UNLEASHED AND UNACCOUNTABLE

The FBI's Unchecked Abuse of Authority

ACLU

AMERICAN CIVIL LIBERTIES UNION

September 2013

Table of Contents

Executive Summary

The Federal Bureau of Investigation serves a crucial role in securing the United States from criminals, terrorists, and hostile foreign agents. Just as importantly, the FBI also protects civil rights and civil liberties, ensures honest government, and defends the rule of law. Its agents serve around the country and around the world with a high degree of professionalism and competence, often under difficult and dangerous conditions. But throughout its history, the FBI has also regularly overstepped the law, infringing on Americans' constitutional rights while overzealously pursuing its domestic security mission.

After the September 11, 2001 terrorist attacks, Congress and successive attorneys general loosened many of the legal and internal controls that a previous generation had placed on the FBI to protect Americans' constitutional rights. As a result, the FBI is repeating mistakes of the past and is again unfairly targeting immigrants, racial and religious minorities, and political dissidents for surveillance, infiltration, investigation, and "disruption strategies."

But modern technological innovations have significantly increased the threat to American liberty by giving today's FBI the capability to collect, store, and analyze data about millions of innocent Americans. The excessive secrecy with which it cloaks these domestic intelligence gathering operations has crippled constitutional oversight mechanisms. Courts have been reticent to challenge government secrecy demands and, despite years of debate in Congress regarding the proper scope of domestic surveillance, it took unauthorized leaks by a whistleblower to finally reveal the government's secret interpretations of these laws and the Orwellian scope of its domestic surveillance programs.

There is evidence the FBI's increased intelligence collection powers have harmed, rather than aided, its terrorism prevention efforts by overwhelming agents with a flood of irrelevant data and false alarms. Former FBI Director William Webster evaluated the FBI's investigation of Maj. Nadal Hasan prior to the Ft. Hood shooting and cited the "relentless" workload resulting from a "data explosion" within the FBI as an impediment to proper intelligence analysis. And members of Congress questioned several other incidents in which the FBI investigated but failed to interdict individuals who later committed murderous terrorist attacks, including the Boston Marathon bombing. While preventing every possible act of terrorism is an impossible goal, an examination of these cases raise serious questions regarding the efficacy of FBI methods. FBI data showing that more than half of the violent crimes, including over a third of the murders in the U.S., go unsolved each year calls for a broader analysis of the proper distribution of law enforcement resources.

With the appointment of Director James Comey, the FBI has seen its first change in leadership since the 9/11 attacks, which provides an opportunity for Congress, the president, and the attorney general to conduct a comprehensive evaluation of the FBI's policies and programs. This report highlights areas in which the FBI has abused its authority and recommends reforms to

ensure the FBI fulfills its law enforcement and security missions with proper public oversight and respect for constitutional rights and democratic ideals.

The report describes major changes to law and policy that unleashed the FBI from its traditional restraints and opened the door to abuse. Congress enhanced many of the FBI's surveillance powers after 9/11, primarily through the USA Patriot Act and the Foreign Intelligence Surveillance Act Amendments. The recent revelations regarding the FBI's use of **Section 215 of the USA Patriot Act** to track all U.S. telephone calls is only the latest in a long line of abuse. Five Justice Department Inspector General audits documented widespread FBI misuse of Patriot Act authorities in 2007 and 2008. Congress and the American public deserve to know the full scope of the FBI's spying on Americans under the Patriot Act and all other surveillance authorities.

Attorney General Michael Mukasey rewrote the FBI's rule book in 2008, giving FBI agents unfettered authority to investigate anyone they choose without any factual basis for suspecting wrongdoing. **The 2008 Attorney General's Guidelines** created a new kind of intrusive investigation called an "assessment," which requires no "factual predicate" and can include searches through government or commercial databases, overt or covert FBI interviews, and tasking informants to gather information about anyone or to infiltrate lawful organizations. In a two-year period from 2009 to 2011, the FBI opened over 82,000 "assessments" of individuals or organizations, less than 3,500 of which discovered information justifying further investigation.

The 2008 guidelines also authorized the **FBI's racial and ethnic mapping program**, which allows the FBI to collect demographic information to map American communities by race and ethnicity for intelligence purposes, based on crass racial stereotypes about the crimes each group commits. FBI documents obtained by the American Civil Liberties Union show the FBI mapped Chinese and Russian communities in San Francisco for organized crime purposes, all Latino communities in New Jersey and Alabama because there are street gangs, African Americans in Georgia to find "Black separatists," and Middle-Eastern communities in Detroit for terrorism.

The FBI also claimed the authority to sweep up voluminous amounts of information secretly from state and local law enforcement and private data aggregators for data mining purposes. In 2007, the FBI said it amassed databases containing 1.5 billion records, which were predicted to grow to 6 billion records by 2012, which is equal to 20 separate "records" for every person in the United States. The largest of these databases, the **Foreign Terrorist Tracking Task Force**, currently has 360 staff members running 40 separate projects. A 2013 Inspector General audit determined it "did not always provide FBI field offices with timely and relevant information."

The next section of the report discusses the ways the FBI avoids accountability by skirting internal and external oversight. The FBI, which Congress exempted from the Whistleblower Protection Act, effectively suppresses internal dissent by **retaliating against employees who report waste, fraud, abuse, and illegality**. As a result, 28 percent of non-supervisory FBI

employees surveyed by the Inspector General said they "never" reported misconduct they saw or heard about on the job. The FBI also aggressively investigates other government whistleblowers, which has led to an unprecedented increase in Espionage Act prosecutions over the last five years. And the FBI's overzealous pursuit of government whistleblowers has also resulted in the inappropriate **targeting of journalists** for investigation, infringing on free press rights. Recent coverage of overbroad subpoenas for telephone records of Associated Press journalists and an inappropriate search warrant for a Fox News reporter are only the latest examples of abuse. In 2010 the Inspector General reported the FBI used an illegal "exigent letter" to obtain the telephone records of 7 New York Times and Washington Post reporters. And the **FBI thwarts congressional oversight** with excessive secrecy and delayed or misleading responses to questions from Congress.

Finally, the report highlights evidence of abuse that requires greater regulation, oversight, and public accountability. These include many examples of the **FBI targeting First Amendment activities** by spying on protesters and religious groups with aggressive tactics that infringe on their free speech, religion, and associational rights. In 2011, the ACLU exposed flawed and biased FBI training materials that likely fueled these inappropriate investigations.

The FBI also operates increasingly outside the United States, where its activities are more difficult to monitor. Several troubling cases indicate the FBI may have requested, facilitated, and/or exploited the arrests of U.S. citizens by foreign governments, often without charges, so they could be held and interrogated, sometimes tortured, and then interviewed by FBI agents. The ACLU represents two **proxy detention** victims, including Amir Meshal, who was arrested at the Kenya border in 2007 and subjected to more than four months of detention in three different East African countries without charge, access to counsel, or presentment before a judicial officer, at the behest of the U.S. government. FBI agents interrogated Meshal more than thirty times during his detention.

Other Americans traveling abroad discover that their government has barred them from flying; the number of U.S. persons on the **No Fly List** has doubled since 2009. There is no fair procedure for those mistakenly placed on the list to challenge their inclusion. Many of those prevented from flying home have been subjected to FBI interviews after seeking assistance from U.S. Embassies. The ACLU is suing the government on behalf of 10 American citizens and permanent residents who were prevented from flying to the U.S., arguing that barring them from flying without due process is unconstitutional.

These FBI abuses of authority must end. We call on President Barack Obama and Attorney General Eric Holder to tighten FBI authorities to prevent unnecessary invasions of Americans' privacy; prohibit profiling based on race, ethnicity, religion and national origin; and protect First Amendment activities. And we call on Congress to make these changes permanent through statute and improve oversight to prevent future abuse. The FBI serves a crucial role in protecting Americans, but it must protect our rights as it protects our security.

Unleashed and Unaccountable: The FBI's Unchecked Abuse of Authority

Introduction

On September 4, 2013, James B. Comey was sworn in as the 7th director of the Federal Bureau of Investigation (FBI). Comey is taking the helm of an agency that has transformed during the 12-year term of Director Robert S. Mueller III into a domestic intelligence and law enforcement agency of unprecedented power and international reach.

Today's FBI doesn't just search for evidence to catch criminals, terrorists, and spies. Working with other government agencies and private companies, it helps gather information about millions of law abiding Americans, tracking our communications and associations. It has mapped American communities based on race, ethnicity, religion, and national origin and exploited community outreach programs to monitor the First Amendment activities of religious groups. It has harassed non-violent political activists with surveillance, unwarranted investigations, and even aggressive nationwide raids that resulted in no criminal charges. The FBI retains the information it collects through its investigations and intelligence activities in vast databases containing billions of records that agents can mine for myriad purposes, even without opening an official investigation or otherwise documenting their searches.

The FBI has exploited secret interpretations of the laws governing domestic surveillance to expand its reach and simply ignored other legal restrictions designed to protect our constitutional rights. It has frustrated congressional, judicial, and public oversight through excessive secrecy, official misrepresentations of its activities, and suppression of government whistleblowers and the press. Even more opaque are the FBI's intelligence and law enforcement exploits abroad. American citizens traveling overseas have been detained by foreign governments at the behest of the U.S. government and interrogated by FBI agents. Other Americans were blocked from flying home because they were placed on the U.S. government's No Fly List and then pressured to become FBI informants when they sought redress at U.S. Embassies. Such abuse is the inevitable product of a deliberate effort by Congress, two presidents, and successive attorneys general to vest the FBI with the powers of a secret domestic intelligence agency.

The FBI has an extremely dedicated and proficient workforce that is given the crucial and enormously difficult mission of protecting our nation from a diverse array of domestic and international threats. When at its best, the FBI uses its law enforcement authorities in a narrowly tailored and focused way to protect American communities from dangerous criminals and defend the national security from foreign spies and terrorists. When it uses its power in a fair and equal manner, the FBI strengthens and reinforces the rule of law by protecting civil rights and holding corrupt government officials and abusive law enforcement officers to account. The tools and authorities the FBI needs to fulfill these critical responsibilities are far too easily abused, however, particularly because they are often exercised under a shroud of secrecy where legal restraints are too easily treated as unnecessary impediments to mission success. Establishing and

maintaining effective checks against error and abuse is necessary for the FBI to remain an effective law enforcement agency and essential to securing liberty and preserving democratic processes.

In the aftermath of the terrorist attacks of September 11, 2001, Congress and the attorney general loosened many of the legal and policy restraints on the FBI that had been designed to curb abuses of a previous era. Ignoring history's lessons, policy makers urged the FBI to take on a greater domestic intelligence role, and it adopted this mission with an overzealous vigor. The FBI's resulting transformation into a secret domestic intelligence agency is dangerous to a free and democratic society, especially because rapidly developing technologies have made it possible for the FBI to gather, catalogue, and analyze massive amounts of information about countless Americans suspected of no wrongdoing at all.

There is already substantial evidence that the FBI has gravely misused its new authorities and capabilities, as this report will detail. And there is little evidence to suggest that these new powers have made Americans any safer from crime and terrorism. Members of Congress continue to struggle to obtain reliable information demonstrating the effectiveness of the FBI's overbroad surveillance programs, and several deadly attacks by persons who had previously been investigated by the FBI raise serious questions about whether the influx of data is making it harder to detect threats, rather than easier.

Congress and the president should take the opportunity presented by this change of leadership at the FBI to conduct a comprehensive examination of the FBI's policies and practices to identify and curtail any activities that are illegal, unconstitutional, discriminatory, ineffective, or easily misused. The purpose of this report is to highlight the changes to FBI authorities that have had the most significant impact on the privacy and civil rights and liberties of Americans; to provide examples of error and abuse over the last 12 years that establish evidence of the need for reform; and to offer an agenda to restore the FBI to its proper role in the American criminal justice landscape as the pre-eminent federal law enforcement agency that serves as a model for all others in its effectiveness and in its respect for individual rights and civil liberties.

I. Tension Between Domestic Intelligence Activities and Constitutional Rights

Every 90 days for the past seven years the FBI has obtained secret Foreign Intelligence Surveillance Court (FISA Court) orders compelling telecommunications companies to provide the government with the toll billing records of *every* American's telephone calls, domestic and international, on an ongoing daily basis.[1] Other programs have collected similar data about Americans' email and Internet activity and seized the content of their international communications, even though there was no evidence they had done anything wrong. State and local police and the general public are encouraged to report all "suspicious" people and activity to the FBI. This is what a domestic intelligence enterprise looks like in our modern technological age.

Many Americans were shocked to learn that they were the targets of such an outrageously overbroad government surveillance program. Even many members of Congress who passed the statute that enabled this surveillance and were charged with overseeing FBI operations were unaware of the way the government was secretly interpreting the law.[2] But the American Civil Liberties Union (ACLU) had long warned that turning the FBI into a domestic intelligence agency by providing it with enhanced surveillance and investigative authorities that could be secretly used against Americans posed grave risks to our constitutional rights.[3]

Our nation's founders understood the threat unchecked police powers posed to individual liberty, which is why fully half of the constitutional amendments making up the Bill of Rights are designed to regulate the government's police powers. The founders realized that political rights could only be preserved by checking the government's authority to invade personal privacy and by establishing effective due process mechanisms to ensure independent oversight and public accountability. As the Supreme Court put it, "[t]he Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."[4]

Yet repeatedly since its very beginning over a hundred years ago, the FBI has claimed the authority not just to investigate and prosecute potential violations of law, but to conduct secret domestic intelligence activities that often skirted constitutional protections. Courts traditionally protect Fourth Amendment rights through the "exclusionary rule," which prohibits law enforcement officers from using the fruits of illegal searches in criminal prosecutions.[5] But this penalty poses little obstacle for intelligence investigations because the information collected in these programs is rarely intended for, or utilized in, criminal prosecutions. When it is necessary for prosecution, information discovered through secret intelligence programs can easily be replicated using traditional law enforcement tools, shielding the intelligence programs from judicial oversight and public scrutiny. And because these intelligence activities take place in secret, victims rarely know the government has invaded their privacy or violated their rights, so they cannot seek redress.

In a previous era, the FBI's unregulated covert domestic intelligence activities went on undiscovered for decades, protected by official secrecy until activists burglarized an FBI office in Media, Pennsylvania, in 1971, and released a thousand domestic intelligence files to reporters.[6] According to the Senate Select Committee established to investigate these illegal intelligence activities, FBI headquarters had opened over 500,000 domestic security files during this time and compiled a list of 26,000 Americans who would be "rounded up" during a national security emergency.[7] It found that these FBI domestic intelligence operations targeted numerous non-violent protest groups, civil rights organizations, and political dissidents with illegal wiretaps, warrantless physical searches, and an array of harassing "dirty tricks" designed to infiltrate, obstruct, discredit, and neutralize "perceived threats to the existing social and political order."[8]

The exposure of the FBI's intelligence abuses led to a series of reforms, including the Foreign Intelligence Surveillance Act (FISA), a law designed to regulate government surveillance for national security purposes and protect Americans' privacy.[9] An initiative to impose statutory limits on the FBI's authority failed, however. By way of compromise, Attorney General Edward Levi issued written guidelines in 1976 which circumscribed the FBI's authority to conduct domestic security investigations.[10] The Attorney General's Guidelines required the FBI to have a criminal predicate consisting of "specific and articulable facts giving reason to believe that an individual or group is or may be engaged in activities which involve the use of force or violence," before opening a full investigations. Upon receipt of information or allegations of criminal activity not meeting this threshold, the guidelines authorized preliminary investigations that allowed FBI agents to develop evidence to justify opening full investigations, but these were strictly limited in both time and scope.

Successive attorneys general modified and reinterpreted the Attorney General's Guidelines over the years and developed additional sets of guidelines regulating the FBI's use of informants and undercover operations. The Bush administration alone amended the various FBI guidelines four times after 9/11. But while the Attorney General's Guidelines can be beneficial in establishing objective standards and reasonable limitations on the FBI's power, they are not self-enforcing. A number of public scandals and investigations by Congress and the Justice Department Inspector General (IG) — both before and after the terrorist attacks of September 11, 2001 — reveal the FBI often violates and/or ignores these internal rules, along with other legal and constitutional limitations.

II. Unleashed: The FBI's Post-9/11 Powers

In the aftermath of the September 11th attacks the FBI sought to rid itself of these legal restraints and expand its investigative and intelligence collection capabilities. Acting during a period of fear and uncertainty, Congress, the White House, and the attorney general gave the FBI enhanced investigative and surveillance authorities to protect the nation from future terrorists they worried were ready to strike again. Other powers the FBI simply assumed for itself, often secretly, and at times in direct violation of existing laws.

A. Surveillance Powers Given and Taken

1. USA Patriot Act

On June 5, 2013, The Guardian published an astonishing Top Secret Foreign Intelligence Surveillance Court (FISA Court) order that compelled Verizon Business Network Services to provide the National Security Agency (NSA) with the "telephony metadata" for *all* of its customers' domestic and international telecommunications on an "ongoing daily basis" for the three-month duration of the order.[11] Metadata includes the telephone numbers called and received, calling card numbers, mobile subscriber identity and station information numbers, and time and duration of calls. This information gives the government a detailed picture of a person's

interests, associations, and activities, including personally intimate or potentially embarrassing information, such as whether they've called a virility clinic, Alcoholics Anonymous, or a suicide hotline. The order was issued pursuant to an FBI request for "business records" under **Section 215** of the USA Patriot Act, which authorizes the FISA Court to issue secret demands for "any tangible things," based on the FBI's declaration that the information is "relevant" to a terrorism or espionage investigation.[12]

The Washington Post reported that tens of millions of Verizon customers' records have been seized under this program, and Sen. Dianne Feinstein (D-Calif.) said this order appeared to be "the exact three-month renewal" of similar orders that began in 2006.[13] With over 200 Section 215 orders issued in 2012, it is very likely that many other telecommunications companies received similar requests for all their customers' metadata as well.[14] And since Section 215 authorizes the government to obtain "any tangible things," it is also likely that the FBI uses the provision to do bulk collection of other types of records. The statute specifically states that FBI agents may seek library circulation and book sales records, medical records, tax returns, and firearms sales records using Section 215, with approval of an FBI Executive Assistant Director.[15]

Rep. James Sensenbrenner (R-Wis.), the original House of Representatives' sponsor of the Patriot Act, said the Foreign Intelligence Surveillance Court's order to Verizon reflected an "overbroad interpretation of the Act" that was "deeply disturbing."[16] Rep. Sensenbrenner said the language in the statute was not intended to authorize such broad collection and questioned how the phone records of millions of innocent Americans could possibly be deemed "relevant" to a terrorism or counterintelligence investigation, as Section 215 requires. Indeed, FBI Director Mueller's 2011 testimony before the Senate Intelligence Committee seeking reauthorization of the Patriot Act suggested the FBI interpreted the statute narrowly and used it sparingly:

> [Section 215] allows us to go to the FISA Court and obtain an order to produce records that may be relevant to, say, a foreign intelligence investigation relating to somebody who's trying to steal our secrets or a terrorist. Upon us showing that the records sought are relevant to this particular investigation—a specific showing it is—the FISA Court would issue an order allowing us to get those records. It's been used over 380 times since 2001.[17]

What the public didn't know at the time was that the Justice Department and the FISA Court had established a secret interpretation of the law that significantly expanded the scope of what the FBI can collect with Section 215, despite the relatively small number of orders issued each year. At the same 2011 hearing, Sen. Ron Wyden (D-Ore.), who has access to this secret interpretation of the law due to his position on the Intelligence Committee but is barred by classification rules from revealing it, challenged Director Mueller:

> I believe that the American people would be absolutely stunned—I think Members of Congress, many of them, would be stunned if they knew how the PATRIOT Act was being interpreted and applied in practice.[18]

Sen. Wyden and Sen. Mark Udall (D-Colo.) have repeatedly complained over the last several years that Justice Department officials have made misleading public statements about the scope of this authority, even as they refused their demands to declassify this secret interpretation of law so that Americans could understand how the government is using Section 215.[19] It took an unauthorized leak of the FISA Court order to give the public — and many members of Congress — their first glimpse of the government's overbroad use of this Patriot Act authority.

Sen. Wyden and Sen. Udall have more recently challenged government claims that the bulk collection of telephone metadata under Section 215 has proven effective in preventing terrorist attacks, arguing they've seen no evidence the program "has provided any otherwise unobtainable intelligence."[20] The ACLU filed a Freedom of Information Act (FOIA) request in 2011 to force the release of records relating to the government's interpretation or use of Section 215, which is still being litigated.[21] After the leak of the classified FISA Court order, the ACLU (a Verizon customer) filed a lawsuit challenging the government's bulk collection of telephone metadata under the Patriot Act.[22]

This is not the first evidence of widespread abuse of this statute, however. Congress passed the USA Patriot Act just weeks after the 9/11 attacks, greatly expanding the FBI's authority to use surveillance tools originally designed for monitoring hostile foreign agents to secretly obtain personal information about Americans not even suspected of wrongdoing. Congress made several provisions temporary. But when Congress first revisited the expiring provisions in 2005 there was very little public information regarding how the statute had been used. So in reauthorizing the Act, Congress required the Justice Department Inspector General to audit the FBI's use of two Patriot Act authorities: National Security Letters (NSLs) and Section 215. Not surprisingly, five Inspector General audits conducted over the next several years confirmed widespread FBI abuse and mismanagement of these intelligence collection tools.

A 2007 Inspector General audit revealed that from 2003 through 2005 the FBI issued over 140,000 **National Security Letters** — secret demands for certain account information from telecommunications companies, financial institutions, and credit agencies that require no judicial approval — almost half of which targeted Americans. It found:

- The FBI so negligently managed this Patriot Act authority it did not even know how many National Security Letters it had issued, which resulted in three years of false reporting to Congress;[23]
- FBI agents repeatedly ignored or confused the requirements of the authorizing statutes and used National Security Letters to collect private information about individuals two or three times removed from the actual subjects of FBI investigations;

- Sixty percent of the audited files did not have the required supporting documentation, and 22 percent contained at least one unreported legal violation;[24]
- FBI supervisors circumvented the law by using control files to improperly issue National Security Letters when no authorizing investigation existed.[25]

In 2008, the IG released a second audit report covering the FBI's use of National Security Letters in 2006 and evaluating the reforms implemented by the DOJ and the FBI after the first audit was released.[26] The 2008 report revealed:

- The FBI was increasingly using National Security Letters to gather information on U.S. persons (57 percent in 2006, up from 53 percent in 2005);[27]
- High-ranking FBI officials improperly issued eleven "blanket National Security Letters" in 2006 seeking data on 3,860 telephone numbers, in an effort to hide that the data had been illegally collected with "exigent letters" (see below);[28] and
- None of the "blanket National Security Letters" complied with FBI policy, and several imposed unlawful non-disclosure requirements, or "gag orders," on National Security Letter recipients.[29]

Two other Inspector General audits reviewed the FBI's use of **Section 215** of the Patriot Act. Though this authority was used much less frequently than NSLs, the audits identified several instances of misuse, including an instance in which the FISA Court rejected a Section 215 application on First Amendment grounds, but the FBI obtained the records anyway without court approval.[30] But in many ways these Inspector General reports gave the public a false sense of security by masking the real problem with Section 215, which was the incredible scope of information the FBI secretly collected under the FISA Court's secret interpretation of the statute.

2. Exigent Letters and a Secret OLC Opinion

The Inspector General reports also revealed that the FBI routinely used "exigent letters," which claimed false emergencies to illegally collect the phone records of Americans.[31] In 2003, the FBI took the extraordinary step of contracting with three telecommunications companies to station their employees within FBI offices so that FBI supervisors could get immediate access to company records when necessary. This arrangement allowed the FBI to circumvent formal legal process, like grand jury subpoenas or National Security Letters, to obtain telephone records. FBI supervisors even made requests written on Post-it notes and took "sneak peeks" over the telecom employees' shoulders to illegally gain access to private telecommunications records. The FBI obtained records regarding approximately 3,000 telephone numbers where no emergency existed and sometimes where no investigation was opened, in clear violation of the Electronic Communications Privacy Act (ECPA).[32] When the Inspector General discovered this abuse, FBI supervisors issued inappropriate "blanket" National Security Letters in an improper attempt to legitimize the illegal data collection.

A particularly troubling aspect of the FBI's use of exigent letters was the fact that it sometimes used them to obtain the communications records of journalists, in violation of their First Amendment rights.[33] These improper data requests circumvented federal regulations and Justice Department policies established to protect press freedoms, which require the exhaustion of less intrusive techniques and attorney general approval before obtaining subpoenas for reporters' communication records.

The FBI initially admitted error with regards to the use of exigent letters and agreed to stop using them, though it tried to justify keeping the information it already collected. But in his final report on exigent letters, the Inspector General revealed that in 2009 the FBI developed a new legal interpretation of the Electronic Communications Privacy Act that allowed the FBI to ask telecommunication companies to provide it with certain communications records without emergencies or legal process.[34] The IG rejected this post-hoc re-interpretation of the law, so the FBI requested a Justice Department Office of Legal Counsel (OLC) opinion.[35] The OLC supported the FBI's argument in a January 2010 secret opinion, with which the Inspector General was clearly uncomfortable. He recommended that Congress examine this opinion and "the implications of its potential use," but there have been no public hearings to evaluate the manner in which the FBI exploits this new interpretation of the law.[36] The Justice Department has refused to release the OLC opinion in response to FOIA requests by media organizations and privacy advocates.[37]

3. Warrantless Wiretapping and the FISA Amendments Act

On December 16, 2005, The New York Times revealed that days after the 9/11 terrorist attacks President George W. Bush authorized the National Security Agency to conduct warrantless electronic surveillance of Americans' telecommunications in violation of the Fourth Amendment and the Foreign Intelligence Surveillance Act.[38] The FBI knew about this illegal surveillance practically from its inception and investigated leads it generated, but did nothing to stop it despite the criminal penalties associated with FISA violations.[39] Moreover, the FBI agents investigating the leads produced from the NSA program reportedly found them of little value, deriding them as "Pizza Hut leads" because they often led to delivery calls and other dead ends.[40]

The Bush administration ultimately acknowledged the existence of a program it called the "Terrorist Surveillance Program," which it said was designed to intercept al Qaeda-related communications to and from the U.S., but a follow-up article by The New York Times reported the program was larger than the officials admitted and involved a government "back door" into domestic telecommunications networks.[41] A 2006 article in USAToday alleged further that major telecommunications companies "working under contract to the NSA" provided the government domestic call data from millions of Americans for "social network analysis."[42]

When James Comey was promoted to deputy attorney general in December 2003, he evaluated the Justice Department's legal support for one portion of this highly classified program,

involving the bulk collection of domestic internet metadata, and found it lacking.[43] To his great credit, he refused to sign a Justice Department re-certification as to the legality of the program and resisted, with the support of FBI Director Mueller, an intense effort by the White House to compel a gravely ill Attorney General John Ashcroft to overrule Comey. The collection continued without Justice Department certification for several weeks, leading Comey, Mueller, and other Justice Department officials to threaten resignation. Comey and Mueller ultimately won legal modifications that assuaged their concerns, but the bulk collection of innocent Americans' internet data continued under a FISA Court order through 2011 and may be going on in some form today.[44] It remains unexplained why Ashcroft, Comey, and Mueller apparently approved other parts of the Terrorist Surveillance Program, including the warrantless interception of Americans' international communications and the collection of Americans' telephone metadata.

The public pressure resulting from the 2005 New York Times article led the Bush administration to bring other portions of the NSA's warrantless wiretapping program under FISA Court supervision in January 2007. But in May of that year an apparently adverse ruling by the FISA Court led the administration to seek emergency legislation from Congress so the program could continue.[45] Congress passed temporary legislation in August 2007 and then enacted the FISA Amendments Act in June 2008, giving the government the authority to seek FISA Court orders authorizing non-individualized electronic surveillance so long as it is targeted at foreigners outside the U.S. But questions about the scope and legality of these programs remain.[46]

The excessive secrecy surrounding the FBI's and NSA's implementation of the FISA Amendments Act exacerbates the threat to Americans' privacy posed by this unconstitutionally overbroad surveillance authority. The FISA Amendments Act is due to expire in 2015, but Congress must not wait to conduct the oversight necessary to curb abuse and protect Americans from unnecessary and unwarranted monitoring of their international communications.

B. Expanding FBI Investigative Authorities

The Bush administration vastly expanded the FBI's power by amending the Attorney General's Guidelines governing FBI investigative authorities four times over 8 years.[47] Each change lowered the evidentiary threshold necessary for the FBI to initiate investigations, increasing the risk that FBI agents would improperly target people for scrutiny based on their First Amendment activities, as they had in the past.

1. Ashcroft Attorney General's Guidelines

Attorney General John Ashcroft first amended the guidelines for general crimes, racketeering, and terrorism investigations in 2002, giving the FBI more flexibility to conduct investigations based on mere allegations.[48] The Ashcroft guidelines:

- Authorized the "prompt and extremely limited checking out of initial leads" upon receipt of any information suggesting the possibility of criminal activity;
- Prohibited investigations based *solely* on First Amendment activities, but authorized inquiries based on statements advocating criminal activity unless "there is no prospect of harm;"[49]
- Expanded the investigative techniques the FBI could use during preliminary inquiries, barring only mail openings and non-consensual electronic surveillance;[50] and
- Increased the time limits for preliminary inquiries to 180 days, with the possibility of two or more 90-day extensions.[51] These changes meant the FBI could conduct intrusive investigations of people for an entire year, including infiltration by informants, without facts establishing a reasonable indication that anyone was breaking the law.

The Ashcroft guidelines also allowed FBI agents to conduct "general topical research" online and "visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally."[52] The FBI later claimed this authority did not require the FBI agents attending public meetings to identify themselves as government officials. Attempting to assuage concerns that the FBI would misuse this expanded authority by targeting First Amendment-protected activity, FBI Director Robert Mueller said in 2002 that the FBI had no plans to infiltrate mosques.[53] Nonetheless, in the ensuing years there was a sharp increase in the FBI's controversial use of informants as *agents provocateur* in mosques and other Muslim community organizations.[54] In 2009, Director Mueller defended these tactics and said he did not expect the Obama administration to require any change in FBI policies: "I would not expect that we would in any way take our foot off the pedal of addressing counterterrorism."[55]

After 9/11, the FBI also increased the number of FBI agents assigned to terrorism matters and rapidly expanded its network of Joint Terrorism Task Forces, in which other federal, state, and local agencies provide additional human resources for terrorism investigations. Today it has 103 Task Forces across the country, employing approximately 4,400 members of federal, state, and local law enforcement; the intelligence community; and the military.[56]

2. Evidence of FBI Spying on Political Activists

Concerned that the combination of expanded authorities and additional resources devoted to terrorism investigations would result in renewed political spying, ACLU affiliates around the country filed FOIA requests in 2004, 2005, and 2006 seeking FBI surveillance records regarding dozens of political advocacy and religious organizations and individual activists.[57] The FBI response revealed that FBI terrorism investigators from a variety of different field offices had collected information about peaceful political activity of environmental activists, peace advocates, and faith-based groups that had nothing to do with terrorism.

These inappropriate FBI investigations targeted prominent advocacy organizations such as the School of the America's Watch, Greenpeace, People for the Ethical Treatment of Animals, the

Rocky Mountain Peace and Justice Center in Colorado, and the Thomas Merton Center for Peace and Justice in Pennsylvania, among many others. In a document that reads as if it were written during the Hoover era, an FBI agent describes the peace group Catholic Worker as having "semi-communistic ideology."[58] Environmental activist and self-described anarchist Scott Crow later submitted his own Privacy Act request to the FBI and received 440 pages of materials documenting FBI surveillance directed against him from 2001 through 2008.[59] The FBI reports exposed the agents' disdain for the activists they investigated, with one suggesting that non-violent direct action was an "oxymoron" and another stating that attendees at an activist camp "dressed like hippies" and "smelled of bad odor."[60]

3. 2010 Inspector General Report Confirms Spying and Lying

In response to a 2006 congressional request, the Justice Department Inspector General audited a small sample (six) of the multiple FBI investigations of domestic advocacy groups uncovered by the ACLU.[61] In a report that wasn't released until 2010, the Inspector General confirmed the FBI abused its authority in these cases and at times improperly collected and retained information detailing the activists' First Amendment activities.[62]

The Inspector General concluded that the FBI's predicate for opening preliminary investigations against these advocacy groups and individuals was "factually weak." In some cases, it was based on unpersuasive, "speculative, after-the-fact rationalizations," because the files lacked the required documentation of the "information or allegation" to justify opening the case.[63] But because the guidelines require such a low "information or allegation" standard for opening preliminary investigations, the Inspector General concluded that opening many of these fruitless and abusive FBI investigations did not initially violate Justice Department policy.[64] Still, the Inspector General did find that the FBI violated the guidelines in some cases by:

- Extending some of these investigations "without adequate basis;"
- Initiating more intrusive full investigations when the facts only warranted preliminary investigations; and
- Retaining information about the groups' First Amendment activities in FBI files, in violation of the Privacy Act.[65]

Controversially, and despite the lack of proper documentation, the Inspector General determined that these investigations were not opened based "solely" on the groups' political activities or beliefs, but rather upon the FBI agents' speculation that the groups or individuals *might* commit a federal crime in the future. This conclusion appeared argumentative, however, because the Inspector General did not explain why the agents opened cases on these particular potential future criminals rather than any other potential future criminals, or whether political viewpoint was a significant factor in these decisions. The report conceded that the documents "gave the impression that the FBI's Pittsburgh Field Division was focused on the [Thomas] Merton Center as a result of its anti-war views."[66] That such baseless investigations of political activists were

found to fall within Justice Department policy clearly reveals that the FBI guidelines' prohibition against investigations based "solely" on First Amendment activity is insufficient to protect First Amendment rights.

Other abuses were identified. In one case, an FBI agent tasked an informant to infiltrate a peace group and to collect details of its First Amendment activities, just so the agent could demonstrate participation in the FBI's informant program.[67] The Inspector General also criticized the FBI for treating non-violence civil disobedience as "acts of terrorism," which had real consequences for the activists, as FBI policy mandates that subjects of terrorism investigations be placed on terrorist watch lists."[68] As a result, the FBI tracked their travel and advocacy activities as well as their interactions with local law enforcement.[69] One activist the FBI investigated was handcuffed and detained during a traffic stop, which the officer justified by alleging the activist was "affiliated with a terrorist organization."[70]

Finally, the Inspector General found that after the ACLU released the records, FBI officials made false and misleading statements to Congress and the American public in an attempt to blunt the resulting criticism.[71] The FBI Executive Secretariat Office responded to a citizen's complaint about the inappropriate investigation of Catholic Worker by stating that the FBI only seeks to prevent violence and does not target "lawful civil disobedience," even though the FBI files on Catholic Worker did document civil disobedience and made no reference to violence or terrorism.[72] The false statements to Congress are discussed further below.

4. Mukasey Attorney General's Guidelines

In December 2008, during the final weeks of the Bush administration, Attorney General Michael Mukasey issued revised Attorney General's Guidelines that authorized the FBI to conduct a new type of investigation, called an "assessment," which does not require FBI agents to establish *any* factual predicate before initiating investigations, so long as they claim their purpose is to prevent crime or terrorism or protect national security.[73] The Mukasey guidelines allow the FBI to utilize a number of intrusive investigative techniques during assessments, including:

- Physical surveillance;
- Retrieving data from commercial databases;
- Recruiting and tasking informants to attend meetings under false pretenses;
- Engaging in "pretext" interviews in which FBI agents misrepresent their identities in order to elicit information; and
- Using grand jury subpoenas to collect subscriber information from telecommunications companies.[74]

Under the Mukasey guidelines, "assessments" can even be conducted against an individual simply to determine if he or she would make a suitable FBI informant. Nothing in the new guidelines protects entirely innocent Americans from being thoroughly investigated by the FBI

under this assessment authority. The new guidelines also explicitly authorize the surveillance and infiltration of peaceful advocacy groups in advance of demonstrations, and they do not clearly prohibit using race, religion, or national origin as factors in initiating assessments, so long as investigations are not based "solely" on such factors.[75]

A 2009 FBI Counterterrorism Division **"Baseline Collection Plan"** obtained by the ACLU reveals the broad scope of information the FBI gathers during assessments:

- Identifying information (date of birth, social security number, driver's license and passport number, etc.);
- Telephone and emailaddresses;
- Current and previous addresses;
- Current employer and job title;
- Recent travel history;
- Whether the person lives with other adults, possesses special licenses or permits, or has received specialized training; and
- Whether the person has purchased firearms or explosives.[76]

The FBI claims the authority to retain all the personal information it collects during these investigations indefinitely, even if the people being assessed are found to be innocent.

The New York Times reported that the FBI opened 82,325 assessments on individuals and groups from March 2009 to March 2011, yet only 3,315 of these assessments developed information sufficient to justify opening preliminary or full investigations.[77] That so few assessments discovered any information or allegation that would meet even the low threshold for opening a preliminary investigation makes clear that the FBI investigated tens of thousands of entirely innocent people under its assessment authority. Moreover, at the conclusion of an assessment or investigation, after "all significant intelligence has been collected, and/or the threat is otherwise resolved," the FBI's Baseline Collection Plan authorizes agents to implement a so-called **"disruption strategy,"** which permits FBI agents to continue using investigative techniques "including arrests, interviews, or source-directed operations to effectively disrupt [a] subject's activities."[78] This resurrection of reviled Hoover-era terminology is troubling, particularly because FBI counterterrorism training manuals recently obtained by the ACLU indicate the FBI is once again improperly characterizing First Amendment-protected activities as indicators of dangerousness.

C. FBI Profiling Based on Race, Ethnicity, Religion and National Origin

Ironically, the FBI's authority to profile based on race, ethnicity, religion, and national origin was enhanced by Justice Department guidance that claimed to ban profiling in federal law enforcement. When issuing the Justice Department Guidance Regarding the Use of Race by Federal Law Enforcement Agencies in 2003, Attorney General Ashcroft said, "[u]sing race… as

a proxy for potential criminal behavior is unconstitutional and undermines law enforcement by undermining the confidence that people have in law enforcement."[79] The ACLU couldn't have agreed more.

But while the guidance prohibited federal agents from considering race or ethnicity "to any degree" in making routine or spontaneous law enforcement decisions (absent a specific subject description), it also included broad exemptions for national security and border integrity investigations, and it did not prohibit profiling based on religion or national origin.[80] Allowing profiling in border integrity investigations disproportionately impacts Latino communities, just as profiling in national security investigations has led to inappropriate targeting of Muslims, Sikhs; and people of Arab, Middle Eastern, and South Asian descent. And given the diversity of the American Muslim population, the failure to ban religious profiling specifically threatens African Americans as well, who comprise from one-quarter to one-third of American Muslims.[81] In effect, Attorney General Ashcroft's ban on racial profiling had the perverse effect of tacitly authorizing the profiling of almost every minority community in the U.S.

1. The FBI Domestic Investigations and Operations Guide

An internal FBI guide to implementing the 2008 Attorney General's Guidelines, called the Domestic Investigations and Operations Guide (DIOG), contains startling revelations about how the FBI is using race and ethnicity in conducting assessments and investigations.[82] While the DIOG repeats the Attorney General's Guidelines' requirement that investigative and intelligence collection activities must not be based "solely" on race, it asserts that FBI agents are authorized to use race and ethnicity when conducting what it calls "domain management" assessments. Through this program, the FBI allows:

- *"Collecting and analyzing racial and ethnic community demographics."* The DIOG authorizes the FBI to "identify locations of concentrated ethnic communities in the Field Office's domain, if these locations will reasonably aid in the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness for the purpose of performing intelligence analysis… Similarly, the locations of ethnically-oriented businesses and other facilities may be collected…"[83]
- *Collecting "specific and relevant" racial and ethnic behavior.* Though the DIOG prohibits "the collection of cultural and behavioral information about an ethnic community that bears no relationship to a valid investigative or analytical need," it allows FBI agents to consider "focused behavioral characteristics reasonably believed to be associated with a particular criminal or terrorist element of an ethnic community" as well as "behavioral and cultural information about ethnic or racial communities" that may be exploited by criminals or terrorists "who hide within those communities."[84]
- *"Geo-mapping."* The DIOG states that "As a general rule, if information about community demographics may be collected it may be 'mapped.'"[85]

The DIOG's instruction that the FBI may collect, use, and map the demographic information of racial and ethnic communities raises concerns that, once these communities are identified and mapped, the FBI will target them for additional intelligence gathering or investigation based primarily, if not entirely, on their racial and ethnic makeup.

Treating entire communities as suspect based on their racial, ethnic, or religious makeup offends American values. It's also counterproductive to effective law enforcement. In fact, an FBI official publicly criticized an equally inappropriate NYPD surveillance and mapping operation targeting Muslims throughout the northeast for undermining law enforcement relations with the community.[86] Newark FBI Special Agent in Charge Michael Ward called the NYPD program "not effective," saying there should be "an articulable factual basis" for intelligence collection and that "there's no correlation between the location of houses of worship and minority-owned businesses and counterterrorism."[87] Unfortunately the FBI is not following his advice.

The FBI unilaterally amended the DIOG in October 2011, giving its agents powers that are not authorized in the current Attorney General's Guidelines issued in 2008.[88] These new powers include blanket permission for agents to search law enforcement and commercial databases without even opening an assessment on the person searched or documenting why the search was performed. The 2011 DIOG amendments also authorized FBI agents to search peoples' trash during an assessment to find derogatory information to pressure them into becoming informants. Since the 2008 Attorney General's Guidelines did not grant these powers, it is difficult to see where the FBI finds authorization for these activities.

The FBI secretly amended the DIOG again in June 2012.[89] Only one section of this new guide has been released, pursuant to an ACLU FOIA request regarding the FBI's policy for obtaining stored e-mails. One substantive change from the 2011 DIOG removes the requirement for FBI agents to specify in affidavits submitted to judges for criminal wiretap warrants whether the interception implicates sensitive circumstances, such as whether it targets public officials or religious leaders.[90] A new subsection requires the agents to discuss the sensitive circumstances with Justice Department prosecutors, but failing to advise the judge evaluating the warrant request would seem to improperly withhold potentially important information that could impact the probable cause determination. It is unknown why this change was made.

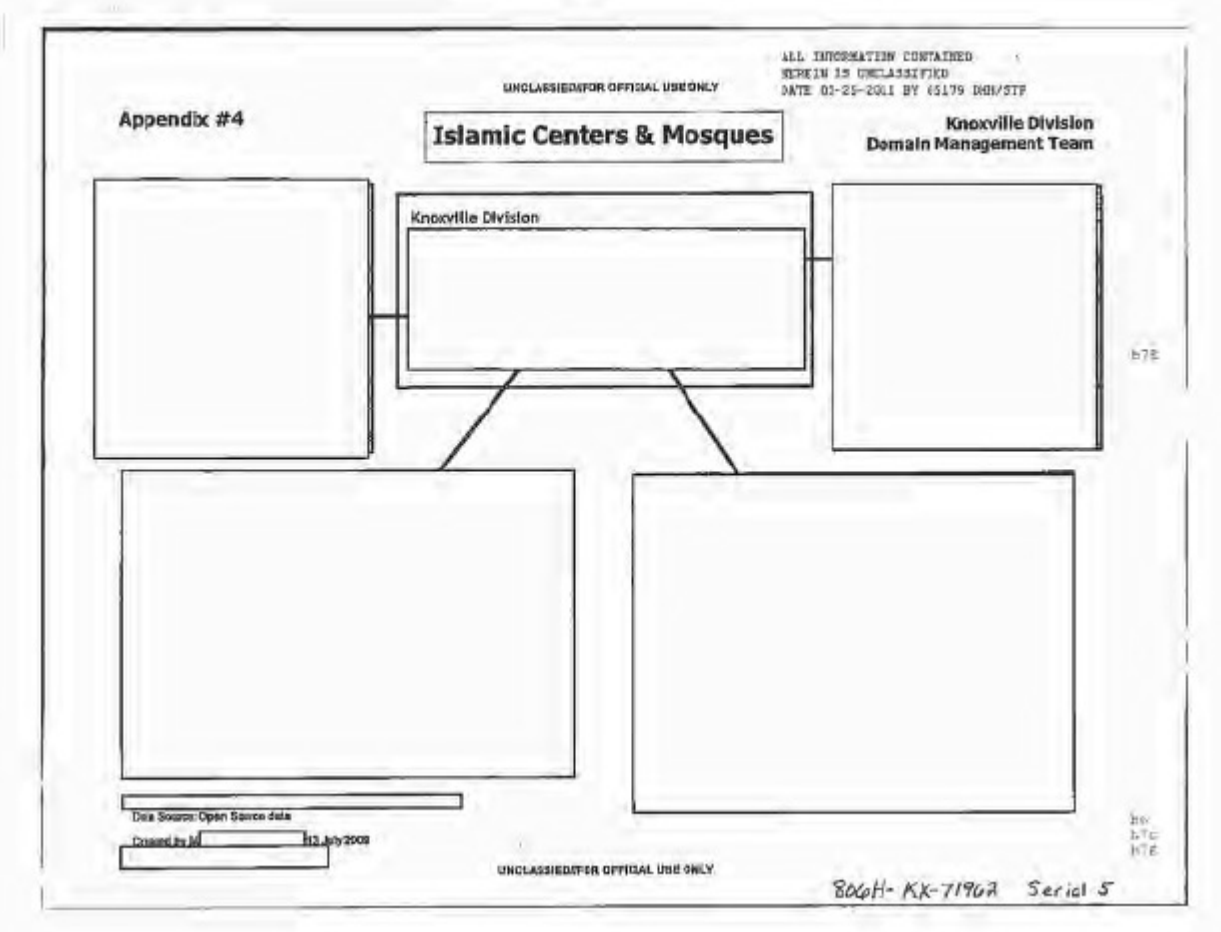
2. FBI Racial and Ethnic Mapping

In 2010, ACLU affiliates throughout the country issued FOIA requests to obtain information about how the FBI's domain management program operates. Although heavily redacted, the documents received from a number of different field offices demonstrate that FBI analysts make judgments based on crude stereotypes about the types of crimes different racial and ethnic groups commit, which they then use to justify collecting demographic data to map where people with that racial or ethnic makeup live. The DIOG claims that collecting community racial and ethnic data and the location of ethnic-oriented businesses and facilities is permitted to "contribute to an

awareness of threats and vulnerabilities, and intelligence collection opportunities," which raises concerns the FBI is seeking to identify these racial and ethnic communities to target them for intelligence collection and investigation in a disparate manner from other communities.[91]

For example, a Detroit FBI field office memorandum entitled "Detroit Domain Management" asserts that "[b]ecause Michigan has a large Middle-Eastern and Muslim population, it is prime territory for attempted radicalization and recruitment" by State Department-designated terrorist groups that originate in the Middle East and Southeast Asia. [92] Based on this unsubstantiated assertion of a potential threat of recruitment by terrorist groups on the other side of the world, the Detroit FBI opened a "domain assessment" to collect and map information on all Muslims and people of Middle-Eastern descent in Michigan, treating all of them as suspect based on nothing more than their race, religion, and national origin. Collecting information about the entire Middle-Eastern and Muslim communities in Michigan is unjust, a violation of civil rights and an affront to religious freedom and American values. It's also a surprisingly ignorant approach for an intelligence agency, because it ignores the fact that many Michigan Muslims are not Middle Eastern or South Asian. The Muslim community is incredibly diverse, and almost than a third of Michigan Muslims is African-American.[93] Treating Muslim communities as monolithic, and universally suspect, isn't good intelligence; it's religious bigotry.

Other documents confirm that the FBI is targeting American Muslims and their religious institutions for intelligence attention through its Domain Management program. Below is a sample of a redacted FBI Knoxville domain management map:



Unfortunately, this type of targeting based on broad-brush racial, ethnic, religious, and national origin stereotyping appears in many different types of domain assessments focusing on a wide array of groups.

A 2009 Atlanta FBI Intelligence memorandum documents population increases among "black/African American populations in Georgia" from 2000 to 2007 in an effort to better understand the purported terrorist threat from "Black Separatist" groups.[94] A 2009 FBI memo justifies opening a domain assessment of Chinese communities by stating that "San Francisco domain is home to one of the oldest Chinatowns in North America and one of the largest ethnic Chinese populations outside mainland China," and "[w]ithin this community there has been organized crime for generations."[95] The same memo justifies mapping the "sizable Russian population" in the region by referencing the existence of "Russian criminal enterprises operating within the San Francisco domain."[96] Several documents from FBI offices in Alabama, New Jersey, Georgia, and California indicate the FBI conducted overly-broad assessments that include tracking communities based on race and national origin to examine threats posed by the criminal gang Mara Salvatrucha (MS-13).[97] While MS-13 certainly represents a criminal threat meriting law enforcement concern, the documents reveal that the FBI uses the fact that MS-13 was originally started by Salvadoran immigrants to justify collecting population data for communities

originating from other Spanish-speaking countries, including Mexico, Cuba, the Dominican Republic, Colombia, and from the U.S. territory of Puerto Rico, even though the FBI acknowledges MS-13 admits "non-Hispanic individuals."[98]

Targeting entire communities for investigation based on racial and ethnic stereotypes is not just unconstitutional, it produces flawed intelligence. The FBI should focus on actual criminal suspects and national security threats, not mapping entire communities based on racial stereotypes.

3. Innocent Victims of Aggressive Investigation and Surveillance

The FBI's overbroad and aggressive use of its investigative and surveillance powers, and its willingness to employ "disruption strategies" against subjects not charged with crimes can have serious, adverse impacts on innocent Americans. Being placed under investigation creates an intense psychological, and often financial, burden on the people under the microscope and their families, even when they are never charged with a crime. All the more so when a heinous crime like terrorism is alleged, and when the investigators are convinced the subject of their investigation is guilty but they just don't have the evidence necessary for arrest. During the FBI's relentless investigation of the 2001 anthrax attacks, for instance, The New York Times reported that several people falling under suspicion lost jobs, were placed on watch lists, had citizenship and visa applications denied, and personal relationships destroyed.[99] The FBI publicly hounded bioterrorism researcher Steven Hatfill for over a year, following him so closely with up to eight FBI surveillance cars that one of them once ran over his foot.[100] FBI officials later acknowledged Hatfill was completely innocent, and the Justice Department paid him $4.6 million in damages. The FBI then turned its sites on another researcher, Bruce Ivins, who suffered a mental breakdown and committed suicide. The National Research Council has since questioned the strength of the scientific evidence supporting the FBI's case against Ivins, but the FBI considers the case closed.[101]

Such deleterious effects can be felt not just by the individuals who come under law enforcement suspicion, but by entire communities. A groundbreaking 1993 study in the United Kingdom by professor Paddy Hillyard documented how emergency anti-terrorism measures treated the Irish living in Britain and Northern Ireland differently in both law and police practice from the rest of the population, effectively marking them as a "suspect community." The study found the British anti-terrorism practices inflicted physical, mental, and financial effects on the Irish community at large, not just those directly targeted, and had a suppressive effect on "perfectly legitimate political activity and debate around the Northern Ireland question."[102]

There is evidence U.S. anti-terrorism enforcement and intelligence efforts are having similar effects on the American Muslim community. In 2009, the ACLU documented the chilling effect aggressive enforcement of anti-terrorism financing laws was having on American Muslim religious practices, particularly in suppressing mosque attendance and charitable giving, which is

an important tenet of Islam.[103] One donor to a Muslim charity interviewed for the ACLU report said:

> Our whole community was approached by the FBI about donations. They've intimidated our whole community… They've been asking about every single Muslim charity. Everyone is aware of this. People aren't giving as much as they should be giving, because of this.[104]

In 2013, civil rights and police accountability groups in New York published a report detailing how an NYPD surveillance program targeting Muslim communities throughout the northeast suppressed Muslims' religious, political, and associational activities.[105] Treating entire communities as suspect because of their race, ethnicity, religion, or national origin violates individual rights and American values and undermines effective law enforcement.

D. Unrestrained Data Collection and Data Mining

The FBI has also claimed the authority to sweep up voluminous amounts of information independent of assessments or investigations. The FBI obtains this data—often containing personally identifiable information—from open or public source materials; federal, state, or local government databases or pervasive information sharing programs; and private companies and then amasses it in huge data bases where it is mined for a multitude of purposes.

1. eGuardian and Suspicious Activity Reports

In 2009, the FBI established a new database called eGuardian to collect reports of "suspicious" behavior generated by state and local law enforcement agencies[106] to be shared broadly with other federal law enforcement agencies, the Department of Homeland Security, and the intelligence community.[107] Like many other suspicious activity reporting (SAR) programs, the standards governing the definition of "suspicious" conduct for reporting to eGuardian are extremely vague and over-broad, making it likely that reports will be based on racial or religious profiling or other bias, rather than objectively reasonable indications of wrongdoing.

The 2008 FBI press release announcing the eGuardian program suggested that people photographing the Brooklyn Bridge or the Washington Monument should be reported.[108] Few eGuardian SARs have been made public, but based on what other SAR programs produce, it is likely that particular religious, racial, and ethnic communities are disproportionately targeted and inappropriately reported for engaging in so-called suspicious activity. National Public Radio and the Center for Investigative Reporting reviewed more than 1,000 pages of SARs submitted from security officials at Minnesota's Mall of America and found that "almost two-thirds of the 'suspicious' people whom the Mall reported to local police were minorities."[109]

It is also clear that eGuardian has become a repository for improperly collected information about First Amendment-protected activities. In 2007, the Pentagon shuttered its Threat and Local

Observation (TALON) database system, which collected reports of suspicious activity near military bases, after media reports revealed that it included information about innocent and constitutionally-protected activity such as anti-war meetings and protests.[110] The Pentagon office that ran TALON was closed, but the improperly collected data collected was turned over to the FBI, and the military now provides SARs directly to eGuardian.[111]

While eGuardian has been established to collect reports "that appear to have a potential nexus to terrorism" — an already inappropriately low standard — even information the FBI deems "inconclusive" can be retained for five years, searched, and used for "pattern and trend analysis."[112] The value of retaining such innocuous data on Americans' behavior is highly questionable and may even harm efforts to identify threats by overwhelming analysts with large volumes of irrelevant data. A George Washington University Homeland Security Policy Institute survey of state and local law enforcement officials who worked with SARs called them "white noise" that impeded effective intelligence analysis.[113]

Another major problem is that eGuardian effectively competes with another federal government SAR. The Intelligence Reform and Terrorism Prevention Act of 2004 established the Information Sharing Environment (ISE) to serve as the conduit for terrorism-related information sharing between state and local law enforcement and the federal government.[114] A March 2013 Government Accountability Office report found that though the two programs share information between them, eGuardian uses a lower evidentiary threshold for inclusion of SARs, which creates risks and privacy problems.

The Government Accountability Office found that "many fusion centers have decided not to automatically share all of their ISE-SARs with eGuardian" because eGuardian doesn't meet ISE standards.[115] One fusion center said it would never provide SARs to eGuardian because of the fusion center's privacy policy.[116] The Government Accountability Office also found that the two systems "have overlapping goals and offer duplicative services."[117] This duplicity wastes resources and creates a risk that potential threats fall between the cracks.

Though the SAR programs have been operational for years, neither the ISE Program Manager nor the FBI track whether SAR programs deter terrorist activities or assist in the detection, arrests, or conviction of terrorists, and they have not developed performance measures to determine whether these programs have a positive impact on homeland security.[118]

2. Mining Big Data

The FBI also has much larger databases, and more ambitious data mining programs, but it goes to great lengths to mask these programs from congressional and public oversight. An FBI budget request for fiscal year 2008 said the FBI had amassed databases containing 1.5 billion records, and two members of Congress described documents predicting the FBI would have 6 billion records by 2012, which they said would represent "20 separate 'records' for each man, woman and child in the United States."[119]

On October 29, 2001, President Bush directed the attorney general to establish a Foreign Terrorist Tracking Task Force (Tracking Task Force) to deny aliens "associated with, suspected of being engaged in, or supporting terrorist activity" entry into the U.S. and to "locate, detain, prosecute and deport any such aliens" already in the country.[120] But this mission quickly expanded as the Tracking Task Force was transferred to the FBI and began ingesting larger and larger data sets. The Justice Department's 2007 data mining report, required by the Patriot Reauthorization Act of 2005, revealed the existence of the Foreign Terrorist Tracking Task Force "Data Mart." The report said the Data Mart included data from government agencies, including the Terrorist Screening Center Database and the Department of Homeland Security's I-94 database, and commercial data from the Airlines Reporting Corporation and private data aggregation companies Choicepoint and Accurint.[121] The data mining report acknowledged these databases contained U.S. person information, but it maintained that the focus of Tracking Task Force data mining queries was on identifying "foreign terrorists."[122] The report clarified, however, that if the FBI's data mining tools establish high "risk scores" for U.S. persons the Tracking Task Force analysts "may look at them to see if they have derogatory information."[123]

But the FBI had even bigger plans. In 2007, it submitted a budget request seeking $100 million over three years to establish the National Security Analysis Center, which would combine the Tracking Task Force with the largest FBI data set, the Investigative Data Warehouse.[124] The Investigative Data Warehouse contains all intelligence and investigative data collected by the FBI across all of its programs, along with "other government agency data and open source news feeds."[125] This data includes, for example, well over a million suspicious activity reports filed by financial institutions each year as required by the Bank Secrecy Act, which was expanded by the Patriot Act to include car dealerships, casinos, pawn shops, and even the post office.[126] The FBI ingests this data directly from the Treasury Department for inclusion in the Investigative Data Warehouse, along with an additional 14 million currency transaction reports submitted annually to document cash transactions over $10,000.[127]

By combining the Investigative Data Warehouse with the Tracking Task Force, the National Security Analysis Center would have access to 1.5 billion records. And based on the budget request, the FBI clearly wanted to obtain more. Congress instead requested a Government Accountability Office audit of the National Security Analysis Center, but the FBI refused to give the auditors access to the program.[128] Congress temporarily pulled funding for the National Security Analysis Center in 2008 because of this impasse, but there has been little public discussion about it since.[129] A 2013 Inspector General report says the Tracking Task Force "incorporated" the National Security Analysis Center and its datasets and expanded its role.[130]

Today the Tracking Task Force has 360 staff members, mostly analysts and contractors, and an annual budget of $54 million.[131] It runs 40 separate projects, and despite its name, no longer limits its mission to the detection of foreign terrorists. According to a 2013 Inspector General report, the Tracking Task Force runs a program called "Scarecrow" that targets "financial schemes" used by U.S. citizens who may be affiliated with the "Sovereign Citizen" movement, a

"FINDUS" project to find known or suspected terrorists within the U.S, and a Traveler Assessment Project "to help identify and assess unknown individuals who may have links to terrorism."[132] According to a 2012 Systems of Records Notice covering all FBI data warehouses, the information in these systems can be shared broadly, even with foreign entities and private companies, and for a multitude of law enforcement and non-law enforcement purposes.[133]

But scientists challenge whether pattern-based data mining to identify potential terrorist threats is a viable methodology. A 2008 study by the National Research Council of the National Academies of Sciences funded by the Department of Homeland Security concluded that "[a]utomated terrorist identification is not technically feasible because the notion of an anomalous pattern—in the absence of some well-defined ideas of what might constitute a threatening pattern—is likely to be associated with many more benign activities than terrorist activities."[134] The National Research Council pointed out that the number of false leads produced by such a system would exhaust security resources and have severe consequences for the privacy of multitudes of innocent people. The study concluded, "[t]he degree to which privacy is compromised is fundamentally related to the sciences of database technology and statistics as well as to policy and process.[135] Given these scientific limitations and privacy implications of using pattern-based data mining to identify potential terrorists, the National Research Council recommended that agencies be required to employ a systematic process to evaluate the "effectiveness, lawfulness and consistency with U.S. values" of such automated systems *before they are deployed* and be subjected to "robust, independent oversight" thereafter.[136]

Tracking Task Force operations do not appear to have been subjected to such systematic evaluation or scrutiny, and as a result the FBI wastes resources on false leads that threaten privacy and security. In a heavily redacted section of the 2013 report's discussion of its effectiveness, the Inspector General concluded that:

- The Tracking Task Force "did not always provide FBI field offices with timely and relevant information," which caused an "inefficient use of field office resources;"[137]
- The Tracking Task Force "rarely made" updates to the Traveler Assessment program (despite an FBI policy that requires them every 90 days) and "may have been providing field offices with traveler threat information that was not consistent with the FBI's current threat picture;"[138] and
- FBI supervisors received Tracking Task Force leads based on information they had already seen, including some they had provided to Tracking Task Force in the first place.[139]

An intriguing redaction in the report's discussion of a Tracking Task Force lead sent to the Phoenix FBI office appears to identify a recurring problem regarding the dissemination of a particular type of information. FBI agents investigating the lead were "unable to determine the individual's nexus to terrorism," and the Inspector General concluded that the Tracking Task Force should "continue to work on minimizing the dissemination of [REDACTED]." This

warning about potentially inappropriate dissemination is remarkable because FBI and Justice Department officials overseeing the Tracking Task Force claimed that they have "not encountered any privacy-related issues or problems." [140]

The Inspector General's statement likely says more about the lack of effective oversight rather than the lack of privacy-related problems. With the plethora of information in the Data Mart and its broad dissemination throughout the law enforcement and intelligence communities, it is hard to imagine that no privacy issues were ever raised. Indeed, the Inspector General went on to describe the FBI's four-year resistance to the Justice Department's Acting Privacy Officer's demands to update the Tracking Task Force's Privacy Impact Assessment, which was required by the E-Government Act of 2002. Despite the privacy officer's objections, the FBI continued operating the Tracking Task Force Data Mart during this period without an approved Privacy Impact Assessment, reflecting both an official disregard for privacy laws and internal oversight.[141]

3. Real Threats Still Slipping Through the Cracks

There is troubling evidence that the flood of information coming into the FBI as a result of its lower evidentiary requirements for investigation and intelligence collection is overwhelming its agents and analysts. Rather than helping them "connect the dots," it appears these overbroad data collection programs are impairing the FBI's ability to properly assess and respond to threat information it receives. While no law enforcement or intelligence agency could reasonably be expected to prevent every terrorist act, several recent attacks by individuals who were previously identified to the intelligence community or investigated by the FBI require a sober evaluation of whether the FBI's broad information collection and data mining methodologies are inundating it with false positives that obscure real threats. In a letter to the FBI seeking records regarding its 2011 investigation of apparent Boston marathon bomber Tamerlan Tsarnaev, House Homeland Security Committee Chairman Michael McCaul (R-Texas) and Rep. Peter King (R-N.Y.) pointed out that this was the sixth terrorist attack by a person who was previously known to the FBI or CIA.[142]

These included Chicagoan David Headley, who travelled freely back and forth to Pakistani terrorist training camps over several years, and then to Mumbai, India, where he conducted surveillance in preparation for the 2008 terrorist attacks by Lashkar-e-Taiba gunmen, which killed 166 people, including four Americans. Headley was already well-known to federal law enforcement according to an investigative report by Pro Publica, as he had felony drug convictions in the U.S. and later worked as a DEA informant.[143] Pro Publica's reporting reveals the FBI had numerous warnings from different individuals over several years that Headley was involved in terrorism. The FBI received its first tip that Headley was a terrorist shortly after 9/11, but closed its investigation based on his denials. The following year the Philadelphia FBI received a second warning from a family friend that Headley was involved with Pakistani militants. An agent performed a records check and closed the case without interviewing Headley.

In 2005, Headley's Canadian wife called an FBI terror tip line and told the FBI about Headley's involvement with the Pakistani terrorist group. She was interviewed several times but Headley was not. In 2007, Headley's second wife, in Pakistan, contacted the U.S. Embassy in Islamabad and told State Department security and U.S. Customs officers about Headley's involvement with the terrorist group, which they in turn reported to the FBI. The FBI received another tip shortly after the Mumbai attacks, from a friend of Headley's mother. FBI attempts to interview Headley were thwarted by a relative who falsely asserted that Headley was in Pakistan. Finally, in 2009 British intelligence identified him meeting with al Qaeda associates in Britain, and the FBI tracked him across Europe and back to the U.S., where he was arrested after a few months of investigation.

The second incident involved Abdulhakim Mujahid Muhammad, also known as Carlos Bledsoe, an American citizen and former gang member with a minor criminal record. In 2009, Muhammad shot two Army recruiters in Little Rock, Ark., in a self-described terrorist attack, killing one. Muhammad was known to the FBI because he had been arrested in Yemen the year before for possessing a false Somali passport and explosives manuals.[144] An FBI agent reportedly interviewed Muhammad twice, once in the Yemeni jail and again upon his return to the U.S.[145] According to ABC News, the Joint Terrorism Task Force opened a preliminary investigation of Muhammad when he returned from Yemen, yet he amassed an arsenal of weapons and successfully attacked the recruiting station without being detected by the investigating agents.[146] He was arrested by local police shortly after the attack.

While hindsight is always 20-20, these cases show critical information is still falling through the cracks at the FBI, even after years of expanding resources and investigative authorities. These cases demonstrate that the FBI's increased data collection activities may be doing more harm than good, as the constant response to false leads resulting from dubious "suspicious activity reports" and data mining programs makes it more difficult for agents to identify true threats that come into the FBI.

Another example involves the 2009 shooting incident in Ft. Hood, Texas, in which Army psychiatrist Major Nidal Hasan killed 13 fellow soldiers. The FBI Joint Terrorism Task Force in Washington, D.C., conducted an assessment of Hasan earlier that year in response to a lead sent from the San Diego office after agents intercepted two e-mails he sent to Anwar al-Aulaqi beginning in late 2008. According to an analysis of the investigation conducted by former FBI and CIA director William Webster, San Diego FBI officials received, evaluated, and catalogued 14 other emailmessages from Hasan to Aulaqi, and two responses from Aulaqi, but did not recognize the link to the original e-mails that sparked the assessment of Hasan, nor advise the D.C. Task Force officer of these additional communications. The Webster Commission later determined that Hasan's e-mails did not reveal "any suggestion of impending wrongdoing by Hasan," though it said that knowledge of these additional e-mails "would have undermined the assumption that Hasan had contacted Aulaqi simply to research Islam," which may have justified further investigation.[147]

In a section of the report subtitled "the data explosion," the Webster Commission identified the "exponential growth in the amount of electronically stored information" as a critical challenge for the FBI.[148] It concluded that the D.C. Joint Terrorism Task Force officer's assessment of Hasan was "belated, incomplete, and rushed, primarily because of their workload."[149] Similarly, the Commission found the San Diego agent and analyst assigned to the Aulaqi investigation were responsible for evaluating almost 30,000 electronic documents by the time of the Ft. Hood shooting, which averaged over 1,500 per month, or from 70 to 130 per work day.[150] The Commission called this pace "relentless" and suggested the failures in the Hasan investigation were "a stark example of the impact of the data explosion" on the FBI.[151]

National Counterterrorism Center (NCTC) Director Michael Leiter similarly cited the daily intake of data into intelligence community data bases in explaining why the NCTC failed to identify attempted so-called underwear bomber Umar Farouk Abdulmutallab as a threat, despite warnings it received from his father. In attempting to put the failure in "context," Leiter said the NCTC receives over 5,000 pieces of information and places more than 350 people on the terrorist watch list each day.[152] Such a deluge of information leads to bloated watch lists that can't be properly managed and therefore become meaningless. Abdulmutallab had been identified as a known or suspected terrorist in the FBI's Terrorist Identities Datamart Environment (TIDE) database, but was not placed on the No Fly List or the Selectee list, which would have subjected him to additional screening. A later Senate Homeland Security Committee investigation found DHS officials "skeptical" of the value of TIDE due to concerns over the quality of data it contained, which they claimed included a two-year-old child and the Ford Motor Company.[153]

The FBI also conducted a three-month assessment of Tamerlan Tsarnaev based on a March 2011 warning from the Russian government that he had developed radical views and planned to travel to Russia to join "underground" groups.[154] Rep. William Keating (D-Mass.), who saw the information provided in the letter during a trip to meet with the Russian security services, said the warning contained detailed information, including that Tsarnaev "wanted to join Palestinian fighters" before deciding to go to Dagestan instead because he knew the language.[155] The FBI's assessment reportedly determined Tsarnaev was not a threat, and it closed in June 2011 (some media reports suggested that FBI rules required closing the assessment after 90 days, but neither the FBI DIOG nor the Attorney General's Guidelines place time limits on assessments).[156] The FBI did place Tsarnaev on terrorism watch lists, however, despite closing the investigation. As a result, Joint Terrorism Task Force officials received alerts when Tsarnaev left for Russia in early 2012 and when he returned six months later, but the FBI did not renew its investigation.[157]

Predicting future dangerousness is all but an impossible task, and it is entirely possible that even Tsarnaev himself could not have predicted in 2011 that he would commit a terrorist attack in 2013. FBI agents cannot be expected to be fortune tellers. But reviewing the facts of this matter is important to determine whether current FBI practices are effective, as Rep. McCaul and Rep. King suggested.

The FBI said its investigation of Tsarnaev was one of over 1,000 assessments the Boston Joint Terrorism Task Force completed in 2011 alone.[158] Just as in the Hasan case, this torrid pace may have diminished the quality of the Tsarnaev assessment. The agents may have also been distracted fulfilling the data collection requirements of the FBI's "baseline collection plan," rather than concentrating on establishing evidence of a possible crime.

Another potentially crucial mistake is that the FBI appears to have focused more on evaluating the first allegation in the Russian warning, that Tsarnaev had developed radical views, rather than the second, which alleged that he planned to travel to Russia to join "underground" groups. Determining whether Tsarnaev held "radical" views would have been inappropriate for a U.S. law enforcement agency that respects the First Amendment and difficult to measure in any event, particularly given the FBI's flawed model of terrorist radicalization. But the allegation regarding Tsarnaev's plans to travel to Russia to join an underground group involved actionable intelligence about potentially illegal activity, as U.S. law prohibits providing material support to designated international terrorist groups. This allegation presented a fact question that the FBI could determine was either true or not true. But Tsarnaev's travel to Russia six months later inexplicably did not trigger a renewed investigation. The FBI did place Tsarnaev on the TIDE watch list, which at that point contained over 700,000 names, and on another watch list called the Treasury Enforcement Communications System (TECS), which is designed to alert Customs agents when a targeted subject travels abroad. Tsarnaev's travel to Russia six months later reportedly "pinged" the TECS system and alerted the Joint Terrorism Task Force members, as did his July 2012 return, but neither resulted in a renewed investigation.[159] This may be the most damning evidence against the FBI's overbroad approach to watch listing. Law enforcement officers repeatedly flooded with false positives from bloated watch lists become trained to ignore hits rather than respond to them. If the FBI's assessment of Tsarnaev was properly focused on whether he planned to join underground groups in Russia, his travel there would have raised alarms and a different result may have been possible.

Perhaps even more troubling, recent media reports indicate Tsarnaev may be implicated in a grisly triple murder in Waltham, Mass., on September 11, 2011, which occurred after the FBI assessment ended but before Tsarnaev travelled to Russia in January 2012.[160] Tsarnaev's potential involvement in serious criminal activity years before the Boston bombing raises additional questions for policymakers about the appropriate distribution of law enforcement resources. According to FBI crime data, in 2011 less than half of the 1.2 million violent crimes in the U.S. were solved through arrest or positive identification of the perpetrator.[161] Included in these unsolved crimes were over a third of the murders committed in 2011 and over 58 percent of the forcible rapes.[162] These numbers have remained fairly consistent over the last several years, even as intelligence activities directed against innocent Americans have increased. It is important to recognize that terrorism is a heinous crime with serious emotional and economic consequences, but it is still worth examining whether diverting the resources currently spent on

overbroad and ineffective suspicionless intelligence collection programs to helping police solve violent crimes would make all American communities safer as a result.

It is also important to note that the FBI has successfully investigated and prosecuted hundreds of defendants charged with terrorism-related offences both before and after 9/11, so it clearly has the tools and the competence necessary to address this problem. But given the impact its increased post-9/11 domestic intelligence powers have on American liberty, we cannot just trust the FBI that these authorities are necessary or effective. What becomes clear from reviewing the terrorist events the FBI failed to interdict is that the data explosion created by its lowered investigative and intelligence collection standards often impairs rather than enhances its ability to identify real threats. As the National Research Council recommended, the government should have to demonstrate the effectiveness of new counterterrorism policies and programs before they are implemented and subject them to strict legal limits and rigorous oversight to protect constitutional rights and privacy.

Preventing every possible terrorist attack is an unrealistic and unreachable goal, yet this imperative drives many of the overzealous collection programs that threaten privacy and civil liberties, even as they fail to produce tangible security benefits. It is time for policy makers and intelligence officials to conduct evidence-based evaluations of all counterterrorism programs and policies to end any that are ineffective or improperly infringe on constitutional rights.

4. Mining Bigger Data: The NCTC Guidelines

Another sign the Foreign Terrorist Tracking Task Force data mining programs are not effective came in March 2012, when the attorney general and director of National Intelligence announced dramatic changes to the National Counterterrorism Center's (NCTC) guidelines to allow it to collect, use, and retain records on U.S. citizens and permanent residents with no suspected ties to terrorism.[163] This wholesale rewrite of intelligence policy, approved over the objection of Department of Homeland Security and Justice Department privacy officers, upended decades-old protections of U.S. person information, subjecting potentially millions of innocent Americans to unjustified scrutiny by the intelligence community.[164] Under the new rules, the NCTC can swallow up entire government databases—regardless of the number of innocent Americans included—and use the information in myriad ways, including pattern-based data mining, for five years. Such unfettered collection is essentially a revival of the Bush administration's Total Information Awareness program, which Congress largely defunded in 2003 because of privacy concerns.[165] These privacy concerns have only increased over the last ten years, as Americans have become even more dependent on advanced information technology. But given the FBI's close collaboration with the NCTC, these changes also raise serious questions about whether the Foreign Terrorist Tracking Task Force program is effective. If the costly Tracking Task Force data mining programs work there would be no need for NCTC to build another system to accomplish the same task.

5. Exploitation of New Technologies

The FBI is also exploiting new technological developments in troubling ways. A tax fraud prosecution in Arizona revealed that the FBI has been failing to inform judges about the particularly invasive nature of "Stingray" devices when it seeks to obtain court orders for location information.[166] Stingray is a brand name for an IMSI catcher, which is a device that obtains identifying information from mobile communication devices—known as international mobile subscriber identity information—by mimicking a cell-phone tower. The IMSI catcher accomplishes this task in a particularly invasive way: by sending signals to all cell phones in the vicinity, including within people's homes, and tricking them into sending signals back to the IMSI catcher. Because it mimics a cell phone tower, the IMSI catcher can intercept the content of communications in addition to the identifying information, and the precise location of the mobile device.

The ACLU of Northern California obtained Justice Department documents showing the FBI has been obtaining pen register orders—which authorize the government to obtain telephone numbers called from and received by a particular mobile device based on a relevance determination—to obtain location data using IMSI catchers, without telling the magistrate judges that this invasive technology would be used.[167] The documents make clear the FBI has routinely used these misleading tactics to conceal its use of this technology over the course of several years.

6. Secret Spying and Secret Law

The public doesn't know the full extent of the FBI's domestic surveillance activities because so much of it takes place in secret, and Sen. Wyden has warned his colleagues that many of them don't know either, because the government secretly interprets laws in ways that expand its collection authorities beyond the plain language in the law.[168] As discussed above, we know the Justice Department has a secret interpretation of the Patriot Act and a secret OLC opinion re-interpreting Electronic Communications Privacy Act, and we know that at times the intelligence community has disregarded the law entirely.[169] We also know that the FBI cooperates with other federal intelligence agencies as well as state and local law enforcement agencies and private entities to enhance its ability to obtain and analyze data about Americans. But official secrecy bars us from knowing all we should—and it is not unreasonable to assume that's exactly the way the government wants it. In a democratic society governed by the rule of law, the public has a need and a right to know the legal parameters regulating government's surveillance of its citizenry.

Secret intelligence activities are particularly odious to a free society because they enable the circumvention of traditional legal and constitutional protections against government violations of individual rights. As the Senate Committee examining the FBI's intelligence abuses in the 1970s explained, a victim of illegal spying "may never suspect that his misfortunes are the intended

result of activities undertaken by his government, and accordingly may have no opportunity to challenge the actions taken against him."[170]

An FBI training presentation obtained by Wired Magazine entitled, "Unique Aspects of the Intelligence Profession," provides a glimpse of the impunity from legal oversight or consequences that intelligence officers assume they possess. It states that "[u]nder certain circumstances, the FBI has the ability to bend or suspend the law and impinge on the freedom of others."[171] This attitude, combined with the FBI's renewed embrace of a "disruption strategy," raise serious concerns about how the FBI implements its intelligence programs that demand attention from Congress.

III. Unaccountable: Evidence of Abuse, Need for Reform

With the substantial increases in the FBI's powers since 9/11, there needs to be an equally robust increase in oversight in order to curb abuse. Unfortunately, the FBI's internal controls have too often proved ineffective at preventing error and abuse, and external oversight has been too easily thwarted by the secrecy necessary to protect legitimate investigations and intelligence operations.

A. Shirking Justice Department Oversight

The five Inspector General reports on the FBI's misuse of its Patriot Act authorities serve as ample demonstration of the lack of effective internal controls within the FBI. The FBI responded to the 2007 reports by establishing new internal compliance policies, but the IG reviewed these reforms during the 2008 audits and found them insufficient to prevent further abuse. The IG criticized the FBI for repeatedly downplaying its violations of intelligence law and policy by describing them as "third party errors" or "administrative errors," arguing this characterization of the problem by FBI management sends "the wrong message regarding the seriousness of violations of statutes, guidelines or policies."[172] The Inspector General re-audited a sample of files previously examined by FBI inspectors and found three times more legal violations than the FBI identified.[173]

The 2008 report on Section 215 of the Patriot Act revealed a troubling incident in which the Foreign Intelligence Surveillance Court rejected an FBI request for a Section 215 order on First Amendment grounds, but the FBI General Counsel ignored this opinion and authorized the issuance of NSLs, which do not require judicial approval, to obtain the same information.[174] That a high-level FBI official would demonstrate such disdain for the court and the law is particularly troubling. The IG also concluded the FBI did not yet fully implement the recommended reforms from 2007, and that it was "too soon to definitively state whether the new system of controls… will eliminate fully the problems with the use of NSLs."[175] Despite these reports of abuse, Congress failed to narrow the FBI's powers, or even obtain a public explanation of the government's interpretation of the scope of its authorities, when the Patriot Act was reauthorized in 2011.[176]

As previously noted, the FBI is primarily regulated through Attorney General's Guidelines. In 2005, the Inspector General audited the FBI's compliance with the various Attorney General's Guidelines and found significant deficiencies that threatened people's rights. The Inspector General found at least one rules violation in a whopping 87 percent of the FBI informant files examined.[177] And even the meager evidentiary requirements of the 2002 Ashcroft amendments to the guidelines were clearly being ignored:

- Fifty-three percent of FBI preliminary inquiries that extended beyond the initial 180-day authorization period did not contain the required documentation authorizing the extension; and
- Seventy-seven percent of those that extended past 270 days contained "no documentation" to justify a second extension.[178] This meant people could remain under investigation for an entire year with no reasonable indication they were involved in illegal activity and without written justification for the continuing scrutiny.

Yet rather than tighten the rules, Attorney General Mukasey significantly loosened the guidelines again in 2008, despite these excessive violations. The Inspector General's 2010 analysis of the FBI's investigations of domestic advocacy groups, which covered only a handful of cases from 2001 to 2006, noted that violations of the 2002 guidelines identified in those investigations would not be violations under the 2008 guidelines.[179]

B. Suppressing Government Whistleblowers

The FBI has a notorious record of retaliating against FBI employees who report misconduct or abuse in the FBI and has used aggressive leak investigations to suppress other government whistleblowers.

Congress exempted the FBI from the requirements of the Whistleblower Protection Act of 1989 and instead required the Justice Department to establish an internal system to protect FBI employees who report waste, fraud, abuse, and illegality. Still, FBI Director Robert Mueller repeatedly vowed to protect Bureau whistleblowers:

> I issued a memorandum on November 7th [2001] reaffirming the protections that are afforded to whistleblowers in which I indicated I will not tolerate reprisals or intimidation by any Bureau employee against those who make protected disclosures, nor will I tolerate attempts to prevent employees from making such disclosures.[180]

Yet court cases and investigations by the Justice Department Office of Professional Responsibility and Inspector General have repeatedly found that FBI officials continue to retaliate against FBI employees who publicly report internal misconduct, including Michael German,[181] Sibel Edmonds,[182] Jane Turner,[183] Robert Wright,[184] John Roberts,[185] and Bassem Youssef.[186] Other FBI whistleblowers choose to suffer retaliation in silence. Special Agent Chad

Joy courageously blew the whistle on a senior FBI agent's serious misconduct during the investigation and prosecution of Alaska Sen. Ted Stevens, which resulted in the trial judge overturning the conviction against him, but only after the senator had lost re-election.[187] Special Agent Joy was publicly criticized by his then-retired supervisor, subjected to a retaliatory investigation, and then taken off criminal cases.[188] Joy resigned and no longer works at the FBI, while the FBI agent responsible for the misconduct in the Stevens' case continues to be assigned high-profile investigations—a clear sign that the FBI culture continues to protect agents involved in misconduct more than those who report it.[189]

These high-profile cases of whistleblower retaliation discourage other FBI personnel from coming forward. A 2009 Inspector General report found that 28 percent of non-supervisory FBI employees and 22 percent of FBI supervisors at the GS-14 and GS-15 levels "never" report misconduct they see or hear about on the job.[190] That such a high percentage of officials in the government's premiere law enforcement agency refuse to report internal misconduct is shocking and dangerous and perpetuates the risk that Americans like Sen. Stevens will continue to be victimized by overzealous investigations and prosecutions.

The FBI has also been involved in suppressing other government whistleblowers through inappropriately aggressive leak investigations. For example, when the U.S. media reported in 2005 that the National Security Agency (NSA) was spying on Americans' communications without warrants in violation of the Foreign Intelligence Surveillance Act, the FBI didn't launch an investigation to enforce the law's criminal provisions. It instead went after the whistleblowers, treating leaks to the American public about government malfeasance as espionage.[191] After more than a year of aggressive investigation and interviews, armed FBI agents conducted coordinated raids on the homes of four former NSA and Justice Department officials and a House Intelligence Committee staffer, treating them as if they were dangerous Mafiosi instead of dedicated federal employees who held the government's highest security clearances. William Binney, who served more than 30 years in the NSA, described an FBI agent pointing a gun at his head as he stepped naked from the shower.[192] The only prosecution, alleging Espionage Act violations against the NSA's Thomas Drake, collapsed at trial in 2011, and the government's methods earned a stern rebuke from Judge Richard D. Bennett:

> I don't think that deterrence should include an American citizen waiting two and a half years after their home is searched to find out if they're going to be indicted or not. I find that unconscionable. … It was one of the most fundamental things in the Bill of Rights that this country was not to be exposed to people knocking on the door with government authority and coming into their homes. And when it happens, it should be resolved pretty quickly, and it sure as heck shouldn't take two and a half years before someone's charged after that event.[193]

The deterrence effect from such enforcement activity isn't felt just by the person ultimately charged, however, or even those searched but never charged. The FBI's

aggressive investigations of whistleblowers send a clear message to other federal employees that reporting government wrongdoing will risk your career, your financial future, and possibly your freedom. And more FBI leak investigations are resulting in criminal prosecutions than ever before. The Obama administration has prosecuted more government employees for leaking information to media organizations than all other previous administrations combined, often charging them with Espionage Act violations and exposing them to draconian penalties.[194] Though leaks of classified information are a common occurrence in Washington, almost invariably these leak prosecutions have targeted federal employees who exposed government wrongdoing or criticized government policy.

B. Circumventing External Controls

1. Targeting Journalists

The FBI's overzealous pursuit of government whistleblowers has also resulted in the inappropriate targeting of journalists for investigation, thereby chilling press freedoms. In 2010, the Inspector General reported that the FBI used an illegal "exigent letter" to obtain the telephone records of seven New York Times and Washington Post reporters and researchers during a media leak investigation, circumventing Justice Department regulations requiring the attorney general's approval before issuing grand jury subpoenas for journalists' records. The FBI obtained and uploaded 22 months' worth of data from these reporters' telephone numbers, totaling 1,627 calls.[195]

More recently, after The Associated Press reported on the CIA's involvement in interdicting a terrorist attack against a U.S. jetliner in May 2012, the Justice Department issued grand jury subpoenas seeking toll records from more than 20 separate telephone lines, including work and personal numbers for reporters and AP offices in New York, Washington, and Connecticut. In total, more than 100 journalists used the telephones covered by the subpoenas.[196] One of the subpoenaed lines was the AP's main number in the U.S. House of Representatives' press gallery.

As worrisome from a constitutional standpoint, a 2010 FBI search warrant application sought Fox News reporter James Rosen's e-mails as part of an investigation into a State Department detailee's alleged leak of classified information regarding North Korea. The search warrant characterized Rosen as a criminal aider, abettor, or co-conspirator in an Espionage Act violation.[197] The claim was made so the agent could avoid the stringent oversight and notice requirements of the Privacy Protection Act, which was enacted specifically to protect reporters' First Amendment rights. The PPA bars the government from obtaining news media-related work product unless there is probable cause to believe the reporter has actually committed a crime. The FBI affidavit claimed Rosen's requests for information from the government official amounted to illegal solicitations to commit espionage and said he groomed the official "[m]uch like an intelligence officer would run an [sic] clandestine source."[198] The affidavit concluded that

"there is probable cause to believe the Reporter… has committed a violation of [the Espionage Act]." While the U.S. government has never prosecuted a journalist for publishing classified information, this characterization of news gathering as criminal activity reveals that at least some FBI and Justice Department officials, and one federal judge who signed the warrant, believe they could do so in criminal leak cases.

2. **Thwarting Congressional Oversight**

The FBI thwarts congressional oversight by withholding information, limiting or delaying responses to members' inquiries, or, worse, by providing false or misleading information to Congress and the American public. These are but a few examples.

When Congress debated the first Patriot Act reauthorization in April 2005, FBI Director Robert Mueller testified that he was unaware of any "substantiated" allegations of abuse of Patriot Act authorities.[199] The 2007 IG audit later revealed the FBI self-reported 19 Patriot Act-related violations of law or policy to the Intelligence Oversight Board between 2003 and 2005.[200] Though misleading, this testimony was technically accurate because President Bush's Intelligence Oversight Board did not meet to "substantiate" any reported violations until the spring of 2007.[201]

During a 2006 Senate Judiciary Committee hearing, Chairman Patrick Leahy (D-Vt.) complained that when he asked Director Mueller if FBI agents had witnessed objectionable interrogation practices in Iraq, Afghanistan, or Guantanamo Bay during a hearing in May 2004, "he gave a purposefully narrow answer, saying that no FBI agents had witnessed abuses 'in Iraq.'"[202] But FBI documents released in December 2004 in response to an ACLU FOIA request revealed that FBI agents had witnessed abusive treatment of detainees at Guantanamo Bay on multiple occasions, which they duly reported to their FBI supervisors in the field and at FBI headquarters. Sen. Leahy said, "I hope that Director Mueller will continue moving away from the Bush Administration's policy of secrecy and concealment on this issue and toward the responsiveness that the American people deserve."[203] To the FBI's credit, a 2008 IG report indicated FBI agents repeatedly documented and reported detainee abuse they witnessed in Iraq, Afghanistan, and Guantanamo Bay.[204] The IG report found the FBI did not properly respond to the agents' request for guidance until after the photographs depicting detainee abuse at Abu Ghraib prison in Iraq were published in April 2004, and a small number of FBI agents did participate in abusive interrogations.

In an FBI oversight hearing in 2008, the late Sen. Arlen Specter criticized FBI Director Mueller for not having told him that President Bush authorized the National Security Agency to eavesdrop on Americans' communications in violation of the Foreign Intelligence Surveillance Act in 2001.[205] Sen. Specter, who had oversight responsibility over the FBI as the Senate Judiciary Committee's Chairman or Ranking Member during the four years the secret program operated, complained that he only learned about the warrantless wiretapping program when it

appeared in The New York Times in late 2005.[206] Sen. Specter pointed out that because Director Mueller knew about the program, and knew that the Intelligence Committees had not been briefed as required by the National Security Act of 1947, he had a responsibility to report it. Mueller responded that he "was of the belief that those who should be briefed in Congress were being briefed."[207] Sen. Feinstein, who served on both the Intelligence and Judiciary Committees, said Mueller's comment that members were fully briefed was "simply not accurate."[208]

As Congress considered a second Patriot Act reauthorization in 2009, Director Mueller was asked about the importance of an expiring provision that allowed the FBI to obtain FISA orders to intercept the communications of unaffiliated "lone wolf" terrorists. He responded, "[a]s to the lone-wolf provision, while we have not — there has not been a lone wolf, so to speak, indicted, that provision is tremendously helpful."[209] He went on, "that is also a provision that has been, I believe, beneficial and should be re-enacted." A few months later the Justice Department advised Sen. Leahy that the government had never used the lone wolf provision.[210]

According to a 2010 IG report, after ACLU FOIA requests exposed inappropriate FBI spying on a Pittsburgh anti-war rally in 2006, unidentified FBI officials concocted a false story claiming the surveillance was an attempt to identify a person related to a validly-approved terrorism investigation who they believed would attend the rally, not an effort to monitor the activities of the anti-war group.[211] The FBI presented this false story to the public in press releases and to Congress through testimony by Director Mueller. When Sen. Leahy requested documentation regarding the FBI's investigation, this false story fell apart because there was no relevant Pittsburgh terrorism investigation. FBI officials then developed a second false story that circulated internally and ultimately sent to Congress a statement for the record that claimed documents couldn't be provided because the investigation was ongoing. When the IG investigated the matter, the FBI failed to provide internal e-mails that may have identified who in the FBI concocted these false stories.[212]

Congress cannot perform its critical oversight function if FBI officials fail or refuse to provide complete, timely, and accurate information upon request.

3. Thwarting Public Oversight with Excessive Secrecy

In addition to secret surveillance and secret interpretations of the law, the FBI is also using excessive secrecy to hide from the public both routine demands for information in criminal cases and its extraordinary covert intelligence abuses.

U.S. Magistrate Judge Stephen W. Smith wrote a law review article in 2012 warning that the FBI and other federal law enforcement officers have created an enormous "secret docket" of "warrant-type applications" for electronic surveillance under the Electronic Communications Privacy Act. These applications for wiretaps, pen registers, and stored communications and subscriber information exploit "a potent mix of indefinite sealing, nondisclosure (i.e. gagging), and delayed-notice provisions" in ECPA to obtain surveillance orders from U.S. magistrate

judges that are only ever seen by the government agents and telephone and Internet service providers that execute the orders. Judge Smith estimates that magistrate judges seal around 30,000 ECPA orders annually. While these seals are supposed to be temporary, they often effectively become permanent due to inaction by the government.[213] In a study in his own division, Judge Smith determined that 99.8 percent of sealed orders from 1995 through 2007 remained sealed in 2008.[214] Magistrate judges are given little judicial guidance on how to address these requests for secrecy. Because these orders remain sealed they cannot be challenged by the subjects of the surveillance, which in turn deprives the magistrate judges of appellate court decisions that would provide guidance on how to interpret ECPA's complex provisions when evaluating future government secrecy demands under the statute.[215] The result is less public oversight of law enforcement surveillance activities.

In a profoundly disturbing case involving covert surveillance, the FBI in 2006 tasked informant Craig Monteilh, a convicted felon, with infiltrating several southern California mosques by pretending to convert to Islam. In a sworn affidavit, Monteilh says his FBI handlers provided him audio and video recording equipment and instructed him "to gather as much information on as many people in the Muslim community as possible."[216] Monteilh's handlers did not give him specific targets, but told him to look for people with certain traits, such as anyone who studied Islamic law, criticized U.S. foreign policy, or "played a leadership role at a mosque or in the Muslim community."[217] Monteilh said he recorded youth group meetings, lectures by Muslim scholars, and talked to people about their problems so FBI agents could later "pressure them to provide information or become informants."[218] Monteilh's handlers told him to attend morning and evening prayers because the Muslims who attended were likely "very devout and therefore more suspicious."[219] Monteilh said he often left the recorder unattended to capture private conversations he was not a party to, and that his handlers knew this and did not tell him to stop. He said the agent told him more than once that "if they did not have a warrant they could not use the information in court, but that it was still useful to have the information."[220]

Monteilh exposed his role as an FBI informant to the Los Angeles Times in 2009.[221] The ACLU of Southern California, the Council on American Islamic Relations of Greater Los Angeles, and the law firm Hadsel, Stormer, Keeny, Richardson & Renick LLP initiated a class action law suit against the FBI on behalf of Southern California Muslims. The suit alleges the FBI unlawfully targeted people based on their religious beliefs in violation of the First Amendment, retained information about their religious practices in FBI files in violation of the Privacy Act, and conducted unreasonable searches in violation of the Fourth Amendment.[222]

In an extraordinary move, the government asserted the "state secrets" privilege to block the lawsuit against the FBI from moving forward.[223] That FBI secrecy demands could prevent U.S. citizens and residents from going into a U.S. court room to protect themselves from unconstitutional FBI surveillance taking place in American communities offends Americans' sense of justice.[224] The federal district court dismissed the illegal surveillance suit against the

FBI based on the assertion of the state secrets privilege, but allowed claims against individual agents for FISA violations to proceed.[225]

During related FOIA litigation, a federal district judge severely criticized the FBI for misleading the court by falsely denying it had records responsive to the FOIA request. The FBI had been interpreting its exclusions under FOIA as authority to provide false no records responses to FOIA requestors under certain conditions. The Justice Department has since amended this policy to prevent false denial of records responses to FOIA requests.

In all of these cases, the FBI could have chosen a path of greater transparency without harming criminal investigations or national security and defended its tactics in courts of law and in the court of public opinion. Its increasing reliance on secrecy to thwart legal challenges to its law enforcement and intelligence activities leaves the public with dangerously little recourse against FBI violations of constitutional rights.

IV. Targeting First Amendment Activity

A. Biased training

FOIA litigation by the ACLU of Northern California, the Asian Law Caucus, and The San Francisco Bay Guardian and later media reports uncovered factually inaccurate FBI training materials that demonstrated strong anti-Arab and anti-Muslim bias.[226] The materials span from 2003 to 2011. They include both amateurish power point presentations that paint Muslims and Arabs as backward and inherently violent and a professionally-published counterterrorism textbook the FBI produced with the Combating Terrorism Center at West Point for training law enforcement. The textbook, "Terrorism and Political Islam," devotes one of five sections to "Understanding Islam," and another to "Cultural and Regional Studies" of Muslim-majority countries, which tends to reinforce the false idea that modern terrorism is predominantly a Muslim phenomenon.[227] Such heavy emphasis on Islam is misguided, as terrorism is a tactic used by many groups claiming allegiance to a multitude of different religions and political ideologies, and potentially distracts from other significant threats. A later report by the Combating Terrorism Center documented that 670 people have been killed and 3,053 injured in attacks by far right extremists in the U.S since 1990, yet far-right extremists are barely mentioned in the textbook except to dismiss them as significant threats.[228] There are many different terrorism threats, and FBI training materials should address each in a factually objective manner based on evidence rather than bias.

The FBI textbook also improperly links Muslims' political activities and opinions with their potential for violence. One essay tells agents they can determine whether Muslims are militant by asking their opinions about the Iraq war and the political situation in Israel and Egypt. Those Muslims answering with "a patriotic and pro-Western stance," according to the article, "could potentially evolve into a street informant or concerned citizen."[229] Biased and erroneous FBI

training can be expected to result in inappropriate targeting of American Muslim communities for investigation and intelligence collection.

To its credit, following media exposure of these biased training materials, the FBI initiated a review of its counterterrorism training materials referencing religion and culture, and issued a statement that "[s]trong religious beliefs should never be confused with violent extremism."[230] The FBI has reportedly removed 800 pages from its training materials, but there has been far too little transparency regarding the standards guiding this review. And unfortunately, the FBI did not review intelligence products that mirrored these biased training materials, despite requests by the ACLU and partner organizations to include them.

The public is well aware that similarly flawed, incorrect, and biased FBI intelligence products do exist. A 2006 FBI intelligence report called "Radicalization: From Conversion to Jihad" asserts that "indicators" that a person is progressing on a path to becoming a terrorist include:

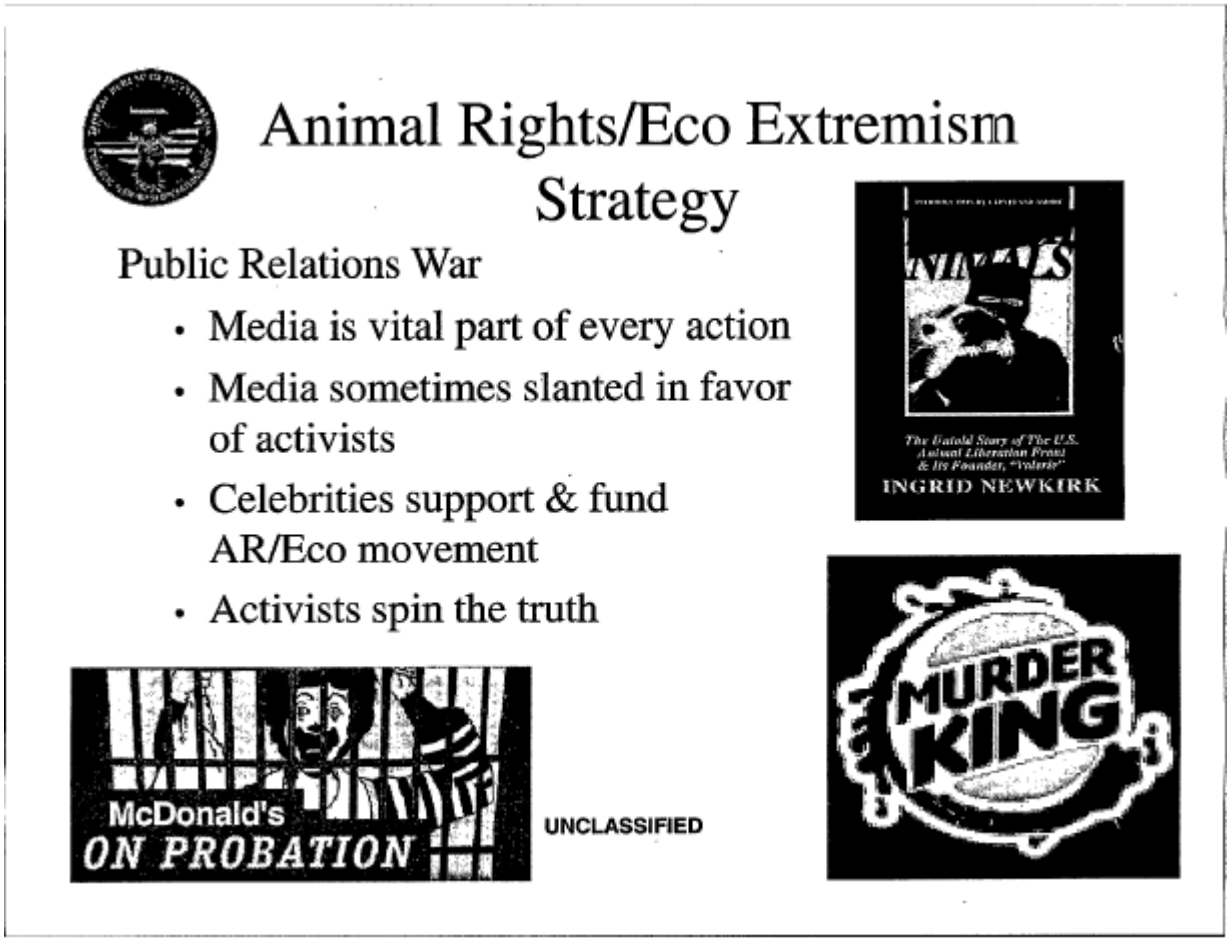
- Wearing traditional Muslim attire
- Growing facial hair
- Frequent attendance at a mosque or prayer group
- Travel to a Muslim country
- Increased activity in a pro-Muslim social group or cause
- Proselytizing[231]

These activities are commonplace and entirely innocuous, and millions of American Muslims who pose no threat to anyone engage in them regularly. More importantly for an agency charged with protecting civil rights, these activities are protected by the First Amendment. While the report notes that "[n]ot all Muslim converts are extremists," it suggests that all are suspect because "they can be targeted for radicalization." This assertion undoubtedly leads to additional law enforcement scrutiny of American Muslims for no reason other than the practice of their faith.[232] The FBI refused a request to withdraw this report, and an FBI spokesman defended its analysis, stating that "[t]hese indicators do not conflict with our statement that strong religious beliefs should never be confused with violent extremism."[233]

Such biased and erroneous information in FBI intelligence reports is likely to drive racial and religious profiling at every stage of the intelligence process. These false indicators can be expected to lead to excessive and unwarranted surveillance and intelligence collection targeting communities agents perceive to be Muslim, which fills FBI data bases with a disproportionate amount of information about Arabs, Middle-Easterners, South Asians, and African-Americans. Further analysis of this biased data pool using data mining tools based on these false indicators could lead to more people from these communities being selected for more intensive investigation and watch listing.[234] It could even result in the application of an FBI "disruption strategy," which might include scouring their records for minor violations that would not

normally be investigated or charged, deportation, security clearance revocation,[235] or employing informants to act as agents provocateur to instigate criminal activity.

But biased training materials were not limited to erroneous information about Muslims. FBI domestic terrorism training presentations on "Black Separatist Extremists" juxtaposed decades-old examples of violence by the Black Panthers and the Black Liberation Army with unorthodox beliefs expressed by a number of different modern groups to suggest, without evidence, that these latter-day groups pose a similar threat of violence.[236] The FBI presentation claims organizations it calls "Black Separatists" have no unifying theme or mission, but "all share racial grievances against the U.S., most seek restitution, or governance base [sic] on religious identity or social principals [sic]."[237] No recent acts of "Black Separatist" terrorism appear in the presentations or in FBI lists of terrorism incidents going back to 1980.[238] FBI domestic terrorism training presentations on "Anarchist Extremists" claim they are "not dedicated to any cause" and merely "criminals seeking an ideology to justify their activities," yet focus heavily on protest activity, including "'passive' civil disobedience."[239] FBI training presentations on "Animal Rights/Environmental Extremism" list "FOIA Requests" as examples of "Intelligence Gathering," and another presentation suggests activists are waging a "public relations war."[240]



Failing to distinguish properly between First Amendment activity, non-violent civil disobedience, and terrorism in FBI training materials leads to investigations and intelligence gathering that improperly target constitutionally-protected activity, endangers political activists by placing them on terrorism watch lists, and suppresses religious and political freedom.

B. Targeting AMEMSA Communities

Arab, Middle-Eastern, Muslim, and South Asian (AMEMSA) communities in the U.S. have faced the brunt of the FBI's overzealous applications of its expanded authorities since 9/11. In the immediate aftermath of the attacks, acting out of fear and ignorance, FBI agents and other federal officials arrested hundreds of Middle-Eastern immigrants, based mostly on minor visa violations, in a pre-emptive measure painfully reminiscent of the Palmer raids.[241] The Justice Department initiated a "hold until cleared" policy that assured the detainees would be held without bond until cleared by the FBI of any links to terrorism, meaning many languished in detention for months.[242] An affidavit signed by an FBI counterterrorism official presented a "mosaic" theory, which argued these detainees should be held despite the lack of individualized evidence of dangerousness until the FBI could develop a fuller picture of the threat and rule out their involvement in terrorism.[243] Attorney General John Ashcroft defended such pre-textual arrests, warning the "terrorists among us" that:

> If you overstay your visa – even by one day – we will arrest you. If you violate a local law, you will be put in jail and kept in custody as long as possible. We will use every available statute. We will seek every prosecutorial advantage. We will use all our weapons within the law and under the Constitution to protect life and enhance security for America.[244]

This statement was the first clear indication that the government would pursue what was soon called the "Al Capone strategy," in reference to the notorious gangster's imprisonment on tax charges rather than violent crimes. This strategy held that government agents should vigorously pursue people they believed to be involved in terrorism using any civil or criminal violation that could be found, no matter how small or unrelated to actual terrorism plotting. The description of an official "disruption strategy" in the FBI's 2009 "Baseline Collection Plan" suggests the FBI is continuing to promote this concept.[245]

Using a "disruption" plan could arguably make sense if the target is actually a terrorist. Many times, however, when the government doesn't have evidence to support a terrorism charge, it is because the person isn't actually involved in terrorism, despite the FBI's suspicions.

But the FBI didn't just pursue immigrants, or wait until it found a legal violation. The FBI also jailed innocent American Muslims by misusing material witness warrants. Indeed, the FBI's flawed terrorism training materials and intelligence products make clear that agents were erroneously taught to view Muslim religious practices and political activism as indicators of terrorism. When the government selectively targets, investigates, and refers for prosecution

people based on race, ethnicity, religion, national origin, or political viewpoint it has a different name: discrimination.

AMEMSA communities in the U.S. have faced different types of degrading, oppressive treatment as a result of the FBI's flawed attitude, training, and policies since 9/11. In 2003, the FBI ordered its field offices to count the number of mosques in their areas as part of one counterterrorism initiative and initiated nationwide programs of "voluntary" interviews throughout AMEMSA communities.[246] U.S. News and World Report revealed in 2005 that FBI agents secretly scanned hundreds of Muslim homes, businesses, and mosques with radiation detection equipment without warrants in at least six cities across the nation.[247] No nuclear weapons were detected. The ACLU obtained documents indicating that from 2007 through 2011 the FBI exploited its community outreach programs to secretly gather information on AMEMSA community organizations and mosques, which was then uploaded to domain management intelligence files and disseminated outside the FBI in violation of the Privacy Act.[248]

The FBI has also aggressively pressured AMEMSA community members to become informants for the FBI, particularly immigrants who must rely on the government to process their immigration and citizenship applications in a fair and timely manner. An FBI training presentation on recruiting informants in the Muslim community suggests agents exploit "immigration vulnerabilities" because Muslims in the U.S. are "an immigrant community."[249] In 2008, the U.S. Citizenship and Immigration Service implemented a covert program to ensure that individuals who pose a threat to national security are not granted immigration benefits, which often gives the FBI wide discretion to deny, approve, or delay citizenship requests, and thereby the leverage to compel Muslim immigrants to become informants.[250] The pervasive and unjustified use of informants to spy in Muslim communities offends American values and inflicts real harm on the innocent people living there, by chilling their ability to exercise constitutionally guaranteed religious freedoms.[251]

The FBI has also sent informants, including some with serious criminal histories, into AMEMSA communities to act as "*agents provocateur*."[252] As stated by the "disruption strategy" described in the FBI's 2009 "Baseline Collection Plan," source-driven operations are one of the FBI's preferred methods of "disrupting" its intended targets.[253] While FBI has long used informants and undercover agents in sting operations, the methodology used against Muslims since 9/11 has been significantly more aggressive. According to a 2011 analysis of federal terrorism prosecutions by Mother Jones magazine, of 508 terrorism defendants prosecuted since 9/11, 158 (31 percent) were caught in sting operations.[254]

In many cases the government agent provides all the instrumentalities of the crime, chooses the target, designs the plot, and provides the gullible subjects financial support or other incentives to carry out the plot. The subjects are often destitute and at times become financially dependent on the informants. For example, a defendant in Chicago was given room and board in the informant's home and provided with a car and spending money.[255] In a case in Newburgh, N.Y.,

the FBI informant offered one of the hesitant defendants, ex-convict James Cromitie, $250,000 to execute the faux plot, raising the question of whether this was a truly terrorism case or a murder-for-hire.[256]

While some of the defendants targeted in these cases were angry and disgruntled—and arguably deserved some law enforcement attention—they mostly did not have violent criminal histories. They also did not acquire weapons on their own nor possess the financial means to obtain them before meeting an FBI informant. Yet instead of addressing the threat as it existed in these cases, the FBI initiated elaborate sting operations using dubious informants, many with criminal records, to prod the subjects to act out, often supplying them with spiritual or political motivation, financial assistance, and sophisticated military hardware at little or no cost. The informant in Newburgh provided the destitute defendants a Stinger surface-to-air missile and plastic explosives.[257] In the Chicago case, the defendant was unable (or unwilling) to raise the paltry $100 the undercover agent was going to charge him for four military hand grenades, so the agent instead traded him the grenades for two used stereo speakers.[258] There is no legitimate reason for the FBI to exaggerate the danger posed to the community in these cases by introducing heavy weapons the defendants clearly would be unable to obtain on their own. Government actions aggrandizing the threat a defendant poses through the introduction of what are no more than harmless stage props only spreads unwarranted public fear, which it often fans with sensational press conferences at the time of arrest. The effect of these FBI tactics is that judges and juries who might otherwise question the FBI's tactics in these cases and entertain an entrapment defense may be less willing to do so out of unjustified concern for public safety, or unease over the potential public reaction. Indeed, the judge in the Newburgh case called it a "fantasy terror operation" and said, "[o]nly the government could have made a terrorist out of Mr. Cromitie, whose buffoonery is positively Shakespearean in scope."[259] Nevertheless, she let the jury's conviction stand and sentenced Cromitie to 25 years in prison.

These questionable investigative methods also tend to increase the potential penalties faced by these defendants, who may be pressured to plead guilty in exchange for more lenient sentences, giving the courts and the public fewer opportunities to examine and evaluate FBI tactics.

C. Targeting Activists

The FBI also targeted political advocacy organizations with renewed vigor after 9/11, as demonstrated through ACLU FOIAs and confirmed by a 2010 Inspector General audit. And FBI training continues to describe political activism as an "extremist" tactic and non-violent civil disobedience as terrorism. The FBI uses many of the same tactics it uses against AMEMSA communities, including invasive surveillance, infiltration, and sting operations using *agents provocateur*.[260] But the FBI has also been using its expanded powers to conduct inappropriately harsh overt investigations that appear designed to suppress political activity. As the Church Committee pointed out decades ago, aggressive investigation can often be more disruptive than

covert action: "[t]he line between information collection and harassment can be extremely thin."[261]

In a recent case in Nevada, Native American political activists representing the American Indian Movement (AIM) appeared at public meetings of the Nevada Wildlife Commission and the Washoe County Wildlife Advisory Board in March 2012 to speak out against a proposed bear hunt, on religious grounds.[262] Shortly thereafter, a law enforcement officer assigned to the FBI's Joint Terrorism Task Force arrived at the home of one AIM activist and workplace of another to question them about their appearance at the public meetings, saying audience members felt threatened when they spoke. The police arrested one of the AIM activists, interrogated her in jail, and tried to get her to sign a document saying she was involved in terrorist activity.[263] She refused and was released without charge. In an email statement given to the Reno-Gazette Journal, a spokesman said the FBI "conducted an assessment and determined no further investigation was warranted at this time." The Reno-Gazette Journal contacted a Department of Wildlife spokesman who said an FBI official had contacted them and asked if the wardens were threatened: "We absolutely answered no, we have not."[264] This use of FBI assessment authority appears to have been intended to intimidate political activists rather than investigate real threats.

More troubling, however, are incidents in which the FBI targeted activists with armed raids. In September 2010, dozens of FBI agents conducted simultaneous raids on peace and labor activists' homes and offices in Chicago, Minneapolis, and Grand Rapids, Mich., seizing documents, computers, and cell phones.[265] An FBI spokesman said the searches were part of a Joint Terrorism Task Force investigation "into activities concerning the material support of terrorism," but there was no "imminent danger" to the public. The FBI also served fourteen of the activists with subpoenas commanding their appearance before a grand jury in Chicago. One activist's bank account was frozen. More than three years later, none of the activists has been charged with a crime, raising troubling questions about whether these aggressive raids were necessary or justified.

Such aggressive law enforcement operations obviously have a devastating impact on these activists' ability to continue their political advocacy. But they also create fear in the larger activist community. Both those who worked directly with the targeted activists now living under a cloud of suspicion and those who didn't, but work on similar political issues, have to worry if they will be the next ones to be raided. Unfortunately, the FBI is only increasing its use of these tactics.

In July 2012, FBI SWAT teams wearing body armor and carrying assault rifles raided at least six homes of alleged anarchists in Portland, Ore., and Seattle and Olympia, Wash., reportedly using flash-bang grenades at some locations.[266] Sealed search warrants reportedly sought "anarchist" literature, computers, cell phones, black clothing, and flags carried at protests.[267] No arrests were made but several people were served with grand jury subpoenas related to the raids. Some have been jailed for refusing to testify before the grand jury. The Oregonian reports that court records

indicate the investigation is targeting an "organized 'black bloc'" that committed vandalism during May Day protests in Seattle in 2012 and broke windows at the federal courthouse there.[268] While vandalism of U.S. government property is indeed a federal crime, the extreme tactics the FBI is using in this case appear to be designed more to send a message to, and potentially "disrupt", this community of activists than to solve serious federal crimes.

Strong-arm tactics have no place in American law enforcement. While FBI agents conducting search warrants must act in a manner to protect themselves and others from violence, force can only be used when necessary to prevent imminent harm. Flash-bang grenades are potentially lethal weapons. They have caused deadly fires, induced heart attacks, and recently killed a police officer who accidently set one off in his garage as he was placing equipment in his patrol car.[269] When FBI agents use their law enforcement powers to suppress or disrupt political activity, they are violating the Constitution they have sworn to defend and undermining the rights of all Americans.

V. Greater Oversight Needed: The FBI Abroad

The FBI is increasingly operating outside the U.S., where its authorities are less clear and its activities much more difficult to monitor. There are three areas in particular that need far greater transparency and action by Congress to protect the rights of U.S. citizens traveling abroad.

A. Proxy Detention

The federal government has an obligation to come to the aid of American citizens arrested in foreign countries, and the State Department has said that assisting Americans incarcerated abroad is one of its most important tasks.[270] Federal law requires that:

> Whenever it is made known to the President that any citizen of the United States has been unjustly deprived of his liberty by or under the authority of any foreign government, it shall be the duty of the President forthwith to demand of that government the reasons of such imprisonment; and if it appears to be wrongful and in violation of the rights of American citizenship, the President shall forthwith demand the release of such citizen, and if the release so demanded is unreasonably delayed or refused, the President shall use such means, not amounting to acts of war and not otherwise prohibited by law, as he may think necessary and proper to obtain or effectuate the release; and all the facts and proceedings relative thereto shall as soon as practicable be communicated by the President to Congress.[271]

Yet the FBI appears to have requested, facilitated, and/or exploited the arrests of U.S. citizens by foreign governments, often without charges, so they could be held and interrogated, sometimes tortured, then interviewed by FBI agents. The ACLU represents two victims of the FBI's proxy detention activities.

Amir Meshal is an American Muslim born and raised in New Jersey.[272] He traveled to Somalia to study Islam in 2006, but had to flee with other civilians when the country became engulfed in civil war at the end of that year. A joint American, Kenyan, and Ethiopian force arrested him at the Kenya border in early 2007. Meshal was subsequently subjected to more than four months of detention, often in squalid conditions. His captors transferred him between three different East African countries without charge, access to counsel, or presentment before a judicial officer, all at the behest of the U.S. government. While foreign officials showed little interest in talking to Meshal, FBI agents interrogated him more than thirty times and told him he would not be permitted to go home until he confessed to being part of al Qaeda. They took his fingerprints and a DNA sample and tried to coerce his confession by threatening him with torture, forced disappearance, and rendition to Egypt, Somalia, or Israel for further interrogation. The FBI agents refused his requests for counsel and did not allow him to make any phone calls to let his family know where he was. The FBI agents made Meshal sign *Miranda* waivers, telling him that if he refused he would not be allowed to go home. After a Kenyan court was poised to hear habeas petitions filed by a Kenyan human rights group on behalf of foreigners seized at the border, Meshal was forcibly transferred to Somalia and then to Ethiopia, where he was again repeatedly interrogated by FBI agents, including one who interrogated him in Kenya. During this entire period Meshal was never charged with a crime nor provided access to counsel or the Red Cross. Meshal was only released and allowed to return home after media reports regarding his prolonged detention led to inquiries from Congress.

Naji Hamdan, a Lebanese-American businessman, was contacted and interviewed by the FBI several times while he was living in Los Angeles over many years, and he was often stopped and interrogated at U.S. airports but he was never arrested or charged with a crime in the U.S.[273] In 2006, he and his family moved the United Arab Emirates where he established a business. In July 2008, FBI agents from Los Angeles summoned him to the U.S. Embassy for an interview. Several weeks later, in August 2008, Hamdan was seized by U.A.E. security forces, held incommunicado for nearly three months, beaten and tortured, and forced to confess to being associated with several different terrorist groups. At one point an American participated in his interrogation, who Hamdan believed to be an FBI agent based on the interrogator's knowledge of previous FBI interviews. Believing the U.S. government was behind Hamdan's detention, the ACLU of Southern California filed a habeas corpus petition in federal court on his behalf, alleging Hamdan was in the constructive custody of the U.S. A week later on November 26, U.A.E. officials transferred Hamdan to criminal detention in the U.A.E.. He was charged with vague terrorism-related crimes and later convicted based on his coerced confessions, but he was sentenced only to time served and deported to Lebanon, where he lives with his family. Documents obtained by the ACLU demonstrate the State Department and FBI were closely monitoring Hamdan's case from the beginning of his detention.

These proxy detentions appear to be continuing under the Obama administration. In December 2010, American teenager Gulet Mohamed was jailed in Kuwait when he went to renew his visa

after spending several months in the country visiting family. According to The New York Times, Mohamed said he was beaten and threatened by his Kuwaiti interrogators and later interviewed by FBI agents who said "he could not return to the United States until he gave truthful answers about his travels."[274] The New York Times confirmed the U.S. had placed Mohamed on the No Fly List.[275] After the media reported his detention, Mohamed's family hired a lawyer to represent him, who alleged the FBI continued to interrogate Mohamed repeatedly without counsel while he remained in Kuwaiti custody, stranded because the U.S. put him on the No Fly List.[276] Mohamed was never charged with a crime and returned to the U.S. in January 2011.

An FBI official admitted in a July 8, 2011, email to Mother Jones Magazine that the FBI may elect to share information with foreign governments and that those governments "may decide to locate or detain an individual or conduct an investigation based on the shared information." The FBI official went on:

> Additionally, there have been instances when foreign law enforcement have detained individuals, independent of any information provided by the FBI, and the FBI has been afforded the opportunity to interview or witness an interview with the individual.[277]

If the FBI is providing information to foreign governments to arrest Americans abroad when there is not sufficient evidence to bring U.S. charges, it may be a violation of constitutional due process rights and an abrogation of the government's obligation to defend the rights of U.S citizens. This conduct is particularly problematic where the cooperating governments have records of abusing human rights.

B. FBI Overseas Interrogation Policy

The ACLU obtained through FOIA the fifth version of an FBI interrogation manual for conducting custodial interrogations in overseas environments, which was written by a supervisor in the FBI's counterterrorism division in 2011 (the third version was copyrighted in 2010, it is unknown when the earlier versions were published).[278] The manual is troubling for many reasons, but particularly because it recommends that FBI agents ask the foreign government or U.S. military officials holding the detainees to isolate them at capture "for several days before you begin interrogation" and throughout the "multi-session, multi-day" interrogation process.[279]

Isolation has long been recognized as a coercive technique that can cause serious psychological distress, and the manual advises FBI agents that in addition to security concerns, an important purpose for requesting isolation is to allow interrogators to take advantage of "the natural fear of the unknown that the detainee will be experiencing."[280] This advice directly conflicts with FBI policy. The FBI Legal Handbook for Special Agents, and the U.S. Supreme Court, explicitly recognizes isolation as a coercive technique that undermines the voluntariness of detainee's statements.[281] The manual also makes repeated, positive references to the CIA's notorious KUBARK interrogation manual and "the Reid Technique," both of which have been criticized

for promoting coercive interrogation practices. The ACLU has asked the FBI to end this practice and provide remedial training to any agents who received this manual.[282]

If FBI agents request isolation of detainees prior to interviews—or participate in interviews in which detainees are being or have been mistreated, tortured, or threatened with torture— they are violating FBI policy and U.S. law. Congress must act to investigate the FBI's conduct abroad and curb this troubling activity.

C. Using the No Fly List to Pressure Americans Abroad to Become Informants

Several audits by the GAO and agency IGs have documented the government's mismanagement of its terrorist watch lists over many years.[283] A 2009 DOJ IG audit found:

> …the FBI failed to nominate many subjects in the terrorism investigations that we sampled, did not nominate many others in a timely fashion, and did not update or remove watchlist records as required… We also found that 78 percent of the initial watchlist nominations we reviewed were not processed in established FBI timeframes."[284]

But rather than narrow and reform its many watch lists, or provide constitutionally-adequate and effective post-deprivation redress procedures so people improperly placed on these lists could remove their names, the FBI appears to be aggressively exploiting these lists in a manner that further violates Americans' civil rights.

This is particularly true for the No Fly List, which is the smallest subset of the FBI's massive Terrorist Screening Center watch list (affecting about 21,000 of the 875,000 people on the larger list), but also the most liberty infringing because it bars air travel to or within the U.S.[285] The GAO reported in 2012 that the number of U.S. persons on the No Fly List has more than doubled since December 2009.[286] In many cases, U.S. citizens and permanent residents only find out that their government is prohibiting them from flying while they are travelling abroad, which all but forces them to interact with the U.S. government from a position of extreme vulnerability, often without easy access to counsel. Many of those prevented from flying home have been subjected to FBI interviews while they sought assistance from U.S. Embassies to return.[287] In several documented incidents, the FBI agents offered to take them off the No Fly List if they agreed to become an FBI informant.

For example, Nagib Ali Ghaleb, a naturalized U.S. citizen residing in San Francisco, traveled to Yemen in 2010 to visit his wife and children and meet with U.S. consular officials concerning delays in his family's previously-approved visa applications.[288] At the airport in Frankfurt, Germany, as he was getting ready to board the last leg of his flight home from Yemen, airline officials delayed his boarding until an FBI agent arrived at the airport and told Mr. Ghaleb that he would not be allowed to fly back to the U.S. Ghaleb returned to Yemen and sought assistance at U.S. Embassy. He was directed to submit to an interview with FBI agents, who questioned

him about his mosque and the San Francisco Yemeni community. The FBI agents asked him to become an informant for the FBI in California, but Mr. Ghaleb said he did not know any dangerous people and would not spy on innocent people in mosques. The FBI agents threatened to have Mr. Ghaleb arrested by the Yemeni government if he did not cooperate.

In 2010, the ACLU and its affiliates filed a lawsuit on behalf of Mr. Ghaleb and other American citizens and permanent residents, including several U.S. military veterans, seven of whom were prevented from returning to the U.S. from abroad, arguing that barring them from flying without due process was unconstitutional.[289] The ACLU sought preliminary relief for those stranded overseas so they could return to the U.S., and the government allowed those Americans to board returning flights without explaining why they were put on the list, or whether they would be barred from flying in the future. The government has now put in place an informal process for U.S. citizens apparently placed on the No Fly List to secure a one-time waiver to fly home, but the constitutional issues in the case remain under litigation. None of the plaintiffs, some of whom are U.S. military veterans, have been charged with a crime, told why they are barred from flying, or given an opportunity to challenge their inclusion on the No Fly List. Many cannot pursue business opportunities or be with friends and family abroad, and U.S. Customs officials even prevented one ACLU client, Abdullatif Muthanna, from boarding a boat in Philadelphia in a failed attempt to travel to see family members living overseas.[290]

The ACLU clients are not the only victims of this practice. In a lawsuit filed in May 2013, American citizen Yonas Fikre alleges that FBI agents from his hometown of Portland, Ore., lured him to the U.S. Embassy in Khartoum under false pretenses while he was travelling in Sudan on business and coerced him into submitting to an interview.[291] The complaint states that the agents denied Fikre's request for counsel, told him he was on the No Fly List, and interrogated him about the mosque he attended in Portland and the people who went there. They asked him to become an informant for the FBI in Portland, offering to take him off the No Fly List and provide financial compensation if he accepted. He refused. Fikre later traveled to the U.A.E., where in 2011 he was arrested and tortured by security officials. In the lawsuit, Fikre charges that his arrest and interrogation were undertaken at the request of the FBI. U.A.E. officials released Fikre without charge after three months, but were unable to deport him back to Portland because the U.S. still included him on the No Fly List. He applied for political asylum in Sweden.[292] In 2012, the U.S. charged Fikre with conspiring to evade financial reporting requirements regarding wire transfers to the Sudan, but made no terrorism allegations against him.[293] And in a more recent case described in The Huffington Post, Kevin Iraniha, an American citizen born and raised in San Diego, says he was barred from flying home after graduating with a master's degree in international law from the University of Peace in Costa Rica in June 2012.[294] Iraniha submitted to an interview with an FBI agent at the U.S. Embassy, but was told that he would not be allowed to fly into the U.S. and would have to drive or take a boat. Iraniha flew to Tijuana, Mexico, and walked across the border.[295]

The FBI should not be allowed to use the No Fly List as a lever to coerce Americans into submitting to FBI interviews or becoming informants. Congress should require the administration to establish a redress process that comports with constitutionally required procedural due process so that persons prohibited from flying can correct government errors and effectively defend themselves against the government's decision to place them on the No Fly List.

VI. Conclusion and Recommendations

FBI abuse of power must be met with efforts of reform, just as much now as in the days of J. Edgar Hoover. President Obama should require the attorney general to tighten FBI authorities to prevent suspicionless invasions of personal privacy, prohibit profiling based on race, ethnicity, religion or national origin, and protect First Amendment activities. But internal reforms have never been sufficient when it comes to the FBI. Congress also must act to make these changes permanent and must increase its vigilance to ensure abuse is quickly discovered and remedied.

We offer these recommendations:

RECOMMENDATIONS FOR THE ATTORNEY GENERAL:

1. The AG must revise the Justice Department Guidance Regarding the Use of Race in Federal Law Enforcement to: 1) remove the national security and border integrity exemptions; 2) prohibit profiling by religion or national origin; 3) clarify that the ban on profiling applies to intelligence activities as well as investigative activities; 4) establish enforceable standards that include accountability mechanisms for noncompliance; and 5) make the guidance applicable to state and local law enforcement working on federal task forces or receiving federal funds.

2. The AG must revise the Attorney General's Guidelines to: 1) remove the FBI's authority to conduct "assessments" without a factual predicate of wrongdoing; 2) prohibit racial and ethnic mapping; and 3) prohibit the FBI from undertaking "Preliminary Investigations" unless they are supported by articulable facts and particularized suspicion, and properly limited in time and scope; 4) prohibit the FBI from tasking informants or using undercover agents in Preliminary Investigations.

3. The AG must direct the Justice Department's Civil Rights Division to investigate the FBI's counterterrorism training materials and intelligence products to identify and remove information that is factually incorrect; exhibits bias against any race, ethnicity, religion or national origin; or improperly equates First Amendment-protected activity or non-violent civil disobedience with terrorism.

4. The AG must direct the Civil Rights Division to investigate the FBI's domain management and racial and ethnic profiling programs and determine whether the FBI used these programs to

improperly target intelligence operations or investigations based on race, ethnicity, religion, or national origin.

5. The AG must direct the Justice Department Inspector General to review the FBI's extraterritorial activities, particularly incidents involving proxy detentions of Americans, FBI interrogation policies and practices, and the improper use of the No Fly List to compel Americans to submit to interviews or agree to become an informant.

6. The AG must end 'secret law' by declassifying and releasing secret legal interpretations of its surveillance authorities, including but not limited to: 1) FISA Court opinions interpreting the scope of U.S. government's surveillance authorities, particularly under Section 215 of the USA Patriot Act and Section 702 of FISA; 2) the January 8, 2010, OLC opinion interpreting the Electronic Communications Privacy Act to allow the FBI to obtain certain communication records without legal process in non-emergency situations; and 3) the June 2012 version of the FBI DIOG.

RECOMMENDATIONS FOR CONGRESS:

1. Congress must intensify its oversight of all FBI policies and practices, particularly those that implicate Americans' constitutional rights. The collection, retention, and sharing of personally identifying information about Americans without facts establishing a reasonable indication of criminal activity poses serious risks to liberty and democracy, and the evidence of abuse is overwhelming. The lessons of the past have been ignored and we are increasingly seeing a return to abusive intelligence operations that target protest groups and religious and racial minorities. Congress must particularly examine FBI activities abroad, where Americans' due process rights and safety are at greatest risk.

2. Congress must narrow the FBI's intelligence and investigative authorities through statute. The Attorney General's Guidelines are changed too often and too easily, and the FBI too often fails to comply with them.

3. Though the FISA Amendments Act and several Patriot Act-related surveillance provisions are set to expire in 2015, new evidence of abuse of these authorities demonstrates that Congress can't wait. Congress should immediately repeal Section 215 of the Patriot Act and Section 702 of FISA.

4. Congress must examine and evaluate all information collection and analysis practices and bring an end to any government activities that are illegal, ineffective, or prone to abuse. Congress should conduct a comprehensive review of all expanded post-9/11 intelligence authorities so thoughtful and effective reforms can be implemented.

5. Congress must amend the Electronic Communications Privacy Act to require a probable cause warrant before the government can search and seize online records and communications, just as

it needs to search documents in the mail or in our homes and offices. Congress should evaluate ECPA sealing and delayed notice provisions to ensure maximum transparency regarding law enforcement surveillance activities.

6. Congress must not implement or fund new intelligence programs without empirical evidence that they effectively improve security and can be implemented without undue impact on privacy and civil rights. We should not sacrifice our liberty for the illusion of security. Any new effort to expand information collection, sharing, or analysis must be accompanied by independent oversight mechanisms and rigorous standards to maintain the accuracy, timeliness, and usefulness of the information and to ensure the privacy of innocent individuals is preserved. Congress should adopt the National Research Council recommendations to require the FBI and other federal agencies to employ a systematic process to evaluate the "effectiveness, lawfulness and consistency with U.S. values" of all automated data mining systems *before they are deployed* and subject them to "robust, independent oversight" thereafter.[296]

7. Congress must pass the End Racial Profiling Act and ban racial profiling in all government intelligence and law enforcement programs.

8. Congress must pass the State Secrets Protection Act, which would restore the states secrets privilege to its common law origin as an evidentiary privilege by prohibiting the dismissal of cases prior to discovery. Congress must ensure independent judicial review of government state secrets claims by requiring courts to examine the evidence and make their own assessments of whether disclosure could reasonably pose a significant risk to national security.

9. Congress must establish due process mechanisms so Americans placed on the No Fly List or other terrorism watch lists that implicate their rights can effectively challenge the government's actions.

---

[1] Laura W. Murphy, Director, Washington Leg. Office, American Civil Liberties Union, The Patriot Act's Section 215 Must Be Reformed (June 14, 2013), http://www.aclu.org/blog/national-security-technology-and-liberty/patriot-acts-section-215-must-be-reformed.

[2] Press Release, Rep. Jim Sensenbrenner, Author of Patriot Act: FBI's FISA Order is Abuse of Patriot Act (June 6, 2013) (on file with author), *available at* http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=337001.

[3] Letter from Laura W. Murphy, Director, Washington Leg. Office, American Civil Liberties Union, & Gregory T. Nojeim, Assoc. Director & Chief Leg. Counsel, Washington Leg. Office, American Civil Liberties Union, to U.S. Senate (Oct. 23, 2001) (on file with author), *available at* http://www.aclu.org/national-security/letter-senate-urging-rejection-final-version-usa-patriot-act. *See also* T*he USA Patriot Act of 2001: Hearing Before the H. Permanent Select Comm. on Intelligence*, 109th Cong. (2005) (statement of Timothy H. Edgard, Nat'l Sec. Policy Counsel, American Civil Liberties Union), *available at* http://www.aclu.org/national-security/testimony-national-security-policy-counsel-timothy-h-edgar-hearing-usa-patriot-act ; *The USA Patriot Act: Hearing Before the H. Judiciary Subcomm. on the Constitution, Civil Rights, & Civil Liberties*, 111th Cong. (2009) (statement of Michael German,

Policy Counsel, American Civil Liberties Union), *available at* http://www.aclu.org/national-security/aclu-testimony-house-judiciary-subcommittee-constitution-civil-rights-and-civil-li; *and The Permanent Provisions of the PATRIOT Act: Hearing Before the H. Judiciary Subcomm. on Crime, Terrorism & Homeland Sec.*, 1112th Cong. (2011) (statement of Michael German, Senior Policy Counsel, American Civil Liberties Union), *available at* https://www.aclu.org/files/assets/ACLU_Testimony_Before_the_HJC_Regarding_the_Patriot_Act.pdf.

[4] Marcus v. Search Warrant, 367 U.S. 717, 729 (1961).

[5] *See* Mapp v. Ohio, 367 U.S. 643 (1961).

[6] Allan M. Jalon, *A Break-In to End All Break-Ins*, L.A. TIMES, Mar. 8, 2006, http://articles.latimes.com/2006/mar/08/opinion/oe-jalon8.

[7] S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT ON SUPPLEMENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK II), S. Rep. No. 94-755, at 6-7 (1976) [hereinafter *Church Comm.*(*Book II)*].

[8] *Id.*

[9] 50 U.S.C. § 1801 et. seq. (2010).

[10] *FBI Statutory Charter: Hearings Before the S. Comm. on the Judiciary*, 95th Cong. Pt. 1, at 22 (1978).

[11] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, June 5, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[12] Secondary Order, In Re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Serv., Inc., on Behalf of MCI Commc'n Serv., Inc., D/B/A Verizon Bus. Serv., (U.S. Foreign Intelligence Surveillance Court Apr. 25, 2013), *available at* http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

[13] Ellen Nakashima, *Verizon providing all call records to U.S. under court order*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_print.html.

[14] Letter from Ronald Weich, Assistant Att'y Gen., Dep't of Justice, to Hon. Joseph R. Biden, Jr., President of the U.S. Senate (Apr. 30, 2012) (on file with author), *available at* http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf.

[15] 18 U.S.C. §1861 (2006), *available at*: http://www.law.cornell.edu/uscode/text/50/1861

[16] Letter from Rep. Sensenbrenner, to Eric Holder, Att'y Gen., Dep't of Justice (June 6, 2013) (on file with author), *available at* http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.

[17] *Current and Projected Nat'l Sec. Threats to the U.S.: Hearing Before the Sen. Select Comm. on Intelligence*, 112th Cong. (2011) (statement of Robert S. Mueller, III, Dir., Fed. Bureau of Investigation), at 46, *available at* http://www.fas.org/irp/congress/2011_hr/ssci-threat.pdf.

[18] *Current and Projected Nat'l Sec. Threats the the U.S.: Hearing Before the S. Select Comm. on Intelligence*, 112th Cong. (2011) (statement of Sen. Ron Wyden), at 48, *available at* http://www.fas.org/irp/congress/2011_hr/ssci-threat.pdf.

[19] See, Charlie Savage, *Senators Say Patriot Act is Being Misinterpreted*, N.Y. TIMES, May 27, 2011, at A17, *available at* http://www.nytimes.com/2011/05/27/us/27patriot.html?_r=0; *and* Letter from Sen. Mark Udall & Sen. Ron Wyden to Eric Holder, Att'y Gen., Dep't of Justice (Sept. 21, 2011) (on file with author), *available at* http://www.documentcloud.org/documents/250829-wyden-udall-letter-to-holder-on-wiretapping.html.

[20] Press Release, Wyden, Udall Issue Statement on Effectiveness of Declassified NSA Programs (June 19, 2013) (on file with author), *available at* http://www.wyden.senate.gov/news/press-releases/wyden-udall-issue-statement-on-effectiveness-of-declassified-nsa-programs.

[21] American Civil Liberties Union v. Fed. Bureau of Investigation, 11 CIV 7562 (S.D.N.Y. Oct. 26, 2011).

[22] Complaint for Declaratory Judgment and Injunctive Relief, ACLU v. Clapper, No.13CIV3994 (S.D.N.Y. June 11, 2013), *available at* http://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf.

[23] OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf [hereinafter *2007 NSL Report*].

[24] *Id.* at 104, 84.

[25] *Id.* at 98.

[26] OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter *2008 NSL Report*].

[27] *Id.* at 9 .

[28] *Id.* at 127, 129 n.116.
[29] *Id.* at 127.
[30] OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006 68 (2008), *available at* http://www.usdoj.gov/oig/special/s0803a/final.pdf [hereinafter *2008 Section 215 Report*].
[31] *See* OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS (2010), *available at* http://www.justice.gov/oig/special/s1001r.pdf [hereinafter *Exigent Letter Report*].
[32] *Id.* at 2, 10.
[33] EXIGENT LETTER REPORT, *supra* note 31, at 89.
[34] *Id.* at 263.
[35] *Id.* at 265, 268.
[36] *Id.* at 288.
[37] Marisa Taylor, *Obama Quietly Continues to Defend Bush Terror Policies*, MCCLATCHY, Jan. 22, 2010, http://www.mcclatchydc.com/2010/01/22/82879/obama-quietly-continues-to-defend.html; Josh Gerstein, *Obama Won't Release Another Surveillance Opinion*, POLITICO, Nov. 11, 2011, http://www.politico.com/blogs/joshgerstein/1111/Obama_wont_release_another_surveillance_opinion.html.
[38] James Risen & Eric Lichtblau, *Bush lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?ei=5090&en=e32072d786623ac1&ex=1292389200.
[39] Eric Lichtblau, *Debate and Protest at Spy Program's Inception*, N.Y. TIMES, Mar. 30, 2008, http://www.nytimes.com/2008/03/30/washington/30nsa.html?_r=3&ref=us&oref=slogin&oref=slogin&.
[40] Lowell Bergman, Eric Lichtblau, Scott Shane & Don Van Natta, Jr., *Spy Agency Data After Sept. 11 Led FBI to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, http://www.nytimes.com/2006/01/17/politics/17spy.html?pagewanted=all.
[41] Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, Dec. 24, 2005, http://www.nytimes.com/2005/12/24/politics/24spy.html?pagewanted=all.
[42] Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at 1A, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.
[43] *See* OFFICE OF THE INSPECTOR GEN., NAT'L SEC. SERV. & THE CENT. SEC. SERV., ST-09-0002 Working Draft (Mar. 24, 2009), *available at*: http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection. (For a full discussion of these events, *see* H. COMM. ON THE JUDICIARY MAJORITY STAFF, REINING IN THE IMPERIAL PRESIDENCY: LESSONS AND RECOMMENDATIONS RELATING TO THE PRESIDENCY OF GEORGE W. BUSH, at 146-165 (2009), *available at* http://judiciary.house.gov/hearings/printers/110th/IPres090113.pdf [hereinafter *Reining in the Imperial Presidency*].
[44] *See* Glenn Greenwald & Spencer Ackerman, *NSA Collected US Email Records in Bulk for More Than Two Years Under Obama*, THE GUARDIAN, June 27, 2013, http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama.
[45] REINING IN THE IMPERIAL PRESIDENCY, *supra* note 43, at 161-166.
[46] FISA Amendments Act of 2008, Pub.L.110-261 (2008).
[47] For a detailed analysis of the changes to the AGG over time, *see* OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES (2005), *available at* http://www.usdoj.gov/oig/special/0509/final.pdf.
[48] John Ashcroft, Atty' Gen., Dep't of Justice, The Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations (2002), *available at* http://legislationline.org/download/action/download/id/1416/file/97a12dc0c5709c1fd0a3898a03b7.pdf [hereinafter *Ashcroft Guidelines*].
[49] Id. at 7.
[50] *See* MARVIN J. JOHNSON, AMERICAN CIVIL LIBERTIES UNION, INTERESTED PERSONS MEMO: ANALYSIS OF CHANGES TO ATTORNEY GENERAL GUIDELINES (2002), *available at*: http://www.aclu.org/national-security/interested-persons-memo-analysis-changes-attorney-general-guidelines#_ftn19.
[51] ASHCROFT GUIDELINES, *supra* note 48.
[52] ASHCROFT GUIDELINES, *supra* note 48, at 22.
[53] *FBI Chief: 9/11 Surveillance Taxing Bureau,* WASH. POST, at A1, June 6, 2002, *available at*: http://www.mail-archive.com/ctrl@listserv.aol.com/msg92774.html.
[54] *See* Trevor Aaronson, *The Informants*, MOTHER JONES, Sept.-Oct., 2011, http://www.motherjones.com/politics/2011/08/fbi-terrorist-informants.

[55] Michael R. Blood, *FBI Director Defends Use of Informants in Mosques*, ASSOC. PRESS, June 8, 2009, *available at* http://www.guardian.co.uk/world/feedarticle/8548433.
[56] *See* FBI.gov, Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs (last visited Apr. 9, 2012).
[57] *See* ACLU.org, FBI/JTTF Spying, http://www.aclu.org/national-security/fbi-jttf-spying (last visited July 1, 2013); and ACLU.org, FBI Spy Files Project: ACLU Client List, http://www.aclu.org/national-security/fbi-spy-files-project-aclu-client-list (last visited July 1, 2013).
[58] Electronic communication from Fed. Bureau of Investigation Los Angeles, Santa Maria Resident Agency, to Fed. Bureau of Investigation Counterterrorism Div. 3, (May 22, 2001) (on file with author), *available at* http://www.aclu.org/spyfiles/jttf/672_674.pdf (Summary of case. Report of 05/19/2001 protest. Proposed development of[REDACTED]ource).
[59] Scott Shane, *For Anarchist, Details of Life as FBI Target*, N.Y. TIMES, May 29, 2011, at A1, *available at* http://www.nytimes.com/2011/05/29/us/29surveillance.html?pagewanted=all.
[60] *Id. see also* N.Y. Times, From Scott Crow's F.B.I. File, http://www.nytimes.com/interactive/2011/05/29/us/29surveillance-text.html (last visited July 1, 2013).
[61] Letter from Rep. Zoe Lofgren, to Glenn A. Fine, Inspector Gen., Dep't of Justice (May 18, 2006) (on file with author).
[62] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S INVESTIGATIONS OF CERTAIN DOMESTIC ADVOCACY GROUPS (2010), http://www.justice.gov/oig/special/s1009r.pdf [hereinafter *Review of FBI's Investigations*].
[63] *Id.* at 186-187.
[64] *Id.*
[65] *Id.*
[66] *Id.* at 186.
[67] *Id.* at 187.
[68] *Id.* at 190.
[69] *Id.* at 183.
[70] *Id.* at 166.
[71] *Id.* at 177, 184.
[72] *Id.* at 184.
[73] MICHAEL B. MUKASEY, DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 17 (2008), http://www.justice.gov/ag/readingroom/guidelines.pdf [hereinafter *2008 AGG*].
[74] *Id.* at 20.
[75] Carrie Johnson, *Rule Changes Would Give FBI Agents Extensive New Powers*, WASH. POST, Sept. 12, 2008, http://articles.washingtonpost.com/2008-09-12/news/36900434_1_fbi-agents-criminal-cases-intelligence.
[76] Electronic communication from Fed. Bureau of Investigation Counterterrorism Div., to all field offices (Sept. 24, 2009) (on file with author), *available at:* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM004887.pdf (Counterterrorism Program Guidance, Baseline Collection Plan).
[77] Charlie Savage, *FBI Focusing on Security Over Ordinary Crime*, N.Y. TIMES, Aug. 24, 2011, at A16, *available at* http://www.nytimes.com/2011/08/24/us/24fbi.html.
[78] Fed. Bureau of Investigation Counterterrorism Div., *supra* note 76, at 11.
[79] DEP'T OF JUSTICE, FACT SHEET: RACIAL PROFILING (June 17, 2003), http://www.justice.gov/opa/pr/2003/June/racial_profiling_fact_sheet.pdf.
[80] DEP'T OF JUSTICE, GUIDANCE REGARDING THE USE OF RACE BY FEDERAL LAW ENFORCEMENT AGENCIES (June 2003), http://www.justice.gov/crt/about/spl/documents/guidance_on_race.pdf.
[81] Scott Keeter, *Why Surveys of Muslim Americans Differ*, PEW RESEARCH CENTER, Mar. 6, 2009, http://www.pewresearch.org/2009/03/06/why-surveys-of-muslim-americans-differ/.
[82] FEDERAL BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE (2008), *available at* http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2008-version [hereinafter *2008 DIOG*].
[83] *Id.* at 32.
[84] *Id.* at 33-34
[85] *Id. at* 33.

[86] Al Baker, *FBI Official Faults Police Tactics on Muslims*, N.Y. TIMES, Mar. 8, 2012, at A25, *available at* http://www.nytimes.com/2012/03/08/nyregion/chief-of-fbi-newark-bureau-decries-police-monitoring-of-muslims.html.
[87] Jason Grant, *Recent NYPD spying uproar shakes FBI's foundations in N.J. terror intelligence*, NEWARK STAR-LEDGER, Mar. 7, 2012, http://www.nj.com/news/index.ssf/2012/03/recent_nypd_spying_uproar_shak.html.
[88] FEDERAL BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATION AND OPERATIONS GUIDE (2011), *available at* http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version [hereinafter *2011 DIOG*].
[89] *See* Nathan Freed Wessler, Staff Att'y, ACLU, *FBI Documents Suggest Feds Read Emails Without a Warrant*, May 8, 2013, http://www.aclu.org/blog/national-security-technology-and-liberty/fbi-documents-suggest-feds-read-emails-without-warrant.
[90] FEDERAL BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATION AND OPERATIONS GUIDE § 18, § 18.7.2.6 (2012), *available at* http://www.aclu.org/files/pdfs/email-content-foia/FBI%20docs/June%202012%20FBI%20DIOG.pdf [hereinafter *2012 DIOG*]; *see also* 2011 DIOG *supra* note 88, at § 18.7.2.10(H).
[91] 2008 DIOG, *supra* note 82, at 32.
[92] Electronic communication from Fed. Bureau of Investigation, to Detroit field office (July 6, 2009) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM011609.pdf (Domain Management).
[93] Kecia Escoe, *Demographic Makeup of Muslims in Michigan*, Muslim Observer, Mar. 1, 2012, http://muslimmedianetwork.com/mmn/?p=10258.
[94] Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Oct. 7, 2009) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM011454.pdf (Intelligence Related to the Black Separatist Threat).
[95] Electronic communication from Fed. Bureau of Investigation, San Francisco, Oakland Resident Agency, to San Francisco (June 8, 2009) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM011495.pdf (Domain Management – Criminal; Asian-Eurasian Criminal Enterprise).
[96] *Id.* at 2.
[97] Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Jan. 21, 2009) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM009170.pdf (Intelligence Related to Mara Salvatrucha Threat); Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Dec. 15, 2008) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM011388.pdf (Intelligence Related to MS-13 Threat); Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Sept. 22, 2008) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM008040.pdf (Intelligence Related to MS-13 Locations); Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Sept. 4, 2008) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM007857.pdf (Intelligence Related to Mara Salvatrucha (MS-13)).
[98] Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Sept. 22, 2008) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM008040.pdf (Intelligence Related to MS-13 Locations); *and* Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Jan. 21, 2009) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM009170.pdf (Intelligence Related to Mara Salvatrucha Threat).
[99] William J. Broad & Scott Shane, *Anthrax Case Had Costs for Suspects*, N.Y. TIMES, Aug. 10, 2008, at A1, *available at* http://www.nytimes.com/2008/08/10/washington/10anthrax.html?pagewanted=1&ref=stevenjhatfill.
[100] Scott Shane, *FBI vehicle hits Hatfill, but he gets the $5 ticket*, BALT. SUN, May 20, 2003, http://articles.baltimoresun.com/2003-05-20/news/0305200401_1_clawson-anthrax-fbi-vehicle.
[101] *See* Amy Goldstein, Nelson Hernandez & Annie Hull, *Tales of Addiction, Anxiety, Ranting*, WASH. POST, Aug. 6, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/05/AR2008080503747.html; *and* Jerry Markon, *Anthrax report casts doubt on scientific evidence in FBI case against Bruce Ivins*, WASH. POST, Feb. 15, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021502251.html.
[102] PADDY HILLYARD, SUSPECT COMMUNITY: PEOPLE'S EXPERIENCE OF THE PREVENTION OF TERRORISM ACTS IN BRITAIN 238, (1993).

[103] AMERICAN CIVIL LIBERTIES UNION, BLOCKING FAITH, FREEZING CHARITY: CHILLING MUSLIM CHARITABLE GIVING IN THE "WAR ON TERRORISM FINANCING," (2009), http://www.aclu.org/human-rights/report-blocking-faith-freezing-charity.
[104] *Id.* at 72.
[105] THE CREATING LAW ENFORCEMENT ACCOUNTABILITY AND RESPONSIBILITY PROJECT, CUNY LAW SCHOOL, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (2013), http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf [hereinafter *Mapping Muslims*].
[106] Fusion centers are state, local and regional information sharing entities which incorporate federal, state and local law enforcement, emergency response and other government agencies and private entities to analyze and disseminate information. For more information *see* ACLU.org, Spy Files: More About Fusion Centers, http://www.aclu.org/spy-files/more-about-fusion-centers (last visited July 1, 2013).
[107] *See* FED. BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR THE EGUARDIAN THREAT TRACKING SYSTEM (2008), *available at* http://www.aclu.org/files/assets/aclueg000047.pdf [hereinafter *eGuardian PIA*]; *and* ACLU.org, Spy Files: More About Suspicious Activity Reporting http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting (last visited July 1, 2013).
[108] FBI.gov, Connecting the Dots Using New FBI Technology, http://www.fbi.gov/news/stories/2008/september/eguardian_091908 (last visited July 1, 2013).
[109] Daniel Zwerdling, G.W. Schulz, Andrew Becker & Margot Williams, *Mall Counterterrorism Files ID Mostly Minorities*, NAT'L PUB. RADIO, Sept. 8, 2011, http://www.npr.org/2011/09/08/140262005/mall-counterterrorism-files-id-mostly-minorities.
[110] AMERICAN CIVIL LIBERTIES UNION, NO REAL THREAT: THE PENTAGON'S SECRET DATABASE ON PEACEFUL PROTEST, (2007), http://www.aclu.org/files/pdfs/safefree/spyfiles_norealthreat_20070117.pdf.
[111] *See* Press Release, Office of the Assistant Sec'y of Def. (Pub. Affairs), DOD to Implement new Interim Threat Reporting Procedures (Aug. 21, 2007) (on file with author), *available at* http://www.defense.gov/releases/release.aspx?releaseid=11251; *and* Press Release, Office of the Assistant Sec'y of Def. (Pub. Affairs), DOD to Implement new Suspicious Activity Reporting System (May 21, 2010) (on file with author), *available at* http://www.defense.gov/releases/release.aspx?releaseid=13553.
[112] EGUARDIAN PIA, *supra* note 107, at 4, 10.
[113] FRANK J. CILLUFFO, JOSEPH R. CLARK, MICHAEL P. DOWNING & KEITH D. SQUIRES, GEO. WASH. U. HOMELAND SEC. POLICY INSTITUTE, COUNTERTERRORISM INTELLIGENCE: FUSION CENTER PERSPECTIVES 31 (2012), *available at* http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf.
[114] Pub. L. 108-458, 118 Stat. 3638 (Dec. 17, 2004).
[115] GOV'T ACCOUNTABILITY OFFICE, INFORMATION SHARING: ADDITIONAL ACTIONS COULD HELP ENSURE THAT EFFORTS TO SHARE TERRORISM-RELATED SUSPICIOUS ACTIVITY REPORTS ARE EFFECTIVE 15-17 (2013), *available at* http://www.gao.gov/assets/660/652995.pdf.
[116] *Id.* at 16.
[117] *Id.* at 17.
[118] *Id.* at 33.
[119] Letter from Rep. Brad Miller and Rep. James Sensenbrenner, Jr., H. Comm. on Sci. & Tech. Subcomm. on Investigations, to Hon. David Walker, Comptroller of the U.S. (June 5, 2007) (on file with author), *available at* http://www.securityprivacyandthelaw.com/uploads/file/miller_snsbrnner_walker_GAO_6_5_07.pdf.
[120] Press Release, Office of the Press Sec'y, White House, Homeland Security Presidential Directive 2 (Oct. 29, 2001) (on file with author), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011030-2.html.
[121] DEP'T OF JUSTICE, REPORT ON "DATA-MINING" ACTIVITIES PURSUANT TO SECTION 126 OF THE USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005 (2007), *available at* http://epic.org/privacy/fusion/doj-dataming.pdf.
[122] *Id.* at 11.
[123] *Id.*
[124] Letter from Chairman Brad Miller, H. Comm. on Sci. & Tech. Subcomm. on Investigations, to Chairman David Obey, H. Comm. on Appropriations (June 16, 2008) (on file with author), *available at* http://www.wired.com/images_blogs/dangerroom/files/61608_miller_to_obey.pdf.

[125] ELECTRONIC FRONTIER FOUND., REPORT ON THE INVESTIGATIVE DATA WAREHOUSE, ELECTRONIC FRONTIER FOUNDATION (2009), https://www.eff.org/issues/foia/investigative-data-warehouse-report.
[126] U.S. DEP'T OF THE TREASURY FIN. CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW – BY THE NUMBERS: ISSUE 18 4 (2012), *available at* http://www.fincen.gov/news_room/rp/files/btn18/sar_by_numb_18.pdf (for all issues, *see* U.S. Dep't. of the Treasury, SAR Activity Review – By the Numbers, http://www.fincen.gov/news_room/rp/sar_by_number.html (last visited July 1, 2013).
[127] *Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements: Hearing Before Subcomm. on Oversight and Investigations of the H. Comm. on Fin. Services,* 110th Cong. (2007) (statement of Deputy Assistant Dir. Salvador Hernandez, Fed. Bureau of Investigation) at 6, *available at* http://archives.financialservices.house.gov/hearing110/hthernandez051007.pdf ; *see also Countering Terrorist Financing: Progress and Priorities: Hearing Before the Comm. on the Judiciary,* 112th Cong. (2011) (questions for the record for Ralph Boelter, Assistant Acting Dir., Fed. Bureau of Investigation), *available at* http://www.judiciary.senate.gov/resources/transcripts/upload/092111QFRs-Boelter.pdf.
[128] Letter from Chairman Brad Miller, *supra* note 124.
[129] Noah Shachtman, *FBI Data-Mining Slashed After G-Men Dis Congress*, WIRED, June 26, 2008, http://www.wired.com/dangerroom/2008/06/there-was-a-tim/.
[130] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S FOREIGN TERRORIST TRACKING TASK FORCE 2 (2013), *available at* http://www.justice.gov/oig/reports/2013/a1318r.pdf.
[131] *Id.*
[132] *Id.* at 5-6.
[133] Notice of a new system of records, 77 Fed. Reg. 40,630 (July 10, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-07-10/html/2012-16823.htm.
[134] NAT'L RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENTS, COMMITTEE ON TECHNICAL AND PRIVACY DIMENSIONS OF INFORMATION FOR TERRORISM PREVENTION AND OTHER NATIONAL GOALS, p. 78 (2008), *available at* http://www.nap.edu/catalog.php?record_id=12452 [hereinafter *NRC Report*].
[135] *Id.* at 4.
[136] *Id.* at 86-91.
[137] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S FOREIGN TERRORIST TRACKING TASK FORCE 11-12 (2013), *available at* http://www.justice.gov/oig/reports/2013/a1318r.pdf.
[138] *Id.* at 16.
[139] *Id.* at 14.
[140] *Id.* at 27.
[141] *Id.* at 28-30.
[142] Letter from Chairman Michael McCaul and Rep. Peter King, H. Comm. on Homeland Sec., to Sec'y Janet Napolitano, et al, Dep't Homeland Sec. (Apr. 20, 2013) (on file with author), *available at* http://www.scribd.com/doc/137320693/Letter-from-Rep-Mike-McCaul-and-Rep-Peter-King.
[143] Sabastian Rotella, *The American Behind India's 9/11 – and how U.S. Botched Chances to Nab Him*, PROPUBLICA, Jan. 24, 2013, http://www.propublica.org/article/david-headley-homegrown-terrorist.
[144] Kristina Goetz, *Muslim who shot soldier in Arkansas says he wanted to cause more death*, COMMERCIAL APPEAL, Nov. 13, 2010, *available at* http://www.knoxnews.com/news/2010/nov/13/muslim-who-shot-solider-arkansas-says-he-wanted-ca/.
[145] James Dao, *A Muslim Son, a Murder Trial, and Many Questions*, N.Y. TIMES, Feb. 17, 2010, at A11, *available at* http://www.nytimes.com/2010/02/17/us/17convert.html?pagewanted=all.
[146] Pierre Thomas, Richard Esposito & Jack Date, *Recruiter Shooting Suspect had Ties to Extremist Locations*, ABC NEWS, June 3, 2009, http://abcnews.go.com/Politics/story?id=7732467&page=1.
[147] WILLIAM H. WEBSTER COMM'N ON THE FED. BUREAU OF INVESTIGATION, COUNTERTERRORISM INTELLIGENCE & THE EVENTS AT FT. HOOD ON NOV. 5, 2009, FINAL REPORT 63, 68 (2012), *available at* http://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission.
[148] *Id.* at 88.
[149] *Id.* at 80.
[150] *Id.* at 88.
[151] *Id.*
[152] *Flight 253: Learning Lessons from an Averted Tradgedy: Hearing Before the S. Comm. on Homeland Sec. and*

Gov't Affairs, 111th Cong. (2010) (statement of Michael Leiter, Dir., Nat'l Counterterrorism Ctr.), *available at* http://www.dni.gov/testimonies/20100127_testimony.pdf.

[153] S. HOMELAND SEC. & GOV'T AFFAIRS COMM., PERMANENT SUBCOMM. ON INVESTIGATIONS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 35 (2012), *available at* http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

[154] Press Release, Fed. Bureau of Investigation, 2011 Request for Information on Tamerlan Tsarnaev from Foreign Government (Apr. 19, 2013) (on file with author), *available at* http://www.fbi.gov/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government.

[155] Kathy Lally, *Russian FSB Describes its Tsarnaev Letter to FBI*, WASH. POST, May 31, 2013, http://articles.washingtonpost.com/2013-05-31/world/39656209_1_dagestan-keating-tamerlan-tsarnaev.

[156] *See e.g.*, Major Garrett, *Was the Ball Dropped in the Tsarnaev Questioning?*, Nat'l J., Apr. 23, 2013, http://www.nationaljournal.com/columns/all-powers/was-the-ball-dropped-in-the-tsarnaev-questioning-20130423.

[157] Mark Hosenball & Tabassum Zakaria, *U.S. Was Alerted to Bombing Suspect's Travel to Russia*, REUTERS, Apr. 24, 2013, http://mobile.reuters.com/article/newsOne/idUSBRE93N1EA20130424?irpc=932; and, Greg Miller, *Anti-terrorism Task Force Was Warned of Tamerlan Tsarnaev's Long Trip to Russia*, WASH. POST, Apr. 25, 2013, http://www.washingtonpost.com/world/national-security/anti-terror-task-force-was-warned-of-tamerlan-tsarnaevs-long-trip-to-russia/2013/04/25/0ed426de-addb-11e2-8bf6-e70cb6ae066e_story.html.

[158] Scott Shane & Michael S. Schmidt, *F.B.I. Did Not Tell Police In Boston of Russian Trip*, N.Y. TIMES, May 10, 2013, at A18, *available at* http://www.nytimes.com/2013/05/10/us/boston-police-werent-told-fbi-got-warning-on-tsarnaev.html.

[159] Eric Schmitt & Michael S. Schmidt, *Slain Bombing Suspect Was Placed on Two Federal Watch Lists in Late 2011*, N.Y. TIMES, Apr. 25, 2013, at A20, *available at* http://www.nytimes.com/2013/04/25/us/tamerlan-tsarnaev-bomb-suspect-was-on-watch-lists.html.

[160] Philip Martin, *Waltham Triple Murder Echos Through Boston Bombing Probe, Florida FBI Shooting Death*, WBGH NEWS, May 23, 2013, http://www.wgbhnews.org/post/waltham-triple-murder-echoes-through-marathon-bombing-probe-florida-fbi-shooting-death.

[161] Fed. Bureau of Investigation, Uniform Crime Reports: Crime in the United States 2011, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2011/crime-in-the-u.s.-2011/clearances (last visited Sept. 5, 2013).

[162] *Id*.

[163] *See* Chris Calabrese, Legislative Counsel, American Civil Liberties Union, The Biggest New Spying Program You've Probably Never Heard Of (July 30, 2012), http://www.aclu.org/blog/national-security-technology-and-liberty/biggest-new-spying-program-youve-probably-never-heard.

[164] Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, WALL ST. J., Dec. 13, 2012, http://online.wsj.com/article/SB10001424127887324478304578171623040640006.html.

[165] Ryan Singel, *Funding for TIA All But Dead*, WIRED, July 14, 2003, http://www.wired.com/politics/law/news/2003/07/59606.

[166] Kim Zetter, *Government Fights for Use of Spy Tool That Spoofs Cell Towers*, WIRED, Mar. 29, 2013, http://www.wired.com/threatlevel/2013/03/gov-fights-stingray-case/.

[167] Linda Lye, Staff Att'y, American Civil Liberties Union of N. Cal., DOJ Emails Show Feds Were Less Than "Explicit" With Judges On Cell Phone Tracking Tool (Mar. 27, 2013), http://www.aclu.org/blog/national-security-technology-and-liberty/doj-emails-show-feds-were-less-explicit-judges-cell.

[168] Charlie Savage, *Senators Say Patriot Act is Being Misinterpreted*, N.Y. TIMES, May 27, 2011, at A17, *available at* http://www.nytimes.com/2011/05/27/us/27patriot.html?_r=0.

[169] In December 2005 the *New York Times* revealed that shortly after the 9/11 attacks President Bush authorized the National Security Agency (NSA) to begin conducting warrantless electronic surveillance within the United States, in violation of the Foreign Intelligence Surveillance Act (FISA), which Congress had established in 1978 as the "exclusive means" for national intelligence wiretapping. *See* Risen & Lichtblau, *supra* note 38.

[170] CHURCH COMM. (BOOK II), *supra* note 7, at 2-3.

[171] Spencer Ackerman, *FBI Taught Agents They Could 'Bend or Suspend the Law,'* WIRED, Mar. 28, 2012, http://www.wired.com/dangerroom/2012/03/fbi-bend-suspend-law/.

[172] 2008 NSL REPORT, *supra* note 26, at 100.

[173] Id.at 95.

[174] 2008 SECTION 215 REPORT, *supra* note 30, at 67-72.

[175] 2008 NSL REPORT, *supra* note 26, at 15.
[176] Press Release, American Civil Liberties Union, Congress Reauthorizes Overbroad Patriot Act Provisions, (May 26, 2011) (on file with author), *available at* http://www.aclu.org/national-security-technology-and-liberty/congress-reauthorizes-overbroad-patriot-act-provisions.
[177] OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES (Redacted Version) p, 93 (2005), *available at* http://www.justice.gov/oig/special/0509/final.pdf.
[178] OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES (Redacted Version) p. 172 (2005), *available at* http://www.justice.gov/oig/special/0509/final.pdf.
[179] REVIEW OF FBI'S INVESTIGATIONS, *supra* note 62, at 198.
[180] *See Oversight Hearing on Counterterrorism: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 16-17 (2002).
[181] Eric Lichtblau, *Report Finds Cover-up in FBI Terror Case*, N.Y. TIMES, Dec. 4, 2005, http://www.nytimes.com/2005/12/04/politics/04fbi.html?pagewanted=print.
[182] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S ACTIONS IN CONNECTION WITH ALLEGATIONS RAISED BY CONTRACT LINGUIST SIBEL EDMONDS, SPECIAL REPORT (2005), *available at* http://www.usdoj.gov/oig/special/0501/final.pdf.
[183] Dan Browning, *Ex-Agent Wins Lawsuit Against FBI*, MINNEAPOLIS STAR-TRIB., Feb. 5, 2007.
[184] Todd Lightly, *Beleaguered FBI Agent Gets Job Back*, CHI. TRIB., Oct. 19, 2005.
[185] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S RESPONSE TO JOHN ROBERTS' STATEMENTS ON 60 MINUTES (2003), *available at* http://www.usdoj.gov/oig/special/0302/report.pdf.
[186] OFFICE OF PROF'L RESPONSIBILITY, DEP'T OF JUSTICE, REPORT OF INVESTIGATION OF WHISTLEBLOWER ALLEGATIONS BY FEDERAL BUREAU OF INVESTIGATION SPECIAL AGENT BASSEM YOUSSEF (2006), *available at* http://www.whistleblowers.org/storage/whistleblowers/documents/order_and_opr_report.pdf.
[187] Neil A. Lewis, *Agent Claims Evidence on Stevens was Concealed,* N.Y. TIMES, Feb. 11, 2009, at A14, *available at* http://www.nytimes.com/2009/02/11/us/politics/11stevens.html?_r=0.
[188] Richard Mauer & Lisa Demer, *Key Players Contest FBI Whistleblower Allegations*, ANCHORAGE DAILY NEWS, Feb. 15, 2009, http://www.adn.com/2009/02/15/691774/key-players-contest-fbi-whistle.html; *and* Tony Hopfinger & Amanda Coyne, *Why is Lead FBI Agent in Botched Ted Stevens Case Still Employed?*, ALASKA DISPATCH, June 6, 2012, http://www.alaskadispatch.com/article/why-lead-fbi-agent-botched-ted-stevens-case-still-employed.
[189] Jill Burke, *Agent Turned Whistleblower Leaves the FBI*, ALASKA DISPATCH, July 14, 2010, http://www.alaskadispatch.com/article/agent-turned-whistleblower-leaves-fbi; *and* Hopfinger & Coyne, *supra* note 189.
[190] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S DISCIPLINARY SYSTEM 39 (2009), *available at*: http://www.justice.gov/oig/reports/FBI/e0902/final.pdf.
[191] *See* Risen & Lichtblau, *supra* note 38; *and* Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USATODAY, May 11, 2006, at 1A, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.
[192] Jane Mayer, *The Secret Sharer*, NEW YORKER, May 23, 2011, *available at* http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all.
[193] U.S. v. Thomas A. Drake, Case No. 1:10-CR-181-RDB (D. Md. July 15, 2011), at 42-43(transcript of proceedings, sentencing before Hon. Richard D. Bennett, United States District Judge,), *available at* http://www.fas.org/sgp/jud/drake/071511-transcript.pdf.
[194] Scott Shane, *Obama Takes a Hard Line Against Leaks to Press*, N.Y. TIMES, June 12, 2010, at A1, *available at* http://www.nytimes.com/2010/06/12/us/politics/12leak.html.
[195] EXIGENT LETTER REPORT, *supra* note 31, at 95-96.
[196] Mark Sherman, *Gov't Obtains Wide AP Phone Records in Probe*, ASSOC. PRESS, May 13, 2013, http://bigstory.ap.org/article/govt-obtains-wide-ap-phone-records-probe.
[197] Ann E. Marimow, *A Rare Peek into a Justice Department Leak Probe*, WASH. POST, May 19, 2013, http://www.washingtonpost.com/local/a-rare-peek-into-a-justice-department-leak-probe/2013/05/19/0bc473de-be5e-11e2-97d4-a479289a31f9_story.html?hpid=z2.
[198] Application for Search Warrant, In re Search of EmailAccount John Doe@gmail.com, No. 10-291-M-01 (D.D.C. Nov. 7, 2011), *available at*: http://apps.washingtonpost.com/g/page/local/affidavit-for-search-warrant/162/.

[199] *USA PATRIOT Act of 2001: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 97, 100 (2005) (statements of Alberto R. Gonzales, Att'y Gen., Dep't of Justice, & Robert S. Mueller, III, Dir., Fed. Bureau of Investigation).
[200] *See* 2007 NSL REPORT, *supra* note 23, at 75..
[201] *See* John Solomon, *Gonzales was told of FBI violations*, WASH. POST, July 10, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/07/09/AR2007070902065.html; *and* John Solomon, *In Intelligence World, a Mute Watchdog*, WASH. POST, July 15, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/07/14/AR2007071400862.html.
[202] *Hearing On FBI Oversight: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. (2006) (statement of Sen. Patrick Leahy), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da11db40a&wit_id=e655f9e2809e5476862f735da11db40a-0-0.
[203] *Id*.
[204] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S INVOLVEMENT IN AND OBSERVATIONS OF DETAINEE INTERROGATIONS IN GUANTANAMO BAY, AFGHANISTAN, AND IRAQ (2008), *available at* http://www.justice.gov/oig/special/s0805/final.pdf.
[205] *Oversight of the Fed. Bureau of Investigation, Hearing Before the S. Comm. on the Judiciary,* 110th Cong. 14-15 (2008), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110shrg53619/pdf/CHRG-110shrg53619.pdf [hereinafter *2008 FBI Oversight Hearing*].
[206] Risen & Lichtblau, *supra* note 38.
[207] 2008 FBI OVERSIGHT HEARING, *supra* note 206, at 14.
[208] *Id.* at 16.
[209] *Oversight of the Fed. Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary,* 111th Cong. 24 (2009), *available at* https://www.fas.org/irp/congress/2009_hr/fbi.pdf.
[210] Letter from Ronald Welch, Assistant Att'y Gen., Dep't of Justice, to Chairman Patrick Leahy, S. Comm. on the Judiciary (Sept. 14, 2009) (on file with author), *available at* https://www.cdt.org/security/20090914_leahy.pdf.
[211] REVIEW OF FBI'S INVESTIGATIONS, *supra* note 62, at 35–59.
[212] *Id.* at 53 n.79.
[213] U.S. Magistrate Judge Stephen W. Smith, *Gagged, Sealed and Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 609 (2012), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2071399.
[214] *Id.* at 613.
[215] *Id.* at 603.
[216] Declarations of Craig Monteilh Submitted by Plaintiffs in Support of Their Opposition to Motions to Dismiss, Yassir Fazaga v. Fed. Bureau of Investigation, Case No. SA CV 11-00301, at 6 (C.D.Cal., Jan. 30, 2012), *available at* http://www.aclu-sc.org/cases/fazaga/declaration-of-craig-monteilh-re-motion-to-dismiss/.
[217] *Id.* at 6-7.
[218] *Id.* at 12.
[219] *Id.* at 16.
[220] *Id.* at 23.
[221] Teresa Watanbe & Scott Glover, *Man Says He Was an Informant for FBI in Orange County*, L.A. TIMES, Feb. 26, 2009, http://articles.latimes.com/2009/feb/26/local/me-informant26.
[222] First Amended Complaint, Yassir Fazaga v. Fed. Bureau of Investigation, Case No. SA CV 11-00301, at 6 (C.D.Cal. Jan. 30, 2012), *available at* http://www.aclu-sc.org/cases/fazaga/first-amended-complaint/.
[223] The state secrets privilege is a long-standing common law privilege that allows the government to block the release of evidence in a lawsuit that would harm national security. The George W. Bush administration increasingly used the privilege to dismiss entire lawsuits at the onset, blocking lawsuits challenging government torture, rendition and warrantless surveillance. The Obama administration's continuing use of this practice, particularly in a case of domestic law enforcement activities directed at Americans is troubling. *See* Nancy Goldstein, *The US National Security Smokescreen*, THE GUARDIAN, Dec. 11, 2011, http://www.theguardian.com/commentisfree/cifamerica/2011/dec/08/us-national-security-smokescreen.
[224] *See* Peter Bibring, American Civil Liberties Union of S. Cal., *You Have the Right to Remain Spied On*, (Aug. 16, 2012), http://www.aclu.org/blog/national-security/you-have-right-remain-spied.
[225] *Id*.
[226] Spencer Ackerman, *FBI 'Islam 101' Guide Depicted Muslims as 7th Century Simpletons*, WIRED, July 27, 2011, http://www.wired.com/dangerroom/2011/07/fbi-islam-101-guide/; Spencer Ackerman, *FBI Teaches Agents:*

'Mainstream' Muslims are 'Violent, Radical, WIRED, Sept. 14, 2011, http://www.wired.com/dangerroom/2011/09/fbi-muslims-radical/; Spencer Ackerman, *New Evidence of Anti-Islam Bias Underscores Deep Challenges for FBI Reform Pledge*, WIRED, Sept. 23, 2011, http://www.wired.com/dangerroom/2011/09/fbi-islam-domination/.

[227] TERRORISM AND POLITICAL ISLAM: ORIGINS, IDEOLOGIES, AND METHODS; A COUNTERTERRORISM TEXTBOOK (Erich Marquardt & Christopher Heffelfinger, eds., Combating Terrorism Ctr. 2008), *available at* https://www.aclu.org/files/fbimappingfoia/20111019/ACLURM000540.pdf.

[228] ARIE PERLIGER, CHALLENGERS FROM THE SIDELINES; UNDERSTANDING AMERICA'S VIOLENT FAR-RIGHT, COMBATING TERRORISM CENTER AT WEST POINT, (Nov. 2012), *available at* http://www.ctc.usma.edu/wp-content/uploads/2013/01/ChallengersFromtheSidelines.pdf. The ACLU criticized some aspects of the report. See, Laura Murphy and Mike German, *Are the FBI and Congress Politicizing Terrorism Intelligence*, ACLU Blog of Rights, Jan. 24, 2013, https://www.aclu.org/blog/national-security/are-fbi-and-congress-politicizing-terrorism-intelligence.

[229] BRIG BARKER & MOLLY AMMAN, FED. BUREAU OF INVESTIGATION SUPERVISORY SPECIAL AGENTS, COUNTERTERRORISM INTERVIEW AND INTERROGATION STRATEGIES: UNDERSTANDING AND RESPONDING TO THE DOMESTIC THREAT: TERRORISM AND POLITICAL ISLAM: ORIGINS, IDEOLOGIES, AND METHODS; A COUNTERTERRORISM TEXTBOOK 369, 378 (Erich Marquardt & Christopher Heffelfinger, eds., Combating Terrorism Ctr.2008), *available at* https://www.aclu.org/files/fbimappingfoia/20111019/ACLURM000540.pdf#page=341.

[230] Press Release, Fed. Bureau of Investigation, FBI Launches Comprehensive Review of Training Program (Sept. 20, 2011) (on file with author); *and* Press Release, Fed. Bureau of Investigation, Response to Media Reporting Regarding Counterterrorism Training (Sept. 15, 2011) (on file with author).

[231] FED. BUREAU OF INVESTIGATION COUNTERTERRORISM DIV., THE RADICALIZATION PROCESS: FROM CONVERSION TO JIHAD 10 (2006), *available at* http://cryptome.org/fbi-jihad.pdf.

[232] *Id.* at 6.

[233] Spencer Ackerman, *New Evidence of Anti-Islam Bias Underscores Deep Challenges for FBI Reform Pledge*, WIRED, Sept. 23, 2011, http://www.wired.com/dangerroom/2011/09/fbi-islam-domination/. *See also* Letter from 27 civil and human rights groups, to FBI Dir. Robert S. Mueller, III (Oct. 4, 2011) (on file with American Civil Liberties Union), *available at* http://www.aclu.org/files/assets/sign_on_letter_to_dir_mueller_re_radicalization_report_10.4.11.pdf.

[234] For example, the ACLU of Pennsylvania represented Erich Scherfen, a commercial pilot, Gulf War veteran and Muslim convert, whose job was threatened when he was told he was barred from flying due to his placement on the No Fly List. *See* Jeanne Meserve, *Name on Government Watch List Threatens Pilot's Career*, CNN, Aug. 22, 2008, http://www.cnn.com/2008/US/08/22/pilot.watch.list/.

[235] For example, the ACLU of Pennsylvania represented Dr. Abdul Moniem El-Ganayni, an American nuclear physicist and volunteer prison imam, whose security clearance was revoked after he publicly criticized the FBI for mistreating Muslims. *See Muslim Man Wants Review of Clearance Revocation*, ASSOC. PRESS, Oct. 14, 2008, *available at* http://usatoday30.usatoday.com/news/nation/2008-10-14-muslim-scientist_N.htm.

[236] *See* Fed. Bureau of Investigation, Black Separatist Extremism , *available at* http://www.aclu.org/files/fbimappingfoia/20120518/ACLURM026634.pdf (PowerPoint presentation); *and* Fed. Bureau of Investigation, Black Separatist Extremists , *available at* http://www.aclu.org/files/fbimappingfoia/20120518/ACLURM026655.pdf (PowerPoint presentation).

[237] *Id*.

[238] *See* FBI.gov, Major Terrorism Cases: Past and Present, http://www.fbi.gov/about-us/investigate/terrorism/terrorism_cases (last visited July 1, 2013).

[239] *See* Fed. Bureau of Investigation, Anarchist Extremism Overview, slide 3, 6 (undated), *available at* http://www.aclu.org/files/fbimappingfoia/20120518/ACLURM026485.pdf (PowerPoint presentation).

[240] *See* Fed. Bureau of Investigation, Animal Rights/Environmental Extremism, slide 4 (undated), *available at* http://www.aclu.org/files/fbimappingfoia/20120518/ACLURM026701.pdf (PowerPoint presentation); *and* Fed. Bureau of Investigation, Animal Rights/ Eco Extremism Trends, slide 34 (undated), *available at* http://www.aclu.org/files/fbimappingfoia/20120518/ACLURM026510.pdf#page=34 (PowerPoint presentation).

[241] *See* Amy Goldstein, *A Deliberate Strategy of Disruption*, WASH. POST, Nov. 4, 2001, http://www.pulitzer.org/archives/6613.

[242] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF JUSTICE, THE SEPTEMBER 11 DETAINEES: A REVIEW OF THE TREATMENT OF ALIENS HELD ON IMMIGRATION CHARGES IN CONNECTION WITH THE INVESTIGATION OF THE SEPTEMBER 11 ATTACKS 37 (2003), *available at* http://www.justice.gov/oig/special/0306/full.pdf.
[243] HUMAN RIGHTS WATCH, PRESUMPTION OF GUILT: HUMAN RIGHTS ABUSES OF POST-9/11 DETAINEES (Aug. 2002), *available at* http://www.hrw.org/reports/2002/us911/USA0802.pdf.
[244] John Ashcroft, Att'y Gen., Dep't of Justice, Prepared Remarks for the U.S. Mayors Conference (Oct. 25, 2001), *available at* http://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks10_25.htm.
[245] Electronic communication from Fed. Bureau of Investigation, to all field offices (Sept. 24, 2009) (on file with author), *available at* http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM004887.pdf (Counterterrorism Program Guidance, Baseline Collection Plan).
[246] *See* Eric Lichtblau, *FBI Tells Offices to Count Local Muslims and Mosques*, N.Y. TIMES, Jan. 23, 2003, http://www.nytimes.com/2003/01/28/politics/28MOSQ.html; *and* Mary Beth Sheridan, *Interviews of Muslims to Broaden*, WASH. POST, July 17, 2004, http://www.washingtonpost.com/wp-dyn/articles/A56080-2004Jul16.html.
[247] David E. Kaplan, *Exclusive: Nuclear Monitoring of Muslims Done Without Search Warrants*, U.S. NEWS & WORLD REP., Dec. 22, 2005, http://www.usnews.com/usnews/news/articles/nest/051222nest.htm.
[248] *See* American Civil Liberties Union, ACLU Eye on the FBI: Exposing Misconduct and Abuse of Authority, http://www.aclu.org/national-security/eye-fbi-exposing-misconduct-and-abuse-authority (last visited July 1, 2013).
[249] Fed. Bureau of Investigation, Targeting – Understanding the Fundamentals, Islamic Ummah – Where to Target, Bates #FBI036163-FBI036174 (on file with author) (PowerPoint presentation).
[250] JENNIE PASQUARELLA, AMERICAN CIVIL LIBERTIES UNION OF S. CAL., MUSLIMS NEED NOT APPLY: HOW USCIS SECRETLY MANDATES THE DISCRIMINATORY DELAY AND DENIAL OF CITIZENSHIP AND IMMIGRATION BENEFITS TO ASPIRING AMERICANS 9 (2013), *available at* http://www.aclusocal.org/CARRP/.
[251] *See* AMERICAN CIVIL LIBERTIES UNION, BLOCKING FAITH, FREEZING CHARITY: CHILLING MUSLIM CHARITABLE GIVING IN THE "WAR ON TERRORISM FINANCING" 76, 77 (2009), *available at* http://www.aclu.org/human-rights/report-blocking-faith-freezing-charity; *and* MAPPING MUSLIMS, *supra* note 105.
[252] Trevor Aaronson, *The Informants*, MOTHER JONES, Sept.-Oct. 2011, *available at* http://www.motherjones.com/politics/2011/08/fbi-terrorist-informants.
[253] PowerPoint Presentation from Fed. Bureau of Investigation, *supra* note 239.
[254] *Terror Trials by the Numbers: Stings, informants, and underwear bombs: Digging through the data from federal terrorism cases*, MOTHER JONES, Sept.-Oct. 2011, *available at* http://www.motherjones.com/politics/2011/08/terror-trials-numbers.
[255] Trevor Aaronson, *The Best Terrorists Money Can Buy*, MOTHER JONES, Sept.-Oct. 2011, *available at* http://www.motherjones.com/politics/2011/08/fbi-terrorist-sting-targets.
[256] Paul Harris, *Newburgh Four: Poor, Black, and Jailed Under FBI 'Entrapment' Tactics*, THE GUARDIAN, Dec. 12, 2011, http://www.guardian.co.uk/world/2011/dec/12/newburgh-four-fbi-entrapment-terror.
[257] *Id*.
[258] *See* Affidavit of Special Agent Jared Ruddy, U.S. v. Derrick Shareef, Case No. 06CR0919, (N.D.Ill. Dec. 8, 2006), *available at* https://www.documentcloud.org/documents/231598-shareefcomplaint.html.
[259] David Shipler, *Terrorist Plots, Hatched by the FBI*, N.Y. TIMES, Apr. 28, 2012, http://www.nytimes.com/2012/04/29/opinion/sunday/terrorist-plots-helped-along-by-the-fbi.html?pagewanted=all.
[260] *See* Andrea Todd, *The Believers*, Elle, May 2008, *available at* http://www.greenisthenewred.com/blog/elle_anna/421/.
[261] S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT ON SUPPLEMENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK III), S. Rep. No. 94-755, at 13 (1976).
[262] J. Delong, *American Indians questioned about Nevada bear hunt by FBI*, RENO-GAZETTE JOURNAL, Apr. 11, 2012.
[263] Ken Ritter, *ACLU Wants FBI Records About Nevada Bear Hunt Foes*, ASSOC. PRESS, Sept. 7, 2012, *available at* http://www.utsandiego.com/news/2012/sep/07/aclu-wants-fbi-records-about-nevada-bear-hunt-foes/.
[264] Delong, *supra* note 263.
[265] Yana Kunichoff, Raids on Activists May Indicate FBI Abuse of Power, Truthout.org (Oct. 10, 2010), *available at* http://www.stopfbi.net/content/raids-activists-may-indicate-fbi-abuse-power.
[266] *FBI Raids Homes of Seattle and Portland Occupy Activists*, SALEM-NEWS, Aug. 13, 2012, http://www.salem-news.com/articles/august132012/occupy-raids.php.

[267] Maxine Bernstein, *Two Portland Residents Facing Federal Grand Jury Subpoena from Seattle Vow They Won't Cooperate*, THE OREGONIAN, Aug. 1, 2012, http://www.oregonlive.com/pacific-northwest-news/index.ssf/2012/08/two_portland_residents_facing.html.
[268] *Id.*
[269] Radley Balko, Swat Officer Killed by Non-Lethal Flash-Bang Grenade, Reason (Mar. 8, 2011), http://reason.com/blog/2011/03/09/swat-officer-killed-by-non-let.
[270] *See* Dep't of State, Arrest or Detention of an American Citizen Abroad, http://travel.state.gov/travel/tips/emergencies/arrest/arrest_3879.html (last visited Apr. 9, 2013).
[271] 22 USC §1732.
[272] *See* Press Release, American Civil Liberties Union, ACLU Lawsuit Charges U.S. Officials Illegally Detained American Citizen (Nov. 10, 2009) (on file with author), *available at* http://www.aclu.org/national-security/aclu-lawsuit-charges-us-officials-illegally-detained-american-citizen.
[273] *See* Anna Louie Sussman, *Naji Hamdan's Nightmare*, THE NATION, Mar. 22, 2010, http://www.thenation.com/article/naji-hamdans-nightmare#.
[274] Mark Mazetti, *Detained American Says He Was Beaten in Kuwait*, N.Y. TIMES, Jan. 6, 2011, at A10, *available at* http://www.nytimes.com/2011/01/06/world/middleeast/06detain.html?_r=2&hp&.
[275] *Id.*
[276] Nick Baumann, *Lawyer: FBI Illegally Interrogating Gulet Mohamed*, MOTHER JONES, Jan. 12, 2011, http://www.motherjones.com/politics/2011/01/gulet-mohamed-fbi-illegal-interrogation.
[277] Emailfrom redacted FBI officials to Nick Baumann, Mother Jones magazine (July 8, 2011, 04:39 PM) (on file with author), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/235035/fbistatementtomotherjones.pdf; *see also* Nick Baumann, *Locked Up Abroad for the FBI*, MOTHER JONES, Sept.-Oct. 2011, *available at* http://www.motherjones.com/politics/2011/08/proxy-detention-gulet-mohamed?page=1.
[278] AUTHOR'S NAME REDACTED, FED. BUREAU OF INVESTIGATION, CROSS CULTURAL, RAPPORT-BASED INTERROGATION, VERSION 5 (Feb. 23, 2011), *available at* http://www.aclu.org/files/fbimappingfoia/20120727/ACLURM036782.pdf.
[279] *Id.* at 7-8.
[280] *Id.* at 8. *See also* PHYSICIANS FOR HUMAN RIGHTS & HUMAN RIGHTS FIRST, LEAVE NO MARKS: ENHANCED INTERROGATION TECHNIQUES AND THE RISK OF CRIMINALITY 31 (2007); *and* NAT'L DEF. INTELLIGENCE COLLEGE, EDUCING INFORMATION: INTERROGATION: SCIENCE AND ART 138 (2006), *available at* http://www.pegc.us/archive/DoD/DIA_EI_rpt_200612.pdf.
[281] FED. BUREAU OF INVESTIGATION, LEGAL HANDBOOK FOR FBI SPECIAL AGENTS 90 (2003), *available at* http://vault.fbi.gov/Legal%20Handbook%20for%20FBI%20Special%20Agents; Halely v. State of Ohio, 332 U.S. 596 (1948).
[282] Letter from Laura W. Murphy, Director of the Washington Legislative Office, American Civil Liberties Union, & Devon Chaffee, Legislative Counsel, American Civil Liberties Union, to FBI Director Robert Mueller, III, (Aug. 2, 2012) (on file with author), *available at* http://www.aclu.org/national-security/letter-director-fbi-regarding-interrogation-primer.
[283] *See* GOV'T ACCOUNTABILITY OFFICE, REP. TO CONGRESSIONAL REQUESTERS: TERRORIST WATCH LISTS SHOULD BE CONSOLIDATED TO PROMOTE BETTER INTEGRATION AND SHARING, GAO-03-322 (2003); OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., DHS CHALLENGES IN CONSOLIDATING TERRORIST WATCH LIST INFORMATION, OIG-04-31 (2004); OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, REVIEW OF THE TERRORIST SCREENING CENTER (REDACTED FOR PUBLIC RELEASE), AUDIT REPORT 05-27 (2005); OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, REVIEW OF THE TERRORIST SCREENING CENTER'S EFFORTS TO SUPPORT THE SECURE FLIGHT PROGRAM (REDACTED FOR PUBLIC RELEASE) AUDIT REPORT 05-34 (2005); OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, FOLLOW-UP AUDIT OF THE TERRORIST SCREENING CENTER (REDACTED FOR PUBLIC RELEASE), AUDIT REPORT 07-41 (2007); OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, AUDIT OF THE U.S. DEPARTMENT OF JUSTICE TERRORIST WATCHLIST NOMINATION PROCESSES, AUDIT REPORT 08-16 (2008); OFFICE OF THE INSPECTOR GEN., U.S. JUSTICE DEP'T, THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES, AUDIT REPORT 09-25 (2009); OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., EFFECTIVENESS OF THE DEPARTMENT OF HOMELAND SECURITY TRAVELER REDRESS INQUIRY PROGRAM, OIG-00-103 (2009).
[284] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES, at iv (2009), *available at* http://www.justice.gov/oig/reports/FBI/a0925/final.pdf.

[285] *See*, Mark Hosenball, *Number of Names on U.S. Counter-terrorism Database Jumps*, REUTERS, May 2, 2013, http://www.reuters.com/article/2013/05/03/us-usa-security-database-idUSBRE94200720130503; *and*, Eileen Sullivan, *US No-Fly List Doubles in 1 Year,* ASSOCIATED PRESS, Feb. 2, 2012, http://www.foxnews.com/us/2012/02/02/ap-exclusive-us-no-fly-list-doubles-in-1-year/.
[286] GOV'T ACCOUNTABILITY OFFICE, ROUTINELY ASSESSING IMPACTS OF AGENCY ACTIONS SINCE THE DECEMBER 25, 2009, ATTEMPTED ATTACK COULD HELP INFORM FUTURE EFFORTS (2012), *available at* http://www.gao.gov/assets/600/591312.pdf.
[287] *See* Shirin Sadeghi, *U.S. Citizen Put on No-Fly list to Pressure Him Into Becoming Informant*, HUFFINGTON POST, June 7, 2012, http://www.huffingtonpost.com/shirin-sadeghi/kevin-iraniha-no-fly-list_b_1579208.html.
[288] Complaint for Injunctive and Declaratory Relief, Latif, et al., v. Holder, No. 10-cv-750 (BR) (D.Or. June 29, 2010), *available at* http://www.aclu.org/files/assets/2010-6-30-LatifvHolder-Complaint.pdf.
[289] *Id.*, *see also* ACLU.org, Latif, et al. v. Holder, et al. – ACLU Challenge to Government No Fly List, http://www.aclu.org/national-security/latif-et-al-v-holder-et-al-aclu-challenge-government-no-fly-list (last visited July 1, 2013).
[290] Memorandum of Points and Authorities in Opposition to Defendant's Motion for Partial Summary Judgment, Latif, et al. v. Holder, No. 10-cv-750 (BR), at 25 n25 (D.Or. Mar. 22, 2013), *available at* http://www.aclu.org/files/assets/nfl_sj_opp.pdf.
[291] Yonas Fikre v. The Fed. Bureau of Investigation, Civil No. 3:13-cv-000899, (D.Or. May 30, 2013), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/705673/yonas-fikre-lawsuit.pdf. *See also* Nigel Duara & Malin Rising, *Yonas Fikre, US Muslim, Claims He Was Tortured At FBI's Behest In United Arab Emirates*, ASSOC. PRESS, Apr. 18, 2012, *available at* http://www.huffingtonpost.com/2012/04/18/us-muslim-tortured_n_1434664.html.
[292] Kari Huus, *American Seeks Political Assylum in Sweden, Alleging Torture, FBI Coercion*, MSNBC, Apr. 18, 2012, http://usnews.nbcnews.com/_news/2012/04/18/11266018-american-seeks-political-asylum-in-sweden-alleging-torture-fbi-coercion?lite.
[293] Nick Baumann, *U.S. Charges Yonas Fikre, American Who Claimed Torture, With Conspiracy*, MOTHER JONES, May 3, 2012, http://www.motherjones.com/mojo/2012/05/yonas-fikre-american-who-claimed-torture-indicted-conspiracy-charges.
[294] Shirin Sadeghi, *U.S. Citizen Put on No-Fly List to Pressure Him Into Becoming FBI Informant*, HUFFINGTON POST, June 7, 2012, http://www.huffingtonpost.com/shirin-sadeghi/kevin-iraniha-no-fly-list_b_1579208.html.
[295] Ashley McGlone & Susan Shroder, *San Diego Man on No-Fly List Returns Home*, SAN DIEGO UNION TRIB., June 7, 2012, http://www.utsandiego.com/news/2012/Jun/06/no-fly-list-keeps-sdsu-grad-grounded-in-costa-rica/.
[296] NRC REPORT, *supra* note 134.