BRENNAN CENTER FOR JUSTICE

WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA

Rachel Levinson-Waldman

Brennan Center for Justice *at New York University School of Law*

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from racial justice in criminal law to Constitutional protection in the fight against terrorism. A singular institution — part think tank, part public interest law firm, part advocacy group, part communications hub — the Brennan Center seeks meaningful, measurable change in the systems by which our nation is governed.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect Constitutional values and the rule of law, using innovative policy recommendations, litigation, and public advocacy. The program focuses on government transparency and accountability; domestic counterterrorism policies and their effects on privacy and First Amendment freedoms; detainee policy, including the detention, interrogation, and trial of terrorist suspects; and the need to safeguard our system of checks and balances.

ABOUT THE AUTHOR

Rachel Levinson-Waldman serves as Counsel to the Brennan Center's Liberty and National Security Program, which seeks to advance effective national security policies that respect constitutional values and the rule of law. She regularly comments on issues relating to national security, privacy, and data retention. Her writing has been featured in publications including the Huffington Post, *Bloomberg View, National Law Journal, New Republic,* and *Wired.*

From 2006 through 2011, Ms. Levinson-Waldman served as Associate Counsel and then Senior Counsel to the American Association of University Professors. In that role, she oversaw the AAUP's in-house legal docket and contributed to amicus briefs and policy issues in a variety of areas, focusing particularly on academic freedom and the First Amendment. She regularly spoke to audiences on matters relating to higher education and free speech, and was a frequent commenter for the higher education press. From 2003 through 2006, Ms. Levinson-Waldman served as a Trial Attorney in the Housing and Civil Enforcement Section of the Civil Rights Division of the Department of Justice, litigating matters under the Fair Housing Act. Prior to joining the Department of Justice, Ms. Levinson-Waldman clerked for the Honorable M. Margaret McKeown of the U.S. Court of Appeals for the Ninth Circuit. Ms. Levinson-Waldman is a 2002 graduate of the University of Chicago Law School and graduated cum laude with a BA in Religion from Williams College.

ACKNOWLEDGEMENTS

The Brennan Center gratefully acknowledges The Atlantic Philanthropies, C.S. Fund, Democracy Alliance Partners, The Herb Block Foundation, Open Society Foundations, and the Security & Rights Collaborative, a Proteus Fund initiative, for their generous support of the Liberty & National Security Program.

This report could not have been written without the time and expertise of a number of individuals, including: Emily Berman, Marion "Spike" Bowman, Christopher Calabrese, Catherine Crump, Mary DeRosa, Laura Donohue, Mike German, Jim Harper, Jameel Jaffer, Jason Leopold, Jennifer Lynch, Ron Marks, Ginger McCall, Kathleen McClellan, Greg Nojeim, John Powers, Michelle Richardson, Julian Sanchez, David Sobel, Peter Swire, John Villasenor, and Marcy Wheeler. Others wished to remain off the record but offered equally valuable contributions.

The other members of the Brennan Center's Liberty and National Security Program provided invaluable input as well, including co-directors Liza Goitein and Faiza Patel, Michael Price, and Amos Toh. The author is also grateful to John Kowal for his insightful suggestions, to Frederick A.O. Schwarz, Jr. for his mentorship, and to Michael Waldman for his strong stewardship of the Brennan Center.

Special thanks go to research associates Jeremy Carp and Shannon Parker. Brennan Center interns, including Jacqueline Cremos, Gene Levin, and Randall Smith, provided useful research help as well. Finally, the author thanks the Brennan Center's Communications staff, especially Seth Hoy, Kimberly Lubrano, and Desiree Ramos Reiner, for their time, creativity, and patience.

Any errors that remain in the report are, of course, the author's alone.

TABLE OF CONTENTS

INFOGRAPHICS

"The massive centralization of … information creates a temptation to use it for improper purposes, threatens to 'chill' the exercise of First Amendment rights, and is inimical to the privacy of citizens."

Report of the Select Committee to Study Governmental
Operations with Respect to Intelligence Activities
(Church Committee)
April 1976[1]

"[T]he value of any piece of information is only known when you can connect it with something else which arrives at a future point in time. … [S]ince you can't connect dots you don't have, it drives us into this mode of: We fundamentally try to collect everything and hang on to it 'forever.'"

Gus Hunt
Chief Technology Officer, Central Intelligence Agency
March 2013[2]

I. INTRODUCTION

Our lives are composed of small details. Any one detail, standing alone, may provide little insight into one's identity, but the aggregation of details can paint a surprisingly accurate and revealing picture. As Justice Sonia Sotomayor observed in a case involving GPS monitoring, information about an individual's location, without more, "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[3] A far more detailed account of a person's travels, friends, beliefs, and hobbies could be generated through information about:

- When she visits her therapist's office
- Her public Facebook postings and tweets
- All of the non-deleted and non-encrypted information on her computer, phone, or iPad
- Whom she emails or calls and when
- The places she travels
- The meetings and gatherings she attends
- Her credit history, driving record, and more

What else do these data points have in common? They are all examples of information the government is authorized to obtain in certain circumstances without suspicion of criminal activity, and keep for law enforcement and national security purposes. The government's sweeping information-gathering powers, dramatically expanded post-9/11, have combined with a top-down mandate to retain information and share it across the federal government for a range of often opaque purposes.

This state of affairs is, historically speaking, a recent one. In the decades immediately preceding 9/11, as a result of serious abuses of power, a web of laws, policies, and guidelines restricted the information that law enforcement and intelligence agencies could gather about Americans and others residing legally in the U.S. As a general rule, agencies could not collect personal information for law enforcement or domestic security purposes without some fact-based justification to suspect involvement in criminal activity or a connection to a foreign power. Information about First Amendment-protected activity also received heightened protection.

The attacks of September 11, 2001, and the intelligence failures preceding them, sparked a call for greater government access to information. Across a range of laws and policies, the level of suspicion required before law enforcement and intelligence agencies could collect information about U.S. persons was lowered, in some cases to zero. Today, for example, customs agents may search and copy the entire contents of a U.S. citizen's laptop when she enters or leaves the country, without any individualized basis for suspicion. Many restrictions on gathering information about First Amendment-protected activity have been similarly weakened. The result is not merely the collection of large amounts of information, but a presumptive increase in the quantity of information that reflects wholly innocuous, and in some cases constitutionally protected, activity.

Other publications, including reports issued by the Brennan Center,[4] have addressed whether lowering the threshold for suspicion to collect information poses an undue risk to civil liberties. This report

addresses a separate question: Regardless of whether the expansion of the government's domestic information collection activity can be expected to yield enough additional "hits" to justify its various costs, how do federal agencies deal with the apparent "misses" — the stores of information about Americans[5] that are swept up under these newly expanded authorities and that do not indicate criminal or terrorist behavior?

One might expect that this information would not be retained, let alone extensively shared among agencies. To the contrary, there are a multitude of laws and directives encouraging broader retention and sharing of information — not only within the federal government, but with state and local agencies, foreign governments, and even private parties. Policymakers remain under significant pressure to prevent the next 9/11, and the primary lesson many have taken from that tragedy is that too much information was kept siloed. Often lost in that lesson is that the dots the government failed to connect before 9/11 were generally not items of innocuous information, but connections to known al Qaeda or other foreign terrorist suspects.[6] Meanwhile, the cost of data storage is plummeting rapidly while our technological capabilities are growing, making it increasingly cheap to store now and search later.[7]

Of course, federal and state agencies must maintain databases to carry out legitimate governmental purposes, including the provision of services, the management of law enforcement investigations, and intelligence and counterterrorism functions. In addition, where law enforcement agencies have reasonable suspicion of possible criminal activity or intelligence components are acquiring information on foreign targets and activity, they must retain information to track investigations, carry out lawful intelligence functions, and ensure that innocent people are not repeatedly targeted.

History makes clear, however, that information gathered for any purpose may be misused. Across multiple administrations, individuals and groups have been targeted for their activism, and sensitive personal information has been exploited for both political and petty reasons. The combination of vastly increased collection of innocuous information about Americans, long-term retention of these materials, enhanced electronic accessibility to stored data, and expanded information-sharing exponentially increases the risk of misuse.

One argument for retaining and sharing all information, regardless of its immediate or likely value, is that the information can be "data mined" to identify hard-to-see patterns that can predict terrorist activity. Although marketers use such tools to predict with surprising accuracy whether a 26-year-old woman in a suburban neighborhood will buy running sneakers or infant formula, researchers have demonstrated persuasively that it is impossible — and unlikely ever to become possible — to predict whether she, or anyone else, will take part in an act of terrorism.[8] Unlike the purchase of Nike or Gerber products, acts of terrorism are so rare and so disparate in origin that there is no regular pattern to be discerned based on a person's everyday activities, making the value of such information for predicting terrorism negligible at best. In the meantime, government counterterrorism databases are becoming so choked with information that analysis becomes impossible, leading Congress and agency experts to criticize the never-ending data consumption.

DATA MINING REPORTING REQUIREMENT

The Federal Data Mining Reporting Act of 2007 requires federal agencies to report to Congress on their data mining activities. Under the Act, data mining involves searching databases to discover patterns that predict terrorist or criminal activity; subject-based data analysis or searches that start with personal identifiers do not qualify, nor do searches for historical trends.
42 U.S.C. § 2000ee-3.

Against this backdrop, this report analyzes the retention, sharing, and use by federal law enforcement and intelligence agencies of information about Americans not suspected of criminal activity.[9] It examines five distinct categories of information. The categories selected all share certain traits: (1) the applicable legal standard was lowered post-9/11 to permit or encourage the collection of information where little or no suspicion of criminal activity exists; and (2) the standards for retention and sharing of the information are at least partially available (albeit not always readily or fully accessible).

The categories are:

1. **Suspicious Activity Reports:** Reports used by federal, state, and local authorities to provide information to the federal government and others about both criminal and non-criminal activity.

2. **Assessments:** FBI investigations that require no suspicion of criminal activity and use a wide range of often intrusive investigate tools.

3. **National Security Letters:** Secret subpoenas that the FBI can deploy to acquire individuals' communication and financial histories in national security investigations without judicial oversight.

4. **Electronic searches at the border:** Suspicionless searches by the Department of Homeland Security (DHS) of travelers' laptops, cameras, PDAs, and other electronic devices at U.S. border crossings.

5. **National Security Agency:** The collection of Americans' communications — both content and "metadata" — by the NSA, as well as the agency's maintenance of databases and data centers about Americans.

Among these data sets, this report finds that in many cases, information carrying no apparent investigative value is treated no differently from information that does give rise to reasonable suspicion of criminal or terrorist activity. Basically, the chaff is treated the same as the wheat. In other cases, while the governing policies do set certain standards limiting the retention or sharing of non-criminal information about Americans, the restrictions are weakened by exceptions for vaguely-described law enforcement or national security purposes. Depending on the data set, presumptively innocuous information may be retained for periods ranging from two weeks to five years to 75 years or more.

And the effect of these extensive retention periods is magnified exponentially by both the technological ability and the legal mandate to share the information with other federal agencies, state and local law enforcement departments, foreign governments, and private entities.

To address these problems, this report recommends the following reforms:

1. Ensure that policies governing the sharing and retention of information about Americans are accessible and transparent.

2. Prohibit the retention and sharing of domestically-gathered data about Americans for law enforcement or intelligence purposes in the absence of reasonable suspicion of criminal activity, and impose further limitations on the dissemination of personally identifiable information reflecting First Amendment-protected activity.

3. Reform the outdated Privacy Act of 1974, which has fallen far short of its goal of protecting the privacy of Americans' personal information, through statutory amendments and establishment of an independent oversight board.

4. Increase public oversight over the National Counterterrorism Center, a massive federal data repository that increasingly is engaged in large-scale aggregation, retention, and analysis of non-terrorism information about Americans.

5. Require regular and robust audits of federal agencies' retention and sharing of non-criminal information about Americans.

These measures will preserve the government's ability to share critical information and safeguard the nation's security while limiting the amount of innocuous information about innocent people that is kept and shared. This will reduce the risk of abuse and misuse, and prevent the government from drowning in data.

II. GOVERNMENT INFORMATION COLLECTION, SHARING, AND RETENTION: HISTORY AND CONSEQUENCES

Broadly speaking, the history of the federal government's collection, retention, and sharing of Americans' personal information falls into three main periods: Cold War and Nixon-era abuses, post-Nixon reforms, and post-9/11 re-expansion of authority. Some of the pre-9/11 restrictions on the collection of information about Americans were put in place in the 1970s precisely because of revelations that personal information about law-abiding citizens had been systematically misused for decades. Successive administrations used such information to disrupt political and social movements or to harass personal or political enemies. While less has been revealed about post-9/11 practices, there are documented instances of law enforcement targeting groups for their political activities, as well as widespread instances of personally motivated misuse of information. An appreciation of this background is critical to understanding the risks accompanying the widescale retention of information about Americans.

A. History

1. Pre-9/11: Widespread Abuse and Reforms

From the Cold War through the abuses of Richard Nixon, the federal government tracked and harassed citizens engaged in a range of constitutionally protected activities.[10] In 1975, the U.S. Senate established a special committee to study and report on the nation's intelligence activities, prompted by allegations of wrongdoing by the major intelligence and law enforcement agencies.[11] Known as the Church Committee after its chair, Sen. Frank Church of Idaho, the committee exposed a range of abuses by the Federal Bureau of Investigation, Central Intelligence Agency, and National Security Agency.

The FBI was among the most active, disrupting various domestic social justice activists and political movements perceived as left-leaning, including women's liberation movements, "every Black Student Union," and Martin Luther King, Jr., himself.[12] Most of these activities were carried out anonymously, allowing the FBI to deny its involvement. The FBI's practice of sharing information extensively within the executive branch significantly magnified its harm. For instance, the FBI provided the largest volume of information for the IRS's Special Service Staff, which President Nixon used as his "enemies list" to target political dissidents for tax investigations.[13] The FBI also disseminated information to other federal agencies — and, in some circumstances, military agencies and the White House — about Vietnam War protestors, nuclear disarmament activists, and religious, civil liberties, and student groups involved in war resistance.[14]

The FBI also provided the bulk of the information that the CIA used in its Operation CHAOS program, a massive domestic spying initiative.[15] The program saw a cadre of CIA officers attempting to collect as much information as possible — at one point 1,000 reports per month from the FBI[16] — in an unsuccessful attempt to unearth evidence of foreign influence on domestic political movements.[17] CIA officers themselves attended anti-war demonstrations and reported on domestic groups to the FBI,[18] sending over 5,000 reports to the Bureau in the CHAOS program's seven years of operation.[19]

The CHAOS program's computer system, known as "HYDRA," ultimately contained files indexing approximately 300,000 Americans.[20]

The National Security Agency aided the FBI and CIA in their domestic surveillance operations.[21] Like the CIA, the NSA was asked to conduct a general investigation of possible foreign influence on various domestic movements.[22] Under the code-name Project Shamrock, the NSA developed watch lists of American citizens and obtained, in real time, copies of the vast majority of all telegraphs leaving the United States.[23] The data collected by the NSA was provided to the CIA,[24] which itself opened and read all correspondence entering and leaving the United States.[25] At least one CIA employee recalled searching the NSA's files "for the names of various well-known civil rights, antiwar, and political leaders."[26]

Following the revelations of these privacy and civil liberties abuses, Congress enacted a number of measures to regulate information collection and sharing by government agencies. The Privacy Act of 1974 restricts the records that a federal agency could keep, requiring that they be "relevant and necessary to accomplish a [required] purpose of the agency."[27] When an agency "establish[es] or revis[es]" the "existence or character" of a database, it must publish a notice in the Federal Register called a System of Records Notice (SORN).[28] The SORN describes the records being kept in the database and their permissible uses. The Act also obligates agencies to give individuals a mechanism to see and challenge the accuracy of their information,[29] and it restricts agencies' maintenance of information about First Amendment-protected activity.[30]

PRIVACY ACT OFFERS LITTLE PROTECTION IN PRACTICE

The Privacy Act, intended to help guard Americans' personal information, is increasingly little more than a fig leaf. The statute requires agencies to specify the permissible "routine uses" for the information in its various databases; these uses must be compatible with the purposes for which the data was originally collected.[31] In practice, however, the uses listed by agencies can be quite broad and vague. Some agencies have developed "standard" routine uses that apply to multiple systems of records. Shortly before 9/11, for instance, the FBI set out "blanket routine uses" to apply to "every existing FBI Privacy Act system of records and to all FBI systems of records created or modified hereafter."[32] The databases to which these blanket uses apply are often not identified or are identifiable only through diligent investigation. Moreover, information can be shared with entities that are not themselves required to abide by the Privacy Act.[33] While this element of the Act is not new, the last decade has seen it leveraged in increasingly powerful ways. The National Counterterrorism Center, for example, may use and retain data that was initially gathered for much more limited purposes.[34] Even among agencies that are subject to the Privacy Act, intra-agency sharing is subject to minimal restrictions, allowing an agency component that gathers information for one purpose to share it with another component that may use it for very different purposes. This creates a troubling loophole at a large, multi-component agency like the Department of Homeland Security, which was cobbled together from independent entities with widely varied missions.[35]

In 1976, Attorney General Edward Levi issued formal Department of Justice guidelines intended to limit the FBI's authority. The Guidelines specified the activities that could trigger an FBI domestic security investigation,[36] prohibited investigations unless there was some basis to suspect that the target was engaged in dangerous and illegal activity,[37] and limited the FBI's ability to investigate First Amendment-protected activities.[38]

The 1978 Foreign Intelligence Surveillance Act (FISA) tightened the regime for collecting foreign intelligence. It required individualized judicial authorization before wiretapping Americans' communications, as well as a finding of probable cause that the American was acting as an agent of a foreign power, and it prohibited surveillance of First Amendment-protected activities.[39] FISA also established the Foreign Intelligence Surveillance Court (FISC), a secret court that hears requests for electronic surveillance and physical searches in foreign intelligence cases.

Across these and other sets of legal rules enacted in the wake of the Church Committee's findings, several critical principles emerged. First, surveillance and other forms of information gathering should take place under defined and transparent rules. Second, law enforcement and intelligence agencies should not collect information about Americans absent a factual predicate for suspicion — a predicate that must rise to the level of probable cause when intruding on communications. Third, agencies should tread lightly when their investigations might implicate First Amendment-protected freedoms. And fourth, investigative activity must be subject to oversight, with electronic surveillance of U.S. persons' communications requiring individualized court orders.

2. *Post-9/11: Increased Information Collection and Sharing*

The lessons learned in the 1970s and the reforms enacted to prevent intelligence abuses unraveled swiftly in the aftermath of the attacks of September 11, 2001. The legal and policy changes enacted in the subsequent years wrought two main changes: the government no longer needed a criminal predicate to gather information about Americans, and the information that was collected could be retained for long periods and often disseminated widely. These changes virtually ensured that the estimated half-petabyte of information stored by government agencies every year — the equivalent of 10 million four-drawer file cabinets of text — would include a significant amount of innocuous, incidentally-collected information about ordinary Americans.[40]

The USA PATRIOT Act of 2001 (Patriot Act) was the first volley. Passed six weeks after the September 11, 2001 attacks, the bill bolstered the intelligence side of the FBI's portfolio. Before the Patriot Act, law enforcement could secretly obtain sensitive records about U.S. persons from third parties for foreign intelligence or international counterterrorism purposes only if the subject of the records was an agent of a foreign power. Under the Patriot Act, however, the Foreign Intelligence Surveillance Court (FISC) may now order the release of "any tangible thing" to law enforcement based on a mere statement of facts asserting the relevance of the items to an investigation.[41] These "tangible things" need not relate to an actual suspect in the investigation. They could include library records, Internet browsing histories, or physical objects or databases. As the nation recently learned – initially from Edward Snowden – the term "relevance" has been interpreted since 2006 to allow bulk collection of Americans' phone records because some small number of them may at some point in the future be germane to an FBI investigation.[42]

The Act also authorized the use of National Security Letters, a form of administrative subpoena used to obtain records from companies providing financial and communications services, under the same broad "relevance" standard.[43] Again, not only does the subject of the records no longer need to be an agent of a foreign power, he or she need not even be a suspect in the investigation.[44] Finally, under the Patriot Act, an investigation may be opened on the basis of the subject's exercise of his or her First Amendment rights, as long as that is not the only factor.[45]

The Foreign Intelligence Surveillance Act was amended in 2007 and again in 2008 to legalize aspects of the warrantless wiretapping program carried out by the National Security Agency in the years following the 9/11 attacks.[46] The amendments dispensed with the requirement that the government obtain an individualized court order whenever a U.S. person was involved; instead, the government could operate a program that would collect Americans' international phone calls and emails as long as the government's actual target was a non-U.S. person located abroad.[47] Again, recent disclosures have revealed how generously that authority is being interpreted.[48]

The rules governing the FBI's domestic investigations were significantly loosened after 9/11 as well. In 2002, Attorney General John Ashcroft permitted FBI agents to attend political or religious gatherings without any reason to suspect the participants of wrongdoing.[49] And in 2008, Attorney General Michael Mukasey authorized FBI agents to open an investigation and use a variety of investigative techniques with "no particular factual predication" — that is, with no reason to suspect involvement in a crime.[50]

In addition to enabling the collection of more information with less cause for suspicion, a series of statutes and executive orders also facilitated the sharing of such information once collected, as described in the timeline below. Many of these efforts can be traced to the 9/11 Commission Report, released in 2004, which criticized the lack of information sharing both within and among agencies.[51] Notably, however, the 9/11 Commission did not suggest that the key to effective counterterrorism was the collection and sharing of information about presumptively law-abiding Americans. Rather, the Commission detailed missed opportunities relating mostly to known terrorism information or criminal activity — including the failure to watchlist several future hijackers about whom the U.S. had actionable intelligence, the failure to share information connected to suspects in the USS Cole bombing, the failure to detect perpetration of visa and passport fraud by several of the hijackers, and the failure to note the arrival of known terrorists in the United States in the summer of 2001.[52] Nevertheless, the architecture of information collection, sharing, and retention quickly expanded to encompass information about Americans far beyond the areas of vulnerability identified by the 9/11 Commission.

B. Consequences of Information Collection, Retention, and Sharing

1. Potential for Misuse, Abuse, and Chilling of Dissent

The collection and retention of non-criminal information about Americans for law enforcement and national security purposes poses profound challenges to our democracy and our liberties. As the Church Committee recognized over four decades ago, "The massive centralization of … information creates a temptation to use it for improper purposes, threatens to 'chill' the exercise of First Amendment rights, and is inimical to the privacy of citizens."[82] In the Committee's words, the retention of information about domestic activity was a "step toward the dangers of a domestic secret police."[83]

Evolving Powers: Government Collection, Retention, and Sharing of Information About Americans

1974

Privacy Act enacted. Act requires federal agencies to protect Americans' personal information and to allow people to view and challenge files about them.[53]

1975-76

Church Committee releases reports detailing abuses by the FBI, CIA, and NSA.[54]

1976

Attorney General Edward Levi releases Guidelines on Domestic Security Investigations, limiting the FBI's reach.[55]

1978

Foreign Intelligence Surveillance Act (FISA) enacted, imposing judicial oversight over surveillance of Americans for foreign intelligence purposes.[56]

2001

Patriot Act enacted. In addition to enabling new investigative powers, the Act endorses the broad sharing of foreign intelligence obtained as part of a criminal investigation with nearly any Federal official if relevant to the performance of his official duties.[57]

2002

Homeland Security Act of 2002 passes. The statute mandates the establishment of procedures to "share relevant and appropriate homeland security information with other Federal agencies."[58]

Attorney General Ashcroft issues a Directive and Guidelines establishing procedures for information-sharing and requiring the creation of a new system that would allow various entities to share and search sensitive information pursuant to the Patriot Act.[59] Ashcroft also amends the Attorney General Guidelines, loosening the requirements for the FBI to spy on Americans.[60]

e-Government Act of 2002 passes. Statute requires agencies to publish Privacy Impact Assessments to evaluate the privacy impact of databases that collect, maintain, or disseminate personally identifiable information about individuals.[61]

2003

The Attorney General, Secretary of Homeland Security, and Director of Central Intelligence establish a presumption of information-sharing, particularly with regard to terrorism, among all federal law enforcement agencies, all intelligence agencies, and the Department of Homeland Security.[62]

President Bush directs the "heads of executive departments and agencies" to begin providing "all appropriate Terrorist Information in their possession, custody, or control" to the Terrorist Threat Integration Center (TTIC) — soon to become the National Counterterrorism Center.[63]

Department of Homeland Security is established.

Federal government launches the fusion center program, a system of data aggregation hubs that are created at the state or city level, receive federal funds, and are cross-staffed with state, local and federal agents.[64]

2004

9/11 Commission publishes report, strongly criticizing failures in information-sharing in the lead-up to the September 11 attacks.[65]

President Bush establishes an "Information Systems Council," whose mission is to develop and oversee a "terrorism information sharing environment" that will "facilitate automated sharing of terrorism information among appropriate agencies."[66]

2004	Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) passes, directing the creation of a domestic Information Sharing Environment (ISE). Among other things, the ISE will receive Suspicious Activity Reports.[67]
2005	President Bush issues Executive Order 13388, ordering all agencies with counter-terrorism functions to share terrorism information with each other.[68] New York Times exposes warrantless wiretapping that was secretly implemented immediately after 9/11.[69]
2006	Patriot Act reauthorized.[70]
2007	Implementing Recommendations of the 9/11 Commission Act of 2007 passes. Among other things, the bill requires the Department of Homeland Security to oversee further information sharing and formalizes the national fusion center program.[71] Federal Data Mining Reporting Act passes. Act requires government agencies to submit annual report to Congress if they use pattern-based data mining.[72] DOJ Inspector General releases audits that are highly critical of FBI's use of Section 215 authority and National Security Letters. Audits conclude that, among other things, FBI has insufficient oversight, misused its NSL authority, and dramatically underreported its requests for information about Americans and others.[73] Protect America Act signed into law. PAA amends FISA to remove individualized warrant requirement for surveillance of U.S. persons' international communications.[74] President Bush releases first National Strategy for Information Sharing, establishing federal program and information sharing platform for creating and sharing Suspicious Activity Reports (SARs).[75]
2008	FISA Amendments Act (FAA) passes, enshrining "programmatic" surveillance (i.e., without individualized warrants).[76] Attorney General Mukasey releases new Attorney General Guidelines. Guidelines allow new level of FBI investigation, "assessments," which do not require any evidence of wrongdoing. Tactics include informants and physical surveillance.[77] Congressional witnesses call for restrictions on retention and sharing of information obtained via National Security Letters.[78]
2009	Department of Homeland Security issues Privacy Impact Assessment for electronic border searches, confirming that officers may search Americans' computers, laptops, and other electronic items at international borders with no suspicion of criminal activity.[79]
2012	National Counterterrorism Center (NCTC) releases revised guidelines. Guidelines allow NCTC to copy databases of non-terrorism information about Americans and search them for up to five years.[80] Senate subcommittee releases report strongly critical of fusion centers, asserting that they endanger citizens' civil liberties while offering little of value to counterterrorism efforts.[81] FISA Amendments Act is renewed for five years without change.
June 2013	Snowden disclosures begin.

The Church Committee surely did not envision modern technology. The FBI of the 1970s, armed with today's technological abilities, would have exponentially more information, easily stored for the long term and readily available in electronic databases, with the potential to cause far more damage to individuals' lives.

These risks are not merely theoretical. While there has been no equivalent of the Church Committee to examine intelligence practices since 9/11 in order to systematically uncover abuses, some evidence of improper activity has surfaced. In the NSA realm, recent disclosures have revealed both inadvertent and intentional misuses of the agency's broad surveillance authority. A 2012 audit concluded that the agency had broken privacy rules thousands of times in the previous twelve months, including acquiring information on "more than 3,000 Americans and green-card holders" and using search terms for communications that were guaranteed to yield many communications with no connection to terrorism.[84] NSA analysts have also misused the agency's surveillance systems to spy on spouses or romantic interests.[85] The revelations of these problems after repeated assurances that the agency was operating in strict conformance with applicable legal standards highlights the inherent risk of surveillance programs that are largely shrouded from public view.[86]

As for the FBI, a 2010 report by the Inspector General of the Department of Justice concluded that in the five years after 9/11, the Bureau improperly gathered and retained information on individuals because of their political and social activism and put targets into federal databases from which it became almost impossible to escape.[87] Among other findings:

- an FBI agent recorded and retained information about the First Amendment activities of a Pittsburgh-based peace and social justice center with no connection to any criminal or terrorist activity;[88]

- while investigating members of the Catholic Worker, a movement dedicated to nonviolent protest and assistance for the homeless, the FBI gathered and retained information on a group organizing a public anti-war rally, information that "contained no observations relating to potential future criminal or terrorist activity;"[89]

- members of Greenpeace who became the targets of "Acts of Terrorism" investigations landed on a federal watchlist that funneled information to the FBI about their national travel and protest activities long after the investigations should have been closed;[90] and

- an investigation of a member of People for Ethical Treatment of Animals (PETA) was opened without sufficient factual basis and the FBI field division overseeing the case failed to comply with FBI policy, resulting in the subject's remaining on federal watchlists for three years after the investigation was closed.[91]

Improper investigation is not harmless, even if no one is arrested or charged. People who come under investigation may be subject to a variety of adverse federal actions, ranging from secondary screenings and lengthy delays when traveling to denial of immigration benefits. Moreover, when people are targeted for surveillance based on their beliefs or associations, the scrutinized groups begin to engage in self-

censorship — a consequence that can be seen in the aftermath of the New York Police Department's monitoring of the city's Middle Eastern and South Asian population. The surveillance and planting of informants in every facet of Muslim life alienated Muslims from their mosques and religious communities, hindered social activism and political debate on a range of issues, and destroyed previously collaborative relationships between Muslim communities and their local police precincts.[92] On college campuses, NYPD officers regularly monitored student email listservs and recorded information about speaker activities; some student groups responded by banning constitutionally protected political discussions in group spaces.[93] These findings are particularly relevant in light of the FBI's post-9/11 authority to map ethnic groups and gathering places.[94]

Even innocuous information gathered for legitimate governmental purposes is vulnerable to abuse, often for petty reasons. A special agent with the U.S. Commerce Department pled guilty in 2009 to "unlawfully obtaining information from a protected computer"; the agent had been indicted for misusing a federal database to track a former girlfriend and her family. The agent had previously threatened to kill the girlfriend or have her and her family deported, and he accessed the database over 150 times in a one-year period to monitor her movements.[95] Recent reports by the FBI's Office of Professional Responsibility depict FBI employees misusing government databases to look up friends working as exotic dancers and conduct searches on celebrities they "thought were hot."[96]

Misuse on the state level will also be of increasing concern as state and federal databases become interoperable. In Colorado, for instance, local police spying on environmental activists shared a list of license plates with the FBI's regional Joint Terrorism Task Force.[97] In Utah, employees of the state's Department of Workforce Services generated and circulated a list of 1,300 state residents whom they falsely accused of being illegal immigrants.[98] A quick search reveals many additional examples.[99]

Finally, centralized storehouses of data are particularly vulnerable to both intentional and inadvertent security breaches. In mid-2008, it was revealed that the director of the secretive Strategic Technical Operations Center at the Marine Corps' Camp Pendleton had been feeding reams of classified federal surveillance files to a local terrorism task force, bypassing any approved sharing processes.[100] These information-sharing breaches may become more common as more data is aggregated and available through a single access point. In fact, the federal Government Accountability Office has reported a significant increase in data breaches since 2006, with more than a third of the incidents in 2011 involving personally identifiable information.[101] The GAO identified limits on data collection and retention as one line of prevention against data breaches.[102]

PITFALLS OF SURVEILLANCE

In 2008, it was revealed that the Maryland State Police had spent years spying on non-violent advocates of civil rights and civil liberties both within and outside of the state.[103] The incident reads like a case study in the pitfalls of surveillance, from improper data collection to retention to sharing.

It began small: A police officer needed a threat assessment of protests that were expected in the lead-up to the execution of two men on death row.

It expanded for reasons largely unrelated to public safety: The police officer sent to check out the protest groups needed experience doing undercover work, and the surveillance was considered a "low-risk training exercise" by a police unit in search of a mission.

The surveillance continued after the original law enforcement need was satisfied: The spy-in-training ultimately spent at least 288 hours doing undercover surveillance, offering weekly reports to her supervisors.

There was mission creep: As the officer spent more time with the activists she was infiltrating, she met activists focused on other causes, and began surveilling those groups as well. The surveillance program ultimately focused on activists working on causes as diverse as promoting human rights, establishing bike lanes, and opposing an electricity rate hike.

It crossed jurisdictional lines: Information about leaders of a national women's antiwar group who did not live in Maryland was put into the state police database.

It crossed into the absurd: Hot on a tip that animal activists might steal chickens from a local chicken farm, a "casually dressed" undercover trooper attended a speech by the president of People for the Ethical Treatment of Animals to see if anyone talked about chickens. (They didn't.)

Technology took over: The anti-terrorism squad running the surveillance operation had been given free federal drug-trafficking software; because the criminal database software did not include categories for the activities of the protest groups they were monitoring, they created terrorism-related categories. A well-known anti-war activist was thus entered into a federal-state information-sharing database as committing the crimes of "Terrorism-anti-government" and "Terrorism-Anti-War-Protestors." Amnesty International was listed as committing the "crime" of "civil rights."

Information was inaccurate: One DC-area activist was listed as having committed the "crime" of "terrorism-animal rights" for having participated in a conference at a hotel in D.C. on "Taking Action for Animals." She did not work on animal rights and was not at the event.

Information spread out of control: At least 53 activists were ultimately labeled as terrorists in state police databases, designations that were then shared with multiple state and federal databases.

It chilled constitutionally-protected speech: After it was revealed that a police trooper had attended a student chapter meeting of the International Socialist Organization at the University of Maryland, one of the students (who was identified as committing the crime of "anarchism" and labeled a terrorist) observed that "having the state police come into our meetings at university-sanctioned events and spy on us for tabling at the student union, that has a chilling effect on students."

The surveillance was unnecessary: While the police agents were troubled about "possible tensions at antiwar and anti-death penalty rallies," their reports "noted repeatedly that they led to no violence and minimal disruptions."

There was a coverup: The police first refused to release any files in response to a public records request; then disclosed some information in response to a lawsuit; then finally admitted that the surveillance program had spanned several years rather than the fourteen months originally acknowledged.

Innocuous, constitutionally-protected information may remain in government hands forever: The police retained the surveillance logs for years after the monitoring ended, and surveillance reports were shared with law enforcement agencies at all levels, including the National Security Agency. Although the Maryland police planned to purge the inappropriate information from their own files, it will be difficult or impossible to purge every other database it was shared with.

2. *Drowning in Data*

Six years after 9/11, a panel of experts convened by the government expressed concern about "an increasing trend in the post-9/11 era for federal agencies to collect as much information as possible in the event that such information might be needed at a future date."[104] That accumulation and storage of data poses significant practical problems: it can obscure useful information entirely, complicate analysis, and make data management more difficult.

This trend has practical, and potentially devastating, consequences. The failure of the intelligence community to intercept the so-called "underwear bomber" — the suicide bomber who nearly brought down a plane to Detroit on Christmas Day 2009 — was blamed in significant part not on insufficient information but on an overabundance of data. An official White House review of the attempted attack observed that a significant amount of critical information was available to the intelligence agencies but was "embedded in a large volume of other data."[105] Similarly, the independent investigation of the FBI's role in the shootings by U.S. Army Major Nidal Hasan at Fort Hood concluded that the "crushing volume" of information was one of the factors that hampered accurate analysis prior to the attack.[106]

Officials across a range of agencies have echoed this assessment. As one veteran CIA agent described it, "The problem is that the system is clogged with information. Most of it isn't of interest, but people are afraid not to put it in."[107] A former official in the Department of Homeland Security branch that handled information coming from fusion centers (a state- or regional-based center that collects, analyzes and shares threat-related information between the federal government, the state, and other partners) characterized the problem as "a lot of data clogging the system with no value."[108] The former chief of the branch was less diplomatic, describing the reporting as, at times, little more than "a bunch of crap … coming through."[109] Even former Defense Secretary Robert Gates has acknowledged that "[n]ine years after 9/11 it makes a lot of sense to … take a look at this and say, 'Okay, we've built tremendous capability, but do we have more than we need?'"[110]

An overabundance of innocuous information can also increase the risk of drawing false connections, as described in more detail in the next section. With increasing quantities of innocuous information about innocent Americans, government agencies will have more opportunities to reach inaccurate conclusions.

ELECTRONIC SURVEILLANCE ENABLES FALSE CONCLUSIONS

The opportunity to draw inaccurate conclusions from surveillance evidence is neatly illustrated by an example outside of the national security context. In February 2013, Tesla Motors gave *New York Times* reporter and electric-car skeptic John Broder one of its cars to test drive on a round-trip between Washington, D.C. and Boston. Following an unfavorable review by Broder,[111] who claimed that the car's battery died before the completion of his trip, Tesla published a rebuttal in which it revealed that the company had surreptitiously collected data on nearly every facet of the car's voyage.[112] The company argued that the data, which included power consumption, speed, ambient temperature, control settings, and location, definitively proved Broder was lying and misrepresenting the car's capabilities.[113] Instead of discrediting Broder, however, the extensive universe of data offered in the rebuttal provided ripe ammunition for a vigorous exchange of accusations over the validity of each side's argument,[114] with Broder using the data to substantiate an entirely different narrative.[115] Despite the seemingly straightforward nature of Tesla's analysis — which, unlike information collected for intelligence purposes, drew exclusively from a limited dataset of known origin — the number of competing connections and inferences taken from the information trove was dizzying.[116] "Even intense electronic surveillance of the actions of a person in an enclosed space," commented technology expert Bruce Schneier, "did not succeed in providing an unambiguous record of what happened."[117]

3. *Limited Value of Pattern-Based Data Mining in Counterterrorism Context*

One chief argument in favor of retaining all information gathered, regardless of its apparent law enforcement value, is that seemingly innocuous information may prove meaningful today or in the future when connected with other "dots" of information (sometimes referred to as the mosaic theory).[118] The process of combining these dots into a pattern that suggests terrorist activity is generally called data mining, or "pattern prediction": analyzing a store of data to tease out patterns connected to certain behaviors, and then looking for matching patterns in other datasets in order to predict other instances in which those behaviors are likely to occur.[119]

The Department of Homeland Security was authorized at its inception to use data mining.[120] A recent study commissioned by the Department of Defense concluded, however, that "there is no credible approach that has been documented … to accurately anticipate" terrorist threats.[121] Put another way, there is simply no known way to effectively identify a potential terrorist by pattern analysis. (This is different from subject-based data mining, which looks for links among specific, identified pieces of information and is more akin to old-fashioned investigative work.[122])

Credit card companies are probably the best-known and most successful users of the pattern-matching model. Their success in detecting credit card fraud is due to a number of factors that are almost entirely lacking in the counterterrorism context: the massive volume of credit card transactions provides a rich body of data; a relatively high rate of credit card fraud means the model can be tested and refined; regular and identifiable patterns accompany the fraud (such as testing a card at a gas station to ensure that it works and then immediately purchasing more expensive items); and the cost of a false positive — what happens when the system erroneously concludes that a card has been stolen — is relatively minimal: a call to the owner and, at worst, premature closure of a legitimate account.[123]

By contrast, there have been — statistically speaking — a relatively small number of attempted or successful terrorist attacks, which means that there are no reliable "signatures" to use for pattern modeling.[124] Even if the number of attacks were to rise significantly, it is improbable that they would exhibit enough common characteristics to allow for successful modeling. Indeed, government agencies and experts who have engaged in rigorous empirical studies of "radicalization" have concluded that there is no particular pathway to terrorism or a common terrorist profile.[125]

Moreover, a counterterrorism data-mining program would look not just at a single type of data, such as credit card transactions, but "trillions of connections between people and events": merchandise purchases, travel preparations, emails, phone calls, meetings, business arrangements, and more.[126] It is close to impossible to identify coherent patterns that could be used to predict terrorist activity within this welter of data.

The adverse consequences of a false positive are vastly more damaging to an individual in the counterterrorism context. As security expert Bruce Schneier has suggested, given the almost overwhelming amount of data available, the most accurate imaginable system would still generate on the order of "1 billion false alarms" — that is, emails, meetings, associations, phone calls, and other

items falsely tagged as terrorism-related — "for every real terrorist plot it uncovers."[127] A person falsely suspected of involvement in a terrorist scheme will become the target of long-term scrutiny by law enforcement and intelligence agencies. She may be placed on a watchlist or even a no-fly list, restricting her freedom to travel and ensuring that her movements will be monitored by the government. Her family and friends may become targets as well.

And unlike credit card fraud, a conclusion of possible terrorist involvement is more likely to be influenced by activities that may be protected by the First Amendment, such as email or phone communications, political activism, religious involvement, or connections to certain ethnic groups. In short, there is a reason the Cato Institute has warned that data mining for counterterrorism purposes "would waste taxpayer dollars, needlessly infringe on privacy and civil liberties, and misdirect the valuable time and energy of the men and women in the national security community."[128]

Patterns of terrorist precursor crimes — crimes commonly carried out as part of the planning and preparation for terrorist attacks — *may* be more susceptible to data mining than the entire universe of human connections and transactions. For instance, someone who has been engaged in visa or passport fraud, money laundering, and running a front business could legitimately be investigated for more nefarious schemes.[129] The 9/11 Commission observed that "counterterrorist investigations often overlap or are cued by other criminal investigations, such as money laundering or the smuggling of contraband."[130]

Because this pattern analysis is premised upon existing criminal activity, some of the concerns about collecting and analyzing information about Americans without any basis for suspicion recede. Nonetheless, given the significant consequences of labeling someone a terrorist suspect, more research is needed to assess whether detectible patterns of precursor crimes can in fact act as an early warning system for terrorist plots.

III. INFORMATION SHARING AND RETENTION: CURRENT LANDSCAPE

Given the well-documented risks of abuse inherent in the government's retention and sharing of large quantities of personal information about Americans, as well as the dearth of evidence that aggregating significant amounts of facially innocuous information is a useful way to identify terrorist plots, a key question arises: What does the government do with the information that is swept up under its newly expanded authorities but does *not* indicate criminal or terrorist activity?

This report first briefly describes three major data centers — two physical, one virtual — where the federal government is housing its growing stores of information about Americans. It then examines five specific types of information collected by federal agencies for law enforcement or national security reasons. The five categories were chosen based on two main characteristics. First, in all five instances, the rules for collection were changed after 9/11 in a manner that virtually ensures that large amounts of innocuous information about law-abiding Americans will be captured, either incidentally or by design. Second, some information about the government's policies and practices for retention and sharing of the data could be procured through diligent efforts. There remain federal data sets for which such information is not publicly available, despite FOIA requests and other efforts to unearth it.

For each category of information collection, the report details the types of information that now may be gathered, to demonstrate the strong likelihood (or, in some cases, certainty) that information about innocent Americans is being caught in the net. Finally, the report examines the rules that govern the retention and sharing of this information. Because much is secret in the national security context, and new revelations emerge regularly about the contours of the government's information management, a comprehensive picture is not feasible. It is nonetheless possible to construct an illuminating overview that suggests a new presumption by the federal government about its citizens: They are potentially guilty until proven innocent, and that it is the government's right and responsibility to accumulate the information that may someday prove their guilt.

A. Data Centers

After 9/11, the government established several actual or virtual data centers to aggregate, compare, data mine, and analyze all of the new information that would be coming in, often for purposes far afield from those for which it was gathered. All of the five categories of information described in Part B appear likely to feed into one or more of these data centers. Accordingly, this report briefly examines the policies and practices that govern the collection, retention, use, and sharing of non-terrorist information about U.S. persons at these centers.

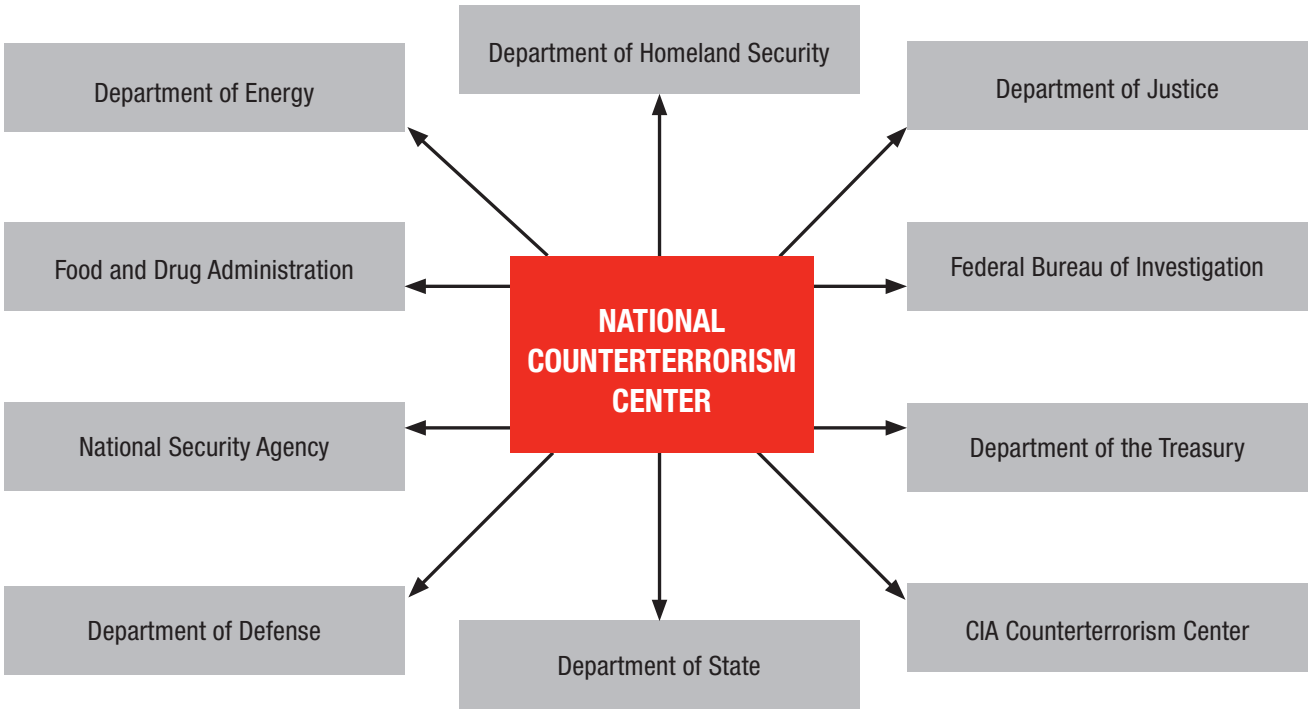
1. National Counterterrorism Center

Established by executive order in 2004, the National Counterterrorism Center, or NCTC, is tucked near the intersection of the Washington Beltway and the road to Dulles Airport. The NCTC operates under the Director of National Intelligence and pulls its employees from other federal agencies, ranging

from the FBI and CIA to the Department of Agriculture and the U.S. Capitol Police.[131] The Center's mission is to "analyz[e] and integrat[e]" all terrorism and counterterrorism intelligence. All agencies with terrorism information in their databanks — regardless of whether the databases themselves are designed for counterterrorism purposes — must share the information with the NCTC.[132] In addition, any agency that is "authorized to conduct counterterrorism activities may request information" from NCTC "to assist it in its responsibilities."[133]

In practice, this means the NCTC receives data from the agencies that are themselves the largest consumers of information about Americans: the NSA, the CIA, the FBI (which gives the NCTC "direct access to FBI raw operational electronic files and databases"[134]), the Department of Homeland Security, and the Office of the Director of National Intelligence.[135] In addition, the NCTC accesses three categories of non-terrorism data: international travel-related datasets, immigration benefits-related datasets, and financial-related datasets.[136]

AGENCIES ABLE TO REQUEST INFORMATION FROM THE NATIONAL COUNTERTERRORISM CENTER



In 2008, the Attorney General and the Director of National Intelligence (DNI) issued guidelines for the NCTC to access other federal agencies' databases of non-terrorism information in order to find possible terrorism data held within them.[137] The 2008 Guidelines established three "tracks" by which the NCTC could access the data, either by conducting or directing searches within those agencies' databases or by copying the database and searching on its own.[138] Under the third track, the NCTC could replicate entire datasets — including non-terrorism datasets — but the replication process had to entirely exclude or remove non-terrorism information about Americans.[139] Moreover, any non-terrorism information that slipped through had to be deleted promptly (generally interpreted as being within 180 days), and none of it could be disseminated or used.[140]

In 2012, however, new guidelines were issued.[141] Under these guidelines, the NCTC may now receive all of the non-terrorism information about Americans in any bulk database it acquires.[142] In addition, the NCTC may "retain and continually access" that information for up to five years — a ten-fold increase from the previous limit.[143] (Data that does qualify as terrorism information may be kept for a minimum of 40 years, as long as it has a terrorism nexus.[144]) Finally, while the 2012 Guidelines include new language about First Amendment rights, the effect is that the NCTC may utilize, keep, or share information about Americans in order to monitor their First Amendment-protected activities or other constitutional rights as long as that is not the *sole* justification for using the data.[145]

The 2012 Guidelines also authorize the NCTC to disseminate a wider range of information about Americans than before, including not only terrorism information but information that "reasonably appears to be necessary to *understand or assess* terrorism information."[146] Some information may be shared for non-counterterrorism purposes, including information suggesting a risk to property, which may be shared with private parties. An individual American can be identified if the identity "may become necessary to understand and assess" the information shared.[147] Under certain circumstances, the NCTC can also provide non-terrorism datasets in bulk (albeit with strict oversight requirements) to other intelligence agencies,[148] which can then keep the datasets for up to five years to continually assess their data.[149] Both the NCTC and any intelligence agency can use data mining as part of their assessments, although the NCTC has reported that it is not currently using pattern-based data mining.[150]

2. Investigative Data Warehouse

The FBI's Investigative Data Warehouse, established in 2004, is a virtual rather than physical data center that is used for both criminal and counterterrorism purposes. The IDW conducts data mining, matching patterns of behavior ostensibly indicative of criminal activity or terrorism against the information in the datasets.[151] As of 2010, the IDW contained over a billion records from the Departments of Treasury, State, and Homeland Security, the Bureau of Prisons, and non-governmental sources, in addition to the FBI.[152] The FBI has reportedly also hoped to add a range of non-criminal databases.[153]

The FBI has no official public notice for the IDW and has asserted the IDW is covered by a vague, existing "umbrella" notice.[154] According to the most recent retention schedule from the National Archives and Records Administration, records stored in the IDW are deleted or destroyed only "when superseded by updated information or when no longer needed for analytical purposes," up to the life of the system itself.[155] In other words, information may be off-loaded when the system updates its database copies, but information that has not been superseded is highly unlikely to be disposed of unless the entire Investigative Data Warehouse is shuttered.

3. National Security Agency Data Center

Even fewer details are available about the government's newest data center, nicknamed the "Spy Center," which the NSA has been building in the small town of Bluffdale, Utah since 2010.[156] Scheduled for completion in the last quarter of 2013, the massive, $2 billion facility covers one million square feet, 10 percent of which is dedicated solely to housing computer servers. [157] Its computers and associated support infrastructure may consume as much electricity as 65,000 homes.[158] Physically large enough to make it the biggest Department of Defense project in the country,[159] the center's potential for data storage is even more impressive, with estimates of its capacity measured in yottabytes, the largest unit of measurement for information yet established.[160] While those estimates have recently been called into question, experts agree that its storage and computing capacity are enormous and bound to increase.[161]

Though details of the data center's construction give a sense of its potential capacity, the policies governing its links to existing databases or explaining what data will be stored there, for what purposes, and for how long, are not public. In his 2012 article on the facility, national security expert James

Bamford asserted the data center would be the centerpiece of NSA collection and code breaking efforts, working to defeat even the best modern encryption and housing massive data sets that would include information from U.S. persons.[162] Government officials dispute these claims, denying plans to "eavesdrop on average Americans" and stating that the data center's primary focus will be to defend the country against cyber attacks.[163] Recent revelations (discussed in Part III.B.5) have, however, cast those denials into some doubt.

B. Categories of Information

1. Suspicious Activity Reports

a. Information Collected

In the aftermath of 9/11, a series of statutes and executive orders established a federal Information Sharing Environment, intended to facilitate the sharing of terrorism-related information among government at all levels, from local to federal, as well as with the private sector.[164] One of the primary types of information to be shared was Suspicious Activity Reports (SARs), a distillation of the "See Something, Say Something" philosophy.[165] Already mandated prior to 9/11 for banks to report certain suspicious transactions, SARs were revamped after 9/11 to allow local, state, and federal law enforcement — sometimes acting on tips from regular citizens, mall security, local retailers and others — to file alerts about "suspicious activity."[166] A subset of SARs documents terrorism-related alerts; because they are shared through the Information Sharing Environment (ISE), these are called ISE-SARs.[167]

From early 2010 to late 2012, the number of ISE-SARs shot up almost tenfold, from about 3,000 in January 2010 to nearly 28,000 in October 2012.[168] According to the FBI, the increase reflects the growth of the Nationwide SAR Initiative, which is the mechanism for law enforcement at all levels to share SAR information, as well as increased reporting from "federal, state, and local partners."[169] The number of FBI terrorism investigations based on ISE-SARs also increased significantly during that period, rising by about 75 percent from 2010 to 2012. The FBI does not, however, systematically track whether those investigations were successful or how many ISE-SARs have contributed significantly to counterterrorism efforts.[170]

The SAR process starts when a private citizen, a law enforcement agency or other government agency, or a private company observes "unusual or suspicious behavior" that may be "reasonably indicative of criminal activity associated with terrorism."[171] This is a highly context-dependent determination. Once the information is received by a local or federal law enforcement agency, the agency reviews the information to determine whether it has connections to other suspicious or criminal activity and completes a report.[172] At the state and local level, the report is sent to the relevant state or regional fusion center for processing, while federal agencies keep the reports within the federal system.[173] In some circumstances, the information is also used immediately to launch a federal terrorism investigation or law enforcement operation.[174]

Once a SAR is at a fusion center or a federal agency, an analyst determines whether there is a "potential terrorism nexus"; this assessment is guided by a "Functional Standard" published by the federal

government.[175] Certain criminal behaviors are considered automatic indicators of a terrorism nexus — for instance, attempting to enter a restricted site without authorization, or damaging physical or cyber infrastructure.[176] Some behaviors that are not criminal can nevertheless trigger a finding of a potential terrorism nexus if they are of a type that would make a "reasonable person" suspicious. These include "eliciting information" about a building's purpose, operations, or security procedures; taking photographs or video of buildings or infrastructure; "demonstrating unusual interest" in facilities or buildings, including using binoculars or taking notes; and attempting to obtain training in military tactics.[177] Because the Functional Standard observes that these non-criminal activities — for instance, asking questions or taking pictures — are protected by the First Amendment in many circumstances, they must be accompanied by "articulable facts and circumstances" suggesting that the behavior is "not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism."[178]

This reasonably indicative standard is a loose one — lower than the "reasonable suspicion" standard that is well-known and time-tested in the criminal justice context.[179] The reasonable suspicion standard itself is a fairly low standard, requiring only something more than a "hunch" of criminal activity. Notably, the Department of Homeland Security has acknowledged that the "reasonably indicative" criterion means "more information about individuals who have no relationship to terrorism may be recorded."[180] Indeed, a review by the Los Angeles-area fusion center of threat reports sent to the FBI's Guardian system in August 2009 noted that "suspicious photography" accounted for the second-largest category of SAR reporting.[181]

If the SAR is determined after analysis to have no nexus to terrorism, it is not shared through the ISE, though it may be kept at the fusion center or the federal agency that originated it.[182] If there is a *potential* terrorism nexus, based on the criteria in the Functional Standard and comparison to information in other databases, the SAR officially becomes an ISE-SAR and is made available to the other participants in the ISE.[183]

Notably, while the Functional Standard is intended to guide all ISE-SAR analyses, the FBI does not fully subscribe to this process. The Bureau has stated that its guidelines for investigating terrorism-related information are broader than the Functional Standard's criteria, and it has directed fusion centers to provide information beyond the boundaries of the Functional Standard.[184] The full parameters for sharing ostensibly terrorism-related information through the ISE-SAR process are therefore unknown.

Moreover, fusion centers have a troubling record when it comes to vetting state and local SARs for entry into the ISE. An October 2012 Senate subcommittee report criticized fusion centers for their analytical and reporting shortcomings, noting that the centers "forwarded 'intelligence' of uneven quality — oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."[185] A third of the reports filed by fusion centers in a recent 13-month period were cancelled by DHS reviewers for "lacking any useful information, for running afoul of departmental guidelines meant to guard against civil liberties or Privacy Act violations, or for having no connection to any of DHS's many missions, among other reasons."[186] Of the unclassified reports that were published, only a quarter of those actually had some nexus to terrorism in the judgment of the Senate's investigators.[187]

SUSPICIOUS ACTIVITY REPORTS REVEAL PROFILING

In 2011, National Public Radio and the Center for Investigative Reporting sought SAR reports from the Mall of America near Minneapolis, Minn., which has its own private counterterrorism unit. Their investigation revealed a SAR process riddled with errors and religious and racial profiling, yielding little of value to counterterrorism investigators. One man was reported because he was taking pictures of a "Flat Stanley" cutout in a construction zone. Two East Indian men were stopped because they were carrying backpacks and taking pictures, much like many other visitors to the Mall. Local police indicated that some of the reports would be kept "for decades." The former counterterrorism director for the FBI was critical of these measures, describing them as "absolutely not worth the effort," and a former Homeland Security official was not aware of a single terrorist arrest stemming from suspicious activity reporting.[188]

b. Retention and Sharing

A March 2013 report from the Government Accountability Office paints a picture of widely varying policies and practices governing the sharing of ISE-SARs, depending on the agency that produces the ISE-SAR or the preferences of the submitting agency.[189] Many fusion centers, for instance, maintain "Shared Spaces" on the ISE, which allow the fusion center to keep control over the content of the reports while permitting other users of the ISE to view the information. The FBI, by contrast, uses an interface called eGuardian, which is the unclassified version of the Bureau's Guardian system. The FBI may upload reports from eGuardian into Guardian, where other parties can download or modify the information.[190] The Department of Homeland Security has warned that this practice bypasses the "read-only" safeguard of Shared Spaces by allowing the FBI and other federal agencies to retain information that a fusion center subsequently removes, enabling the FBI to "amass[] copies of databases that may be inaccurate or out of date."[191] Some fusion centers submit their reports to both Shared Spaces and eGuardian; some use Shared Spaces regularly and eGuardian on a case-by-case basis; and others use either Shared Spaces or eGuardian but not both.[192]

Given this patchwork of practices, it is impossible to describe comprehensively with whom ISE-SARs are shared or how long they are kept. Nonetheless, some practices are known. ISE-SARs in a fusion center's Shared Space may be kept up to five years depending on the individual center's retention policy.[193] In addition, any ISE-SAR for which a nexus to terrorism has not been definitively ruled out, including reports reflecting First Amendment-protected activity, will be maintained in the FBI's eGuardian system for five years, generally viewable by a wide range of law enforcement agencies.[194] Similarly, the Department of Homeland Security may maintain ISE-SARs in its own SAR Server for five years.[195] Even ISE-SARs ultimately found by the FBI to have *no* nexus to terrorism are kept in eGuardian for six months, and ISE-SARs that are "deleted" from eGuardian are removed only from eGuardian itself — not from any databases to which they have migrated.[196] *All* ISE-SARs, regardless of their nexus to terrorism, are saved in the FBI's classified Guardian system for five years (a time period that restarts any time someone "queries" the ISE-SAR[197]), after which the reports are retained in the FBI's Sentinel database for another 30 years.[198] In short, even an ISE-SAR with no nexus to terrorism is kept for decades.

Retention Schedules for SARs in the FBI's eGuardian and Guardian Systems

	Outcome of FBI threat assessment		
FBI system	**No nexus to terrorism**	**Inconclusive nexus to terrorism**	**Nexus to terrorism**
eGuardian	Deleted after 180 days	Deleted after 5 years	Deleted after 5 years
	After deleted, retained in or by Guardian (see below) ACS/Sentinel (30 years) NARA	After deleted, retained in or by Guardian (see below) ACS/Sentinel (30 years) NARA	After deleted, retained in or by Guardian (see below) ACS/Sentinel (30 years) NARA
Guardian	Deleted after 5 years	Deleted after 5 years	Deleted after 5 years
	If queried prior to deletion, then no change	If queried prior to deletion, then after 5 years, supervisor can view until 10 years, then deleted completely	If queried prior to deletion, then after 5 years, supervisor can view until 10 years, then deleted completely
	After deleted, retained in or by ACS/Sentinel (30 years) NARA	After deleted, retained in or by ACS/Sentinel (30 years) NARA	After deleted, retained in or by ACS/Sentinel (30 years) NARA

ACS: Automated Case Support system (the FBI's former case management system)
Sentinel: The FBI's case support system they are transitioning to (FBI's current case management system)
NARA: National Archives Records Administration
Source: FBI.

Source: *U.S. Gov't Accountability Office, GAO-13-233, Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports are Effective* 53 (2013)

Finally, because eGuardian is a terrorism database, the ISE-SARs in the system, including those with no nexus to terrorism or only a questionable link, would automatically be accessible to the National Counterterrorism Center. It seems likely that information from ISE-SARs would be fed to the FBI's Investigative Data Warehouse as well. Accordingly, the retention, use, and sharing policies for ISE-SARs described above are effectively augmented by the policies of those data centers.

2. Assessments

a. Information Collected

As discussed, the FBI's domestic investigations are governed by a set of guidelines issued by the Attorney General. Soon after 9/11, Attorney General John Ashcroft released new guidelines authorizing the "extremely limited checking out of leads."[199] While these represented a new phase of investigations, they came with only limited investigative tools.

In 2008, however, Attorney General Michael Mukasey significantly expanded this avenue of information gathering by introducing a new category of inquiries called "assessments." While assessments require an "authorized purpose" and a "clearly defined objective," they require "no particular factual predication."[200] In other words, the FBI need not have any factual basis to believe that the subject of an assessment has committed a crime or engaged in any wrongdoing, nor does the FBI need to have a particular subject in mind; assessments allow for the monitoring of groups or movements. At the same time, assessments allow the collection and retention of a wide range of information and may be carried out using a variety of intrusive techniques.[201]

ASSESSMENT TOOLS

The investigative tools available during an assessment include:

- Engaging in unlimited physical surveillance of a person's home, office, car, or any other destination.[202]
- Collecting information about the target's roommates or live-in partner.[203]
- Placing a government informant anywhere for nearly any reason.[204]
- Interviewing any person or organization, potentially concealing the agent's FBI affiliation or the purpose for the interview.[205]
- Attending any public meeting undercover to observe those participating and their activities: for example, a gathering of the American Civil Liberties Union or the National Rifle Association; an open meeting of Alcoholics Anonymous; or, with supervisory permission, a religious service.[206]
- Requesting or receiving any record that a local, state, federal, or tribal government agency, private company, individual, or foreign government chooses to provide.[207] Governmental records could include employment, benefits, welfare, marriage, divorce, and driver's history information, as well as Social Security, passport, and driver's license numbers.
- Obtaining nearly any information from other FBI or DOJ files or employees. The Attorney General Guidelines imply that personnel records on current or former DOJ employees may be available, which could include information about drug use and visits to therapists for mental health counseling.[208]
- Gathering nearly any publicly available information, including public Facebook or Twitter postings, blog posts, and website comments; retrieving anything discarded in a public trash container; and searching commercial databases.[209] Commercial databases could contain public legal records, credit and purchase history, bankruptcy filings, consumer business relationships, medical information, lists of websites visited, and driving records.[210]
- Conducting pattern-based data mining, with supervisory approval.[211]

Many of these "tools" may be deployed even before an assessment has been opened — that is, without a "clearly defined objective" or supervisory approval. There need only be a "reason to undertake these activities that is tied to an authorized FBI criminal or national security purpose."[212]

Assessments fall into five categories, which run the gamut from seeking information about threats to national security, to assessing possible informants, to obtaining foreign intelligence information.[213] One type of assessment permits the acquisition of information — whether in response to a lead or simply "proactively" — about any potential threats to national security.[214] This type requires no supervisory approval before it is opened; while a supervisor must re-approve the assessment every 30 days after the first month, it may remain open "until factual information is developed that warrants opening a predicated investigation or until a judgment can be made that the target does not pose a terrorism or criminal threat."[215] In other words, until and unless a negative is proven, the assessment can remain open, allowing for continued collection of information on presumptively innocent people.

Race, ethnicity, religion, or national origin can also be factors in deciding to launch an assessment, as long as they are not the *only* basis for initiating the assessment; First Amendment-protected speech may also be a factor in opening an investigation and may itself be investigated.[216] Such latitude creates opportunities for abuse and misdirection of resources. The Department of Justice's Inspector General found, for instance, that the FBI had continued to pursue an investigation in the face of substantial questions about the underlying evidence in large part because the target, a lawyer, was a convert to Islam and had once represented a terrorism defendant in a child custody case.

THE CASE OF BRANDON MAYFIELD

On May 6, 2004, the FBI arrested Portland-based attorney Brandon Mayfield as a material witness in connection with the March 2004 terrorist attacks on commuter trains in Madrid, Spain. Mayfield, an American-born convert to Islam and former lieutenant in the Army, was held for two weeks and then released without being charged.[217] Although the FBI initially reported that Mayfield was investigated and detained based solely on similarities identified between his fingerprints and those found on a bag of detonators linked to the attack[218] — an identification that turned out to be incorrect — a 2006 review by the Department of Justice's Inspector General raised serious questions about the role played by Mayfield's religion and his prior representation of a terrorist defendant.[219] The report concluded that Mayfield's "representation of a convicted terrorist and other facts developed during the field investigation, including his Muslim religion, also likely contributed to the examiners' failure to sufficiently reconsider the identification after legitimate questions about it were raised."[220] As one of the fingerprint examiners conceded, "if the person identified had been someone without these characteristics, like the 'Maytag Repairman', the Laboratory might have revisited the identification with more skepticism and caught the error."[221] The FBI issued a written apology and reached a $2 million settlement with Mayfield in November 2006.[222]

In a recent 24-month stretch, nearly 43,000 terrorism-related assessments were opened, culminating in fewer than 2,000 "predicated investigations" — i.e., investigations that are based on some suspicion of criminal activity or threat to national security — a rate of less than 5 percent.[223] Presumably, even fewer of these predicated investigations resulted in prosecutions, although those statistics are not available.

b. Retention and Sharing

The low rate of assessments that turn up wrongdoing begs the question of what happens to all the chaff that has been collected. In light of the FBI's history of investigative abuses and its current capabilities, one might expect that information not leading to an investigation would be retained for a relatively short amount of time and not disseminated widely.

To the contrary, however, the 2008 Mukasey Guidelines contemplate practically unlimited retention of all information collected. According to the Guidelines, "[i]nformation obtained at all stages of investigative activity [including Assessments] is … to be retained and disseminated … *regardless of whether it furthers investigative objectives in a narrower or more immediate sense*."[224] The Domestic Investigations and Operations Guide expands on this policy:

> Even if information obtained during an Assessment does not warrant opening a Predicated Investigation, the FBI may retain personally identifying information for criminal and national security purposes. In this context, the information may *eventually* serve a variety of valid analytic purposes as pieces of the overall criminal or intelligence picture are developed to detect and disrupt criminal and terrorist activities.[225]

Even information that reveals constitutionally protected expression or association can be retained if it is "pertinent to or relevant to the FBI's law enforcement or national security activity" as "determined by the circumstances," which are not defined or delimited.[226] Only if an item has "*no foreseeable future evidentiary or intelligence value*" for the FBI or the 16 other member agencies of the Intelligence Community will it be returned or destroyed.[227] In practice, this is a directive to keep all information.

Moreover, this data is evidently kept for decades. In 2009 Congressional testimony, former FBI director Robert Mueller confirmed Rep. Jerrold Nadler's (NY-10) assessment that the FBI "keep[s] for 20 years information about innocent people, private information that [the FBI has] collected in the course of an investigation … which it turns out they had nothing to do with."[228] Documentation for the Central Records System, an FBI database that covers persons "who relate in *any manner* to official FBI investigations," adds that intelligence and national security matters may be kept for thirty years (emphasis added).[229]

In addition to keeping it for decades, the FBI can share information arising out of an assessment:

- within the FBI and with any other component of the Department of Justice;
- with any federal, state, local, or tribal agency if the information is related to the agency's responsibilities. If the agency is part of the federal Intelligence Community, the FBI must accept the agency's statement that the information is relevant; and
- with any party, including a private company or corporation, where the dissemination of the information "is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or threat to the national security, or to obtain information for the conduct of an authorized FBI investigation."[230]

Finally, a significant amount of information in assessment files is likely to be sent to or accessible by the FBI's Investigative Data Warehouse, and the National Counterterrorism Center is likely to have access to search for international terrorism information.[231] The identities of the subjects of assessments, as well as of his or her associates and other interviewees, may be shared with the IDW for long-term data mining and correlation.[232]

MORE POWERS ON THE HORIZON: DOMESTIC SURVEILLANCE DRONES

The use of domestic surveillance drones may soon become another established mechanism for gathering information about Americans. The Customs and Border Protection arm of the Department of Homeland Security already has acquired Predator drones for use in border surveillance, and the FBI recently admitted that it has dabbled in domestic drone surveillance.[233] This relatively limited use is certain to increase, as Congress in 2012 directed the Federal Aviation Administration (FAA) to establish safety guidelines allowing for the operation of civilian drones in the national airspace by September 2015.[234] The FAA has predicted that as many as 30,000 drones could be operating in American airspace by the year 2030.[235] While the FAA and DHS are in the process of considering the privacy and civil liberties issues raised by the domestic use of drones, no policy has been issued, and the FBI has no operational guidelines in place to manage its domestic drone surveillance, including the use or retention of the information it gathers.[236]

The widespread deployment of drones, coupled with the surveillance technology they carry, would provide unprecedented surveillance capacity. A defense agency has developed a camera that can be sent three-plus miles above the ground to capture a 15-square-mile view of the area below at a high resolution, capturing and archiving up to 1 million terabytes, or 5,000 hours of high-definition footage, per day.[237] Other technologies in use or development include night vision technology; technology to see through buildings and foliage; and "video analytics" to recognize and track people or vehicles from afar and flag "suspicious" patterns of movement.[238]

Some state and local governments have introduced or passed legislation that would require law enforcement agencies to obtain warrants before using drone surveillance.[239] Even with a warrant, however, the nature of drone surveillance virtually guarantees that the activities of innocent Americans will be captured along with those of the target. The rules governing the retention and sharing of information obtained through drone surveillance will thus be of great importance.

3. National Security Letters

a. Information Collected

Once the FBI receives information or an allegation that a federal crime or threat to national security may occur or has occurred, it has the authority to initiate a predicated investigation. [240] In a predicated national security investigation, one of the available tools is a National Security Letter.

A National Security Letter (NSL), is a form of administrative subpoena that allows the FBI to obtain a wide variety of customer information from banks, communications companies, consumer credit companies, and more. NSLs are several steps below search warrants: the FBI need not have probable cause to believe a crime has occurred, no judge oversees their use, and companies served with an NSL are obligated to comply as long as the government certifies certain information.[241] NSLs are typically accompanied by a gag order that prohibits the recipient from disclosing either the content or the existence of the request to anyone other than an attorney.[242] Since 9/11, the use of NSLs has risen sharply, increasing nearly six-fold from 2000 to 2006. Moreover, NSLs have shifted from a tool used primarily during investigations of foreigners to one used primarily during investigations of Americans.[243]

STATUTES AUTHORIZING NATIONAL SECURITY LETTERS

Three important statutes allow the FBI (and sometimes other government agencies) to use NSLs to obtain a range of information:[244]

- **The Right to Financial Privacy Act** (RFPA): financial information from banks, credit unions, investment companies and more, as well as purchases of travelers checks, credit card transactions, and purchases or sales at a pawnbroker, travel agency, or real estate company, among others.[245]

- **The Fair Credit Reporting Act** (FCRA): basic credit history information, or full consumer credit reports in international terrorism investigations.[246] Full credit reports could reflect any closed or delinquent bank accounts, current and previous residences, overdue child support payments, foreclosures and bankruptcies, and salary and life insurance information.[247]

- **The Electronic Communications Privacy Act** (ECPA): customer information from email and phone companies, including basic account information, when and to whom an email was sent or a phone call made, and all historical information for any given phone number, as well as billing records.[248]

National Security Letters originated as exceptions to 1970s- and 1980s-era consumer privacy statutes, allowing the FBI to bypass otherwise stringent limitations on government access to various financial and communications-related materials in situations where national security was allegedly at stake. In their original incarnations, NSLs were available only in full FBI investigations, not preliminary investigations, and they required a certification that the subject of the records was a foreign power or an agent of a foreign power, with "specific and articulable facts" provided in support of that conclusion.[249]

The Patriot Act lowered that standard. NSLs are now available in preliminary national security investigations, which require "information or an allegation" indicating that a threat to national security may occur, but not the "articulable factual basis" required by full FBI investigations.[250] In addition, almost all NSLs may be issued upon a certification that the information is "relevant to," "necessary for," or "sought for" a counterterrorism or counterintelligence investigation[251] — no specific and articulable facts or relationship to a foreign power are necessary. Indeed, the subject of the records need not be a suspect in the investigation; he or she can be a witness, associate, victim, or anyone else, as long as his or her records are deemed "relevant."

As the FBI's internal guidance on NSLs observes, "[t]he standard of relevance is not exceedingly difficult to meet."[252] Thus, NSLs were deployed in approximately one-third of all FBI counterterrorism, counterintelligence, and cyber investigations during the last year for which statistics are publicly available.[253] As the DOJ's Inspector General has observed, NSLs allow the collection of "vast amounts of digital information."[254] And the underlying investigation may be based in part on an American's First Amendment-protected activities.[255]

WHAT'S THE BIG DEAL?

Some have argued that the criteria introduced by the Patriot Act simply harmonized the requirements for national security investigations with those for criminal investigations.[256] As other observers have noted, there are critical differences between national security and criminal investigations that make the low "relevance" standard potentially more problematic in the national security context, including the difference in structure between the two types of investigations and the long-lasting gag orders that accompany most National Security Letters.[257]

b. Retention and Sharing

As with its other intelligence investigations, the FBI appears to be authorized to keep NSL-derived information for 30 years after the investigation's closure.[258] In addition, the FBI can disseminate information to another federal agency if the information is "clearly relevant" to the agency's "authorized responsibilities" (for financial and communications-related information) or is "necessary" for the agency's "approval or conduct of a foreign counterintelligence investigation" (for limited credit information).[259] Incongruously, the statute allowing disclosure of a full credit report contains no limitations on dissemination.[260] The financial and communications NSL statutes also declare that the Attorney General Guidelines govern the dissemination of NSL-derived information, but the Guidelines provide little

specific guidance beyond indicating that information may be shared with law enforcement agencies, the Intelligence Community, and foreign governments.[261] Because the FBI's information-sharing with other federal agencies and the intelligence community is often governed by non-public information-sharing agreements, it is next to impossible for the public to understand what happens to the fruits of these secretive subpoenas.[262]

In 2007, the Department of Justice Inspector General (IG) issued a report that was highly critical of the FBI's use of its NSL authority. Among other things, the IG noted that "neither the Attorney General's NSI [National Security Investigation] Guidelines nor internal FBI policies require the purging of information derived from NSLs in FBI databases, regardless of the outcome of the investigation."[263] In the wake of that report, the Department of Justice and the Office of the Director of National Intelligence convened an NSL Working Group in 2007. The Working Group was directed to examine the FBI's use and retention of NSL-derived information, with "special emphasis on the protection of privacy interests."[264]

The Group concluded that existing regulations were adequate to protect Americans' privacy and issued recommendations that largely would have expanded the information available for storage and retention.[265] The Inspector General's Office roundly criticized the proposal, noting that:

- Existing regulations, which the Working Group deemed adequate to protect Americans' privacy, had failed to prevent "serious abuses" of National Security Letters in the past;[266]
- A proposal to upload and retain a wide array of financial and credit information "provide[d] no meaningful constraint and require[d] no balancing of privacy interests against genuine investigative needs" and would have resulted in a "standard so broad as to be meaningless;"[267]
- The failure of the Working Group to further limit the existing 30 year period for retention of NSL-derived data was not "sufficiently protective of the privacy interests of individuals who have been determined not to be of investigative interest;"[268] and
- The volume of data collected and retained in the Investigative Data Warehouse made it particularly critical to ensure — as the Working Group had failed to do — that email and phone-related data, particularly where it had "no identified investigative value," is "not made widely available to the world-wide law enforcement community."[269]

As a result of the concerns identified by the Inspector General, the Department of Justice withdrew the report in 2008, intending to reconvene the Working Group to reconsider the report and proposal.[270] The same year, during Congressional hearings on the ultimately failed National Security Letters Reform Act of 2007, witnesses across the ideological spectrum identified limitations on retention, use, and dissemination as a critical — and missing — aspect of National Security Letters.[271] After an additional scolding by the Inspector General during 2009 Senate testimony, the Department of Justice developed Procedures for Collection, Use, and Storage of Information Derived from National Security Letters ("NSL Procedures"), which were approved by Attorney General Eric Holder in 2010.[272]

Although the public version of the NSL Procedures provides general guidance about information collection, the use and storage guidelines are heavily redacted, making it unclear whether they fully address the criticisms of the Inspector General. What is known about the procedures emerged in 2011 Congressional testimony by Todd Hinnen, Acting Assistant Attorney General for National Security.[273] According to his testimony, any information that is "responsive to the NSL and has *potential* investigative value" may be uploaded into FBI databases, including the Bureau's main case management system, Sentinel.[274] It is not clear whether the NSL must have value to the specific investigation for which it was issued or — as in the assessment context — simply possible value for future investigations. And responsive financial information — whether or not it has any investigative value — is evidently sequestered in a database for future analysis and possible data mining.[275]

Information that is sent to Sentinel (which generally is kept for 20 to 30 years after an investigation's closure) can be accessed and queried by FBI agents as well as a small number of staff in other government agencies, including the Department of Homeland Security, the Terrorist Screening Center, and the National Counterterrorism Center.[276] Telephone records obtained through NSLs are also uploaded into the FBI's Telephone Applications, which can be used to analyze a subject's calling patterns.[277]

Notably, despite the range of materials that Sentinel stores and manages for the FBI, the Bureau has not published a stand-alone public notice or Privacy Impact Assessment for the system. One obscure document indicates that Sentinel is covered by an "umbrella" notice for the FBI's Central Records System (CRS), which does not mention Sentinel (or its precursor, the Automated Case Support system).[278] The Government Accountability Office (GAO) has criticized the Department of Justice for the "broad scope" of the Central Records System notice, and the GAO has observed that it is "unclear" from the CRS's System of Records Notice "how any given record in this system is to be used."[279]

In addition, NSL-derived information is uploaded into the Investigative Data Warehouse — which is also ostensibly covered by the Central Records System notice[280] — presumably for long-term retention and data mining.[281] From there, it may also be shared with state and local law enforcement agencies and entered into their databases.[282] Finally, databases with information gleaned from National Security Letters are, by definition, likely to be available to the National Counterterrorism Center, as NSLs are only available in national security-related investigations.

4. Border Searches of Electronics

a. Information Collected

In the past decade, the Department of Homeland Security has asserted the authority to seize and inspect the contents of any electronic devices that travelers, including U.S. citizens, have with them while crossing the border. These could include laptop computers or tablets with personal journals, emails, confidential or privileged work documents, medical and financial records, and website browsing history; cameras containing photos of international trips and intimate family moments; and smartphones with records of phone calls, texts, and online searches.[283]

While the so-called "border exception" to the Fourth Amendment is longstanding, the federal government has not always construed its authority so broadly.[284] Prior to September 11, 2001, Customs and Border Protection (CBP) — the main law enforcement arm of DHS — directed that Customs officers "should not read [travelers'] personal correspondence," except where agents had reasonable suspicion the documents fell into certain delineated categories, and documents and papers could not be seized or copied without probable cause to believe they were related to a crime.[285]

After September 11, 2001, the newly-created Department of Homeland Security (DHS) lowered the bar for examining, seizing, and sharing materials. In 2007, DHS issued Field Guidance to its investigative arm, Immigration and Customs Enforcement (ICE), on handling electronic information obtained from "Persons of National Security Interest." The memo noted that "ICE's ability to exploit this [electronic] media represents a unique opportunity to collect, analyze and disseminate valuable information" — unique presumably because the contemplated search and seizure would require a warrant if done anywhere besides the border.[286] The guidance also set out the basic principles that are in place today: no individualized suspicion is necessary for border searches; all "computers, cellular phones, and other electronic media" may be searched out of the owner's presence; and the owner need not be notified of the search.[287]

In 2008, DHS published a border search policy that was expanded upon in a 2009 Privacy Impact Assessment (PIA).[288] (Under a 2002 statute, all agencies must publish PIAs to evaluate the privacy impact of databases that collect, maintain, or disseminate personally identifiable information about individuals.[289]) The 2009 PIA sets out a process by which an examination and search "may be conducted without a warrant and without suspicion."[290] Specifically, any CBP officer may pull aside any passenger for additional inspection based on the officer's unspecified observations or "hunches."[291] At that point, all of the passenger's belongings can be inspected outside of his presence — not only documents, books, and magazines, but also "computers, storage disks, hard drives, phones, personal digital assistants (PDAs), cameras, and other electronic devices."[292]

DHS has no express policy against targeting travelers on the basis of their exercise of their First Amendment rights. In addition, DHS has rejected arguments that its suspicionless searches violate either the First Amendment or the Fourth Amendment's prohibition against unreasonable searches and seizures.[293]

During the last year for which numbers are publicly available (fiscal year 2010), nearly 5,000 people had their electronic devices searched at the border.[294] To be sure, this is a small fraction of the total number of border crossings.[295] It appears, however, that the border search authority has been used, at least on occasion, to target particular travelers on non-criminal grounds. Travelers involved in political or social activism have reported intrusive searches and long delays, and — despite DHS's conclusion that it is not disproportionately targeting travelers based on national origin[296] — individuals of Muslim heritage have reported similar experiences coupled with questions about their religion and beliefs.[297]

TARGETED AT THE BORDER

- A firefighter, Gulf War veteran, and local homeland security responder, who is also a convert to Islam, has been stopped at the border multiple times; questioned about his political views, religious beliefs, and charitable contributions; and had his laptop and cell phone searched.[298]

- A Muslim U.S. citizen and Yale graduate student who provides expert consulting to media outlets, the National Counterterrorism Center, and the Department of State has been stopped at the border on multiple occasions, been interrogated about his religious activities and his lectures, and had his laptop searched and data on his cell phone seized and copied.[299]

- An award-winning filmmaker and journalist whose films examined issues including the American occupation of Iraq, detentions at Guantanamo Bay, and domestic surveillance was stopped nearly every time she exited or entered the country for six years; her electronics have been seized and retained for weeks.[300]

- A volunteer with the Bradley Manning Support Network was placed on a government watchlist,[301] stopped upon his return from a vacation in Mexico, and questioned about his political activities and beliefs.[302] His laptop, camera, and USB drive were taken and returned seven weeks later, without explanation, beyond the period permitted by CBP rules.[303] After he sued, a federal judge ruled that travelers retain their First Amendment rights and may not be targeted on the basis of their lawful associations "simply because the initial search occurred at the border." However, the judge did not disturb the agency's ability to conduct a search without suspicion of criminal activity as long as the search is not based on the person's lawful associations.[304]

b. Retention and Sharing

This broad latitude to search devices is coupled with the authority to keep and share it on grounds short of suspicion of criminal activity. While the Privacy Impact Assessment acknowledges that "CBP and ICE do not make the information sharing process fully transparent to the public," certain parameters are known.[305] For instance, without any basis for suspicion, CBP may detain an electronic device for five days, a period that can be extended in the event of unidentified extenuating circumstances.[306] A phone, computer, or camera may be detained because the connecting time between flights is short or the content is in a foreign language.[307] During that time, CBP can search the device and share it with any other federal agency for analysis.[308]

Alternatively, instead of detaining the device, CBP or ICE can copy the contents of the device — without any suspicion of criminal activity — to conduct a more in-depth search at its convenience, within 30 days

unless a supervisor approves an extension.[309] The traveler has no right to be notified that the contents of his electronic device have been copied.[310] DHS may also solicit technical assistance to decrypt any encrypted information — again, "without a reasonable articulable suspicion that the data on the electronic device is evidence of a crime."[3111] The agency providing the assistance may retain the materials if it has a "valid basis for its own independent authority;"[312] as illustrated in this report, that authority can be wide-ranging. (Materials may also be shared with other agencies for subject matter assistance, though only with reasonable suspicion that the data on the electronic device is evidence of a crime.[313])

In addition, copies of electronic information that are seized by CBP or ICE may be kept if retention is "required for a law enforcement purpose"; while this standard lacks a clear definition, it is almost certainly lower than reasonable suspicion.[314] More broadly, both ICE and CBP can retain copied information without probable cause if the data "*relates* to immigration, customs, and other enforcement matters" — a relatively generous standard — as long as the retention is "consistent with the privacy and data protection standards of the system of records" in which the information is kept.[315]

Importantly, none of these restrictions on retention and sharing apply to notes or written impressions *about* the encounter.[316] Thus, even in the event that a device was returned to the traveler and copies of its contents destroyed, notes recording what a traveler was reading or the content of his data may still be maintained in a database.

Information captured at border searches — including notations regarding those searches — may also be stored in and shared through other databases. For instance, records of searches of electronic devices and detentions — though not copies of the information itself — are entered into the government's TECS database and stored for up to 75 years.[317] While some information about such searches may legitimately need to be stored for oversight and auditing purposes,[318] TECS, which stores CBP data relating to travelers entering or leaving the United States, also appears likely to feed into the FBI's Investigative Data Warehouse.[319] In addition, information detained and seized by ICE may go to a variety of databases, which keep information for 5, 15, or 20 years.[320] Many of the records in these databases may be used or shared broadly, often for undefined national security and intelligence activities.[321] In one ICE system, information with no relevance to a criminal investigation may also be kept in order to help DHS develop pattern-matching algorithms.[322] Finally, because the NCTC has indicated that it accesses international travel-related databases, much of the information gathered at the border is likely to be available to the NCTC for up to five years.

When information can be shared so broadly and retained for so many purposes, a traveler's ability to challenge inaccuracies in the information is particularly critical. The Privacy Impact Assessment (PIA) for searches of electronics at the border offers only one route, though: "If the information is used as evidence in a civil or criminal prosecution, or if an individual is in immigration proceedings," the individual can challenge the information himself or call witnesses to do so.[323] The PIA adds that the passenger is to blame for any errors: "Any inaccurate information is the result of the traveler having inaccurate information on his or her electronic devices, rather than errors in the copying…."[324] Since the information could include anything — emails from a friend, a record of websites accessed by a relative who borrowed the computer, documents written by a colleague who previously used the same laptop — saying that any "inaccuracies" are the travelers' responsibility and can be resolved in a court of law is a fairly minimal safeguard.[325]

SEARCHES OF ELECTRONICS AT THE BORDER

Traveler is entering or leaving the country by air, land, or sea.

Without suspicion of any criminal activity, based on just a "hunch" or "intuition," a **border officer can search** the traveler's laptop, tablet, phone, hard drive, or other electronic device. The officer can **detain the device** to see if there's probable cause to **seize it as evidence** of a crime, or **copy the information** on the device to **search at a later date.** The traveler **need not be present** during the search. The detention and search generally must be completed within **5 to 30 days.**

During that time, several things can happen:

1. **RELEVANT INFORMATION:** The search reveals information that's relevant to customs, immigration, or other laws enforced by DHS. Information can be **RETAINED.**
2. **PROBABLE CAUSE:** The search uncovers facts that indicate a likely violation of the laws enforced by CBP or ICE. Device can be **SEIZED.**
3. **NEED ASSISTANCE:** CBP/ICE can share the device or the information on it with any federal agency for either **TECHNICAL** or **SUBJECT MATTER** assistance.

TECHNICAL ASSISTANCE is specialized or scientific help. CBP/ICE **does not need** to have **reasonable suspicion** of criminal activity.

SUBJECT MATTER ASSISTANCE is analytical help from an expert or another law enforcement agency. CBP/ICE **must have reasonable suspicion** of criminal activity.

Either way, **device and/or information on it** can be **retained if:**

1. There's any evidence of criminal activity relating to laws enforced by CBP or ICE.
2. There's any evidence of violation of a law that subjects the device to civil forfeiture.
3. The information relates to a law enforced by the agency with which it's shared.

If none of these conditions is met, device must be returned and all information destroyed, **unless** the information is "required for a law enforcement purpose" and retention is consistent with the Privacy Act.

In addition, as a general matter, any information that is lawfully seized can be shared with any state, local, federal, or foreign law enforcement authority "in furtherance of enforcement of their laws."

MORE POWERS ON THE HORIZON: BIOMETRICS

Biometrics — data points that "identify an individual based on his or her distinguishing physiological and/or behavioral characteristics"[326] — are among the fastest-growing datasets collected by the federal government. As agencies' databases grow and incorporate more types of biometrics, they are also increasingly interoperable, meaning that information is shared seamlessly from one database to the other.

The Department of Homeland Security has the federal government's largest biometrics database, the Automated Biometric Identification System (known as IDENT).[327] First established in 1994 for the Immigration and Naturalization Service,[328] IDENT began being used for other purposes after 9/11.[329] IDENT takes in information from other agencies, including the Department of State, the FBI, the Department of Defense, and other collaborating organizations.[330] The biometric data stored in IDENT is shared within DHS and with other governmental agencies at all levels for a variety of functions, including national security, law enforcement, and intelligence.[331] Information in IDENT is currently kept for 75 years, though DHS is reconsidering that retention period.[332]

The FBI's primary biometrics database is the Integrated Automated Fingerprint Identification System (IAFIS), containing fingerprints for over 74 million individuals.[333] These fingerprints are housed not just for criminal purposes but to conduct employment checks, confer certain professional licenses, and carry out unidentified "national security purposes."[334] In the fall of 2014, the FBI plans to fully transition to its new biometrics system, Next Generation Identification; NGI will enable capture and searching of iris scans, facial pictures, and scars in addition to fingerprints, as well as markers like tattoos.[335] These types of identifiers pose particular privacy risks, as they can be used to identify someone from afar and without their consent. While the FBI has asserted that pictures from gatherings, social media, and other public assemblies or online sources will not go into the database,[336] an FBI PowerPoint containing photos of political rallies suggests that the FBI may be taking (or planning to take) more information into its biometrics databases than publicly acknowledged.[337] The FBI typically keeps civil identification records until the subject is 75 years old and criminal identification records until the subject is 99 years old, though the Bureau is petitioning for an extension to 110 years.[338]

In 2008, DOJ and DHS initiated a major biometrics sharing and interoperability initiative, intended to give some reciprocal access to users of IDENT and IAFIS.[339] The FBI is also pursuing a biometrics sharing plan with the Department of Defense,[340] as well as "sharing relationships" with 77 foreign countries, some governed only by ad hoc agreements.[341] Observers are cautioning that measures in the proposed immigration bill could lead to the creation of a national biometric identification system for all Americans.[342]

5. National Security Agency

The National Security Agency (NSA) is an element of the Department of Defense. Its mandate is to collect "signals intelligence" — intelligence gleaned from communications systems and other kinds of electronic systems — for foreign intelligence purposes.[343] Despite its foreign focus, the NSA has the authority to gather fairly extensive amounts of information about Americans, and recent revelations indicate that it is exercising this authority in a range of ways.[344] Given the frequency of these revelations and the ongoing declassification of previously secret documents, more information is likely to emerge after the publication of this report.

a. Information Collected

i. Programmatic surveillance of electronic communications

Beginning in 1978, the Foreign Intelligence Surveillance Act (FISA) provided the statutory structure for the NSA's surveillance activities. FISA required the NSA to obtain authorization from the secret Foreign Intelligence Surveillance Court (FISC), for any surveillance of Americans' domestic or international communications. To secure the necessary authorization, the NSA until recently had to establish probable cause that the American was an agent of a foreign power. The NSA's intelligence-gathering activities are further guided by an Executive Order issued in the early days of the Reagan administration, which imposes various limitations on the NSA's ability to operate domestically.[345]

On the day of the September 11, 2001 attacks, President George W. Bush secretly authorized the NSA to initiate a domestic surveillance program that bypassed these long-standing restrictions.[346] This program, coupled with a variety of other classified intelligence activities, came to be known collectively as the President's Surveillance Program (PSP).[347] One part of the program, known as the Terrorist Surveillance Program (TSP), allowed the NSA — without judicial oversight — to gather the content of Americans' communications, including phone calls, emails, text messages, and more, as long as the other party to the communication was outside the country and was believed to be affiliated with al-Qaeda.[348] The NSA also provided intelligence reports to the FBI, CIA, and NCTC.[349]

After a public outcry, the Terrorist Surveillance Program was technically terminated in 2007. The FISA Court and Congress ultimately ratified the program, however, and Congress amended FISA in 2007 (the Protect America Act) and 2008 (the FISA Amendments Act or FAA) to grant the agency even broader data-gathering powers.[350] The statute now allows the acquisition of communications involving Americans if the following conditions are met: a "significant purpose" of the surveillance is to gather "foreign intelligence," broadly defined to include information that "relates to the conduct of the foreign affairs of the United States";[351] at least one party to the communication is "reasonably believed" to be a non-U.S. person located overseas; and a non-U.S. person is the true "target" of the surveillance.[352]

Moreover, the government need not obtain individualized permission from the FISC in order to intercept such communications. Instead, only the overall program must pass judicial muster; the specific person or persons whose communications will be monitored are not identified to the court.[353]

This surveillance scheme, which is available as an alternative to a targeted FISA warrant (required where an American is the actual target of surveillance), is often referred to as programmatic or "Section 702" surveillance, after the part of the FAA in which it was authorized.

The FAA expressly contemplates that the international communications of presumptively innocent Americans will be collected. Because the true target is supposedly the non-citizen on the other end of the call or e-mail (or discussed within it), this collection of Americans' information is termed "incidental." Americans' communications are also gathered through "inadvertent" collection, which takes place when the procedures designed to ensure that only non-U.S. persons are targeted fail.

There is reason to believe that "inadvertent" collection, like "incidental" collection, is commonplace. For one, reports indicate that the NSA requires only a 51 percent certainty that its targets are foreign when conducting programmatic surveillance such as PRISM and the upstream collection described below.[354] For another, the NSA's targeting procedures, leaked by Edward Snowden in 2013, provide that "[i]n the absence of specific information regarding whether a target is a U.S. person, a person . . . whose location is not known will be presumed to be a non-United States person."[355] In short, while the NSA has long refused to disclose the number of presumptively innocent Americans whose communications are collected under Section 702, that number is certain to be high.[356] (The agency has recently agreed to make some numbers available, but they appear unlikely to paint the full picture of the program's effect on Americans.[357]) Additionally, the NSA's method of collecting targeted communications occasionally captures entire inboxes, including wholly domestic communications.

One method of collecting Internet content under Section 702 is the PRISM program that Edward Snowden revealed in June 2013. PRISM funnels communications from companies like Google, Apple, and Facebook to the NSA if the communications contain certain search terms chosen by the NSA.[358] Another recently-revealed method of collecting Internet content is "upstream collection." Unlike PRISM, this program gives the NSA direct access to the data packets traveling through both domestic and international fiber optic cables, also called the Internet "backbone."[359] Multiple programs employ upstream collection to gather and analyze reams of data. For instance, the NSA is reportedly copying all emails and text messages with one end outside of the United States in order to pull out communications that match certain "selectors" relevant to foreign intelligence, as broadly defined by the FAA.[360] Reports also indicate that the agency has collaborated with domestic telecommunications companies to give it the ability, under certain circumstances, to directly access up to approximately 75 percent of U.S. communications.[361]

On top of these collection authorities, a program called XKEYSCORE allows the government to search essentially any Internet activity using approved search terms. XKEYSCORE's capabilities are vast; it stored 41 billion records — content and metadata — in a single 30-day period in 2012.[362] Because it selects so much data, it must feed much of it to other specialized databases; these databases make XKEYSCORE the largest data repository for the NSA.[363]

ii. Bulk collection of Americans' telephone records

The NSA has been acquiring bulk "metadata" about Americans' phone calls — when a call is made, to which phone number, and how long it lasts — since soon after 9/11. Initially, most of the major

telecommunications carriers voluntarily provided this information.[364] When the program was revealed in the press in 2005, one of the companies asked to be provided instead with a court order that compelled its cooperation.[365] As a result, the NSA and FBI together persuaded the FISA Court that this bulk collection was permissible under Section 215 of the Patriot Act, the section that allows the production of "tangible things" that are "relevant" to an authorized counterterrorism or counterintelligence investigation.[366] The FISA Court has accordingly issued regular orders to the major telecommunications companies since 2006, directing the companies to provide their customers' calling information to the NSA daily.[367]

Under this new interpretation, metadata about all Americans' phone calls — international and domestic — is compiled on the theory that the database may produce relevant information when it is searched in the future.[368] The data need not be relevant at the moment of collection, and all Americans' records may be collected despite the certainty that the vast majority will have no current or future relevance.

b. Retention and Sharing

i. Programmatic surveillance of electronic communications

The FISA Amendments Act requires the Attorney General and the Director of National Intelligence to adopt procedures to limit or "minimize" the retention of information about U.S. persons (whether "incidentally" or "inadvertently" collected) and to prevent its dissemination unless it is evidence of a crime.[369] While the FISC reviews these minimization procedures for adequacy at the initiation of the program, it has no authority to oversee their implementation, except at the program's annual reauthorization.[370]

Under the NSA's now declassified minimization procedures for communications it acquires under Section 702, the agency may retain communications to, from, or about an American if they contain foreign intelligence information (an expansively defined concept that includes information relating to the foreign affairs of the U.S.), evidence of a crime, certain cybersecurity-related information, or information "pertaining to a threat of serious harm to life or property."[371] While Americans' communications that do not meet those criteria are generally to be "destroyed upon recognition," the NSA is nevertheless permitted to retain these communications for up to six years from the start of surveillance.[372] And the NSA may share "unminimized communications" with the FBI and CIA, subject to those agencies' minimization procedures, which are not public.[373]

There is at least one exception to the six-year retention limit. The government may, through upstream collection, obtain not just a single communication but a snapshot of an American's email box that contains multiple messages. While some of the emails in the inbox will involve the targeted foreign address, others may be wholly domestic exchanges with no known foreign intelligence value.[374] The entire set of communications in the inbox is known as a multi-communication transaction (MCT).[375] A recently declassified FISC opinion reveals that the government secretly collected MCTs for three years, until it finally notified the Court in 2011.[376] The Court estimated that the government was receiving tens of thousands of "wholly domestic" emails through this program.[377]

While the FISC ultimately approved the collection program, which remains in place today, the Court raised serious problems with the way the NSA was handling the data. These wholly domestic communications were subject to little special handling or marking, and most communications were kept for at least five years even though they were unlikely to have foreign intelligence value.[378] As the Court put it, "NSA's proposed handling of MCTs tends to *maximize* the retention of such information, including information of or concerning United States persons with no direct connection to any target."[379] The Court therefore concluded that the handling procedures violated both FISA and the Fourth Amendment.[380] In response, the government reduced the retention period for MCTs to three years from the start of surveillance and imposed special marking and handling restrictions.[381]

The data flagged and retained by the XKEYSCORE system is also retained for varying lengths of time, depending upon the type of information. Because the amount of data that is scanned and stored is vast, XKEYSCORE itself can store it for only a limited time: three to five days for content, and 30 days for metadata.[382] Other databases receiving information from XKEYSCORE keep the content of emails and email metadata for up to five years.[383]

In a sharp shift from its earlier practice, the government in 2011 secretly persuaded the FISC to allow searches of all of these databases of email communications, with the exception of the MCTs, using Americans' email addresses and phone numbers as search terms.[384] This policy, which allows the government to search for Americans' communications without a warrant, was a reversal of a policy instituted in 2008 at the government's request. [385] While these searches cannot be implemented until procedures are put into place to guide them, the ability to conduct these "back-door searches" confirms warnings issued in recent years by Sen. Wyden and others on the Senate Intelligence Committee.[386]

If the NSA outright violates the FAA's proscriptions and "*intentionally* target[s] a United States person or a person not reasonably believed to be outside the United States," that information must be purged from NSA databases without exception.[387] The procedures do not, however, direct the NSA to notify other government agencies that might have received the information to purge it as well.

Notably, the semiannual assessments issued by the Attorney General and Director of National Intelligence have regularly flagged violations of the targeting and minimization procedures. A 2012 assessment revealed an uptick in compliance incidents, including violations of U.S. privacy rules by foreign governments with access to Americans' data, retention of phone metadata records beyond the five-year deadline, and erroneous targeting of Americans and green card holders.[388]

ii. Bulk collection of Americans' telephone records

The phone metadata collected pursuant to Section 215 of the Patriot Act is retained for five years.[389] The FISC has imposed limitations on the use of this metadata. The NSA may query the database only when it has an "identifier" — for instance, a telephone number — for which there is a "reasonable, articulable suspicion" that it is "associated with a particular foreign terrorist organization."[390] If the telephone number is believed to belong to an American, the suspicion cannot be based "*solely* on activities protected by the First Amendment."[391]

NSA COLLECTION OF EMAILS AND PHONE CALLS: TARGETING

Is desired target a non-U.S. person reasonably believed to be outside the U.S.?

NO If the desired target is a U.S. person or is reasonably believed to be within the U.S., **THEN THEY CANNOT BE TARGETED INTENTIONALLY.**

- If person is nevertheless **INTENTIONALLY TARGETED**, all information gathered must be purged from the NSA's databases. (But the NSA is not required to inform other agencies that might have received the information or reports based on it).
- If communications of a U.S. person or someone in the U.S. are collected **INADVERTENTLY,** then they can be kept and used in accordance with minimization procedures.

YES If an NSA analyst is 51 percent certain that the target is not a U.S. person and is outside the U.S., or the location/status of a person cannot be determined after conducting due diligence, then:

Is there a **FOREIGN INTELLIGENCE PURPOSE** – i.e., will it gather information relating to the U.S.'s foreign affairs?

YES If the target is a non-U.S. person outside the U.S., and the acquisition would serve a foreign intelligence purpose, then the person may be **TARGETED** and **COMMUNICATIONS ACQUIRED**.

- If the target **TURNS OUT** to have been a U.S. person or within the U.S. at the time of the targeting, then (a) acquisition must be terminated but (b) the communications that were acquired may be kept and used in accordance with the minimization procedures.

NSA COLLECTION OF EMAILS AND PHONE CALLS: MINIMIZATION

If the NSA has incidentally acquired Americans' communications as part of its targeting of non-Americans, then:

- The NSA may retain them for up to **SIX YEARS*** to analyze whether they contain (a) foreign intelligence information or (b) evidence of a crime.
- Additionally, communications that **MAY BE RELATED** to the "authorized purpose of the acquisition" can be sent to NSA analysts for further review.

Are the communications **DOMESTIC** (all participants inside the U.S.) or **FOREIGN** (at least one end is outside the U.S., but communications are to, from, or about a U.S. person)?

FOREIGN communications can be RETAINED if:

- They are **NECESSARY FOR THE MAINTENANCE OF TECHNICAL DATA BASES.**
- Circumstances would allow dissemination.
- They are **EVIDENCE OF A CRIME** that has been, is being, or is about to be committed.

DOMESTIC communications can be RETAINED if:

- They are **REASONABLY BELIEVED** to contain **SIGNIFICANT FOREIGN INTELLIGENCE INFORMATION.**
- They are **REASONABLY BELIEVED** to contain **EVIDENCE OF A CRIME** that has been, is being, or is about to be committed.
- They are **REASONABLY BELIEVED** to contain information related to cryptography, traffic analysis, or cybersecurity.
- They contain information pertaining to a **THREAT OF SERIOUS HARM TO LIFE OR PROPERTY.**

Some of this information may be shared with the FBI as well.

REPORTS based on **FOREIGN COMMUNICATIONS** that are with or about a U.S. person **CAN BE DISSEMINATED** if:

- The U.S. person's identity is deleted.
- The U.S. person's identity remains, if the receiving official needs the information for his official duties and the identity of the American or the nature of the communications meet certain criteria.

In addition, **UNMINIMIZED COMMUNICATIONS** including U.S. persons' information can be **DISSEMINATED** to:

- The CIA and the FBI, under certain circumstances.
- Foreign governments, only for technical or linguistic assistance, and the foreign government cannot retain the communications for their own purposes or disseminate them internally.**

* Six years from the beginning of the FISC order authorizing surveillance.

** A recent *Guardian* article noted, however, that the U.S. and Israel have an agreement allowing Israeli intelligence to use unminimized communications including U.S. persons' identities.

These restrictions have several significant caveats, however. First, while the FISC requires that this "reasonable, articulable suspicion" (RAS) requirement be met, the NSA does not have to go back to the Court to justify particular queries; instead, the agency itself decides when it has satisfied its obligation. Second, while the administration has emphasized the fact that only 300 identifiers were used to query the data during 2012, it has also acknowledged that it can obtain additional phone numbers that are up to three "hops" out from the original number.[392] These hops refer to the number of connections from the original number: the first "hop" is to phone numbers the original number is in contact with, the second hop is numbers in contact with the "first hop" numbers, and the third hop is the numbers in contact with those "second hop" numbers.[393] While the agency may not run a three-hop analysis on every contact, a decision to do so could give it access to the phone records of millions of Americans.[394]

THE NSA REPEATEDLY VIOLATES ITS OWN PROCEDURES

On September 10, 2013, the administration declassified a large cache of documents related to the NSA's phone metadata program. The documents — which were released too late to be incorporated into the body of this report — reveal ongoing instances of non-compliance by the NSA with its own minimization procedures and the FISA Court's directives, as well as repeated misrepresentations to the Court regarding the scope and operation of its surveillance programs.[395] More specifically, these materials reveal that:

- For two and a half years, the NSA searched all incoming phone metadata using an "alert list" of phone numbers, most of which did not meet the test of "reasonable, articulable suspicion" (RAS) that the FISA Court required.[396] As of early 2009, when the FISA Court was notified of the issue, just under 2000 of the nearly 18,000 identifiers on the alert list — or barely 11 percent — were RAS-approved.[397] As the Court later described it, "[c]ontrary to the government's repeated assurances, NSA had been routinely running queries of the [telephone] metadata using querying terms that did not meet the required standard for querying."[398]
- The NSA initially allowed its analysts to go even more than three "hops" from the initial query phone numbers, until the government told the Court in early 2009 that it would cease the practice.[399]
- In March 2009, after a series of admissions about the NSA's failures to comply with the FISA Court's minimization procedures, a FISA Court judge excoriated the government for its handling of the surveillance program. He observed that the NSA had engaged in "daily violations of the minimization procedures,"[400] criticized the government's "repeated inaccurate statements,"[401] and concluded that the minimization procedures had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall … regime has never functioned effectively."[402] As a result, the Court required the NSA to obtain Court approval every time it queried the database, except in case of an emergency.[403] (The Court lifted this requirement in September 2009.[404]) Whether this key restriction on the NSA's use of Americans' data functions effectively today is unknown.

- NSA Director Keith Alexander acknowledged that no one person at the NSA actually understood the technical setup of the phone metadata database.[405]
- Each audit or review of the NSA's operations yielded new evidence of compliance violations.[406]

Notably, Senators Ron Wyden (D-OR) and Mark Udall (D-CO) — both members of the Senate Intelligence Committee with access to classified information — have responded to this round of revelations by stating that bulk collection of phone metadata should be ended because the program poses a threat to Americans' civil liberties while offering nothing of unique value.[407] The senators also warned that information has yet to be released about "violations pertaining to the bulk email records collection program."[408]

On September 11, the *Guardian* newspaper published another top-secret document disclosed by Edward Snowden, this one revealing that the NSA "routinely shares raw intelligence data with Israel without first sifting it to remove information about US citizens."[409] The agreement between the NSA and the Israeli intelligence service also permits Israel to retain files with the identities of U.S. persons — as long as they are not U.S. government officials — for up to one year.[410] This agreement is significant because it directly contradicts the NSA's minimization procedures, which prohibit raw intelligence from being shared with a foreign government unless it is for technical or translation assistance, and then only if the foreign government guarantees that it will not make a record of the data or distribute it internally.[411]

IV. POLICY RECOMMENDATIONS

The recommendations below would impose limitations on the long-term retention and sharing of non-criminal information about Americans, while adding to the transparency necessary to ensure that a robust national security system does not tread on Americans' rights.

1. Ensure that every dataset and database has a publicly available policy, and make the government's use, sharing, and retention practices as transparent as possible.

Without information about the disposition of information in the government's possession, the public cannot assess the reasonableness of government information-collection programs. While the Privacy Act would already seem to require transparency when it comes to databases about Americans, too many collection and retention programs remain far too opaque.

Accordingly, each time the government collects information from or about U.S. persons, the policies governing the collection, retention, sharing, and use of the information should be made publicly and clearly available. Where data is shared with the private sector or foreign entities — which are often subject to few restrictions on their own use of the information — the sharing should be subject to public, well-delineated memoranda of understanding or sharing agreements. These agreements should prohibit further sharing without permission of the sharing agency or for purposes inconsistent with the original use, and should impose data privacy responsibilities upon the recipients, with sanctions — including a freezing of future information sharing — in the event of significant violations.

In the rare circumstances where disclosure of the policy or agreement would pose a danger to national security, a redacted or summarized version of the policy should be made available.

2. Require reasonable suspicion of criminal activity to retain or share information about Americans for law enforcement or intelligence purposes.

Given the demonstrated potential for misuse and the sparse public evidence of benefit, domestically collected information about Americans should not be retained or shared for law enforcement or intelligence purposes unless: (1) there is objective reason to suspect criminal activity, and the information is relevant and material to the suspected crime; or (2) the information must be shared for a temporary and limited purpose, such as translation or decryption assistance. If it is shared for such a purpose, the assisting agency must return all data following its analysis and purge it from its own system.

The bar for meeting the reasonable suspicion standard is low: An officer need only point to "specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch of criminal activity."[412] Where an investigation is grounded in reasonable suspicion, information about potential suspects, victims, and witnesses may legitimately need to be retained; these records will be necessary to manage the investigation, to meet prosecutorial disclosure obligations, and to ensure that a suspect who has been exonerated is not targeted

multiple times. When data has been collected without reasonable suspicion of some criminal activity, however, the risks of keeping and sharing that information outweigh the scant public evidence of benefits.

In addition, some information that is properly retained in investigative files under this standard may refer to the exercise of First Amendment freedoms or to race, religion, or ethnicity. Because information reflecting constitutionally-protected activities or status is particularly susceptible to misuse, the identity of the person involved should be masked when shared or when retained beyond the close of the investigation to ensure that it is not accessible in the future unless strictly relevant and necessary to an authorized investigation. If constitutionally protected information is to be shared without masking the identity, the official making the sharing decision should articulate all of the facts in support of that decision, and a supervisor should sign off.

Finally, until and unless pattern-based data mining is demonstrated to be a valid counterterrorism tool, personally identifiable information about Americans not suspected of any criminal activity should not be kept solely for the purpose of current or future data mining.

3. Reform the Privacy Act to better protect against the long-term retention and broad sharing of innocuous, sensitive personal information, and institute oversight mechanisms.

The Privacy Act was intended to strictly limit the circumstances under which information about Americans is retained and shared.[413] Riddled with exceptions for national security and law enforcement, however, it has been largely transformed in the nearly forty years since its passage into a procedural, box-checking exercise rather than a substantive check on the government's power.[414] Indeed, many elements of the Privacy Act have been identified as woefully inadequate almost since its inception and as particularly unsuited for the computer age.[415] In 2008, the Government Accountability Office recommended a host of changes to the Privacy Act, some of which are reflected below.[416] The Privacy Act and the e-Government Act of 2002, which augments the transparency mission of the Privacy Act by requiring agencies to publish Privacy Impact Assessments, should be fortified to reflect the intent underlying their passage, as follows:

a. Amend the Privacy Act to cover all federal systems of records.

The Privacy Act covers only databases from which an individual's data is retrievable using a personal identifier (such as his or her name).[417] As the Government Accountability Office and others have observed, the advent of computerized databases and data-mining have increased the number of databases that do not retrieve information that way and therefore are not subject to the strictures of the Privacy Act.[418] To ensure that the Privacy Act's protections are not rendered obsolete by new technologies, the Privacy Act should be amended to cover all systems of records held by the federal government that contain personally identifiable information.

b. *Establish an independent body to monitor compliance with the spirit and letter of the Privacy Act.*

In 1974, when the Privacy Act was debated and approved, the Senate was poised to establish a Federal Privacy Board to "oversee the gathering and disclosure of information concerning individuals" by various government agencies.[419] Despite broad Congressional support, however, President Ford's opposition and other factors ultimately resulted in the Board's defeat.

There is thus no outside body that oversees implementation of the Privacy Act, and agencies are not obligated to respond to or act upon public comments made in response to published notices of databases.[420] The 1974 Senate committee that championed the Privacy Act anticipated the problems that might arise from this gap in oversight when it established the now expired Privacy Protection Commission:

> Providing a right of access and challenge to records, while important, is not a sufficient legislative solution to threats to privacy. [I]t is not enough to tell agencies to gather and keep only data which is reliable by their rights for whatever they determine is their intended use, and then to pit the individual against government, armed only with a power to inspect his file, and a right to challenge it in court if he has the resources and the will to do so.[421]

An external board or agency could fill this gap by overseeing agencies' compliance with both the spirit and the letter of the Privacy Act. Such a panel could:

- Ensure that agencies publish required notices and that the notices adequately educate the public about the agency's use of individuals' data.
- Review agencies' invocation of database exemptions and their statements justifying the exemptions (as recommended below).
- Assess agencies' reliance on "routine uses" for information sharing, described in Part II.A.2. In furtherance of this oversight, agencies could be required or encouraged to:
    - Accompany each routine use with a statement describing why that use is consonant with the original purpose or purposes of the database.
    - Ensure that when information is shared with an entity that is not itself subject to the Privacy Act, a public memorandum of understanding or information-sharing agreement explains why the information is being shared and obligates the recipient to protect the privacy of the information to at least the same degree as the sharing agency.
    - Restrict both routine uses and intra-agency sharing to uses that are "clearly compatible with the original purpose" of the system of records, with agencies specifically describing the relevant purposes.[422]
    - Limit the establishment of "blanket" routine uses, particularly where the databases subject to those routine uses are not specifically identified.
    - Publish a public report, at least annually, enumerating the number of times information has been shared pursuant to each routine use set out for each database or system of records.
- Maintain a publicly-available archive of its findings and recommendations to assist in creating a common law or "best practices" regarding the implementation of the Privacy Act.

c. Bolster the transparency necessary to vindicate the promise of the Privacy Act.

The protections of the Privacy Act — and the ability to vindicate those protections by challenging an agency's actions, bringing suit,[423] or raising public awareness of abuses — carry little weight if individuals cannot learn that their personal information is being compiled in a database. While the Privacy Act requires that agencies provide notice of information collection and give individuals access to their data, agencies may exempt databases from the provisions requiring transparency and an opportunity to challenge the accuracy of personal information.[424] In particular, agencies may exempt from these provisions any database broadly related to law enforcement or national security without specifying how the exemption satisfies the Act — leading to some of the information gaps described above.[425]

In addition, even when agencies do publish the required notices or Privacy Impact Assessments, there is no centralized access point for those materials. While the Office of Management and Budget (OMB) is tasked with overseeing agencies' implementation of both statutes,[426] it has been regularly criticized for its apparent lack of interest in enhancing the accessibility of Privacy Act notices.[427]

Two steps would assist in remedying these barriers to transparency:

1. Each agency that exempts a database from the Privacy Act under the law enforcement exemption should publish a statement justifying the exemption, with specific reference to the elements of the exception that are enumerated in the statute.

2. The OMB should establish a centralized portal on its website for access to all required Privacy Act and e-Government Act notices, and make clear when a notice applies to databases that are not referenced in the notice itself.

4. Increase public oversight over the National Counterterrorism Center.

a. Require the NCTC to report regarding its use of its Track 3 authority.

In light of the NCTC's significant new abilities to acquire and retain non-terrorism information about Americans under its expanded "Track 3" authority (see Part III.A.1), transparency is critical. The NCTC should disclose:

1. how often the Center is invoking its expanded authority and under what circumstances;

2. how that rate of use compares to the use of its narrower authorities; and

3. why its other, more limited information-gathering authorities were insufficient in these instances.

The Center should issue a report to Congress detailing this information at least annually, with a copy — redacted or summarized if necessary — provided to the public.

b. Commission a public study and report regarding the effectiveness of the NCTC and the need for a five-year retention period for non-terrorism information.

The NCTC was created to carry out the sharing and analysis of terrorism-related information called for by the 9/11 Commission, and its mission is focused on international terrorism. Today, however, the NCTC is empowered to collect vast amounts of non-terrorism information about Americans, and there has been no public study of whether the NCTC is effectively carrying out its mission. In the context of fusion centers, Congressional oversight committees have concluded that these entities consume vast amounts of money in exchange for little in the way of either results or accountability. An independent study of the NCTC's practical contributions to counterterrorism and compliance with its oversight obligations would help determine whether the benefits in fact do outweigh the risks. In addition, the study could assess whether a ten-fold increase in retention time for databases of non-terrorism information about Americans is necessary or if a shorter period would accomplish the same goals.

5. Require regular and robust reviews of agency collection, retention, and use of Americans' information.

Finally, even the best policies are effective only when they are followed. As it stands, the public has minimal ability to perform an oversight role: individuals have little opportunity to learn about, let alone contest, the contents of files that are most likely to be shared with a range of entities for undefined national security and intelligence purposes. Indeed, people who have not planned or committed a crime would have little reason even to think that sensitive information they have not affirmatively provided to the government is nevertheless being gathered, retained, and shared. It is therefore critical that any governmental agency or component that collects, keeps, and shares innocuous information about U.S. citizens and residents be subject to regular and robust audits, ideally by an external body or an inspector general, to ensure that it is complying with data privacy mandates. An external board could also explore possible technological solutions to some of the privacy challenges identified in this report, including mechanisms to ensure that information removed from one database is removed from other databases as necessary.

One additional element is critical to the protection of civil liberties and the public's right to know as well as a robust national security strategy: effective Congressional oversight. The increasing difficulty — and dysfunctionality — of Congressional oversight over the intelligence community has been the subject of independent studies,[428] and members of Congress have recently warned that their ability to conduct effective oversight is being stymied by a variety of factors.[429] How to ensure adequate congressional oversight of intelligence activities is a question that goes beyond the scope of this report. In light of the expanding authorities of both the law enforcement and intelligence community, however, rigorous and effective Congressional oversight is imperative and must be a part of any discussion and solution.

V. CONCLUSION

In the wake of September 11, 2001, the verdict was clear: The failure of law enforcement and intelligence agencies to share critical information had contributed directly to the devastating success of the attacks. The government thus designed a series of both bureaucratic and physical structures to collect, share, and retain increasing volumes of information about its own people. The mantra of "connecting the dots" took hold, and little distinction was made between items of information that trigger suspicion and items that do not.

In the post-9/11 era, multiple government agencies acquire an ever-increasing amount of information about Americans who are not suspected of any criminal activity; keep it for extended lengths of time; and share it widely with other agencies, private entities, and foreign governments. Records that used to require a substantial commitment of physical space can now be "efficiently mine[d] … for information years into the future."[430] Although written policies govern this retention and sharing in many instances, that is not always the case, and the policies that do exist often vitiate, in practice, the procedural protections guaranteed by the Privacy Act.

Mounting, bipartisan evidence has demonstrated, however, that the widescale collection and retention of personal information about Americans not suspected of criminal activity invites abuse without any significant demonstrated benefit. The increasing ease of collecting and keeping a "substantial quantum of intimate information about any person … may 'alter the relationship between citizens and government in a way that is inimical to democratic society.'"[431]

Now is the time to adopt policies that allow the government to carry out its vital law enforcement and security missions while ensuring that the government is not constructing near-permanent electronic dossiers on every citizen and resident. Failure to do so risks the diminution of our democracy.

ENDNOTES

1 Select Comm. to Study Gov't Operations with Respect to Intelligence Activities, Final Report, S. Rep. No. 94-755, bk. III, at 778 (1976) [hereinafter Church Committee Report], *available at* http://www.intelligence.senate.gov/churchcommittee.html.

2 Matt Sledge, *CIA's Gus Hunt On Big Data: We 'Try to Collect Everything and Hang On To It Forever,'* Huffington Post (Mar. 20, 2013, 4:52 PM EST), www.huffingtonpost.com/mobileweb/2013/03/20/cia-gus-hunt-big-data_n_2917842.html.

3 U.S. v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

4 *See* Emily Berman, Brennan Ctr. for Justice, Domestic Intelligence: New Powers, New Risks (2011), *available at* http://www.brennancenter.org/publication/domestic-intelligence-new-powers-new-risks; Faiza Patel, Brennan Ctr. for Justice, Rethinking Radicalization (2011), *available at* http://www.brennancenter.org/sites/default/files/legacy/RethinkingRadicalization.pdf.

5 Specifically, this report focuses on "U.S. persons": U.S. citizens and lawful permanent residents as defined in 50 U.S.C. § 1801(i). This definition of U.S. persons also includes certain corporations or unincorporated associations, but this report does not address corporate privacy issues.

6 *See*, *e.g.*, Nat'l Comm'n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report 181-82, 192-93 (2004) [hereinafter 9/11 Commission Report], *available at* http://www.9-11commission.gov/report/911Report.pdf.

7 *See*, *e.g.*, John Villasenor, Brookings Inst., Recording Everything: Digital Storage as an Enabler of Authoritarian Governments 3-4 (2011), *available at* http://www.brookings.edu/~/media/research/files/papers/2011/12/14%20digital%20storage%20villasenor/1214_digital_storage_villasenor.pdf; Jennifer Valentino-DeVries, *The Economics of Surveillance*, Wall St. J., Sept. 28, 2012 (noting that storage and use of a gigabyte of information, which cost almost $19 in 2005, cost less than $2 in 2012, and is expected to drop to 66 cents in 2015), *available at* http://blogs.wsj.com/digits/2012/09/28/the-economics-of-surveillance/.

8 *See* Jeff Jonas & Jim Harper, Cato Inst., Policy Analysis No. 584: Effective Counterterrorism and the Limited Role of Predictive Data Mining (2006), *available at* http://www.cato.org/publications/policy-analysis/effective-counterterrorism-limited-role-predictive-data-mining. Jonas and Harper observe, for instance, that "[c]orporations that study consumer behavior have millions of patterns that they can draw upon to profile their typical or ideal consumer. … Terrorism has no similar indicia. With a relatively small number of attempts every year and only one or two major terrorist incidents every few years – each one distinct in terms of planning and execution – there are no meaningful patterns that show what behavior indicates planning or preparation for terrorism." *Id.* at 7-8.

9 The collection, retention, and dissemination of innocuous information is problematic across a range of circumstances, and other groups have authored compelling works on the particular dangers posed to immigrant communities, among others. *See, e.g.*, Jennifer Lynch, Elec. Frontier Found. & Immigration Policy Ctr., From Fingerprints to DNA: Biometric Collection in U.S. Immigrant Communities and Beyond (2012), *available at* https://www.eff.org/sites/default/files/filenode/BiometricsImmigration052112.pdf. Those issues are important as well; however, this report focuses particularly on U.S. persons to highlight the risks to individuals who do not otherwise have reason to come to the attention of the government.

10 *See generally* Church Committee Report, *supra* note 1, bk. II, at 66, 77, 84-89, 99-102, 170, 211-16. http://www.intelligence.senate.gov/churchcommittee.html. *See also* Christopher M. Ford, *Intelligence Demands in a Democratic State: Congressional Intelligence Oversight*, 81 Tul. L. Rev. 721, 737-38 (2007).

11 *See*, *e.g.*, *A Look Back… The Church Committee Meets*, CIA (Mar. 27, 2008, 6:55 AM) https://www.cia.gov/news-information/featured-story-archive/2008-featured-story-archive/a-look-back-the-church-committee-meets.html.

12 *See* Church Committee Report, *supra* note 1, bk II, at 8-9; *id.*, bk. III, at 155, 158-60. *See also* Ford, *supra* note 10, at 738; *see also Like All Frauds Your End is Approaching*, Letters of Note (Jan. 5, 2012), http://www.lettersofnote.com/2012/01/king-like-all-frauds-your-end-is.html.

13 Church Committee Report, *supra* note 1, bk. II, at 255.

14 *Id.* at 253-59.

15 *Id.*, bk. III, at 693-94.

16 *Id.* at 694.

17 *Id.* at 719-20.

18 *Id.* at 713-14.

19 *Id*. at 716.
20 *Id*. at 695.
21 *Id*. at 738.
22 *Id*. at 746.
23 *Id*. at 740, 743-44, 749-50, 767-70.
24 *Id*. at 778.
25 *Id*., bk. II, at 6, 58.
26 *Id*., bk. III, at 778.
27 Privacy Act of 1974, Pub. L. No. 93-579, § 3, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a(e)(1) (2013)).
28 Privacy Act of 1974, Pub. L. No. 93-579, § 3, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a(e)(4)).
29 Privacy Act of 1974, Pub. L. No. 93-579, § 3, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a(d) (2013)).
30 Privacy Act of 1974, Pub. L. No. 93-579, § 3, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a(e)(7) (2013)).
31 5 U.S.C. § 552a(a)(7), (b)(3), (e)(4)(D).
32 System of Records Notice, 66 Fed. Reg. 33558 (June 22, 2001), available at http://www.fbi.gov/foia/privacy-act/66-fr-33558.
33 *See*, *e.g.*, U.S. Gov't Accountability Office, GAO-08-536, Alternatives Exist for Enhancing Protection of Personally Identifiable Information 32-42 (2008) [hereinafter Alternatives Exist], *available at* http://www.gao.gov/assets/280/275558.pdf.
34 *See* Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, Wall St. J., Dec. 12, 2012, at A1, *available at* http://online.wsj.com/article_email/SB10001424127887324478304578171623040640006-lMyQjAxMTAyMDEwMzExNDMyWj.html?mod=wsj_valettop_email.
35 *See* Alternatives Exist, *supra* note 33, at 39.
36 For an extensive history and analysis of the Levi Guidelines and the subsequent Attorney General's Guidelines, *see* Berman, *supra* note 4.
37 Edward H. Levi, U.S. Dep't of Justice, Domestic Security Investigation Guidelines § I.A, I-II (1976) (hereinafter Levi Guidelines); *Id.* §§ I-II. *See also FBI Oversight: Hearing Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 95th Cong. § II.A, at 521-60 (1976).
38 Levi Guidelines, *supra* note 37, § II.B.
39 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 105(a)(3)(A), 92 Stat. 1790 (codified as amended at 50 U.S.C. § 1805(a)(3)(A), (e) (2000)). For the definition of U.S. person, *see* 50 U.S.C. § 1801(i) (2012).
40 MeriTalk & NetApp, Beacon Report: Big Data, Big Brains 1 (2012), *available at* www.meritalk.com/bigdatagap; *see also* Scott M. Fulton, *U.S. Government Has More 'Big Data' Than It Knows What to Do With*, ReadWrite.com (May 10, 2012), http://readwrite.com/2012/05/10/us-government-has-more-big-data-than-it-knows-what-to-do-with.
41 USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 365 (codified as amended at 50 U.S.C. § 1861(a)(1) (2012)). *See also* 1 David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions 2d, at 349 (2d ed. 2012).
42 *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian, June 5, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also* Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*,Wall St. J., July 8, 2013, *available at* http://online.wsj.com/article/SB10001424127887323873904578571893758853344.html.
43 USA PATRIOT Act, Pub. L. No. 107-56, § 505, 115 Stat. 365 (codified as amended at 18 U.S.C. § 2709(b) (2012) and 12 U.S.C. § 3414(a)(5)(A) (2012)).
44 USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 365 (codified as amended at 50 U.S.C. § 1861(b)(2)(A) (2012)); USA PATRIOT Act, Pub. L. No. 107-56, § 505, 115 Stat. 365 (codified as amended at 18 U.S.C. § 2079(b) (2012)); 5 U.S.C. § 552a(e)(7) (2013).
45 USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 365 (codified as amended at 50 U.S.C. § 1861(a)(1) (2012)); USA PATRIOT Act, Pub. L. No. 107-56, § 505, 115 Stat. 365 (codified as amended at 18 U.S.C. § 2709(b) (2012)).
46 Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552; FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436; *see also* James Risen, *Bush Signs Law to Broaden Reach of Wiretapping*, N.Y. Times, Aug. 6, 2007, *available at* http://www.nytimes.com/2007/08/06/washington/06nsa.html; Shailagh Murray, *Obama Joins Fellow Senators in Passing New Wiretapping Measure*, Wash. Post, July 10, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/07/09/AR2008070901780.html.

47 FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436 (codified as amended at 50 U.S.C. § 1881a (2013)).

48 *How the NSA's Surveillance Procedures Threaten Americans' Privacy*, Am. Civil Liberties Union (June 21, 2013), https://www.aclu.org/nsa-surveillance-procedures; Amy Davidson, *How Many Americans Does the N.S.A. Spy On? A Lot of Them*, The New Yorker, June 21, 2013, *available at* http://www.newyorker.com/online/blogs/closeread/2013/06/how-many-americans-does-the-nsa-spy-on-a-lot-of-them.html; Benjamin Wittes, *The Minimization and Targeting Procedures: An Analysis*, Lawfare (June 13, 2013, 4:19 PM), http://www.lawfareblog.com/2013/06/the-miminization-and-targeting-procedures-an-analysis/.

49 John Ashcroft, U.S. Dep't of Justice, The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations § VI.A., B. (2002) [hereinafter Ashcroft Guidelines]; Berman, *supra* note 4, at 17.

50 Michael Mukasey, U.S. Dep't of Justice, The Attorney General Guidelines for Domestic FBI Operations § II (2008) [hereinafter Mukasey Guidelines], *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf; *see also* Berman, *supra* note 4, at 22.

51 9/11 Commission Report, *supra* note 6, at 79; *see also* Lawrence Wright, *The Agent*, The New Yorker, July 10, 2006, *available at* http://www.newyorker.com/archive/2006/07/10/060710fa_fact_wright#ixzz2FoIashwe.

52 9/11 Commission Report, *supra* note 6, at 7-9; *see also* Jonas & Harper, *supra* note 8, at 2 ("In the days and months before 9/11, new laws and technologies like predictive data mining were not necessary to connect the dots. What was needed to reveal the remaining 9/11 conspirators was better communication, collaboration, a heightened focus on the two known terrorists, and traditional investigative processes."); *id.* at 2-4 (detailing the connections among the terrorists and the way the attackers were "hiding in plain sight").

53 Privacy Act of 1974, Pub. L. No. 93-579, § 3, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552 (2013)).

54 Church Committee Report, *supra* note 1.

55 Levi Guidelines, *supra* note 37.

56 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 105(a)(3)(A), 92 Stat. 1790 (codified at 50 U.S.C. § 1805(a)(3)(A), (e) (2000)).

57 USA PATRIOT Act, Pub. L. No. 107-56, § 203(b)(1), 115 Stat. 365 (codified as amended at 18 USC § 2517(6) (2013)); USA PATRIOT Act, Pub. L. No. 107-56, § 203(a)(1), d(1), 115 Stat. 365 (codified as amended at Fed. R. Civ. P. 6(e)(3)(C), (e)(3)(C)(i)(V) (2001) (repealed)).

58 Homeland Security Act of 2002, Pub. L. No. 107-296, § 892, 116 Stat. 2253 (codified at 6 U.S.C § 482).

59 Memorandum from John Ashcroft, U.S. Att'y Gen., to the Deputy Att'y Gen. et al., Coordination of Information Relating to Terrorism (April 11, 2002), *available at* http://www.fas.org/irp/agency/doj/agdirective6.pdf; Ashcroft Guidelines, *supra* note 49.

60 Ashcroft Guidelines, *supra* note 49.

61 E-Government Act of 2002, Public Law 107-347, §208, 116 Stat. 2899 (codified as amended at 44 U.S.C. Ch. 36). In fact, the notion of "personally identifiable information" is being called into question by privacy scholars as the growing multitude of databases increasingly makes identification of individuals easier even where information has supposedly been anonymized. *See, e.g.*. Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information,"* 53 Communications of the ACM 24, *available at* http://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, *available at* http://www.uclalawreview.org/?p=1353.

62 U.S. Dep't of Justice et al., Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (2003), *available at* http://www.fas.org/sgp/othergov/mou-infoshare.pdf.

63 Directive on Integration and Use of Screening Information to Protect Against Terrorism, 39 Weekly Comp. Pres. Doc. 1234 (Sept. 16, 2003) *available at* http://www.gpo.gov/fdsys/pkg/WCPD-2003-09-22/pdf/WCPD-2003-09-22-Pg1234-2.pdf. (directing heads of executive departments and agencies to provide terrorist information to the TTIC), Terrorism information constitutes "all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to — (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals." Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016(a)(4), 118 Stat. 3665 (codified as amended at 6 U.S.C. § 485(a)(5)(2012)).

64 *See, e.g.*, *National Network of Fusion Centers Fact Sheet*, U.S. Dep't of Homeland Sec., http://www.dhs.gov/national-network-fusion-centers-fact-sheet (last visited Feb. 14, 2013).

65 9/11 Commission Report, *supra* note 6.

66 *See* Exec. Order No. 13,356, 69 Fed. Reg. 53,599 (Aug. 27, 2004), *revoked by* Exec. Order. No. 13,388, 70 Fed. Reg. 62,023 (Oct. 25, 2005).

67 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016, 118 Stat. 3638 (codified as amended at 6 U.S.C. § 485 (2012)).

68 Exec. Order No. 13,388, 70 Fed. Reg. 67,325 (Oct. 25, 2005).

69 James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0.

70 USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192.

71 Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 205, 121 Stat. 308 (codified as amended at 6 U.S.C. § 124b (2012)).

72 Federal Agency Data Mining Reporting Act of 2007, Pub. L. No. 110-53, § 804, 121 Stat. 266 (codified as amended at 42 U.S.C. § 2000ee–3 (2013)).

73 Office of the Inspector Gen., U.S. Dep't of Justice, A Review of the Federal Bureau of Investigation's Use of National Security Letters (2007) [hereinafter 2007 OIG Report], *available at* https://www.fas.org/irp/agency/doj/oig/natsec.pdf; Office of the Inspector Gen., U.S. Dep't of Justice, A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records (2007), *available at* http://www.justice.gov/oig/special/s0703a/final.pdf

74 Protect America Act of 2007, Pub. L. No. 110-55, §102, 121 Stat. 552 (codified at 50 U.S.C. §§ 1805a-1805c (repealed 2008)).

75 Exec. Office of the President, National Strategy for Information Sharing app. 1, at A1-6 to A1-7 (2007), *available at* www.ise.gov/sites/default/files/nsis_book.pdf.

76 FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436 (codified as amended at 50 U.S.C. § 1881a (2013)).

77 Mukasey Guidelines, *supra* note 50, § II.A., at 19-20.

78 *National Security Letters Reform Act of 2007: Hearing on H.R. 3189 Before the Subcomm. on the Constitution, Civil Rights and Civil Liberties of the H. Comm. on the Judiciary*, 110th Cong. 91-109 (2008) [hereinafter *2008 NSL Hearing 1*], *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg41795/pdf/CHRG-110hhrg41795.pdf (statement of David Kris, Former Deputy Attorney Gen., U.S. Dep't of Justice); *National Security Letters: The Need for Greater Accountability and Oversight: Hearing Before the S. Comm. on the Judiciary,* 110th Cong. 8-11 (2008) [hereinafter *2008 NSL Hearing 2*], *available at* https://www.fas.org/irp/congress/2008_hr/letters.html (statement of James A. Baker, Former Counsel for Intelligence Policy, U.S. Dep't of Justice); *id*. at 7-8 (statement of Sheldon Whitehouse, Sen., U.S. Congress).

79 U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Border Searches of Electronic Devices (2009) [hereinafter 2009 Border Searches PIA], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.

80 Office of the Dir. of Nat'l Intelligence & U.S. Dep't of Justice, Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information Datasets Containing Non-Terrorism Information 9, 11 (2012) [hereinafter 2012 NCTC Guidelines], *available at* http://www.fas.org/sgp/othergov/intel/nctc_guidelines.pdf.

81 Staff of the Subcomm. on Investigations of the S. Comm. on Homeland Sec., 112th Cong., Federal Support for and Involvement in State and Local Fusion Centers 1, 27 (Comm. Print 2012) [hereinafter Federal Support for Fusion Centers], *available at* http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

82 Church Committee Report, *supra* note 1, bk. III, at 778.

83 *Id.* at 717.

84 *See* Barton Gellman, *NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds*, Wash. Post, Aug. 15, 2013, *available at* http://articles.washingtonpost.com/2013-08-15/world/41431831_1_washington-post-national-security-agency-documents.

85 *See*, *e.g.*, Adam Gabbatt and agencies, *NSA Analysts 'Wilfully Violated' Surveillance Systems, Agency Admits*, Guardian, Aug. 24, 2013, *available at* http://www.theguardian.com/world/2013/aug/24/nsa-analysts-abused-surveillance-systems; Chris Strohm, *Lawmakers Probe Willful Abuses of Power by NSA Analysts*, Bloomberg, Aug. 24, 2013, *available at* http://www.bloomberg.com/news/2013-08-23/nsa-analysts-intentionally-abused-spying-powers-

multiple-times.html; *see also* Press Release, Sen. Chuck Grassley, Grassley Presses for Details about Intentional Abuse of NSA Authorities (Aug. 28, 2013), *available at* http://www.grassley.senate.gov/news/Article.cfm?customel_dataPageID_1502=46858.

86 *See*, *e.g.*, Dan Farber, *President Obama Outlines Four NSA Reform Initiatives*, CNET (Aug. 9, 2013, 1:13 PM), http://news.cnet.com/8301-13578_3-57597814-38/president-obama-outlines-four-nsa-reform-initiatives/ (quoting President Obama as saying that NSA "programs are operating in a way that prevents abuse"); Edward Moyer, *NSA Admits to Some Deliberate Privacy Violations*, CNET (Aug. 23, 2013, 1:08 PM), http://news.cnet.com/8301-13578_3-57599916-38/nsa-admits-to-some-deliberate-privacy-violations/ (noting that in early August, NSA Director Keith Alexander said that "no one has willfully or knowingly disobeyed the law or tried to invade your civil liberties or privacy").

87 Office of the Inspector Gen., U.S. Dep't of Justice, A Review of the FBI's Investigations of Certain Domestic Advocacy Groups (2010) [hereinafter 2010 DOJ IG Report], *available at* http://www.justice.gov/oig/special/s1009r.pdf.

88 *Id.* at 176.

89 *Id.* at 184.

90 *Id.* at 183.

91 *Id.* at 182.

92 Muslim Am. Civil Liberties Coal. et al., Mapping Muslims: NYPD Spying and its Impact on American Muslims 29-32 (2013) [hereinafter Mapping Muslims], *available at* http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

93 *Id.* at 40-45.

94 Fed. Bureau of Investigation, Domestic Investigations and Operations Guide §§ 4.3.3.2.1 to .2 (2011) [hereinafter 2011 DIOG], *available at* http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version.

95 *United States v. Robinson*, No. 5:07-cr-00596-JF (N.D. Cal. Aug. 25, 2009); Henry K. Lee, *Ex-Agent Indicted in Misuse of Database*, S.F. Gate (Sept. 19, 2007, 4:00 AM), http://www.sfgate.com/bayarea/article/Ex-agent-indicted-in-misuse-of-database-2522021.php.

96 Scott Zamost & Kyra Phillips, *FBI Misconduct Reveals Sex, Lies and Videotape*, CNN (Jan. 27, 2011, 10:07 AM), http://articles.cnn.com/2011-01-27/us/siu.fbi.internal.documents_1_fbi-employees-occasional-employee-fbi-s-office?_s=PM:US.

97 *Statement-Kirsten Atkins, Target of Illegal Spying*, Am. Civil Liberties Union (Feb. 22, 2006), http://www.aclu.org/national-security/statement-kirsten-atkins-target-illegal-spying.

98 *Utah Launches Investigation of Leak of Immigrants' Information*, CNN (July 22, 2010, 4:12 PM), http://www.cnn.com/2010/US/07/22/utah.attorney.general/index.html?eref=rss_latest&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+rss%2Fcnn_latest+%28RSS%3A+Most+Recent%29.

99 *See*, *e.g.*, Danielle Bell, *Ottawa Cop Demoted for Database Misuse*, Ottawa Sun, Sept. 26, 2012, *available at* http://www.ottawasun.com/2012/09/26/ottawa-cop-demoted-for-misuse-of-data-bases (senior staff sergeant accessed police databases 169 times over nearly four years for personal reasons); *Former Montreal Detective Used Police Database to Help Mafia*, Toronto Sun, Nov. 22, 2012, *available at* http://www.torontosun.com/2012/11/22/former-montreal-detective-used-police-database-to-help-mafia# (Montreal police detective used a police database to run license plates and pass information to members of an organized crime syndicate); Christine Hauser, *Sergeant Said to Misuse Terror-Watch Database*, N.Y. Times, Nov. 21, 2008, at A31, *available at* http://www.nytimes.com/2008/11/21/nyregion/21sergeant.html; *see also* Sewell Chan, *Police Sergeant Guilty of Misusing Terror Database*, N.Y. Times, Jan. 14, 2009, http://cityroom.blogs.nytimes.com/2009/01/14/police-sergeant-pleads-guilty-to-misusing-database/ (reporting that a New York City police sergeant illicitly used a state database to retrieve information from a national terrorist watch list for an acquaintance involved in a child-custody case); Lee, *supra* note 95 (special agent with U.S. Commerce Department indicted in 2007 by federal grand jury for misusing a federal database to track a former girlfriend and her family; agent had previously threatened to kill the girlfriend or have her and her family deported, and he accessed database over 150 times in a one-year period to monitor her movements); Jessica Lussenhop, *Is Anne Marie Rasmusson Too Hot to Have a Driver's License?*, City Pages (Feb. 22, 2012), http://www.citypages.com/2012-02-22/news/is-anne-marie-rasmusson-too-hot-to-have-a-driver-s-license/ (over a hundred officers from eighteen agencies across Minnesota accessed the driving records of a female ex-police officer to look at her picture and glean personal details about her, claiming the practice was common place despite state laws requiring all searches to have an investigative purpose); Tom Lyons, *The Odd Loose Ends in Database Misuse*, Sarasota Herald-Tribune, Oct. 11, 2012, at BNV1, *available at* http://www.heraldtribune.com/article/20121011/ARCHIVES/210111025 (secretaries at Florida state attorney's office accessed driver and

vehicle information database, limited to official police and prosecutorial use, to perform unauthorized searches for information on candidate for state attorney); Allison Manning, *Cops Criticized for 'Misuse' of Databases*, PoliceOne.com (Apr. 2, 2012), http://www.policeone.com/police-products/software/Data-Information-Sharing-Software/articles/5360910-Cops-criticized-for-misuse-of-databases/ (last visited Sept. 23, 2013) (officials misusing police databases in Ohio included police officer who looked up a woman's personal information and stopped her car more than a dozen times, police officer who "threw items into the front yard of two people he looked up," and three deputies who looked up the "wife of a man with whom one of the deputies had a dispute"); *Former Montgomery Co. Officer Guilty of Police Database Misuse*, Daily Record (Apr. 27, 2011, 4:46 PM), http://thedailyrecord.com/2011/04/27/former-montgomery-co-officer-guilty-of-police-database-misuse/ (former police officer accessed law enforcement databases to assist her drug-dealing fiancé); Levi Pulkkinen, *IRS Worker Caught Snooping on Ex, Others,* SeattlePi.com (Apr. 23, 2012, 9:44 PM), http://www.seattlepi.com/local/article/IRS-worker-caught-snooping-on-ex-others-3498550.php (IRS technician who had previously looked up her ex-husband's tax return pled guilty to misusing her access to IRS databases to review other people's personal information, including a relative with whom she had had a falling out); Aaron Rupar, *In Minneapolis, Private Information Database Abuse 'Endemic,' Attorney Says*, City Pages (Sept. 26, 2012, 12:27 PM), http://blogs.citypages.com/blotter/2012/09/in_minneapolis_private_information_database_abuse_endemic_attorney_says.php (employees in Minneapolis's department of housing charged with accessing driver's license databases for personal purposes; one of the employees also shared his log-in information with other employees).

100 *See* Rick Rogers, *Records Detail Security Failure in Base File Theft*, San Diego Union-Tribune, May 22, 2008, *available at* http://www.utsandiego.com/uniontrib/20080522/news_1n22theft.html; *Law Enforcement Records Sought in Stolen Pendleton Surveillance Documents*, Am. Civil Liberties Union (July 15, 2008), http://www.aclusandiego.org/presidential-power/presidential-power-presidential-power/law-enforcement-records-sought-in-stolen-pendleton-surveillance-documents-massive-number-of-files-stolen-according-to-press-report/.

101 U.S. Gov't Accountability Office, GAO-12-961T, Federal Law Should Be Updated to Address Changing Technology Landscape 13 (2012), *available at http://www.gao.gov/assets/600/593146.pdf* (statement of Gregory Wilshusen).

102 *Id.* at 10.

103 *See* Lisa Rein, *Police Spied on Activists In Md.*, Wash. Post, July 18, 2008, *available at* http://articles.washingtonpost.com/2008-07-18/news/36816482_1_peace-activists-state-police-police-superintendent; Lisa Rein & Josh White, *Little Data Disclosed In Files, Activists*, Wash. Post, Nov. 20, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/story/2008/11/20/ST2008112000054.html; Lisa Rein & Josh White, *More Groups Than Thought Monitored in Police Spying*, Wash. Post, Jan. 4, 2009, *available at* http://articles.washingtonpost.com/2009-01-04/news/36854512_1_undercover-trooper-current-police-superintendent-white-supremacist-group.

104 Alternatives Exist, *supra* note 33, at 35.

105 The White House, Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack 3 (n.d.), *available at* http://www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf.

106 *Lessons from Fort Hood: Improving Our Ability to Connect the Dots: Hearing Before the Subcomm. on Oversight, Investigations, and Mgmt. of the H. Comm. on Homeland Security*, 112th Cong. 2 (2012) (statement of Douglas E. Winter, Deputy Chair, William H. Webster Commission on the Fed. Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas on November 5, 2009).

107 David Ignatius, *A Breakdown in CIA Tradecraft*, Wash. Post, Jan. 6, 2010, *available at* http://articles.washingtonpost.com/2010-01-06/opinions/36805490_1_cia-base-cia-veteran-agency-officers.

108 Federal Support for Fusion Centers, *supra* note 81, at 27.

109 *Id*. The Church Committee highlighted this problem some thirty-five years ago when it observed that "the amount [of information] disseminated within the Executive branch has often been so voluminous as to make it difficult to separate useful data from worthless detail." Church Committee Report, *supra* note 1, bk II, at 253.

110 Dana Priest & William Arkin, *Top Secret America: A Hidden World, Growing Beyond Control*, Wash. Post, July 19, 2010, *available at* http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/.

111 John M. Broder, *Stalled Out on Tesla's Electric Highway*, N.Y. Times, Feb. 8, 2013, *available at* http://www.nytimes.com/2013/02/10/automobiles/stalled-on-the-ev-highway.html?pagewanted=1&_r=0.

112 Elon Musk, *A Most Peculiar Test Drive*, Tesla Motors (Feb. 13, 2013), http://www.teslamotors.com/blog/most-peculiar-test-drive.

113 *Id.*

114 *See, e.g.*, Rebecca Greenfield, *Elon Musk's Data Doesn't Back Up His Claims of New York Times Fakery*, The

Atlantic Wire (Feb. 14, 2013), http://www.theatlanticwire.com/technology/2013/02/elon-musks-data-doesnt-back-his-claims-new-york-times-fakery/62149/; Peter Valdes-Dapena, *Test Drive: DC to Boston in a Tesla Model S*, CNNMoney (Feb. 25, 2013), http://money.cnn.com/2013/02/15/autos/tesla-model-s/.

115 John M. Broder, *That Tesla Data: What it Says and What it Doesn't*, N.Y. Times, Feb. 14, 2013, *available at* http://wheels.blogs.nytimes.com/2013/02/14/that-tesla-data-what-it-says-and-what-it-doesnt/.

116 *See* Bruce Schneier, *Automobile Data Surveillance and the Future of Black Boxes*, Schneier.com (Feb. 18, 2013), http://www.schneier.com/blog/archives/2013/02/automobile_data.html.

117 *Id.*

118 *See*, *e.g.*, David Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 Yale L.J. 628, 630-1 (2005) ("The 'mosaic theory' describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. … Since the attacks of September 11, 2001 … the mosaic theory has made a comeback.").

119 Mary DeRosa, Ctr. for Strategic and Int'l Studies, Data Mining and Data Analysis for Counterterrorism 4 (2004), *available at* http://csis.org/files/media/csis/pubs/040301_data_mining_report.pdf; K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, Colum. Sci. & Tech. L. Rev., Dec. 2003, at 1, 22-23, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=546782 ("Data mining generally identifies patterns or relationships among data items or records that were not previously identified (and are not themselves data items) but that are revealed in the data itself. Thus, data mining extracts information that was *previously unknown.*") (internal citations omitted).

120 *See*, *e.g.*, Privacy Office, Dep't of Homeland Sec., 2012 Data Mining Report to Congress i-ii (2013), *available at* http://www.dhs.gov/sites/default/files/publications/privacy/Reports/2012-data-mining-report-to-congress.pdf (noting that the Homeland Security Act of 2002, as amended, authorized DHS to use data mining).

121 JASON, Mitre Corp., Rare Events § 1.5, at 8 (2009), *available at* http://www.fas.org/irp/agency/dod/jason/rare.pdf. A National Academies of Science report echoed this finding, determining that terrorist identification via data mining (or by "any other known methodology") was "neither feasible as an objective nor desirable as a goal of technology development efforts." Nat'l Research Council, Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment 3-4 (2008), *available at* http://epic.org/misc/nrc_rept_100708.pdf.

122 *See* DeRosa, *supra* note 119, at 3-4. While these connections may be hard to find because of the *volume* of data, they do not require predictions about future events. The conclusions of the 9/11 Commission suggest that subject-based data analysis could have helped unravel the plot and prevent the attacks.

123 *See* Bruce Schneier, *Why Data Mining Won't Stop Terror*, Wired, Mar. 9, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/03/70357?currentPage=all; *see also* Richard Barrington, *2011 Credit Card Facts and Statistics*, IndexCreditCards (Jan. 10, 2011) http://www.indexcreditcards.com/finance/creditcardstatistics/2011-report-on-credit-card-usage-facts-statistics.html (noting that as of 2010, there were nearly 1.5 billion credit cards in circulation in the United States, and nearly 55 million credit card transactions every day).

124 *See* Jonas & Harper, *supra* note 8, at 7-8 ("With a relatively small number of attempts every year and only one or two major terrorist incidents every few years – each one distinct in terms of planning and execution – there are no meaningful patterns that show what behavior indicates planning or preparation for terrorism. Unlike consumers' shopping habits and financial fraud, terrorism does not occur with enough frequency to enable the creation of valid predictive models").

125 Patel, *supra* note 4, at 8; Marc Sageman, Leaderless Jihad: Terror Networks in the Twenty-First Century 72 (2008); Clark McCauley & Sophia Moskalenko, *Mechanisms of Political Radicalization: Pathways Toward Terrorism*, 20 Terrorism & Political Violence 415, 418 (2008); Richard English, Terrorism: How to Respond 52 (2009).

126 Schneier, *supra* note 123.

127 *Id*. The Department of Defense JASON study described this problem as the high risk of "false alarm rates … in the face of massive clutter." JASON, *supra* note 121, at 1.

128 Jonas & Harper, *supra* note 8, at 1.

129 *See*, *e.g.*, DeRosa, *supra* note 119, at 12 ("Terrorist plots are rare and difficult to predict reliably, but preparatory and planning activities in which terrorists engage can be identified. Detecting combinations of these low-level activities – such as illegal immigration, operating front businesses, money transfers, use of drop boxes and hotel addresses for commercial activities, and having multiple identities – could help predict terrorist plots."); Siobhan O'Neil, Cong. Research Serv., RL34014, Terrorist Precursor Crimes: Issues and Options for Congress 1 (2007), *available at* http://www.fas.org/sgp/crs/terror/RL34014.pdf ("Irrespective of ideology or strategic goals, all

terrorist groups have several basic needs in common: funding, security, operatives/support, propaganda, and means and/or appearance of force. In order to meet these needs, terrorists engage in a series of activities, some of which are legal, many of which are not, including various fraud schemes, petty crime, identity and immigration crimes, the counterfeit of goods, narcotics trade, and illegal weapons procurement, amongst others."); *see also* M. Elaine Nugent, et. al., Am. Prosecutors Research Institt., Local Prosecutors' Response to Terrorism (2005), *available at* https://www.ncjrs.gov/pdffiles1/nij/grants/211202.pdf.

130 9/11 Commission Report, *supra* note 6, at 424. Similarly, the would-be Millenium bomber Ahmed Ressam and his collaborators "were reported to all be involved in a series of criminal activities, to include credit card fraud, pick pocketing, shoplifting, and stealing identity documents." O'Neil, *supra* note 129, at 20; *see also* David E. Kaplan, *Paying for Terror: How Jihadist Groups Are Using Organized-Crime Tactics – and Profits – to Finance Attacks on Targets Around the Globe*, U.S. News & World Report, Nov. 27, 2005, *available at* http://www.usnews.com/usnews/news/articles/051205/5terror.htm (noting that the 2004 Madrid train bombings were financed "almost entirely with money earned from trafficking in hashish and ecstasy").

131 *See Careers*, Nat'l Counterterrorism Ctr., http://www.nctc.gov/careers/careers.html (last visited Sept. 9, 2013).

132 National Security Act of 1947, Pub. L. No. 80-235, 61 Stat. 496 (codified as amended at 50 U.S.C. ch. 15(2007)); U.S. Dep't of Justice et al., *supra* note 62. The Center was also given the authority to "receive, retain, and disseminate information" from any domestic government agency or other source; each agency that holds terrorism information must provide the Center with access to the information. Exec. Order No. 13,354, 69 FR 53,589 (Aug. 27, 2004), *available at* www.gpo.gov/fdsys/pkg/FR-2004-09-01/pdf/04-20050.pdf.

133 50 U.S.C. § 404*o*(e)(2) (2013).

134 Fed. Bureau of Investigation, National Information Sharing Strategy 5 (2008), *available at* http://www.hsdl.org/?view&did=29800.

135 Walter Pincus & Dan Eggen, *325,000 Names on Terrorism List*, Wash. Post, Feb. 14, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021402125.html; *see also Ten Years After 9/11: Are We Safer?: Hearing Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 112th Cong. (2011) (statement of Matthew Olsen, Director, Nat'l Counterterrorism Ctr.), *available at* http://www.dni.gov/files/documents/Newsroom/Testimonies/20110913_testimonies_olsen.pdf.

136 Nat'l Counterterrorism Ctr., Symposium Overview of NCTC's Data Access as Authorized by the 2012 Attorney General Guidelines (2013) (on file with author).

137 *See* U.S. Attorney Gen. & Dir. of Nat'l Intelligence, Memorandum of Agreement between the Attorney General and the Director of National Intelligence on Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center of Terrorism Information Contained with Datasets Identified as Including Non-Terrorism Information and Information Pertaining Exclusively to Domestic Terrorism (2008), *available at* http://www.fas.org/sgp/othergov/intel/nctc-moa2008.pdf.

138 *Id.* at 5-7.

139 *Id.* at 6.

140 *Id.* at 3; Civil Liberties and Privacy Office, Office of the Dir. of Nat'l Intelligence, Information Paper: Description of Civil Liberties and Privacy Protections Incorporated in the Updated NCTC Guidelines 1 (2013), *available at* http://nctc.gov/docs/CLPO_Information_Paper_on_NCTC_AG_Guidelines_-_1-22-13.pdf.

141 2012 NCTC Guidelines, *supra* note 80.

142 *Id*. at 8-9. The Guidelines also require that "terms and conditions" be developed to govern the process by which the NCTC accesses or acquires each dataset or database from another federal agency (which are referred to as "data providers"). *Id*. at 3, 5-6. Those Terms and Conditions documents have not yet been made public.

143 *Id*. at 9-10. Notably, this five-year window is defined as the "temporary retention period"; the permanent retention period for actual terrorism information is far longer. It also appears that the NCTC could access information via Tracks 1 or 2, determine that it warrants more study, and make a "determination" that Track 3 acquisition and replication is necessary, starting the five-year clock at that point. According to the Guidelines, "the temporary retention period shall commence when the data is made generally available for access and use following both the determination period discussed … above, and any necessary testing and formatting." *Id.* at 9.

144 Office of the Dir. of Nat'l Intelligence, N1-576-09-1, Request for Records Disposition Authority (2009), *available at* http://www.archives.gov/records-mgmt/rcs/schedules/independent-agencies/rg-0576/n1-576-09-001_sf115.pdf. This schedule relates to terrorism information stored in NCTC's Terrorist Identities Datamart Environment (TIDE), retained under NCTC's Terrorist Identities Records SORN, ODNI/NCTC-009 (72 Fed. Reg. 73,896 (Dec. 28, 2007)). For Terrorism Information retained under NCTC's Knowledge Repository SORN, ODNI/NCTC-004 (76 Fed. Reg. 42,747 (July 19, 2011)), NCTC is currently working with the National Archives

and Records Administration (NARA), to develop a disposition schedule that will cover these records (See ODNI/NCTC-004, "Retention and Disposal" section). (Email from NCTC Civil Liberties and Privacy Officer, on file with author.)

145 2012 NCTC Guidelines, *supra* note 80, at 5.

146 *Id.* at 12 (emphasis added). The NCTC can also share information if it needs help determining whether the data is "terrorism information," though recipients are restricted from sharing the information further without approval of the NCTC. *Id*. at 12-13.

147 *Id*. at 13-14 (emphasis added).

148 *Id*. at 14-15.

149 *Id.* at 3.

150 *Id*. at 3-4; *see also* Office of the Dir. of Nat'l Intelligence, 2010 Data Mining Report 6 (2011), *available at* http://www.au.af.mil/au/awc/awcgate/dni/data_mining_report_for_jan-dec-2010.pdf.

151 *See, e.g.*, Ellen Nakashima, *FBI Shows Off Counterterrorism Database*, Wash. Post, Aug. 30, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/08/29/AR2006082901520.html; *see also* Elec. Frontier Found., Report on the Investigative Data Warehouse § 4 (2009) [hereinafter Report on IDW], *available at* https://www.eff.org/issues/foia/investigative-data-warehouse-report.

152 *See* Report on IDW, *supra* note 151 (identifying a number of the databases but noting that the names of others were redacted from documents provided in response to a FOIA request); *see also* Fed. Bureau of Investigation, N1-65-10-31, Request for Records Disposition Authority (2010), *available at* http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-10-031_sf115.pdf.

153 Nat'l Security Branch, Fed. Bureau of Investigation, The National Security Analysis Center: An Element of the FBI's National Security Branch 538 app. (2006), *available at* http://www.wired.com/images_blogs/threatlevel/2009/09/nsac_data_sets.pdf.

154 *See* Fed. Bureau of Investigation, Response to Investigative Data Warehouse (IDW) Press Article for Senate Appropriations Committee (2006), *available at* www.eff.org/files/filenode//092807_idw010000FBI-PIA-response.pdf [hereinafter FBI Response to IDW Press]. In addition, the e-Government Act of 2002 requires all agencies to conduct and publish Privacy Impact Assessments for electronic "information systems." The statute does not apply to national security systems, which would include the IDW, but the IDW carries out criminal as well as counterterrorism functions. *See* E-Government Act of 2002, Public Law 107-347, §208, 202(i), 116 Stat. 2899 (codified at 44 U.S.C. § 3501(2002)) (Privacy Provisions; National Security Systems); *see also* Memorandum from Joshua Bolten, Director, Office of Mgmt. & Budget, Exec. Office of the President, to Heads of Executive Departments and Agencies, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), *available at* www.whitehouse.gov/omb/memoranda_m03-22. Nevertheless, the FBI has asserted that the data warehouse is statutorily exempted from the e-Government Act as a national security system. Thus, although the FBI has evidently done a voluntary Privacy Impact Assessment for the IDW, it remains secret. FBI Response to IDW Press, *supra* note 154.

155 NARA Schedule N1-576-09-1, *supra* note 144.

156 *NSA Utah Data Center*, Facilities (Sept. 14, 2011), http://www.facilitiesmagazine.com/utah/buildings/nsa-utah-data-center.

157 *See* James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, Wired (Mar. 15, 2012, 7:24 PM), www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1; *see also NSA Utah Data Center*, *supra* note 156.

158 Bamford, *supra* note 157; *NSA Utah Data Center*, *supra* note 156.

159 Press Release, Nat'l Sec. Agency, Groundbreaking Ceremony Held for $1.2 Billion Utah Data Center (Jan. 6, 2011), *available at* http://www.nsa.gov/public_info/press_room/2011/utah_groundbreaking_ceremony.shtml.

160 *Id.* For scale, a single yottabyte would represent 500 *quintillion* pages of text, and would be large enough to store, for example, 4000 copies of every single piece of internet traffic produced globally in 2010. Bamford, *supra* note 157.

161 Kashmir Hill, *Blueprints of NSA's Ridiculously Expensive Data Center in Utah Suggest it Holds Less Info than Thought,* Forbes (July 24, 2013, 5:11 PM), http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/.

162 Press Release, *supra* note 159.

163 Elizabeth Prann, *NSA Dismisses Claims Utah Data Center Watches Average Americans*, Fox News, (Mar. 28, 2012) http://www.foxnews.com/politics/2012/03/28/nsa-dismisses-claims-utah-data-center-watches-average-americans/.

164 *See* The White House, National Strategy for Information Sharing: Successes and Challenges In Improving Terrorism-Related Information Sharing 7 (2007), *available at* www.ise.gov/sites/default/files/nsis_book.pdf; Exec. Order No. 13,356, 69 Fed. Reg. 53599 (Sept. 1, 2004); Intelligence Reform and Terrorism

Prevention Act of 2004 Pub. L. No. 108-458, §1016, 118 Stat. 3665 (codified as amended at 6 U.S.C. § 485 (2013)) (directing the establishment of the ISE and requiring the designation of an ISE Program Manager); Exec. Order No. 13,388, 70 Fed. Reg. 62,023 (Oct. 27, 2005) (superseding Exec. Order No. 13,356, 69 Fed. Reg. 53,599 (Sept. 1, 2004)) (facilitating work of Program Manager, expediting establishment of the ISE, and restructuring the Information Sharing Council); Memorandum to the Heads of Executive Department and Agencies, Guidelines and Requirements in Support of the Information Sharing Environment (Dec. 16, 2005), *available at* http://www.gpo.gov/fdsys/pkg/PPP-2005-book2/pdf/PPP-2005-book2-doc-pg1863.pdf.

165 *Nationwide SAR Initiative*, ISE, www.ise.gov/nationwide-sar-initiative (last visited March 18, 2013); *"If You See Something, Say Something" Campaign*, U.S. Dep't of Homeland Sec., www.dhs.gov/if-you-see-something-say-something-campaign (last visited Sept. 24, 2013) (describing campaign and including information about SAR reporting).

166 For background information about SARs and related civil liberties concerns, *see*, *e.g.*, Jerome B. Bjelopera, Cong. Research Serv., R40901, Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background Issues for Congress (2011) [hereinafter SAR Issues], *available at* http://fpc.state.gov/documents/organization/166837.pdf; Thomas Cincotta, Polit. Research Associates, Platform for Prejudice: How the Nationwide Suspicious Activity Reporting Initiative Invites Racial Profiling, Erodes Civil Liberties, and Undermines Security (2010), available at http://www.publiceye.org/liberty/matrix/reports/sar_initiative/sar-full-report.pdf; *More About Suspicious Activity Reporting*, Am. Civil Liberties Union (June 29, 2010), http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting. "Suspicious activity" is defined as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Information Sharing Environment (ISE) Functional Standard (FS) for Suspicious Activity Reporting (SAR), Version 1.5 (ISE-FS-200), 2 (2009) [hereinafter ISE-SAR Functional Standard], *available at* http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf.

167 ISE-SAR Functional Standard, *supra* note 166; *see also If You See Something, Say Something*, Dep't of Homeland Sec., www.dhs.gov/if-you-see-something-say-something-campaign (last visited Dec. 3, 2012) ("Only reports that document behavior reasonably indicative of criminal activity related to terrorism will be shared with federal partners.").

168 U.S. Gov't Accountability Office, GAO-13-233, Information Sharing: Additional Actions Could Help Ensure that Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective 33 (2013) [hereinafter GAO Information Sharing], *available at* http://www.gao.gov/assets/660/652995.pdf.

169 *Id.* at 35.

170 *Id.* at 34-36.

171 ISE-SAR Functional Standard, *supra* note 166, at 8 ("It is important to emphasize that context is an essential element of interpreting the relevance of such behaviors to criminal activity associated with terrorism").

172 *Id.* at 9.

173 *Id.*

174 *Id.*

175 *Id.*

176 *Id.* at 29 (Part B).

177 *Id.* at 29-30 (Part B).

178 *Id.* at 29 (Part B).

179 Interestingly, the Department of Defense, seemingly alone among federal agencies, requires that where information about ethnicity, race, religion, or the exercise of constitutional rights is entered, there must be a "*reasonable suspicion of* a *direct* relationship between such information and a *specific* criminal act or behavior that may pose a threat to DOD personnel, facilities, and forces in transit" – a bar that appears to be higher than the Functional Standard's reasonable indication standard. *See* Memorandum from Michèle Flournoy, Under Secretary of Defense for Policy, Dep't of Defense to Secretaries of the Military Departments, et. al., Directive-Type Memorandum (DTM) 10-018 – Law Enforcement Reporting of Suspicious Activity 12 (Oct. 1, 2010), *available at* http://www.fas.org/irp/doddir/dod/dtm-10-018.pdf (emphasis added).

180 U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative 5 (2010)[hereinafter ISE-SAR PIA], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise.pdf.

181 Joint Regional Intelligence Ctr., Intelligence Assessment: Guardian Incident Review: August 2009 3 (2009), *available at* http://info.publicintelligence.net/LA-RTTACguardianincidents.pdf.

182 ISE-SAR Functional Standard, *supra* note 166, at 9-10.

183 *Id.* at 10.
184 GAO Information Sharing, *supra* note 168, at 15-16.
185 Federal Support for Fusion Centers, *supra* note 81, at 1, 27.
186 *Id.* at 32.
187 *Id.*.
188 *Database: Mall of America Suspicious Activity Reports*, NPR (Sept. 7, 2011, 11:59 AM), http://www.npr.org/2011/08/18/139756444/database-mall-of-america-suspicious-activity-reports; *Under Suspicion at the Mall of America*, NPR (Sept. 7, 2011, 12:01 PM), http://www.npr.org/2011/09/07/140234451/under-suspicion-at-the-mall-of-america.
189 GAO Information Sharing, *supra* note 168, at 23-24.
190 *Id.* at 25. The FBI has told the Government Accountability Office that in February 2013, it began enabling fusion centers to directly remove their ISE-SARs from eGuardian, though the reports are still retained in Guardian and other FBI systems. *Id.* at 24.
191 *Id.* at 20.
192 *Id.* at 23-24.
193 *Id.*
194 *See* Fed. Bureau of Investigation, Privacy Impact Assessment for the eGuardian Threat Tracking System, Section 2.3, *available* at http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat; *see also id.* section 8.1 (describing the range of government agencies with access to eGuardian).
195 ISE-SAR PIA, *supra* note 180, at 5.
196 GAO Information Sharing, *supra* note 168, at 24.
197 *Id.* at 53.
198 *Id.*
199 Ashcroft Guidelines, *supra* note 49.
200 2011 DIOG, *supra* note 94, § 5.1. An "authorized purpose" is one authorized by the Attorney General Guidelines – "i.e., to further an FBI Assessment, Predicated Investigation, or other authorized function such as providing assistance to other agencies." *Id.* § 4.2.1.
201 *Id.* §5.1. While agents carrying out assessments are advised to use the "least intrusive method" that would accomplish their operational goal, they are also directed "not [to] hesitate to use any lawful method" necessary. *See id.* § 4.1.1(E), (F); 4.4.3.
202 *Id.* §18.5.8.
203 Memorandum from Counterterrorism Div., Fed. Bureau of Investigation, to all Field Offices, Counterterrorism Program Guidance, Baseline Collection Plan, Administrative and Operational Guidance 5 (Sept. 24, 2009) [hereinafter FBI Baseline Collection Plan], *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM004887.pdf ("Does your subject live alone or with other adults? If the subject lives with other adults, do you have any reason to believe that the other adults are involved with any criminal or national threat behavior of the subject?").
204 2011 DIOG, *supra* note 94, §18.5.5.3(G).
205 *Id.* §§ 5.1.1.5, 18.5.6, 18.5.6.4.9.
206 *Id.* §§ 18.5.1.1, 5.1.1.3.
207 *Id.* §§ 5.1.1.3, 5.1.1.6, 18.5.7.1, 18.5.3.
208 Mukasey Guidelines, *supra* note 50, at 20.
209 2011 DIOG, *supra* note 94, at 5.1.1.1, 8.5.; *In re National Security Letter*, Order Granting Motion to Set Aside NSL Letter, No. C. 11-02173 SI (N.D. Cal. March 14, 2013).
210 *See*, *e.g.*, 2011 DIOG, *supra* note 94, §4.4.3(D); Privacy Rights Clearinghouse, Comments to FTC: Protecting Consumer Privacy in an Era of Rapid Change, (2011), *available at* https://www.privacyrights.org/ftc-protecting-consumer-privacy-report-comments; Kim Zetter, *Brave New Era for Privacy Fight*, Wired, Jan. 13, 2005, *available at* http://www.wired.com/politics/security/news/2005/01/66242?currentPage=all.
211 2011 DIOG, *supra* note 94, §§ 18.5.2.3-18.5.2.4.
212 *Id.* § 5.1.
213 *Id.* § 5.4.1.
214 *Id.* § 5.4.1(A).
215 FBI Baseline Collection Plan, *supra* note 203, at 3 (emphasis added); *see also* 2011 DIOG, *supra* note 94, § 5.6.2 (clarifying that a Type 1 & 2 Assessment does not require supervisory approval; other types of assessments requires some type of approval or supervisory assignment, though the details are redacted); *id.* § 5.6.3.1.3 ("An FBI employee

may open a Type 1 & 2 Assessment without supervisor approval."); *id.* § 5.6.3.1.1 (imposing no time limit on Type 1 & 2 Assessment, but offering a nonbinding suggestion that "it is anticipated that such Assessments will be relatively short").

216 2011 DIOG, *supra* note 94, §§ 4.1.1(C), 4.1.2 ("If a well-founded basis to conduct investigative activity exists … and that basis is not *solely* activity that is protected by the First Amendment or on the race, ethnicity, national origin on religion of the participants – FBI employees may assess or investigate these activities …. In such a situation, the investigative activity would not be based solely on constitutionally-protected conduct or on race, ethnicity, national origin or religion.") (emphasis added).

217 *See, e.g.*, Sarah Kershaw & Eric Lichtblau, *Bomb Case Against Lawyer is Rejected*, N.Y. Times, May 25, 2004, *available at* http://www.nytimes.com/2004/05/25/us/bomb-case-against-lawyer-is-rejected.html; Colleen Mastony, *Fingerprint Mismatch Sets Attorney Free*, Chi. Trib., May 21, 2004, *available at* http://articles.chicagotribune.com/2004-05-21/news/0405210311_1_brandon-mayfield-fingerprints-material-witness. In an interview, Mayfield observed that the arrest warrant appeared to have been based in part on the fact that he was Muslim, that his wife was Muslim, that he advertised in Muslim yellow pages, and that he visited the local mosque. Amy Goodman & Juan Gonzàles, *Falsely Jailed Attorney Brandon Mayfield Discusses His Case After Feds Award $2 Million and Written Apology*, Democracy Now (Nov. 30, 2006), www.democracynow.org/2006/11/30/exclusive_falsely_jailed_attorney_brandon_mayfield.

218 *See, e.g.*, *Oregon Man Arrested in Spain Bombings Probe*, FOXNews.com (May 7, 2004), http://www.foxnews.com/story/0,2933,119243,00.html; *see also* Office of the Inspector Gen., U.S. Dep't of Justice, A Review of the FBI's Handling of the Brandon Mayfield Case 18 (2006) [hereinafter Mayfield Report], *available at* http://www.justice.gov/oig/special/s0601/exec.pdf.

219 Mayfield Report, *supra* note 218.

220 *Id.* at 179; *see also* Dan Eggen, *Patriot Act Partly Blamed in Madrid Case*, Wash. Post, Mar. 11, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/03/10/AR2006031002027.html; David Stout, *Inquiry Says FBI Erred in Implicating Man in Attack*, N.Y. Times, Jan. 7, 2006, *available at* http://www.nytimes.com/2006/01/07/politics/07terror.html?pagewanted=print; Andrew Zajac, *FBI Faulted for Error in Terror Case*, Chi. Trib., Jan. 7, 2006, *available at* http://articles.chicagotribune.com/2006-01-07/news/0601070080_1_brandon-mayfield-inspector-general-glenn-fine-usa-patriot-act.

221 Mayfield Report, *supra* note 218, at 179.

222 Press Release, Fed. Bureau of Investigation, Statement on Brandon Mayfield Case (May 24, 2004), *available at* http://www.fbi.gov/news/pressrel/press-releases/statement-on-brandon-mayfield-case; Eric Lichtblau, *U.S. Will Pay $2 Million to Lawyer Wrongly Jailed*, N.Y. Times, Nov. 30, 2006, *available at* http://www.nytimes.com/2006/11/30/us/30settle.html?ex=1322542800&en=0450419c94570958&ei=5088&partner=rssnyt&emc=rss&_r=0; *U.S. to Pay $2 Million for False Terror Arrest*, CBSNews.com (Sep. 10, 2009, 1:33 PM), http://www.cbsnews.com/2100-201_162-2216468.html.

223 Jerome P. Bjelopera, Cong. Research Serv., R41780, The Federal Bureau of Investigation and Terrorism Investigations 12 (2013), *available at* http://www.fas.org/sgp/crs/terror/R41780.pdf.

224 Mukasey Guidelines, *supra* note 50, at 16 (emphasis added).

225 2011 DIOG, *supra* note 94, § 5.12 (emphasis added).

226 *Id.* § 5.12.

227 *Id.* § 18.4 (emphasis added).

228 *Federal Bureau of Investigation: Hearing Before the H. Judiciary Comm.*, 111th Cong. 35-36 (2009) (statement of Robert Mueller, Dir., Fed. Bureau of Investigation), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg49782/html/CHRG-111hhrg49782.htm.

229 Notice of Modified Systems of Records, 63 Fed. Reg. 8659-02, 8671 (Feb. 20, 1998), *available at* http://www.fbi.gov/foia/privacy-act/63-fr-8659 (emphasis added); *see also* Office of the Inspector Gen., U.S. Dep't of Justice, A Review of the Federal Bureau of Investigation's Use of National Security Letters 68 n.41 (2008) [hereinafter 2008 OIG Report], *available at* http://www.justice.gov/oig/special/s0803b/final.pdf ("The length of time that the FBI retains investigative information … depends on several factors…. In general, information related to intelligence investigations is retained in the FBI's files … for 30 years after a case is closed, and information related to criminal investigations is retained for 20 years after a case is closed").

230 Mukasey Guidelines, *supra* note 50, at 16-17, 35-36.

231 Among the datasets included in the IDW is the FBI's Universal Name Index (UNI), which appears likely to include information from FBI assessments. *See, e.g.*, *Name Checks: Frequently Asked Questions*, Fed. Bureau of Investigation [hereinafter *Name Checks*], *available at* http://www.fbi.gov/stats-services/name-checks/name-checks-faqs. The UNI by its terms incorporates information from FBI "investigations," and assessments are referred

to in the DIOG as a type of "investigative activity." *See* 2011 DIOG, *supra* note 94, § 18-3.

232 *Report on the Investigative Data Warehouse*, Elec. Frontier Found. (Apr. 2009), https://www.eff.org/issues/foia/investigative-data-warehouse-report#1; *Name Checks, supra* note 231.

233 Press Release, U.S. Customs and Border Protection, CBP Receives Fourth Predator-B in Arizona: Agency Now Operates 9 Unmanned Aircraft (Dec. 27, 2011), *available at* http://cbp.gov/archived/xp/cgov/newsroom/news_releases/archives/2011_news_archive/12272011.xml.html; *Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary,* 113th Cong. (2013), *available at* http://www.judiciary.senate.gov/hearings/hearing.cfm?id=36ffa9c8160f81a25730563dc7e8c551 (statement of Robert S. Mueller, Dir., Fed. Bureau of Investigation); *see also* Letter from Rand Paul, Sen., U.S. Cong, to Robert S. Mueller, Dir., Fed. Bureau of Investigation (June 20, 2013) [hereinafter Rand Paul Letter], *available at* http://www.paul.senate.gov/files/documents/MuellerDrones.pdf.

234 H. R. Rep. No. 112-381, at 63-66 (2012), *available at* http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp112C6RZq&r_n=hr381.112&dbname=cp112&&sel=TOC_212580&.

235 Richard M. Thompson II, Cong. Research Serv., R42701, Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses 2 (2012), *available at* http://www.fas.org/sgp/crs/natsec/R42701.pdf.

236 *See Announcement: Unmanned Aircraft Systems Test Site Selection (UASTSS)*, Fed. Aviation Admin. (Feb. 14, 2013), https://faaco.faa.gov/index.cfm/announcement/view/13143; U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Robotic Aircraft for Public Safety (RAPS) Project 3 (2012), *available at* http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_st_raps_nov2012.pdf; Rand Paul Letter, *supra* note 233.

237 *See NOVA*: *What Drones Can See* (Public Broadcasting Service broadcast Jan. 17, 2013), *available at* http://video.pbs.org/video/2325492143; *see also* William Matthews, *One Sensor to Do the Work of Many*, DefenseNews (Mar. 1, 2010, 3:45 AM), http://www.defensenews.com/article/20100301/DEFFEAT01/3010309/One-Sensor-Do-Work-Many.

238 Am. Civil Liberties Union, Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Surveillance 4-5 (2011), *available at* https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf.

239 *See, e.g.*, Brian Montopoli, *Lawmakers Move to Limit Domestic Drones*, CBSNews.com (May 16, 2013, 6:00 AM), http://www.cbsnews.com/8301-201_162-57584695/lawmakers-move-to-limit-domestic-drones/.

240 There are two types of predicated investigations: preliminary investigations and full investigations. Preliminary investigations may be initiated "on the basis of information or an allegation indicating" that a federal crime or threat to national security may have occurred; full investigations require "an articulable factual basis" indicating that a federal crime or threat to national security may have occurred. Mukasey Guidelines, *supra* note 50, at 21-22.

241 *See* 12 U.S.C. § 3414(5)(A); 15 U.S.C. §§ 1681u(a), (b); 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b); *see also* Michael German et al., *National Security Letters: Building Blocks for Investigations or Intrusive Tools?*, Am. Bar Ass'n (Sept. 1, 2012, 5:10 AM), http://www.abajournal.com/magazine/article/national_security_letters_building_blocks_for_investigations_or_intrusive_t/.

242 In early 2013, a federal judge in California struck down as unconstitutional the statute allowing NSLs to be used to obtain communications information, based on the gag order provision, and ordered the government not to issue any more NSLs to communications companies or to enforce the gag order in any outstanding NSLs. The decision was stayed to allow the government to appeal. *See In re National Security Letter*, No. C. 11-02173 SI (N.D. Cal. Mar. 14, 2013) (order granting motion to set aside NSL letter).

243 2007 OIG Report, *supra* note 73, at xvi-xx; 2008 OIG Report, *supra* note 229, at 9. Because the official numbers exclude the NSLs issued to email and phone companies, which constitute the vast majority of NSLs issued, the DOJ's recent statement that it issued about 16,000 NSL requests in 2011 likely far understates the actual numbers. Letter from Ronald Weich, Assistant Attorney Gen., to Joseph R. Biden, Vice President (Apr. 30, 2012), *available at* https://www.fas.org/irp/agency/doj/fisa/2011rept.pdf (noting that the 16,511 requests pertained to about 7,200 persons); *see also* 2007 OIG Report, *supra* note 73, at xviii (describing ECPA NSLs as representing the majority of all NSLs issued). Despite the lack of comprehensive numbers, some communications companies have, in consultation with the FBI, started releasing broad information about NSLs issued for their subscribers' information. *See, e.g.*, Richard Salgado, *Transparency Report: Shedding more light on National Security Letters*, Google Public Policy Blog (Mar. 5, 2013), http://googlepublicpolicy.blogspot.com/2013/03/transparency-report-shedding-more-light.html; Microsoft Corp., 2012 Law Enforcement Requests Report (March 2013), *available at* http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/.

244 The National Security Act of 1947 was also amended in 1994 to authorize NSLs to be used in gathering credit and

financial records information for federal employees with security clearances who are required to give their consent as a condition for clearance. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, §802, 108 Stat. 3423 (codified as amended at 50 U.S.C. § 436(a)(1) (2000)). That authority is not relevant to this report.

245 12 U.S.C. § 3401 (2013); 2007 OIG Report, *supra* note 73, at xii.

246 15 U.S.C. § 1681u (2013); *see also* 2007 OIG Report, *supra* note 73, at xiii (citing to Intelligence Authorization Act for Fiscal Year 1996, Pub. L. No. 104-93, § 601(a), 109 Stat. 961 (codified as amended at 15 U.S.C. § 1681u (Supp. V. 1999)) (noting that limited credit history information would include "the names and addresses of all financial institutions at which a consumer maintains or has maintained an account; and consumer identifying information limited to name, current address, former addresses, places of employment, or former places of employment"). Under a Patriot Act amendment to the FCRA, the FBI and other government agencies that investigate or analyze international terrorism can also obtain full consumer credit reports with a certification that the information is "necessary" to the agency's work. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 358(g), 115 Stat. 365 (codified as amended at 15 U.S.C. § 1681v (2013)).

247 *Credit Report Contents*, Comprehensive Counseling for Consumers of America, http://www.ccfcofamerica.com/contents.html, (last visited Sept. 9, 2013).

248 18 U.S.C. § 2709 (2013); 2007 OIG Report, *supra* note 73, at 13, xii-xiii. Using this information, the FBI can identify a subject's "family members, associates, living arrangements, and contacts." *Id*. at xxiv.

249 18 U.S.C. § 2709(b)(1)(B) (1996); 12 U.S.C. § 3414(a)(5)(A) (1996); 15 U.S.C. § 1681u(a)(2) (1996).

250 *See* Ashcroft Guidelines, *supra* note 49, at 21-22; Mukasey Guidelines, *supra* note 50, at 21-22; *see also* 2007 OIG Report, *supra* note 73, at 45.

251 USA PATRIOT Act of 2001 § 505, 18 U.S.C. § 2709(b)(1), (2) (2013), 12 U.S.C. § 3414(a)(5)(A) (2013), 15 U.S.C. § 1681u(a), (b) (2013) (U.S. Code citations are to relevant parts only); 15 U.S.C. § 1681v (2013).

252 Memorandum from General Counsel, Nat'l Security Law Policy and Training Unit, Fed. Bureau of Investigation, to All Divisions, Comprehensive Guidance on National Security Letters 5 (June 1, 2007) [hereinafter NSL Guidance Memo], *available at* http://epic.org/privacy/nsl/New_NSL_Guidelines.pdf. The Patriot Act made National Security Letters easier to issue in several other ways as well. NSLs may now be signed by Special Agents in Charge at any FBI field office, not just by senior officials at FBI headquarters. 2007 OIG Report, *supra* note 73, at x (citing to Section 505 of the Patriot Act).

253 2008 OIG Report, *supra* note 229, at 109 (referring to 2006); *In re* National Security Letter, No. C 11-02173 SI, at 13 (N.D. Cal. Mar. 14, 2013) (order granting motion to set aside NSL Letter).

254 2008 OIG Report, *supra* note 229, at 71.

255 USA PATRIOT Act of 2001 § 505.

256 Valerie Caproni & Steven Siegel, *The National Security Tool that Critics Love to Hate*, Patriots Debate: Contemporary Issues in National Security Law (Harvey Rishikof, Stewart Baker & Bernard Horowitz eds., 2012), *available at* http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch5/ch5_ess2.html.

257 Michael German & Michelle Richardson, *Reply to the FBI*, Patriots Debate: Contemporary Issues in National Security Law (Harvey Rishikof, Stewart Baker & Bernard Horowitz eds., 2012), *available at* http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch5/ch5_res1.html.

258 2008 OIG Report, *supra* note 229, at 68 n.41.

259 12 U.S.C. § 3414(a)(5)(B) (2013); 18 U.S.C. § 2709(d) (2013); 15 U.S.C. § 1681u(f) (2013).

260 *See* 15 U.S.C. § 1681v (2013)*; see also* 1 David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions § 20:9, at 750 (2d ed. 2012) ("The limitation in Section 1681u [for limited credit information] is particularly anomalous because Section 1681v of the FCRA [for full credit information] allows the government to obtain the same information that it may obtain under Section 1681u, and Section 1681v contains no limitation on the dissemination of information obtained through an NSL. Accordingly, if the FBI issues an NSL under Section 1681u, it confronts limitations on its ability to disseminate the information it receives, but if the FBI or another government agency issues an NSL under Section 1681v, it may disseminate the information as it sees fit.").

261 12 U.S.C. § 3414(a)(5)(B) (2013); 18 U.S.C. § 2709(d) (2013); Mukasey Guidelines, *supra* note 50, at 37, 41.

262 2007 OIG Report, *supra* note 73, at xxvi.

263 *Id*. at xlii.

264 2008 OIG Report, *supra* note 229, at 7.

265 For instance, in addition to recommending that information derived from NSLs be "minimized" to protect information about Americans, the Working Group proposed that case agents have fairly wide latitude to tag information as having "investigative value" if it "contribut[ed]" to a national security investigation, which would allow for longer storage and access. 2008 OIG Report, *supra* note 229, at 64 n.34 (citing the Foreign

Intelligence Surveillance Act of 1978 § 101, 50 U.S.C. § 1801(h) (2013)); *id*. at 66 (quoting NSL Working Group Memorandum, Attachment 1). A wide array of financial, credit, telephone, and email-related information also would have been uploaded into FBI-wide databases, including into the Investigative Data Warehouse. *Id*. at 67, 68 (quoting in part NSL Working Group Memorandum, Attachment 1). Specifically, financial and credit information would only need to have "current or reasonably potential" investigative value, while telephone and email-related information would only need to be "responsive" to the initial request. *Id.*

266 *Id*. at 69.

267 *Id*. at 70.

268 *Id*.

269 *Id*. at 71-72.

270 *Id*. at 7-8, 65; *see also id*. app., at A-12, A-13.

271 David Kris, a high-ranking national security lawyer in the Bush and Obama administrations, described the absence of "rigorous minimization procedures concerning acquisition, retention and dissemination of information" from National Security Letters as "a very notable omission." *See 2008 NSL Hearing*, *supra* note 78, at 91 (statement of David Kris, Former Deputy Attorney Gen., U.S. Dep't of Justice). Similarly, James A. Baker, who served as Counsel for Intelligence Policy in the Office of Intelligence Policy and Review for most of the Bush administration, "urge[d]" a Senate panel to implement "adequate and statutorily mandated minimization procedures with respect to" the types of information obtained via National Security Letters. *See 2008 NSL Hearing 2*, *supra* note 78, at 10 (statement of James A. Baker, Former Counsel for Intelligence Policy, U.S. Dep't of Justice). Senator Sheldon Whitehouse echoed these concerns, highlighting what he called the "'what do you [do] with it' problem": "once you've got [information from National Security Letters], what do you do with it, how long can you keep it, do you destroy it, who can you connect to it, all that sort of stuff." *See id.* at 28 (statement of Sheldon Whitehouse, Sen., U.S. Congress).

272 For scolding, see *Reauthorizing the USA Patriot Act: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 15 (2009), *available at* http://www.justice.gov/oig/testimony/t0909.pdf (statement of Glenn A. Fine, Inspector General, U.S. Dep't of Justice) (urging the Department of Justice to "promptly consider the Working Group's proposal and issue final minimization procedures for NSLs that address the collection of information through NSLs, how the FBI can upload NSL information in FBI databases, the dissemination of NSL information, the appropriate tagging and tracking of NSL derived information in FBI databases and files, and the time period for retention of NSL obtained information."). The Inspector General further observed that "[a]t this point, more than 2 years have elapsed since after our first report was issued, and final guidance is needed and overdue." *Id*. For public version of NSL procedures, see NSL Guidance Memo, *supra* note 252.

273 *Permanent Provisions of the Patriot Act: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 10-22 (2011) [hereinafter *Patriot Act Provisions Hearing*], *available at* http://judiciary.house.gov/hearings/printers/112th/112-15_65486.PDF (statement of Todd Hinnen, Acting Assistant Att'y Gen. for National Security, U.S. Dep't of Justice).

274 *Id*. at 21. While Hinnen refers to the Automated Case Support System (ACS), *id*. at 18, ACS has since been replaced by Sentinel. *See, e.g.*, John Foley, *FBI's New Sentinel System: Exclusive Look*, Information Week (Mar. 30, 2012, 11:37 AM), http://www.informationweek.com/government/enterprise-applications/fbis-new-sentinel-system-exclusive-look/232800018. The 2007 Inspector General report also indicates that raw data from national security letters is kept in various FBI and intelligence classified databases. 2007 OIG Report, *supra* note 73, at 30.

275 *Patriot Act Provisions Hearing*, *supra* note 273, at 21.

276 2007 OIG Report, *supra* note 73, at xv, 28-29.

277 *Id*. at xv, 30.

278 *See* Fed. Bureau of Investigation, Exhibit 300: Capital Asset Plan and Business Case Summary 9 (2007), *available at* http://www.justice.gov/jmd/2009justification/exhibit300/fbi-sentinel.pdf. This document indicates that the FBI has exempted Sentinel from the Privacy Impact Analysis process because it is a national security system, but notes that the Bureau has nevertheless drafted a secret PIA. The document also clarifies that the Privacy Act does require a System of Records Notice (SORN) for Sentinel, and directs readers to the FBI-002 system, which is the Central Records System (CRS), on the Department of Justice's Privacy Act page. *See DOJ Systems of Records*, U.S. Dep't of Justice, http://www.usdoj.gov/jmd/privacyact.html. None of the linked SORNs for the CRS reference Sentinel or the Automated Case Support System. In addition, the first SORN, which does not appear to have been superseded in substance, states that the FBI has retention periods of "15 years for criminal related matters and 30 years for intelligence and other type matters." Notice of Modified Systems of Records, 63 Fed. Reg. 8659-02, 8683 (Feb. 20, 1998), *available at* http://www.fbi.gov/foia/privacy-act/63-fr-8659. As indicated by Director Mueller's comments and the DOJ OIG's report, however, criminal matters appear to be kept for twenty years, not fifteen.

279 *See* Alternatives Exist, *supra* note 33.

280 *See* FBI Response to IDW Press, *supra* note 154.

281 2007 OIG Report, *supra* note 73, at xv, 30.

282 *Id*. at xxvi.

283 U.S. Dep't of Homeland Security, U.S. Customs and Border Protection Border Search of Electronic Devices Containing Information Training: Assessment and Recommendations 1-2 (2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-report-cbp-training-border-searches-electronic-devices.pdf (listing examples of electronic devices). The Privacy Impact Assessment for DHS's border search program does state that "ICE policy and certain laws, such as the Privacy Act and the Trade Secrets Act, requires the special handling of some types of sensitive information including attorney-client privileged information, proprietary business information, and medical information." 2009 Border Searches PIA, *supra* note 79, at 13.

284 *See* Robert M. Bloom, *Border Searches in the Age of Terrorism*, 78 Miss. L.J. 295, 295-328 (2009), *available at* http://lawdigitalcommons.bc.edu/lsfp/240; Yule Kim, Cong. Research Serv., RL34404, Border Searches of Laptop Computers and Other Electronic Storage Devices 1-3 (2009), *available at* http://www.fas.org/sgp/crs/homesec/RL34404.pdf.

285 U.S. Customs and Border Protection, Customs Directive No. 3340-006A, Procedures for Examining Documents and Papers § 6.2.1 (2000), *available at* http://www.immigration.com/sites/default/files/cbpdocsandpapers.pdf. Customs officers were permitted to "glance at documents and papers" to determine whether they constituted "merchandise," including books or other printed materials, or "prohibited materials" such as copyright violations and stolen property. *Id*. § 6.4.1. Because "merchandise" included books, pamphlets, and other printed materials, *id*., CBP still claimed fairly broad authority to review First Amendment-protected materials without grounds for suspicion. The 2000 directive did not, however, give CBP officers the authority to review memos, letters, messages, website history, and other similar personal information. *Id*.

286 Memorandum from Dir., Office of Investigations, U.S. Immigration and Customs Enforcement, to Assistant Directors, All Deputy Assistant Directors, All Special Agents in Charge, Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry (Mar. 5, 2007), *available at* http://www.aclu.org/files/pdfs/natsec/laptopsearch/dhs_20100816_DHS000691-DHS000692.pdf.

287 *Id.*

288 U.S. Customs and Border Protection, Policy Regarding Border Search of Information (2008), *available at* http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf (last visited Feb. 18, 2013); 2009 Border Searches PIA, *supra* note 79.

289 E-Government Act of 2002, Pub. L. No. 107-347, § 208(b), 116 Stat. 2899 (codified as amended in statutory notes at 44 U.S.C. § 3501 (2013)).

290 2009 Border Searches PIA, *supra* note 79, at 3 (citing United States v. Ramsey, 431 U.S. 606 (1977)).

291 *Id*. at 6; U.S. Dep't of Homeland Security, Civil Rights/Civil Liberties Impact Assessment: Border Searches of Electronic Devices 17 (2011) [hereinafter 2011 CR/CL Assessment], *available at* https://www.dhs.gov/sites/default/files/publications/Redacted%20Report.pdf.

292 2009 Border Searches PIA, *supra* note 79, at 6-7.

293 *See id*. (no reference to First Amendment); 2011 CR/CL Assessment, *supra* note 291, at 15, 17-18 (concluding that DHS policies do not violate the First or Fourth Amendments).

294 Susan Stellin, *Border Agents' Power to Search Devices Is Facing Increasing Challenges in Court*, N.Y. Times, Dec. 3, 2012, *available at* http://www.nytimes.com/2012/12/04/business/court-cases-challenge-border-searches-of-laptops-and-phones.html?ref=technology&_r=0&pagewanted=all; *see also* 2011 CR/CL Assessment, *supra* note 291, at 1 (noting that just over 3600 travelers were subject to electronic device searches in fiscal year 2009, and nearly 4600 were in 2010).

295 *See CBP's 2012 Fiscal Year in Review*, U.S. Customs and Border Protection (Feb. 1, 2013), http://www.cbp.gov/xp/cgov/newsroom/news_releases/national/02012013_3.xml (indicating that over 350 million travelers per year cross the U.S. border, 98 million of those at air borders).

296 *See* Email from Tamara Kessler, Acting Officer, Office for Civil Rights & Civil Liberties, U.S. Dep't of Homeland Security, *in* 2011 CR/CL Assessment, *supra* note 291 (asserting that most of the referrals for secondary inspection for travelers with Arab or Muslim names had been "mandatory," not discretionary); Tamara Kessler, Office for Civil Rights and Civil Liberties, U.S. Dep't of Homeland Security, Bi-Weekly Report (2012), *in* 2011 CR/CL Assessment, *supra* note 291 (report for the week of October 11).

297 *See* Muslim Advocates, Unreasonable Intrusions: Investigating the Politics, Faith & Finances of Americans Returning Home 28 (2009) [hereinafter Unreasonable Intrusions], *available at* http://www.defendingdissent.org/pdf/Unreasoneable_Intrusions_2009.pdf; Ellen Nakashima, *Clarity Sought on Electronics Searches*, Wash. Post, Feb. 7, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/

article/2008/02/06/AR2008020604763.html.

298 Unreasonable Intrusions, *supra* note 297, at 28.

299 *Id.* at 38.

300 Glenn Greenwald, *U.S. Filmmaker Repeatedly Detained at Border*, Salon, Apr. 8, 2012, *available at* http://www.salon.com/2012/04/08/u_s_filmmaker_repeatedly_detained_at_border/.

301 Susan Stellin, *The Border is a Back Door for U.S. Device Searches*, N.Y. Times, Sept. 9, 2013, *available at* http://www.nytimes.com/2013/09/10/business/the-border-is-a-back-door-for-us-device-searches.html?pagewanted=all.

302 Press Release, Am. Civil Liberties Union, ACLU Sues Homeland Security Over Seizure of Activist's Computer (May 13, 2011), *available at* http://www.aclu.org/free-speech/aclu-sues-homeland-security-over-seizure-activists-computer/.

303 *Id.*

304 *See* Catherine Crump, *Judge Rules in Favor of Bradley Manning Supporter and Allows Lawsuit Challenging Laptop Search*, Am. Civil Liberties Union (Mar. 29, 2012, 12:43 PM), http://www.aclu.org/blog/free-speech-technology-and-liberty/judge-rules-favor-bradley-manning-supporter-and-allows; Kevin Poulsen, *Friend of Bradley Manning Drops Lawsuit Against Feds Over Seized Laptop*, Wired (May 29, 2013, 5:37 PM), www.wired.com/threatlevel/2103/05/lawsuit_dropped.

305 2009 Border Searches PIA, *supra* note 79, at 16.

306 *Id.* at 7.

307 *Id.* at 5.

308 *Id.* at 7.

309 *Id.* at 8, 11. A CBP officer must obtain supervisory approval before copying a device's contents; an ICE Special Agent does not. *Id.* For the 30-day limit, *see id.* at 8. If detention by an ICE agent takes longer than thirty days, an ICE supervisor must approve an extension and must re-approve every fifteen days after that. *Id.* at 8-9. The time limit for CBP to search copied information does not appear to be specified, though the former Chief Privacy Officer for DHS has stated that the review and destruction timelines apply equally to copied information. Marry Ellen Callahan, *Privacy issues in border searches of electronic devices*, U.S. Dep't of Homeland Security 4 n.9 (Oct. 2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_privacy_issues_border_searches_electronic_devices.pdf.

310 2009 Border Searches PIA, *supra* note 79, at 8 ("Copying may take place where CBP or ICE does not want to alert the traveler that he is under investigation….").

311 *Id.* at 9.

312 *Id.* (regarding requests for assistance by CBP); for requests for assistance by ICE, *see id.* ("Demands [by ICE] to assisting federal agencies also include the requirement to return or destroy the information after assistance has been rendered *unless the agency possesses independent legal authority to retain such information*.") (emphasis added). Mary Ellen Callahan, former Chief Privacy Officer for DHS, has said that "DHS cannot and will not disclose information discovered outside the scope of its authorities when conducting a border search of electronic devices." Callahan, *supra* note 309, at 4 n.8. It is unclear what this means, since the PIA in fact expressly authorizes CBP and ICE to share information that relates to any crimes, not simply those crimes that DHS enforces.

313 2009 Border Searches PIA, *supra* note 79, at 9.

314 *Id.* at 10.

315 2011 CR/CL Assessment, *supra* note 291, at 8.

316 2009 Border Searches PIA, *supra* note 79, at 8; U.S. Immigrations and Customs Enforcement, Directive No. 7-6.1, Border Searches of Electronic Devices 2 (2009), *in* 2009 Border Searches PIA, *supra* note 79 (labeled as Attachment 2).

317 U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing 14 (2010) [hereinafter 2010 TECS System PIA], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf; 2009 Border Searches PIA, *supra* note 79, at 6, 8, 21, 23 (record of interaction entered into TECS); *id.* at 8 (copy itself not accessible). TECS used to stand for Treasury Enforcement Communication System; in its current form, "TECS" is no longer considered an acronym and is simply the name of the system.

318 *See* 2011 CR/CL Assessment, *supra* note 291, at 17 (noting that "the absence of information about *why* a particular search was performed renders supervision more difficult," and recommending that CBP officers conducing a device search enter the rationale for the search into the TECS system).

319 2010 TECS System PIA, *supra* note 317, at 14. 2009 Border Searches PIA, *supra* note 79, at 6, 8, 15.

320 For instance, the Search, Arrest, and Seizure Records System of Records keeps records for five years after final disposition and then transfers them to the Federal Records Center, where they are kept for another fifteen years. 2009 Border Searches PIA, *supra* note 79 at 15; United States Immigration and Customs Enforcement – 008 Search,

Arrest, and Seizure Records System of Records Notice, 73 Fed. Reg. 74732, 74734 (Dec. 9, 2008) [hereinafter 2008 System of Records Notice], *available at* www.gpo.gov/fdsys/pkg/FR-2008-12-09/html/E8-29055.htm. Information may also be retained in ICE's system of Intelligence Records (IIRS); originally devised as a database for gang-related information, the system now contains a broad array of information, including "documents and electronic data […] collected by DHS from or about individuals during … border searches" – evidently whether or not related to intelligence matters. U.S. Immigration and Customs Enforcement – 006 Intelligence Records System of Records, 75 Fed. Reg. 9233, 9235 (Mar. 1, 2010) [hereinafter 2010 System of Records Notice], *available at* www.gpo.gov/fdsys/pkg/FR-2010-03-01/html/2010-4102.htm. Individuals covered by the system include persons "associated with law enforcement investigations or activities" conducted by any domestic or foreign law enforcement agency "where there is a potential nexus to ICE's law enforcement and immigration enforcement responsibilities or homeland security in general"; individuals who are associated in any way with suspicious activities or threats reported by governments, organizations, individuals, or the private sector, including the persons who made the report; and anyone identified in intelligence reporting that ICE receives or reviews. *Id.* The SORN also states that an information technology system called the Intelligence Fusion System (IFS) will include all of the categories above as well as "individuals identified in public news reports," among other categories; since this predates DHS's more recent statements about limits on its use of news reports and social media, it is possible that this limited category has been superseded. *Id.* Other records maintained in the system include terrorist watchlist information, "records pertaining to known or suspected terrorists, terrorist incidents, activities, groups, and threats," intelligence reporting from other groups or agencies, public-source information published "on individuals and events of interest to ICE," records from commercial data aggregators, and suspicious activity and threat reports from ICE and from outside entities. *Id.* As with the Search, Arrest, and Seizure database, all information that "may aid in establishing patterns of unlawful activity" will be retained, whether relevant or necessary to an investigation. U.S. Immigration and Customs Enforcement-006 Intelligence Records System, 75 Fed. Reg. 12437, 12438 (Mar. 16, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-03-16/pdf/2010-5618.pdf. In addition, records of border searches of electronics will also be stored for twenty years in the IFS, which offers intelligence analysts access to a range of datasets. 2010 System of Records Notice, *supra* note 320, at 9237; *see also* U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Law Enforcement Intelligence Fusion System (IFS) 12 (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_ifs.pdf.

321 2008 System of Records Notice, *supra* note 320, at 74734; Department of Homeland Security U.S. Immigration and Customs Enforcement – 008 Search, Arrest, and Seizure System of Records Final Rule, 74 Fed. Reg. 45080 (Aug. 31, 2009) [hereinafter 2009 System of Records Notice], *available at* www.gpo.gov/fdsys/pkg/FR-2009-08-31/html/E9-20761.htm; *see also* 2010 System of Records Notice, *supra* note 320, at 9236-37.

322 2009 System of Records Notice, *supra* note 321, at 45081 ("[I]n the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, *it is appropriate to retain all information that may aid in establishing patterns of unlawful activity*.") (emphasis added).

323 2009 Border Searches PIA, *supra* note 79, at 21.

324 *Id*.

325 In 2013, DHS's Office of Civil Rights and Civil Liberties issued its 2011 assessment of the impact of electronic border searches on civil rights and civil liberties, in which it concluded that imposing a reasonable suspicion requirement on searches of electronic devices at the border "would be operationally harmful without concomitant civil rights/civil liberties benefits." 2011 CR/CL Assessment, *supra* note 291, at 17. CBP did agree to record more information about why searches were performed, and travelers will now have an opportunity to file a complaint that a border search violated their freedom of speech or press. U.S. Dep't of Homeland Security, Civil Rights/Civil Liberties Impact Assessment: Border Searches of Electronic Devices (2013), *available at* http://www.dhs.gov/sites/default/files/publications/crcl-border-search-impact-assessment_01-29-13_1.pdf (executive summary). Finally, CBP will now have a policy advising officers that conducting "specially rigorous searching" on the grounds of the traveler's race, religion, or ethnicity is impermissible. *Id*.

326 Anil Jain, Lin Hong, & Sharath Pankanti, *Biometric Identification*, 43 Comm. of the ACM 91 (2000), *available at* http://www.andrew.cmu.edu/course/67-302/BiometricsACM.pdf.

327 While the biometrics databases for the Department of Homeland Security and the Department of State share the same name (Automated Biometric Identification System), they have different acronyms (DHS IDENT vs. DOS ABIS).

328 *See* U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) 2 (2012) [hereinafter 2012 IDENT PIA], *available at* http://www.dhs.gov/sites/

default/files/publications/privacy-pia-nppd-ident-06252013.pdf.

329 U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) 2 (2006), *available at* www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf (noting that "the intended use of IDENT has expanded beyond that for which it was initially designed.").

330 *Id*. at 3.

331 2012 IDENT PIA, *supra* note 328, at 10.

332 *Id*. at 25.

333 *Integrated Automated Fingerprint Identification System: Fact Sheet*, Fed. Bureau of Investigation (Feb. 6, 2013), http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_facts.

334 Fed. Bureau of Investigation, Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS) § I.2 (2008), *available at* http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system; *see also* Fed. Bureau of Investigation, Privacy Impact Assessment: Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability 1-2 (2012) [hereinafter 2012 IAFIS/NGI PIA], *available at* http://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-interoperability-1; Fed. Bureau of Investigation, Privacy Impact Assessment: Integrated Automated Fingerprint Identification System National Security Enhancements § 3.1, *available at* http://www.fbi.gov/foia/privacy-impact-assessments/iafis.

335 Aliya Sternstein, *FBI is On Track to Book Faces, Scars, Tattoos in 2014*, Nextgov (July 19, 2012), http://www.nextgov.com/big-data/2012/07/fbi-track-book-faces-scars-tattoos-2014/56876/; *see also* Fed. Bureau of Investigation, Exhibit 300: Capital Asset Summary 1 (2013), *available at* http://www.itdashboard.gov/investment/exhibit300/pdf/011-000003457.

336 *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. 3 (2012), *available at* http://judiciary.senate.gov/pdf/12-7-18PenderTestimony.pdf (statement of Jerome Pender, Deputy Assistant Dir., Criminal Justice Info. Services Div., Fed. Bureau of Investigation).

337 Richard W. Vorder Bruegge, Fed. Bureau of Investigation, Facial Recognition and Identification Initiatives 4 (2010), *available at* https://www.eff.org/sites/default/files/filenode/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf (PowerPoint presentation).

338 *See* Fed. Bureau of Investigation, Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes – Channeling § 3.4 (2008), *available at* www.fbi.gov/foia/privacy-impact-assessments/firs-iafis ("NARA has determined that civil fingerprint submissions are to be destroyed when the individual reaches 75 years of age and criminal fingerprints are to be destroyed when the individual reaches 99 years of age."); Fed. Bureau of Investigation, Privacy Impact Assessment, Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Repository for Individuals of Special Concern (RISC) § 3.4 n. 7 (2012), *available at* http://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-risc ("The FBI is seeking NARA's approval to increase this [retention of criminal subjects' fingerprints] to 110 years of age").

339 2012 IAFIS/NGI PIA, *supra* note 334, § I.1; *see also* U.S. Dep't of Homeland Security et al., Memorandum of Understanding among the Department of Homeland Security, the Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, and the Department of State Bureau of Consular Affairs for Improved Information Sharing Services 3-4 (2008), *available at* http://ccrjustice.org/files/FBI-DOS-DHS%20agreement-%20ICE%20FOIA%2010-2674.001718-001736.pdf.

340 *See* Criminal Justice Info. Services, Fed. Bureau of Investigation, CJIS Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings: Information Only Agenda (2012), *available at* https://www.eff.org/sites/default/files/filenode/FBI_CJIS_Advisory_Board_June2012_Staff_Papers.pdf (informational topic I); *see also* Subcomm. on Biometrics and Identity Mgmt., Nat'l Science and Tech. Council, The National Biometrics Challenge 8 (2011), *available at* www.biometrics.gov/Documents/BiometricsChallenge2011_protected.pdf (noting that in September 2009, DOD and FBI signed an MOU allowing "deeper integration" between ABIS and IAFIS, and in March 2011, DOD and DHS entered into an MOU that establishes the "policy framework" for ABIS-IDENT interoperability).

341 *See* Criminal Justice Info. Services, Fed. Bureau of Investigation, CJIS Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings: Informational Topics (2012), *available at* https://www.eff.org/sites/default/files/filenode/FBI-CJIS_Biometric_Sharing_Update2012.pdf (information topic F).

342 *See* Richard Sobel, *New ID rules would threaten citizens' rights*, CNN.com (June 13, 2013, 7:47 AM), http://www.

cnn.com/2013/06/13/opinion/sobel-id-immigration.

343 Exec. Order No. 12333, 46 Fed. Reg. 5994 (Dec. 4, 1981), *available at* http://www.archives.gov/federal-register/codification/executive-order/12333.html; *Signals Intelligence*, Nat'l Security Agency, http://www.nsa.gov/sigint/ (last visited Aug. 31, 2013).

344 *See, e.g.*, Siobhan Gorman & Jennifer Valentino-Devries, *New Details Show Broader NSA Surveillance Reach,* Wall St. J., Aug. 20, 2013, *available at* http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html; Glenn Greenwald, Laura Poitras & Ewan MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, Guardian, Sept. 11, 2013, *available at* http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

345 Exec. Order No. 12333, *supra* note 343.

346 Inspector Gen. of the Dep't of Defense et al., Unclassified Report on the President's Surveillance Program 5 (2009), *available at* http://www.fas.org/irp/eprint/psp.pdf.

347 *Id*. at 1, 5-6. ("The specific intelligence activities that were permitted by the Presidential Authorizations remain highly classified, except that beginning in December 2005 the President … acknowledged that these activities included the interception without a court order of certain international communications where there is 'a reasonable basis to conclude that one party to the communication'" is related in some way to al-Qaeda. "The President and other Administration officials referred to this publicly disclosed activity as the 'Terrorist Surveillance Program'…. We refer to other intelligence activities authorized under the Presidential Authorization as the 'Other Intelligence Activities.' The specific details of the Other Intelligence Activities remain highly classified, although the Attorney General publicly acknowledged the existence of such activities in August 2007. Together, the Terrorist Surveillance Program and the other Intelligence Activities comprise the PSP.").

348 *Id*. at 1. The program was initially based on the executive's "inherent power" to gather foreign intelligence. *Id*. at 13. After internal dissent, an additional rationale was added: Congress's resolution authorizing the wars in Iraq and Afghanistan included the implicit authority to capture communications related to those areas.

349 *Id*. at 2.

350 Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552; FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436. *See also* Inspector Gen. of the Dep't of Defense et al. *supra* note 346, at 30-31. In addition, Title III of the FISA Amendments Act of 2008 defines the President's Surveillance Program as "the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program)." FISA Amendments Act of 2008 § 301(a)(3).

351 50 U.S.C. § 1801(e)(2)(b) (2013) (defining foreign intelligence).

352 Edward C. Liu, Cong. Research Serv., R42725, Reauthorization of the FISA Amendments Act 7 (2012), *available at* http://www.fas.org/sgp/crs/intel/R42725.pdf; *see also* 50 U.S.C. § 1881a(a), (b). Foreign intelligence includes information "with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to" the national defense, the security, or the conduct of the foreign affairs of the United States. 50 U.S.C. § 1801(e)(2). Foreign intelligence also refers to information that relates to (or if concerning a U.S. person is necessary to) "the ability of the United States to protect against (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power." *Id.* § 1801(e)(1).

353 50 U.S.C. § 1881a(g)(2) (2013). The FBI is also authorized to gather information under FISA for intelligence and law enforcement purposes, and the government's broadened authority under FISA largely applies to the FBI as well. For instance, the FBI may obtain an order for the production of "tangible things," which is a broad category that can include "books, records, papers, documents, and other items." 50 U.S.C. § 1861 (2013).

354 *See, e.g.*, Marc Ambinder, *Minimize This!*, The Week (June 16, 2013, 2:20 AM), http://theweek.com/article/index/245694/minimize-this.

355 Eric. H. Holder, Jr., U.S Dep't of Justice, Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended 4 (2009) [hereinafter NSA Targeting Procedures], *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf.

356 *See* Letter from I. Charles McCullough, III, Inspector Gen., U.S. Intelligence Community, to Sen. Ron Wyden & Sen. Mark Udall 1 (June 15, 2012), *available at* http://www.wired.com/images_blogs/dangerroom/2012/06/IC-

IG-Letter.pdf.

357 *See* James R. Clapper, *Official Statement: DNI Clapper Directs Annual Release of Information Related to Orders Issued Under National Security Authorities*, Office of the Dir. Of Nat'l Intelligence (Aug. 29, 2013), http://icontherecord.tumblr.com/post/59719173750/dni-clapper-directs-annual-release-of-information; *Administration Continues to Disappoint on Transparency Around NSA Surveillance*, Ctr. for Democracy and Tech. (Aug. 30, 2013), https://www.cdt.org/pr_statement/administration-continues-disappoint-transparency-around-nsa-surveillance (noting that Intelligence Community will report number of "targets" rather than number of people actually affected).

358 Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Guardian, June 6, 2013, *available at* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

359 Brett Max Kaufman, *A Guide to What We Know About the NSA's Dragnet Searches of Your Communications*, Am. Civil Liberties Union (Aug. 9, 2013, 10:39 AM), https://www.aclu.org/blog/national-security/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications; Craig Timberg, *The NSA slide you haven't seen*, Wash. Post, July 10, 2013, *available at* http://articles.washingtonpost.com/2013-07-10/business/40480665_1_nsa-slide-prism; Jennifer Valentino-DeVries & Siobhan Gorman, *What You Need to Know on New Details of NSA Spying*, Wall St. J., Aug. 20, 2013, *available at* http://online.wsj.com/article/SB10001424127887324108204579025222244858490.html.

360 Charlie Savage, *NSA Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013, *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?ref=todayspaper&pagewanted=all.

361 Valentino-DeVries & Gorman, *supra* note 359.

362 Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'* Guardian, July 31, 2013, *available at* http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

363 *Id*. Another program that previously collected email metadata, which was justified on the basis on shifting legal rationales, was shut down on 2011 because it wasn't producing information of value; it appears that XKEYSCORE may have picked up where that program left off. *See, e.g.*, Siobhan Gorman & Jennifer Valentino-DeVries, *Details Emerge on NSA's Now Ended Internet Program*, Wall St. J., June 27, 2013, *available at* http://online.wsj.com/article/SB10001424127887323689204578572063855498882.html; Julian Sanchez, *What the Ashcroft 'Hospital Showdown' on NSA Spying Was All About*, Ars Technica (July 29, 2013), http://arstechnica.com/tech-policy/2013/07/what-the-ashcroft-hospital-showdown-on-nsa-spying-was-all-about0/; Ali Watkins & Jonathan S. Landay, *Documents show NSA violated court orders on collection of phone records*, Charlotte Observer (July 31, 2013), http://www.charlotteobserver.com/2013/07/31/4204917/documents-show-nsa-violated court.html#.UifCYH_B_To.

364 *See* Ewan MacAskill, *NSA Paid Millions to Cover PRISM Compliance Costs for Tech Companies*, Wash. Post, Aug. 22, 2013, *available at* http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid; T. Chase Meacham, *PRISM: The 8 Tech Companies Who Gave Your Data to the Government Have this to Say about the Scandal*, PolicyMic (June, 2013), http://www.policymic.com/articles/47231/prism-the-8-tech-companies-who-gave-your-data-to-the-government-have-this-to-say-about-the-scandal.

365 Charlie Savage & James Risen, *New Leak Suggests Ashcroft Confrontation Was Over NSA Program*, N.Y. Times, June 27, 2013, *available at* http://www.nytimes.com/2013/06/28/us/nsa-report-says-internet-metadata-were-focus-of-visit-to-ashcroft.html?pagewanted=all.

366 50 U.S.C. § 1861(2)(A) (2013).

367 *See, e.g.*, *In re* Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things From [REDACTED], No. BR 13-80 (FISA Ct. Apr. 25, 2013) (primary order granting government request for the production of tangible things), *available at* http://www.fas.org/irp/news/2013/07/215_order.pdf; *In re* Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things From [REDACTED], No. BR13-80 (FISA Ct. Apr. 25, 2013) (secondary order granting government request for the production of tangible things), *available at* http://s3.documentcloud.org/documents/709012/verizon.pdf; *see also* Barton Gellman, *U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata*, Wash. Post, June 15, 2013, *available at* http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story_1.html (for reference to other phone providers); Greenwald, *supra* note 42; John Ribeiro, *US Court Renews Permission to NSA to Collect Phone Metdata*, PCWorld (June 21, 2013, 10:48 PM), http://www.pcworld.com/article/2044883/us-court-renews-permission-to-nsa-to-collect-phone-metadata.html.

368 Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA

Patriot Act 2 (2013) [hereinafter White Paper], *available at* http://www.documentcloud.org/documents/750211-administration-white-paper-section-215.html.

369 50 U.S.C. § 1881a(d)(1), (e)(1), (f)(1) (2013).

370 50 U.S.C. § 1881a(i)(1)(A), (l)(3). *See also* U.S. Dep't of Justice & Office of the Dir. of Nat'l Intelligence, Background Paper on Title VII of FISA 2 (2012) (included as an attachment to Letter from James Clapper, Dir., National Intelligence, & Eric H. Holder, Attorney Gen., U.S. Dep't of Justice, to Rep. John Boehner, Sen. Harry Reid, Rep. Nancy Pelosi, Sen. Mitch McConnell (Feb. 8, 2012), *available at* http://intelligence.senate.gov/pdfs112th/dni_ag_letter.pdf). With respect to the FBI's use of the products of surveillance, properly collected information is destroyed after ten years or after the FBI's "use has been exhausted," whichever comes later. *See* Fed. Bureau of Investigation, N1-65-90-3, Request for Records Disposition Authority (1990), *available at* http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-90-003_sf115.pdf (also stating that surveillance tapes of persons who are not the proper subjects of a FISA collection order – i.e., of a spouse or child – should be destroyed "in accordance with minimization requirements," with the suggestion that the tapes are destroyed more or less immediately); *see also* Fed. Bureau of Investigation, N1-065-09-9, Request for Records Disposition Authority (2009), *available at* http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-09-009_sf115.pdf (directing that erroneously collected information – for instance, information provided for dates outside those specified in the FISA order – be deleted or destroyed within 60 days of notifying the Foreign Intelligence Surveillance Court of the error).

371 Eric. H. Holder, Jr., U.S Dep't of Justice, Minimization Procedures Used by the National Security Agency in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended 3, 8-9 (2011) [hereinafter 2011 NSA Minimization Procedures], *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. In some circumstances, the Director of the NSA must make a specific finding that the information meets one of the categories, and there are certain restrictions on the retention and dissemination of the information. *Id.* at 8. Notably, the Signals Intelligence Directive on which much of these minimization procedures seem to be based permits retention of Americans' communications if there is a threat of harm to a person, but does not mention property. United States Signals Intelligence Directive No. 18 § 5.4(d)(2), at 7 (July 27, 1993), *available at* http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-02.htm.

372 Ellen Nakashima, *Obama Administration Had Restrictions on NSA Reversed in 2011*, Wash. Post, Sept. 7, 2013, *available at* http://www.washingtonpost.com/world/national-security/obama-administration-had-restrictions-on-nsa-reversed-in-2011/2013/09/07/c26ef658-0fe5-11e3-85b6-d27422650fd5_story.html.

373 2011 NSA Minimization Procedures, *supra* note 371, at 11; U.S. Attorney Gen. & Dir. of Nat'l Intelligence, Semiannual Assessment of Compliance With Procedures and Guidelines Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence 19 (2013), *available at* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

374 [REDACTED NAME], [REDACTED NO.], slip op. at 33 n.31 (FISA Ct. Oct. 3, 2011), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf; *see also id.* at 36 (specifying types of communications that could include these wholly domestic communications).

375 *Id.* at 28.

376 *Id.* at 28-29.

377 *Id.* at 33.

378 *Id.* at 59-61.

379 *Id.* at 59 (emphasis added).

380 *Id.* at 61-63, 78-79; *see also* 50 U.S.C. §§ 1801(h)(1), 1821, (4)(A).

381 [REDACTED NAME], [REDACTED NO.], slip op. at 7, 12-13 (FISA Ct. Nov. 30, 2011), *available at* http://www.dni.gov/files/documents/November%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf; *see also* 2011 NSA Minimization Procedures, *supra* note 371, at 4-6. The government also informed the Court that it planned to purge from its systems all data that had been acquired under the unconstitutional procedures to the extent possible. *See* [REDACTED NAME], [REDACTED NO.], slip op. at 30-31 (FISA Ct. Sept. 25, 2012), *available at* http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.

382 Greenwald, *supra* note 362.

383 *Id.* Marc Ambinder, *What's XKEYSCORE?*, The Week (July 31, 2013, 3:58 PM), http://theweek.com/article/

index/247684/whats-keyscore*; 21% of Database Query Errors in NSA Report Involved the Internet Dragnet Database*, EMPTYWHEEL (Aug. 16, 2013), http://www.emptywheel.net/2013/08/16/21-of-the-database-query-errors-in-1q-2012-involved-the-phone-dragnet-database/.

384 *Compare* Nakashima, *supra* note 372, *and* 2011 NSA MINIMIZATION PROCEDURES, *supra* note 371, at 6, *and* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, GUARDIAN, Aug. 9, 2013, *available at* http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls, *with* ERIC. H. HOLDER, JR., U.S DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 3-4 (2009) [hereinafter 2009 MINIMIZATION PROCEDURES], *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document ("Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will not include United States person names or identifiers….").

385 Nakashima, *supra* note 372.

386 *Id*.; Ball & Ackerman, *supra* note 384.

387 NSA TARGETING PROCEDURES, *supra* note 355, at 8 (emphasis added).

388 *See* Gellman, *supra* note 84; Memorandum from Chief, Signals Intelligence Division Oversight & Compliance, to Dir., Signals Intelligence Division, Nat'l Security Agency (May 3, 2012), *available at* http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/#document/p1/a115757; *see also Summary of FISA Amendments Act FOIA Documents Released on Nov. 29, 2010*, AM. CIVIL LIBERTIES UNION 2-3 (2010), http://www.aclu.org/files/pdfs/natsec/faafoia20101129/20101129Summary.pdf; U.S. ATTORNEY GEN. & DIR. OF NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE (2009), *available at* http://www.aclu.org/files/pdfs/natsec/faafoia20101129/FAAODNI0001.pdf; U.S. ATTORNEY GEN. & DIR. OF NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE (2008), *available at* http://www.aclu.org/files/pdfs/natsec/faafoia20101129/FAAODNI0041.pdf.

389 *See* Letter from James Clapper, Dir., National Intelligence, to Sen. Ron Wyden 2 (July 26, 2013), *available at* http://www.wyden.senate.gov/download/?id=285dc9e7-195a-4467-b0fe-caa857fc4e0d (stating that "raw records [collected pursuant to Section 215] may only be retained for up to five years.").

390 WHITE PAPER, *supra* note 368, at 3.

391 *Id*. (emphasis added).

392 *Id*. at 4.

393 *Id*. at 3-4.

394 Pete Yost & Matt Apuzzo, *With 3 'Hops,' NSA Gets Millions of Phone Records*, YAHOO (July 31, 2013), http://news.yahoo.com/3-hops-nsa-gets-millions-phone-records-204851967.html.

395 *See generally* Spencer Ackerman, *NSA Violations Led Judge to Consider Viability of Surveillance Program*, GUARDIAN, Sept. 10, 2013, *available at* http://www.theguardian.com/world/2013/sep/10/nsa-violated-court-rules-data-documents; Siobhan Gorman & Devlin Barrett, *NSA Violated Privacy Protections, Officials Say*, WALL ST. J., Sept. 10, 2013, *available at* http://online.wsj.com/article/SB10001424127887324094704579067422990999360.html.

396 *See In re* Application of Federal Bureau of Investigation for an Order Requiring Production of Tangible Things From [REDACTED], No. BR 06-05 (FISA Ct. May 18, 2006) (order granting government request for tangible things), *available at* http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf (for requirement of reasonable, articulable suspicion); *In re* Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Jan. 28, 2009) (order initially addressing the disclosure of the alert list), *available at* http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf; *In re* Production of Tangible Things From [REDACTED], No. BR 08-13, slip op. at 4-5 (FISA Ct. Mar. 2, 2009) (order granting the government's request for the production of tangible things but prohibiting access to the alert list metadata except as approved by the court on a case-by-case basis), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf (observing that via the alert list, "the NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non-RAS approved telephone identifiers on its alert list against the BR metadata in order to identify any matches. Such access was prohibited by the governing minimization procedures…."); *see also* Benjamin Wittes, Lauren Bateman and Matt Danzer, *The Latest NSA Documents II: The Crap Hits the Fan*, LAWFARE (Sept. 11, 2013, 3:50 p.m.), http://www.lawfareblog.com/2013/09/the-latest-nsa-documents-ii-the-crap-hits-the-fan/.

397 *See* Memorandum of the United States in Response to the Court's Order Dated Janaury [sic] 28, 2009 at 11, *In re* Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://

www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

398 *Id*. (citing *In re* Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Mar. 2, 2009), *supra* note 396.

399 *Id*. at 20.

400 *In re* Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Mar. 2, 2009), *supra* note 396, at 9.

401 *Id*. at 11.

402 *Id*.

403 *Id*. at 18; *see also* Wells Bennett and Matt Danzer, *The Latest NSA Documents IV: Things Get Worse*, Lawfare (Sept. 11, 2013, 9:49 p.m.), http://www.lawfareblog.com/2013/09/the-latest-nsa-documents-vi-non-compliance-redux-with-some-more-doj/.

404 *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 09-13, slip op. at 5-7 (FISA Ct. Sept. 3, 2009) (order granting the government's request for the production of tangible things and lifting prior restrictions on its access to BR metadata), *available at* http://www.dni.gov/files/documents/section/pub_Sep%203%202009%20Primary%20Order%20from%20FISC.pdf.

405 *In re* Production of Tangible Things From [REDACTED], No. BR 08-13 (FISA Ct. Mar. 2, 2009), *supra* note 396, at 8.

406 *See, e.g.*, Raffaela Wakeman & Wells Bennett, *The Latest NSA Documents V: the NSA Investigates Its Metadata Compliance Problems, Takes Remedial Steps, and Reports Back to the FISC*, Lawfare (Sept. 12, 2013, 4:57 PM), http://www.lawfareblog.com/2013/09/the-latest-nsa-documents-v-the-nsa-investigates-its-metadata-compliance-problems-takes-remedial-steps-and-reports-back-to-the-fisc/; Wells Bennett, *The Latest NSA Documents VI, Non-Compliance Redux, with More DOJ*, Lawfare (Sept. 13, 2013, 5:52 PM), http://www.lawfareblog.com/2013/09/the-latest-nsa-documents-vi-non-compliance-redux-with-some-more-doj/.

407 Press Release, Wyden and Udall Statement on the Declassification of FISA Court Opinions on Bulk Collection of Phone Data (Sept. 10, 2013), *available at* http://www.wyden.senate.gov/news/press-releases/wyden-and-udall-statement-on-the-declassification-of-fisa-court-opinions-on-bulk-collection-of-phone-data.

408 *Id*.

409 Glenn Greenwald, Laura Poitras & Ewan MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, Guardian, Sept. 11, 2013, *available at* http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

410 *See* National Security Agency, Central Security Service & Israeli SIGNIT National Unit, Memorandum of Understanding (MOU) Between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons § IV(b)(5), *available at* http://s3.documentcloud.org/documents/785495/doc1.pdf.

411 2009 Minimization Procedures, *supra* note 384, at 8-9 (2009); *see also* 2011 Minimization Procedures, *supra* note 371, § 8(b), at 11-13 (using same language).

412 United States v. Mason, 628 F.3d 123, 128 (4th Cir. 2010) (quoting United States v. Branch, 537 F.3d 328, 336 (4th Cir. 2008)).

413 S. Rep. No. 99-1183, at 6916-18, 6920 (1974). As Republican Senator Barry Goldwater observed during legislative debates over the Act, for instance, "A person who fears that he will be monitored may, either subconsciously or consciously, fail to fully exercise his constitutionally guaranteed liberties. The mere existence of such fear erodes basic freedoms and cannot be accepted in a democratic society." 120 Cong. Rec. H10950-10972 (daily ed. Nov. 21, 1974) (statement of Sen. Barry Goldwater), *reprinted in* S. Comm. on Gov't Operations & H. Comm. on Gov't Operations, 90th Cong., Legislative History of the Privacy Act of 1974, at 972 (1976), *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

414 Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, Wall St. J., Dec. 12, 2012, *available at* http://online.wsj.com/article_email/SB10001424127887324478304578171623040640006-lMyQjAxMTAyMDEwMzExNDMyWj.html?mod=wsj_valettop_email (quoting a Privacy Act consultant to government agencies as observing: "All you have to do is publish a notice in the Federal Register and you can do whatever you want.").

415 *See, e.g.*, Alternatives Exist, *supra* note 33, at 21-26; U.S. Gov't Accountability Office, GAO-08-795T, Privacy: Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information 13-20 (2008) [hereinafter Statement of Linda Koontz], *available at* www.gao.gov/new.items/d08795t.pdf (prepared statement of Linda Koontz, Dir., Information Mgmt. Issues, U.S. Gov't Accountability

Office, before the S. Comm. on Homeland Security and Governmental Affairs); U.S. Gov't Accountability Office, GAO-12-961T, Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape 5-7 [hereinafter Statement of Gregory C. Wilshusen] (2012), *available at* http://www.gao.gov/assets/600/593146.pdf (prepared statement of Gregory C. Wilshusen, before the S. Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, and D.C. of the S. Comm. on Homeland Security and Governmental Affairs).

416 Alternatives Exist, *supra* note 33; Statement of Linda Koontz, *supra* note 415.

417 Privacy Act of 1974 § 3, 5 U.S.C. § 552a(a)(5) (2013) (defining a "system of records" as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual").

418 Statement of Gregory C. Wilshusen, *supra* note 415, at 7; Alternatives exist, *supra* note 33, at 22-25.

419 *See* S. Rep. No. 93-1183, at 6919 (1974).

420 The Privacy and Civil Liberties Oversight Board, established by recommendation of the 9/11 Commission, is tasked with "ensur[ing] that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism," and the Board specifically oversees the sharing of terrorism information within the government. 42 U.S.C. § 2000ee(c)(2) (2013). The Board is not, however, designed to field individual concerns regarding the impact or implementation of the Privacy Act, and it is focused specifically on counterterrorism rather than law enforcement more broadly. *Id*. § 2000ee(d).

421 S. Rep. No. 93-1183, *supra* note 419.

422 *See* Alternatives Exist, *supra* note 33, at 42.

423 *See* 5 U.S.C. § 552a(g)(1)(D) (allowing individuals to sue an agency that violates the Privacy Act "in such a way as to have an adverse effect on [the] individual").

424 5 U.S.C. § 552a(j), (k).

425 5 U.S.C. § 552a(k)(2) (2013) (exception for "investigatory material compiled for law enforcement purposes"); *see also* 5 U.S.C. § 552a(j)(2) (2013) (allowing an agency to exempt a system of records from sections of the Privacy Act if the records consist of "(A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision," but not requiring the agency to specify which of those categories the database satisfies).

426 5 U.S.C. § 552a(v) (2013); Memorandum from Joshua B. Bolten, Dir. Office of Mgmt. & Budget, to All Executive Agencies, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2013), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22#a.

427 *See*, *e.g.*, *Recommended Principles for Updating Privacy Laws*, Ctr. for Democracy and Tech. (June 27, 2008), https://www.cdt.org/policy/recommended-principles-updating-privacy-laws ("The OMB's lack of leadership has been criticized since 1983, when House Committee on Government Operations pointed out that OMB had not updated its guidance in the first nine years of the Act's passage. Most recently, GAO's "Alternatives Exist for Enhancing Protection of Personally Identifiable Information" reported noted the OMB failed to act on GAO recommendations in 2006 to clarify Section 208 guidelines to apply to commercial data re-sellers.").

428 *See* Dennis McDonough et al., Ctr. for Am. Progress, No Mere Oversight: Congressional Oversight of Intelligence is Broken (2006), *available at* http://www.americanprogress.org/issues/security/news/2006/06/13/2019/no-mere-oversight/.

429 *See*, *e.g.*, Spencer Ackerman, *NSA Warned to Rein in Surveillance as Agency Reveals Even Greater Scope*, Guardian, July 17, 2013, *available at* http://www.theguardian.com/world/2013/jul/17/nsa-surveillance-house-hearing (noting that generally only intelligence committees received briefings, not whole Congress, and quoting Congresswoman as saying that annual report to Congress about Section 215 phone metadata collection was "less than a single page and not more than eight sentences"); Gellman, *supra* note 84 (observing that fewer than 10% of members of Congress have a staff member with the necessary security clearance "to read the reports and provide advice about their meaning and significance"); Glenn Greenwald, *Members of Congress Denied Access to Basic Information About NSA*, Guardian, Aug. 4, 2013, *available at* http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access; Peter Wallsten, *Lawmakers Say Administration's Lack of Candor on Surveillance Weakens Oversight*, Wash. Post, July 10, 2013, *available at* http://www.washingtonpost.com/politics/lawmakers-say-administrations-lack-of-candor-on-surveillance-weakens-oversight/2013/07/10/8275d8c8-e97a-11e2-aa9f-c03a72e2d342_story.html; *see also* Brian Beutler, *Senate Intel Committee Blocks Former Staffer From Talking To Press About Oversight*

Process, TalkingPointsMemo (June 18, 2013, 12:00 AM), http://tpmdc.talkingpointsmemo.com/2013/06/senate-committee-silences-former-aide-who-attempted-to-criticize-congressional-intelligence-oversigh.php.

430 U.S. v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

431 *Id.* (quoting United States v. Cuevas-Perez, 640 F.3d 272, 258 (7th Cir. 2011) (Flaum, J., concurring)).

STAY CONNECTED TO THE BRENNAN CENTER

Sign up for our electronic newsletters at **www.brennancenter.org/signup.**

Latest News | Up-to-the-minute info on our work, publications, events, and more.

Voting Newsletter | Latest developments, state updates, new research, and media roundup.

Justice Update | Snapshot of our justice work and latest developments in the field.

Fair Courts | Comprehensive news roundup spotlighting judges and the courts.

Twitter | www.twitter.com/BrennanCenter
Facebook | www.facebook.com/BrennanCenter

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

Foreign Law Bans: Legal Uncertainties and Practical Problems
Faiza Patel, Amos Toh, and Matthew Duss

A Proposal for an NYPD Inspector General
Faiza Patel and Andrew Sullivan

Domestic Intelligence: Our Rights and Our Safety
Faiza Patel, editor

Smart on Surveillance: Best Practices for Law Enforcement Information Sharing
Michael Price

Federal Judicial Vacancies: The Trial Courts
Alicia Bannon

Reforming Byrne JAG to Protect Public Safety and Reduce Mass Incarceration
Lauren-Brooke Eisen, Inimai Chettiar, and Nicole Fortier

The Case for Voter Registration Modernization
Brennan Center for Justice

Democracy & Justice: Collected Writings, Vol. VI
Brennan Center for Justice

How to Fix Long Lines
Lawrence Norden

For more information, please visit www.brennancenter.org

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
646-292-8310
www.brennancenter.org