinguished people and groups—the Markle Task Force on National Security in the Information Age,¹ the Department of Defense Technology and Privacy Advisory Committee,² the Department of Homeland Security Privacy and Integrity Advisory Committee,³ the 9/11 Commission,⁴ the Cantigny Conference on Counterterrorism Technology and Privacy,⁵ and others. What is most urgently needed, therefore, is not a great deal of new knowledge, but greater political will to ensure that we protect both security and privacy.

Good Privacy and Good Security Are Often Consistent

It has become almost a truism to say that privacy and national security are not inconsistent, but over the past five years I have been struck by how closely connected the two objectives really are. The failure to take privacy seriously has scuttled public and policymaker support for many promising security programs. But good privacy protection not only can help build support for the appropriate use of personal data to enhance security, it can also contribute to making those tools more effective. For example, data integrity—ensuring that data are accurate, complete, up-to-date, and appropriately stored and linked—is a key privacy principle. But it clearly enhances security as well. Legal obligations requiring data integrity inevitably make those data more useful for security application as well.

In March 2003, the Justice Department exempted the FBI’s National Crime Information Center from the Privacy Act’s requirements that data be “accurate, relevant, timely and complete,”⁶ and in August 2003, the Department of Homeland Security exempted the TSA’s passenger screening database from the Privacy Act’s requirements that government records include only “relevant and necessary” personal information.⁷ These efforts to avoid privacy obligations raise important security issues as well. Mismatched data and misidentified individuals pose serious risks for both privacy and security.

Similarly, the Department of Defense General’s December 2003 audit of the Department’s Total (later, “Terrorism”) Information Awareness program concluded that DOD’s

¹ See <http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php>.

² See <http://www.fredhcate.com/Publications/TAPAC_Report%20Final.pdf>.

³ See http://www.dhs.gov/xinfo/share/committees/editorial_0512.shtm.

⁴ See <<http://www.9-11commission.gov/>>.

⁵ See “The Cantigny Principles on Technology, Terrorism, and Privacy,” *National Security Law Report*, Feb. 2005, at 14.

⁶ *Privacy Act of 1974; Implementation*, 68 Federal Register 14140 (2003) (DOJ, final rule).

⁷ *Privacy Act of 1974: Implementation of Exemption*, 68 Federal Register 49410 (2003) (DHS, final rule).

failure to consider privacy adequacy during the early development of TIA led the Department to “risk spending funds to develop systems that may not be either deployable or used to their fullest potential without costly revision.”⁸ The report noted that this was particularly true with regard to the potential deployment of TIA for law enforcement: “DARPA need[ed] to consider how TIA will be used in terms of law enforcement to ensure that privacy is built into the developmental process.”⁹ Greater consideration of how the technology might be used would not only have served privacy, but also likely contributed to making TIA more useful as well.

As this example suggests, privacy protections often build discipline into counter-terrorism efforts that serves other laudatory purposes. By making the government stop and justify its effort to a senior official, a congressional committee, or a federal judge, warrant requirements and other privacy protections often help bring focus and precision to law enforcement and national security efforts. In point of fact, courts rarely refuse requests for judicial authorization to conduct surveillance. As government officials often note, one reason for these high success rates is the quality of internal decision-making that the requirement to obtain judicial authorization requires.

As the Technology and Privacy Advisory Committee, appointed by Secretary of Defense Donald Rumsfeld in 2003, noted in the introduction to its recommendations for new privacy protections:

Our conclusion, therefore, that data mining concerning U.S. persons inevitably raises privacy issues, does not in any way suggest that the government should not have the power to engage in data mining, subject to appropriate legal and technological protections. Quite the contrary, we believe that those protections are essential *so that* the government can engage in appropriate data mining when necessary to fight terrorism and defend our nation. And we believe that those protections are needed to provide clear guidance to DOD personnel engaged in anti-terrorism activities.¹⁰

Existing Privacy Law is Inadequate

The current law applicable to the government’s collection and use of personal data for whatever purpose, but especially in the context of national security, is confusing, outdated, and wholly inadequate. This has been demonstrated in detail in countless law review articles and reports, so let me take advantage of those to highlight five of its most immediate inadequacies.

⁸ Department of Defense, Office of the Inspector General, *Information Technology Management: Terrorism Information Awareness Program* (D-2004-033) 4 (2003).

⁹ *Id.* at 7.

¹⁰ U.S. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 48 (2004).

First, the law suffers from what Professor Daniel Solove has described as “profound complexity.”¹¹ Professor Orin Kerr has written that “the law of electronic surveillance is famously complex, if not entirely impenetrable.”¹² Courts agree with these assessments and have “described surveillance law as caught up in a ‘fog,’ ‘convoluted,’ ‘fraught with trip wires,’ and ‘confusing and uncertain.’”¹³

Second, much of that complexity reflects numerous distinctions, many of which are difficult to apply and frankly make little sense today. The law includes major distinctions based on the location of the surveillance, the purposes for which the intercepted information is sought, and whether the target is a “U.S. person” or a “non-U.S. person.” Yet these distinctions are increasingly unworkable and unjustifiable in a world of digital communications and networks that ignore national borders, terrorist threats within the borders of the United States, and the growing integration of foreign intelligence, domestic intelligence, and law enforcement.

Lawmakers must explicitly re-examine these distinctions to determine if they should be retained. If not, they should be abandoned, and the consequences dealt with explicitly. For example, if gathering intelligence to prevent terrorist attacks is to become a major focus of domestic surveillance, then stronger protections are needed to protect against misuse and mission creep. If the distinctions are to be retained, then they must be made workable and meaningful.

Third, the law today results in significant inconsistencies. For example, the very high protection for communications under Title I of the Electronic Communications Privacy Act¹⁴ does not extend to video surveillance if sounds are not captured at the same time. Meanwhile, the much weaker protection of Foreign Intelligence Surveillance Act¹⁵ does apply to silent video surveillance. “Foreign agents therefore receive protection against silent video surveillance whereas United States citizens do not.”¹⁶ Similarly, protection for stored communications hinges on whether the message has been stored for more than 180 days. Why? Telephone calls and e-mail receive significantly different protection from government surveillance without any apparent reason.

Fourth, for all of this law, key intelligence questions remain without clear answers. For example, do any of these laws apply to “data mining” or searches for keywords or relationships conducted by computer? Is it possible to show probable cause, under either the high standard of Title I of ECPA or the weaker standard of FISA, for searches that target a pattern of behavior rather than an identified person? There is disagreement as to whether the current law permits the

¹¹ Daniel J. Solove, “Electronic Surveillance Law,” 72 *George Washington Law Review* 1264, 1292 (2004). The article provides an excellent description and analysis of electronic surveillance law in the United States.

¹² Orin S. Kerr, “Lifting the ‘Fog’ of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law,” 54 *Hastings Law Journal* 805, 820 (2003).

¹³ Solove, “Electronic Surveillance Law,” *supra* at 1293.

¹⁴ Wiretap Act, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522).

¹⁵ Foreign Intelligence Surveillance Act of 1978 Pub L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. § 1801-1811).

¹⁶ Solove, “Electronic Surveillance Law,” *supra* at 1280.

Foreign Intelligence Surveillance Court or other courts to approve surveillance on a programmatic, as opposed to individualized, basis. If it does not, it should. Courts should have the legal capability to approve computerized searches of data to identify particular people, relationships, or patterns that warrant further investigation, subject of course to appropriate protections. In some instances, it may be that such searches should not even require judicial approval, for example, if conducted with wholly anonymized data. But the law should be updated to reflect the potential of such inquiries and to provide means for them to be authorized and limited as necessary to protect privacy.

Similarly, how should opened e-mail and voice mail messages be treated? The Department of Justice argues that they are merely remotely stored files and therefore do not fall within the protection of Title II of ECPA.¹⁷ Why aren't they simply stored communications that are directly covered by Title II (the Stored Communications Act)?

Fifth, much of this law seems outpaced by technological change. In 2004, TAPAC wrote in its final report:

Laws regulating the collection and use of information about U.S. persons are often not merely disjointed, but outdated. Many date from the 1970s, and therefore fail to address extraordinary developments in digital technologies, including the Internet. . . . Dramatic advances in information technology, however, have greatly increased the government's ability to access data from diverse sources, including commercial and transactional databases. . . .

. . . . Current laws are often inadequate to address the new and difficult challenges presented by dramatic developments in information technologies. And that inadequacy will only become more acute as the store of digital data and the ability to search it continue to expand dramatically in the future.¹⁸

Many statutory protections for personal privacy have been effectively reduced by the proliferation of digital technologies. For example, the Center for Democracy & Technology has noted that when the statutory authorization was adopted for the NSA to carry out electronic surveillance outside of the United States, "an international telephone call was a rarity for an ordinary person in the U.S. and e-mail was non-existent."¹⁹ Today, technological changes have rendered many if not most of U.S. persons' communications "potentially exposed to the NSA, whose computer processing power has surely grown by many factors."²⁰

¹⁷ Computer Crime and Intellectual Property Section, U.S. Department of Justice, *Manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* III.B (2001).

¹⁸ U.S. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 6 (2004).

¹⁹ Center for Democracy & Technology, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology* 3 (2006).

²⁰ *Id.*

When the ECPA's distinctions about whether a message is "in transit" or "in storage" were adopted in 1986, users downloaded email from their service provider onto their local computer. Messages therefore were not stored centrally after being read. Today, many e-mail systems are accessed through Web interfaces, so email is by default stored on servers belonging to third parties. "As a result of ECPA's complex rules, the same email message will be subject to many different rules during its life span. These complex rules likely do not match the expectations of email users."²¹

Nevertheless, the government actively exploits the distinctions. For example, the FBI's Key Logger System, which records individuals' keystrokes on their computers, was designed to collect data only when the users' machines were not connected to the Internet. When a user logs on, the keystroke recording stops, so that the agency can argue that the device is not capturing communications "in transit," but merely "in storage," and therefore is not required to comply with Title I of the ECPA.²² In the context of devices connected to the Internet, these distinctions are nonsensical.

There is no better example of the impact of technological change on the law than the exemption from the Fourth Amendment created by the Supreme Court for records held by third parties. The Supreme Court held in 1976 in *United States v. Miller*²³ that there can be no reasonable expectation of privacy in information held by a third party. The case involved cancelled checks, to which, the Court noted, "respondent can assert neither ownership nor possession."²⁴ Such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business,"²⁵ and therefore the Court found that the Fourth Amendment is not implicated when the government sought access to them:

The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.²⁶

The Court reinforced its holding in *Miller* in the 1979 case of *Smith v. Maryland*, involving information about (as opposed to the content of) telephone calls.²⁷ The Supreme Court found that the Fourth Amendment is inapplicable to telecommunications "attributes" (e.g., the

²¹ Id. at 11.

²² See *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001); see generally Solove, "Electronic Surveillance Law," *supra* at 1281-82.

²³ *United States v. Miller*, 425 U.S. 435 (1976).

²⁴ Id. at 440.

²⁵ Id. at 442.

²⁶ Id. at 443 (citation omitted).

²⁷ 442 U.S. 735 (1979).

number dialed, the time the call was placed, the duration of the call, etc.), because that information is necessarily conveyed to, or observable by, third parties involved in connecting the call.²⁸ “[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.”²⁹

As a result, under the Fourth Amendment, the use of “pen registers” (to record out-going call information) and “trap and trace” devices (to record in-coming call information) does not require a warrant because they only collect information about the call that is necessarily disclosed to others.

The third party exemption from the Fourth Amendment made little sense in the two cases in which it was created. Individuals who write checks and dial telephone calls do not “voluntarily” convey information to third parties. They have no choice but to convey the information if they wish to use what in the 1970s were the overwhelmingly dominant means of making large-value payments or communicating over physical distances.

Moreover, the information collected and stored by banks and telephone companies is subject to explicit or implicit promises that it will not be further disclosed. Most customers would be astonished to find their checks or telephone billing records printed in the newspaper. As a result of those promises and the experience of individuals, the expectation that such information would be private was objectively reasonable and widely shared. The Court’s decisions to the contrary, while they served important law enforcement objectives, made little logical or practical sense and did not reflect the expectations of either the public or policymakers, as recognized by the Court itself in *United States Department of Justice v. Reporters Committee for Freedom of the Press*:

In an organized society, there are few facts that are not at one time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster’s initial definition, information may be considered “private” if it is “intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public.” . . .

In sum, the fact that “an event is not wholly ‘private’ does not mean that an individual has no interest in limiting disclosure or dissemination of the information.”³⁰

Irrespective of whether the exemption made sense when decided, excluding records held by third parties from the protection of the Fourth Amendment makes less sense today because of

²⁸ Id. at 743.

²⁹ Id.

³⁰ 489 U.S. 749, 763-64, 779 (1989) (citations omitted).

the extraordinary increase in both the volume and sensitivity of information about individuals necessarily held by third parties.

Professor Solove has written: “We are becoming a society of records, and these records are not held by us, but by third parties.”³¹ Those records include detailed information about individuals’ behavior, communications, and relationships. Or in the words of Professor Kathleen Sullivan: “Today, our biographies are etched in the ones and zeros we leave behind in daily digital transactions.”³² Because the data are digital, the cost of duplicating, transporting, storing, and using them is negligible. In addition, thanks to the proliferation of digital technologies and networks, and tremendous advances in the capacity of storage devices and parallel decreases in their cost and physical size, those records are linked and shared more widely and stored far longer than ever before. Information aggregators in the private sector that already combine personal data from thousands of private-sector sources and public records. They maintain rich repositories of information about virtually every adult in the country, which are updated daily by a steady stream of incoming data.³³

Removing the protection of the Fourth Amendment from all of these records solely because they are held by third parties results in a significant reduction in the constitutional protection for personal privacy—not as the result of a conscious legal decision, but through the proliferation of digital technologies. Meanwhile, these same technologies, because of the granular and revealing nature of the data they store, make privacy more important.

The shortcomings of current privacy law are at the heart of many of the national security controversies that have occupied Congress and the Administration. To be frank, neither side has much to be proud of in its behavior. The Administration has cited to those shortcomings as justification for not following the law as written, but it has failed to propose specific language to improve the laws or, in many instances, to even raise the issue of the law’s inadequacy until its extralegal surveillance activities were exposed by the press. Congress, too, despite repeated requests from courts, Administration officials, and scholars, has resisted meaningful reform of privacy law.

Compliance with Clearly Articulated Standards Is Necessary

Compliance with the law is not merely a legal obligation, but in a system of representative government, a moral one as well. It is therefore incumbent on the Administration to adhere to the law, and to respond to the law’s many inadequacies by seeking to have them changed through the process set forth in the Constitution. Actions in the service of national security, no matter how well intentioned, that fail to follow the law, are always unjustified, and their incursion on person privacy, however slight, is always inappropriate as a result.

³¹ Daniel J. Solove, “Digital Dossiers and the Dissipation of Fourth Amendment Privacy,” *75 Southern California Law Review* 1083, 1089 (2002).

³² Kathleen M. Sullivan, “Under a Watchful Eye: Incursions on Personal Privacy,” *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* 128, 131 (2003).

³³ See generally U.S. Government Accountability Office, *Personal Information*, GAO 06-421 (2006).

Senator Sam Ervin (D-N.C.) wrote more than 30 years ago: “Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets we stand naked before official power.”³⁴

Our own history has shown us repeatedly that the risk to privacy is especially great when information is assembled for intelligence purposes. The Church Committee final report, which detailed abuses of intelligence information involving every President from Franklin Roosevelt through Richard Nixon, wrote:

The tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our investigative findings. Intelligence collection programs naturally generate ever-increasing demands for new data. And once intelligence has been collected, there are strong pressures to use it against the target.³⁵

This should not be surprising, given that intelligence agents are not limited by the need to investigate particular crimes, they can obtain sensitive personal information under low threshold standards, and they operate largely in secret.

In this situation, when “we stand naked before official power,” it is the law that protects us. But law should not be viewed only as an impediment, but also as a facilitator of appropriate information sharing. The law can empower government officials to collect, share, and use data. One of the most significant effects of the inadequacy of existing privacy law, and of the Administrations tendency to simply ignore those laws it does not like, is to deny those officials charged with protecting our nation’s security the clear direction and confident authorization that law at its best can provide. This was something the members of TAPAC heard frequently from even high-ranking Department of Defense officials: “tell us what the rules are so we can follow them.”

Similarly, by establishing policies and requiring the use of technologies to enhance the security and effectiveness of intelligence data, the law can enhance agent and agency trust. By establishing what is and is not permitted, it can enable the private sector to cooperate in providing data. And by setting parameters, ensuring oversight, and protecting privacy, the law should be the cornerstone of public and policymaker trust, without which promising intelligence programs have collapsed.

TAPAC stressed both the inadequacy of law applicable to the collection and use of personal data for national security and the urgent need for clarifying those laws to guide national security officials. Describing the law as “disjointed,” “inconsistent,” and “outdated,” the Committee wrote: “Current laws are often inadequate to address the new and difficult challenges

³⁴ Introductory Remarks of Senate Sam J. Ervin on S. 3418, Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579), Senate Committee on Government Operations and House Committee on Government Operations Subcom. on Government Information and Individual Rights, May 1, 1974.

³⁵ *Final Report on Intelligence Activities and the Rights of Americans*, supra at ___.

presented by dramatic developments in information technologies. And that inadequacy will only become more acute as the store of digital data and the ability to search it continue to expand dramatically in the future.”³⁶ Enacting a new regulatory structure, the report continued, is necessary both to “protect civil liberties” and to “empower those responsible for defending our nation to use advanced information technologies—including data mining—appropriately and effectively.”³⁷ “It is time to update the law to respond to new challenges.”³⁸

Proposing a detailed new legal regime is beyond the scope of this statement or my abilities, but many others have undertaken this task. I wish to note in particular the recommendations of TAPAC. The eight members of this “blue ribbon”³⁹ bipartisan independent committee reflected an impressive array of private practice, corporate and academic experience, and philanthropic and government service.⁴⁰ Although focused on data mining, their recommendations (summarized in the table below) reflect a comprehensive and thoughtful approach applicable to a wide range of government security programs based on personal data.

TAPAC proposed that government data mining require:

- written authorization by agency heads;
- compliance with minimum technical requirements for data mining systems (including data minimization, data anonymization, creation of an audit trail; security and access controls, and training for personnel involved in data mining);
- special protections for data mining involving databases from other government agencies or from private industry;
- programmatic authorization from the Foreign Intelligence Surveillance Court before engaging in data mining that involves personally identifiable information concerning U.S.

³⁶ *Safeguarding Privacy in the Fight Against Terrorism*, supra at 6.

³⁷ *Id.*

³⁸ *Id.*

³⁹ Ronald D. Lee & Paul M. Schwartz, “Beyond the ‘War’ on Terrorism: Towards the New Intelligence Network,” 103 *Michigan Law Review* 1446, 1467 (2005).

⁴⁰ The members were: Newton N. Minow, Chairman, Senior Counsel to the law firm of Sidley Austin Brown & Wood and chairman of the Federal Communications Commission under President Kennedy; Floyd Abrams, 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, president of the Markle Foundation and previously senior vice president and general counsel of Aetna, Inc., and an attorney in White House and DOJ; Griffin Bell, former Managing Partner of King & Spalding, a judge on the U.S. Court of Appeals for the Fifth Circuit, and Attorney General of the United States; Gerhard Casper, President Emeritus of Stanford University and the Peter and Helen Bing Professor in Undergraduate Education at Stanford; William T. Coleman, Jr., a Senior Partner and the Senior Counselor in O’Melveny and Myers and Secretary of Transportation during the Ford Administration; the late Lloyd N. Cutler, founding partner of the law firm of Wilmer, Cutler & Pickering and Counsel to Presidents Clinton and Carter; and John O. Marsh Jr., Distinguished Professor of Law at George Mason University, former member of Congress, Counselor to President Ford, and the longest-serving Secretary of the Army. *Safeguarding Privacy in the Fight Against Terrorism*, supra at 93-96.

persons that has not been anonymized, and case-by-case authorization from the Court before reidentifying previously anonymized information concerning U.S. persons; and

- regular audits to ensure compliance.⁴¹

⁴¹ Id. at 49-52.

IMPACT OF TAPAC RECOMMENDATIONS ON GOVERNMENT DATA MINING

(i.e., searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government)

Type of Information	New Recommended Requirements
Data mining that is <i>not</i> known or reasonably likely to involve personally identifiable information about U.S. persons (i.e., U.S. citizens and permanent residents)	No new requirements
Data mining limited to foreign intelligence that does <i>not</i> concern U.S. persons .	No new requirements
<p>Data mining known or reasonably likely to involve personally identifiable information about U.S. persons:</p> <ul style="list-style-type: none"> ▶ If based on particularized suspicion about a specific individual, including searches to identify or locate a specific individual (e.g., a suspected terrorist) from airline or cruise ship passenger manifests or other lists of names or other nonsensitive information about U.S. persons. ▶ If concerning federal government employees that is solely in connection with their employment. ▶ If limited to searches of information that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law. ▶ If conducted with deidentified data (i.e., data from which personally identifying elements such as name or Social Security Number have been removed or obscured) ▶ If conducted with personally identifiable information. 	<p>No new requirements</p> <p>No new requirements</p> <p>1. Administrative authorization (set forth in Rec. 2.1), which may be granted on a “per program” or “per search” basis; and 2. Regular compliance audits (set forth in Rec. 2.5).</p> <p>All new requirements apply (i.e., administrative authorization, compliance with technical requirements, special rules for third-party databases, and regular compliance audits, as set forth in Recs. 2.1, 2.2, 2.3, and 2.5), <i>except for</i> need to obtain a Foreign Intelligence Surveillance Court order (set forth in Rec. 2.4).</p> <p>All new requirements apply (as set forth in Recs. 2.1-2.5), <i>including</i> application to the Foreign Intelligence Surveillance Court (Rec. 2.4), which can be made on a “per program” or “per search” basis.</p>

Certain data would be excluded from these new requirements, such as data that are limited to foreign intelligence that does not involve U.S. persons; data concerning federal government employees in connection with their employment; data that are collected based on particularized suspicion; and searches to identify or locate a specific individual (e.g., a suspected terrorist) from airline or cruise ship passenger manifests or other lists of names or other nonsensitive information about U.S. persons.⁴² The report also recommended that data mining that is limited to information that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law—should be subject to “only the requirements that it be conducted pursuant to the written authorization of the agency head and auditing for compliance.”⁴³

TAPAC’s blueprint may not be perfect in all respects, but it has been lauded by scholars and practitioners on both sides of the debate and, perhaps more importantly, it has been criticized by voices on both sides. It is not the end of your quest, but it might be a useful beginning.

External Authorization and Oversight Are Essential

A law is no better than the quality of the oversight that it provides and the enforcement that accompanies it. This is particularly true in the area of national security, where much of the activity is classified or otherwise takes place outside of the public eye. It is therefore essential that the law provide for effective judicial and legislative oversight. “Effective” in this context means at a minimum that courts review applications for warrants or orders, that the government have the obligation to report back on how the warrants or orders were used, and that courts have the power to compel such information if the government fails to comply. Which court and the nature and timing of the authorization are important issues to be settled, but the concepts of separation of powers and of “interposing the courts between the privacy of citizens and the potential excesses of executive zeal” are too important to be ignored.⁴⁴

Effective oversight also means that the Administration should be required by law to report regularly to Congress, or identified committees thereof, on the conduct of national security activities, especially those involving personal privacy, and to provide the information necessary for Congress to carry out its oversight functions. Finally, there should be reliable means for ensuring that individuals and agencies that do not follow the law are subject to dissuasive sanctions, including criminal penalties.

The work of the Privacy and Civil Liberties Oversight Board is important, and I certainly applaud it, but the Board is simply not constituted in a way to allow it to fulfill its charge to “ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism.”⁴⁵ There are no requirements for a bi-partisan selection

⁴² Id. at 46-47.

⁴³ Id. at 47.

⁴⁴ Sullivan, “Under a Watchful Eye: Incursions on Personal Privacy,” *supra* at 129.

⁴⁵ Intelligence Reform and Terrorism Prevention Act Pub. L. No. 108-458, § 1061(c)(3), 118 Stat. 3638, 3685 (codified at 50 U.S.C. § 601).

process or for political balance, as is the case with many other independent agencies and commissions. Its members are all appointed by the President and serve at his pleasure. And the board lacks guaranteed funding or the basic powers, such as that to issue subpoenas, necessary to effective oversight. The shortcomings in the Board's construction, together with the fact that it took the President six months to appoint members and the Senate another eight months to take up their confirmation, send a signal that privacy is not that important to the Administration or to Congress.

Given all of those shortcomings, I believe it is remarkable what you have done, and what you are doing, to raise the visibility of privacy issues in the pursuit of national security and to enhance the protection for that privacy even within a government that seems not to care much about the issue. But those actions, as impressive and laudable as they are, are no substitute for independent oversight and rigorous enforcement of legal obligations.

The Use of Private-Sector Data Presents Special Risks

Since the terrorist attacks of September 11, 2001, government agencies have stepped up efforts to access personally identifiable information from the private sector for a variety of uses designed to enhance public and national security. The 2004 GAO report on government data mining found that more than one-fourth of all government data mining projects involved accessing data from the private sector.⁴⁶

The "special protections" for national security programs involving third-party databases from private industry recommended by TAPAC included:

- The agency engaging in the data mining should take into account the purpose for which the data were collected, their age, and the conditions under which they have been stored and protected when determining whether the proposed data mining is likely to be effective.
- If data are to be used for purposes that are inconsistent with those for which the data were originally collected, the agency should specifically evaluate whether the inconsistent use is justified and whether the data are appropriate for such use.
- Data should be left in place whenever possible. If this is impossible, they should be returned or destroyed as soon as practicable.
- Government agencies should not encourage any person voluntarily to provide data in violation of the terms and conditions (usually reflected in a privacy policy) under which they were collected.
- Government agencies should seek data in the order provided by Executive Order 12333: from or with the consent of the data subject, from publicly available sources, from proprietary sources, through a method requiring authorization less than probable cause

⁴⁶ GAO Data Mining Report, supra at 3.

(e.g., a pen register or trap and trace device), through a method requiring a warrant, and finally through a method requiring a wiretap order.

- Private entities that provide data to the government upon request or subject to judicial process should be indemnified for any liability that results from the government's acquisition or use of the data.
- Private entities that provide data to the government upon request or subject to judicial process should be reasonably compensated for the costs they incur in complying with the government's request or order.⁴⁷

Rationality Matters

One common theme that runs through many of the reports that address national security and privacy is the importance of ensuring that personal information is not collected and used (especially without consent) without there being basic guarantees that the system for which the data are sought will be rational. At a minimum, this seems to require an explicit determination that:

- the system is likely to accomplish a stated worthwhile purpose;
- that purpose is sufficiently worthwhile to warrant the system's costs and impact on other values (including privacy and other civil liberties) involved;
- the personal information is necessary to the success of that system;
- the data are appropriate for the intended use, taking into account the purpose(s) for which the data were collected, their age, and the conditions under which they have been stored and protected;
- the information is protected from accidental or deliberate misuse, disclosure, or alteration;
- the system is subject to clear rules governing its operation so that suppliers and users of data, as well as members of the public, know to the greatest extent possible how the system works, what it is intended to accomplish, and the limits to which it is subject;
- the system's operation is consistent with those rules and applicable laws;
- there is meaningful oversight of the system and enforcement of the rules under which it operates; and
- there is appropriate redress for individuals who believe that the system is not operating appropriately or that they have been harmed by the operation of the system.

⁴⁷ Id. at 50-51.

The more sensitive the information sought and the greater the potential threat to personal privacy, the more clearly each of these should have to be demonstrated. But even where the potential risk to privacy is slight, if the system is irrational, I would argue it should not be tolerated.

Unfortunately, a disregard for basic rationality has been a hallmark of so many U.S. national security programs that this has contributed to undermining public and professional confidence in those programs and in the protections for privacy that they offer. This has been particularly evident with aviation security, under which travelers in the United States are subjected to remarkable intrusions into the privacy of their persons and luggage, despite the fact that the GAO and others repeatedly report the ineffectiveness and incompleteness of these measures as implemented.⁴⁸ In the aftermath of the September 11th terrorist attacks, Congress enacted a requirement that all airline passengers present government-issued identification documents, even while recognizing that such documents are easy to obtain fraudulently from federal and state agencies, as well as to purchase online.

The Transportation Security Administration sought to use personal data to evaluate the risks posed by individual passengers, without having in place any system for correcting inaccuracies in its records or providing redress to affected passengers. The system it finally put in place has proved less than successful. One librarian at the Law School where I teach was forced to use the system after her name was apparently mistaken for someone on one of the terrorist watch lists. After supplying five forms of notarized identification to the TSA, the agency sent her back a letter clearing her to fly on which it misspelled her name. There is still no system for aggrieved passengers to seek compensation for their injuries. After a raft of thefts from checked luggage, the TSA quietly prosecuted dozens of its screeners for theft, but when I wrote the head of the TSA suggesting that it might enhance accountability to include individual screener's badge number or other identification number on those inserts telling passengers that they have searched the luggage, I received a response back that it to do so would violate screeners' "privacy."

Meanwhile, we recently learned that the debate over the TSA and its inability to manage data effectively was really only a sideshow, distracting public attention away from the government's Automated Targeting System that was—and, apparently, still is—creating and storing risk profiles on international passengers without regard for notice, redress, accuracy, or the niceties of complying with the Privacy Act.⁴⁹

I want to focus special attention on the importance of redress. Paul Rosenzweig, when a Senior Legal Research Fellow at The Heritage Foundation, wrote wisely that "[t]he only certainty is that there will be false positives."⁵⁰ False positives impose many costs: in economic

⁴⁸ Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security*, at 4-6, 72 (2003), and sources cited therein.

⁴⁹ Ellen Nakashima & Spencer S. Hsu, "U.S. Plans to Screen All Who Enter, Leave Country," *Wash. Post*, Nov. 3, 2006, at A18.

⁵⁰ Paul Rosenzweig, *Proposals for Implementing the Terrorism Information Awareness System*, Heritage Foundation Legal Memorandum #8 (2003).

terms, to informational privacy, to national security (which is undermined when scarce resources are spent investigating non-threats), and in public annoyance and undercutting public support for counter-terrorism efforts. Given the inevitability of false positives, some form of redress, consonant with the purpose of the data use, is essential for detecting and correcting or otherwise responding to false positives.

Redress isn't just about vindicating the rights of innocent people injured by government data systems and the actions based on them. It isn't just about fairness. It is also about using the most obvious and effective tool available to date to ensure that the information on which we base our national security initiatives is accurate and appropriate. This is a vast challenge, as inaccuracy or inappropriateness can result in so many different ways. Data may be inaccurate to start with; they may be aggregated inaccurately;⁵¹ they may be applied to the wrong individual, especially given the complete inadequacy of current forms of government identification; they may be inadequate for a given use; they may become inaccurate with age, especially if stored without being updated (as the FBI and other agencies have indicated that are doing); they may be compromised while in storage or when being transferred among users; they may be breached; and so on. Both private- and public-sector agencies wrestle with these challenges every day.

⁵¹ The TAPAC report notes the magnitude of this challenge:

- Names may be recorded in a variety of different ways in different records (e.g., J. Smith, J.Q. Smith, John Q. Smith).
- Individuals change their names; this is especially likely for women. There are approximately 2.3 million marriages and 1.1 million divorces every year in the United States, often resulting in changed last names (and also changed addresses).⁵¹
- Many people share names. There are tens of thousands of John Smiths in the United States alone. This is true even of less common names. The information about each of those John Smiths must be kept separate.
- Many individuals have more than one address (e.g., home, office, vacation home, post office box), and are likely to change addresses. As of 1998 there were 6 million vacation or second homes in the United States, many of which were used as temporary or second addresses. And, according to the U.S. Postal Service, approximately 17 percent of the U.S. population—about 43 million Americans—changes addresses every year.⁵¹ 2.6 million businesses file change-of-address forms every year.
- Inclusion of Social Security Numbers improves the likelihood of a correct match to the account holder, but is no guarantee. Even when accounts include SSNs, identification may be difficult because accounts for the same household may reflect different primary SSNs (e.g., husband, wife, minor beneficiary) and because of the presence of transcription errors in recording strings of numbers. Most records do not include SSNs.
- Different companies, or different divisions within the same company, may record or rely on different pieces of information. For example, a retailer may organize its store records by customer name; its catalog sales unit may use residential telephone number; and its e-commerce division may rely on e-mail address.
- Institutions maintain records in a wide variety of formats and on many different technological platforms.

One of the most effective and widely used techniques for guarding against these risks is providing individuals with access to the data, or at least with information about the sources and general categories of data, when they are adversely affected by their use. This is the foundation of the Fair Credit Reporting Act and other privacy laws and it is by far the most cost-effective means we have to improve data accuracy. I am astounded by the inability, and apparently even unwillingness, of the TSA and other security-related agencies to put in place effective redress mechanisms. Surely this is a requirement for any form of broad, data-based security system to be effective, and I applaud your recent efforts to focus attention on this glaring omission.

Meaningful redress is clearly fundamental to rationality, and security systems that fail the test of common sense not only ignore or trivialize privacy, but also undermine support for the systems themselves and the security that they provide. This concern is not limited to Administration officials. One of the most striking features of Congress' response to TIA and other data mining programs was the erratic and inconsistent behavior by policymakers.

After all, it was only three months after Congress required DHS to engage in data mining with private-sector data that it prohibited DOD from deploying data mining tools within the United States, collecting or using data about U.S. persons, or developing other elements of TIA, including translation software, networks to link the intelligence community, and other tools that had few if any privacy implications.⁵² Seven months later, Congress blocked the development of TIA entirely, but then established rules for how classified funding for TIA might be used. TIA's opponents in Congress and the privacy advocacy community proudly claimed that they had "killed" TIA, but the statutory language suggests that they had merely driven it from public view.⁵³ Moreover, President Bush stated in his signing statement that the classified annex "accompanies but is not incorporated as a part of the Act" and therefore would be considered by the President as merely "advisory in effect."⁵⁴ Ironically, the part of TIA that Congress did eliminate entirely was the funding for the development of privacy enhancing technologies.

The immediate result, therefore, of congressional intervention was to drive the development and deployment of data mining at DOD from public view, relieve it of the statutory restrictions that had previously applied to it, block funding for research into privacy enhancing technologies, and undermine the policy debate over the appropriate roles for and limits of data mining. Law and technology scholar K.A. Taipale writes:

At first hailed as a "victory" for civil liberties, it has become increasingly apparent that the defunding [of TIA] is likely to be a pyrrhic victory. . . . [N]ot proceeding with a focused government research and development project (in which Congressional oversight and a public debate could determine appropriate rules and procedures for use of these technologies and, importantly, ensure the

⁵² S. Amend. 59 to H.J. Res. 2 (Jan. 23, 2003).

⁵³ See K. A. Taipale, "Data Mining and Domestic Security: Connecting The Dots to Make Sense of Data," 5 Columbia Science and Technology Law Review 1, 48, n.96 (2003) ("The former TIA projects Genisys and Genoa II are believed to be included in the classified annex to the Defense Appropriations Bill," citing to the statement of Major General Paul Nielson before TAPAC, Nov. 20, 2003).

⁵⁴ Statement on Signing the Department of Defense Appropriations Act, 2004 (Oct. 6, 2003).

development of privacy protecting technical features to support such policies) is likely to result in little security and, ultimately, brittle privacy protection.

Indeed, following the demise of IAO and TIA, it has become clear that similar data aggregation and automated analysis projects exist throughout various agencies and departments not subject to easy review.⁵⁵

Congress' inconsistent treatment of similar technologies confuses the public and government officials charged with following these widely varying statutes. It runs the risk of compromising the protection of both national security and information privacy. The impact may be particularly strong with regard to research and innovation into better ways of protection privacy and security. After all, what federal funding agency would invest seriously in an area where Congress had already acted to ban research once, and what investigator would invest her career in research on such a politically sensitive subject? It is instructive to remember that DARPA—developer of TIA—also funded the development of the precursor of the Internet as a secure tool for connecting defense researchers. Where would the World Wide Web be today if Congress, at the infancy of ARAPNet in the 1960s, had prohibited further research because the emerging technologically posed a clear threat to privacy?

The Importance of the Long View

Many government leaders today act, and sometimes actually say, that in the face of the terrorist threat, privacy must give way to security. Alexander Hamilton, exhorting the people of New York to ratify the Constitution, wrote in Federalist Paper 8 in 1787 that “safety 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.”⁵⁶ “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.”⁵⁷

My research suggests that there are two things wrong with the natural tendency that Hamilton described. The first is that the failure to take privacy seriously in the context of national security will necessarily weaken both privacy and security.

The second problem with the “security at the expense of privacy” argument is that respect for privacy, and the other civil liberties that privacy facilitates, is a core obligation of democratic government. This is true even when the nation faces grave threats and even when we are at war. Acting as though by compromising one we can enhance the other ignores not only the available evidence about the relationship of privacy and security, but the future judgment of history as well.

⁵⁵ Taipale, *supra* at 4 (citations omitted).

⁵⁶ Alexander Hamilton, “The Consequences of Hostilities Between the States” (Federalist Paper 8), *New York Packet*, Nov. 20, 1787.

⁵⁷ *Id.*

As Aharon Barak, President of the Supreme Court and a former Attorney General of Israel, a nation long familiar with terrorism, has written:

Indeed, the struggle against terrorism is not conducted outside the law, but within the law, using tools that the law makes available to a democratic state. Terrorism does not justify the neglect of accepted legal norms. This is how we distinguish ourselves from the terrorists themselves. They act against the law, by violating and trampling it, while in its war against terrorism, a democratic state acts within the framework of the law and according to the law.⁵⁸

Or as the U.S. Supreme Court has written: “It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties . . . which makes the defense of the Nation worthwhile.”⁵⁹

⁵⁸ Aharon Barak, “Foreword: A Judge on Judging: The Role of a Supreme Court in a Democracy,” 116 *Harvard Law Review* 16, 151 (2002).

⁵⁹ *United States v. Robel*, 389 U.S. 258, 264 (1967).

Biographical Information

Fred H. Cate is a Distinguished Professor of Law, Adjunct Professor of Informatics, and director of the Indiana University Center for Applied Cybersecurity Research. Professor Cate works at the forefront of privacy, security, and other information law and policy issues.

He is a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams; a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals; and a member of Microsoft's Trustworthy Computing Academic Advisory Board. He also serves as reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information.

Professor Cate served as counsel to the Department of Defense Technology and Privacy Advisory Committee, reporter for the third report of the Markle Task Force on National Security in the Information Age, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, and chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities.

He has testified before the Committee on Banking, Housing, and Urban Affairs and the Committee on Commerce, Science, and Transportation in the U.S. Senate, and the Committee on Ways and Means, the Committee on Energy and Commerce, the Committee on Government Reform, the Committee on Banking and Financial Services, and the Committee on the Judiciary in the U.S. House of Representatives.

Professor Cate speaks frequently before professional, industry, and government groups. He has spoken throughout the United States and in Belgium, Canada, China, Finland, Germany, Italy, Japan, Switzerland, Taiwan, Trinidad & Tobago, and the United Kingdom.

He has held fellowships at the American Enterprise Institute, the Annenberg Washington Program in Communications Policy Studies, and the Brookings Institution.

He is the author of many articles and books, including *Privacy in the Information Age* and *The Internet and the First Amendment*, both of which were selected for the *Choice* Outstanding Academic Books list by the Association of College and Research Libraries, and *Privacy in Perspective*. He serves on the board of editors of *Privacy & Information Law Report*.

Professor Cate is a senator and fellow of the Phi Beta Kappa Society and an elected member of the American Law Institute. He attended Oxford University and received his J.D. and his A.B. with Honors and Distinction from Stanford University. He is listed in *Who's Who in the World*, *Who's Who in America*, and *Who's Who in American Law*.

tel (812) 855-1161; fax (812) 855-0555
fcate@indiana.edu; www.fredhcate.com