The National Suspicious Activity Reporting Initiative and the Production of U.S. Domestic Intelligence

Kenneth Farrall

In the summer of 2002, controversy over U.S. government plans to fight the terrorist threat erupted into public discourse. The Terrorism Information and Prevention System (TIPS), introduced by Attorney General Ashcroft as part of President Bush's Freedom Corps initiative, would deputize millions of American workers to be on the lookout for suspicious activity. Specifically, the TIPS program looked to enlist "American workers who, in the daily course of their work, are in a unique position to see potentially unusual or suspicious activity in public places."[1] Among the professions targeted were meter readers, truck drivers, mail carriers, and train conductors. A pilot program was set to begin with one million informants in ten cities, more than 4 percent of their aggregate population. TIPS volunteers would be given a special toll-free telephone number and website where they could submit reports of any suspicious behavior.

Reaction to the proposed program was overwhelmingly negative. Newspaper editorials pointed out that the percentage of citizen spies in the TIPS program would exceed that of Cold War East Germany's notorious Stasi program. *New York Times*' columnist William Safire galvanized opposition with his November 14 column, "You Are a Suspect."[2] CNET columnist Lisa Bowman asked, "Is Your Cable Guy a Spy?"[3] Although ultimately failing to advance in the legislative process, an explicit ban on funding for the TIPS or any similarly conceived program was drafted and amended to that fall's Homeland Security bill.

In the midst of this public firestorm, the U.S. Department of Justice (DoJ) tried to dilute some of the more problematic aspects of the program, but it eventually shelved TIPS altogether. The democratic process had worked, it appeared. The U.S. government announced plans for a vast domestic spy network. First, the newspapers, and then Congress, cried foul, and the government decided not to adopt the plan. As it turns out, however, the TIPS program is alive and well and already has a scope and sophistication beyond anything described in Ashcroft's original program, employing not only a range of individuals in the private sector but also enrolling the nation's more than 800,000 law enforcement personnel as the new front line of domestic intelligence.

The program has proceeded largely unnoticed, in part due to its generic sounding name, the National Suspicious Activity Reporting Initiative (NSI), a focal point of the broader, equally generic sounding information sharing environment (ISE). The story of suspicious activity reporting (SAR) is highly intertwined with that of fusion centers, a term which is much more salient within the privacy advocacy community. SAR can be understood as a key discursive product of fusion centers through which information is circulated among federal intelligence agencies. The ISE-SAR program is both a standard for harmonizing existing or traditional data production (such as routine police reporting) and an initiative to increase the scope and coverage of domestic intelligence.[4]

The goal of this chapter is to describe the formal establishment of the nationwide suspicious activity reporting initiative, its importance in the ongoing evolution of the U.S. domestic intelligence system, and the need for increased public scrutiny. I first explore the role of language in our understanding of intelligence practices and provide some very brief historical context of U.S. domestic intelligence policy. Following this linguistic and historical perspective, I describe at some length the logic and sites of suspicious activity report production. Finally, I conclude with a brief discussion of the potential dangers of this program, both to civil liberties and national security and the importance of increased transparency. A wide range of government documents, nongovernmental organization (NGO) publications, trade press, and mass media publications was examined during the research process.[5]

Understanding Intelligence and Its Production

Executive Order 12333

For much of the U.S. intelligence community, a core document that establishes the institutional meaning of intelligence is Executive Order 12333 issued by Ronald Reagan in 1981 and recently amended by President Bush. The document remains a key directive in shaping the roles and responsibilities of U.S. intelligence agencies and organizations. The document has been read in different ways. For example, in a 1985 note in the *Cornell Law Review*, Sherri Conrad claims that it was an unconstitutional extension of CIA power designed to counter constraints placed on the agency in the 1970s:

> On December 4, 1981, President Ronald Reagan promulgated Executive Order 12333, establishing United States intelligence guidelines. Restrictions on the Central Intelligence Agency (CIA) were instituted in the 1970s in response to disclosures of widespread wrongdoing. The Order reflects the President's determination to "unleash" America's intelligence community from those limitations. The Order allows the CIA, America's chief foreign intelligence gathering entity, to direct domestic counterintelligence, foreign intelligence, covert operations, and law enforcement activity against United States citizens. The drafters of the Order ignored the statutory limits on intelligence gathering activity codified in the National Security Act. The President's action thus constitutes a statutorily impermissible license for renewed government intrusion, and the Order should be revoked.[6]

Others, such as the privacy and civil liberties office of the director of national intelligence (DNI), have highlighted the ways in which the document protects civil liberties and civil rights. The order, for example, places strict limits on how intelligence agencies ". . . can collect, retain, and disseminate information about 'U.S. persons.'"[7] If the information does not fit into one of ten specific categories, the intelligence agency must not "collect" it.[8] Further, the DNI office notes that the amended order now has a section explicitly addressing the maintenance of privacy and civil liberties.

It is critical, however, to understand just what is meant when we talk about intelligence and its collection. While the executive order offers definitions for "intelligence," "intelligence community," and "intelligence activity," the definitions are circular and can be modified at any time by the president or the director of national intelligence.[9] Further, it is not entirely clear how this definition applies to "domestic intelligence," those activities conducted by the intelligence community within national boundaries or on U.S. citizens abroad. And the use of the term *collection* entails important assumptions about the nature of the information that can obscure the logic of its production.[10]

Production versus Collection

In her examination of the role of language and metaphor in science, Anne Salmond argues that, in the West, knowledge is nearly always conceived as a landscape, while facts are objects to be found within this landscape:

> Facts are depicted as hard, solid, concrete and tangible—they are to be picked up, collected, gathered, dug up, sorted, sifted, weighed, balanced, arranged and looked at. . . . Facts are objects, described in group nouns, with a physical existence and of natural origin. . . . A fact may be mineral, to be mined and excavated, or vegetable, to be gathered and preserved, cultivated and even cooked (from raw facts to half-baked theories). This is the true metaphorical basis of "objectivity," presupposed in our everyday talk about what is. It is also the linguistic rationale for the persistent idea that field-work is data gathering, as though the important features of another society will be lying about on the ground for our collection.[11]

Major privacy advocates today regularly define problems related to surveillance and privacy in terms of personal information collection. In his book, *The Digital Person*, one of the most important works today warning of the dangers of the emerging dossier society, Daniel Solove writes that "[j]ust as the Food and Drug Administration (FDA) regulates food and drugs . . . we need a federal agency to regulate the collection and use of personal information."[12] David Lyon defines surveillance as "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered."[13] Gary Marx writes that the contemporary commercial state is "inconceivable without the massive collection of personal data."[14]

When we speak of "collecting" or "gathering" personal information, we are participating in the long, linguistic tradition of treating information and facts as natural objects existing out there in the landscape. In many contexts, particularly in those circumstances where real-time surveillance, or third-party aggregation and analysis (data mining) is a concern, this particular metaphoric approach works quite well. As with any metaphor, however, the approach highlights certain aspects of the problem while hiding others. The terms *collection* and *capture* include a built-in assumption that the information gathered already exists "out there" before it is collected. Although *collection* is an active term, it is passive in relation to the data itself. *Collection* properly articulates an individual context if the collector is unaware of or has no control over the how and why a particular record or file is produced.

Focusing on collection ignores the very critical processes and raw materials that lead to the creation of information in the first place, processes that need to be much better understood if policy is to have any chance at regulating the emergence of state surveillance systems worldwide.

The Sites and Logics of Production

> Cognition is the most socially conditioned activity of man, and knowledge is the paramount social creation.[15]

A great deal of work in the academic field known as "social construction of reality" has challenged the notion that "facts" exist out there in the world waiting to be discovered. Latour and Woolgar, for example, have shown that seemingly objective scientific facts are not discovered but are thoroughly constituted by the material setting of the laboratory.[16] Summarizing the early work of Ludwig Fleck on the *Genesis and Development of a Scientific Fact*, Jan Golinksi explains:

> The social character of knowledge is revealed by the circumstances of its production within a specific interactive community . . . which sustains a distinctive mode of reasoning.[17]

I do not wish to enter the active discourse over the relative merits of the social constructivist critique of modern science, but the insights they offer are particularly useful when considering intelligence information. Information is not simply "out there." It is produced within specific social, institutional, and technological contexts. Without first the production of information, its "objectivation"[18] into material form manifested in our common world, information cannot be collected.

I use the terms *site* and *logic* as heuristics for exploring production. The term *site of production* has multiple meanings depending on context. It may refer to the institutional location of a particular system of records, such as the IRS or the FBI. It may refer to the actual physical location of suspicious activity report production, whether it occurs within an office at the subject's place of employment or inside a police car on a state highway, or a combination of physical locales that may be involved in the production and storage of electronic records. Questions about what is produced, who produces it, and where they produce are also critical to understanding the sites of production.

The term *logic of production* refers primarily to both the *how* (specific procedures and data formats) and the *why* (production criteria, vetting) of production. The logic for federal-level suspicious activity reports include specific data attributes required of the report as well as a vetting process, akin to quality control in a manufacturing plant. Other aspects of the how of production might include specific training scenarios given to potential report producers. What specific criteria are given to the producers, and do they end up following these criteria?

Intelligence Production versus Intelligence Collection

Marilyn Peterson, at the Bureau of Justice Assistance, highlights the distinction between information and intelligence: while the former may be collected, the latter is produced.[19] Intelligence is what emerges after analysis is performed on streams of incoming data. While there is clearly some value in this distinction, we must be careful to recognize that all data is first produced, though the logic of this production may be hidden or obscured. The use of *production* within intelligence circles is exclusively for those intelligence products, such as bulletins and reports, that are formulated based on analyses of incoming (collected) data streams. But this "collected" information was also produced within some context, by a logic that may or may not be under the control of the particular intelligence agency.

In a recent RAND report, Gregory Treverton defines "domestic intelligence" as

> efforts by government organizations to gather, assess, and act . . . on information about individuals or organizations in the United States or U.S. persons elsewhere that is not necessarily related to the investigation of a known past criminal act or specific planned criminal activity.[20]

Treverton uses the three-part *gather*, *assess*, and *act* categories to describe the function and role of intelligence. Peterson's "production" occurs after the assessment stage and prior to action. The term *gather*, however, and its semantic sibling, *collect*, may mask prior moments of information production—more than the simple capture of a once external media object, but not quite production of the final, postassessment "intelligence product."

Again, in many contexts, "collection" works. Phone records, for example, are collected by the FBI and later used as the basis for some form of higher-level report. From the perspective of the phone company, however, we can understand the phone record as being the "product" of certain institutional decisions over time and a service architecture that evolved quite independently of the DoJ. SARs, however, are not simply collected in this way. They are *produced* under emerging, state-sponsored institutional logics that need to be carefully examined. To understand the significance of this new phase of intelligence gathering, I consider, in brief, how the initiative fits in the broader scope of U.S. domestic intelligence history.

A Brief (Three-Phase) History of U.S. Domestic Intelligence

As a largely heuristic device, and to simplify a very complex tapestry of law and policy that has impacted the evolution and configuration of the U.S. domestic intelligence environment over the past several decades, I break down its history into three phases: (1) the COINTELPRO period of intelligence abuses from the late 1920s to the mid 1970s; (2) the post-Church period of legal and policy constraints from 1974 until 2001; and (3) the war-on-terror period that has followed the September 11 terrorist attacks of 2001.

COINTELPRO

Senator Frank Church (D-ID) chaired the U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities in 1975. Over a period of nine months, the committee interviewed more than 800 officials and held 250 executive and 21 public hearings, investigating widespread intelligence abuses by the CIA, FBI, and NSA.[21] The Church Committee's fourteen reports, issued between 1975 and 1976, have been called the most thorough investigation of U.S. intelligence agencies ever released to the public. Their reports chronicled widespread intelligence abuses by the CIA, the FBI, and the U.S. military from the 1920s through the early 1970s.

The reports concluded that U.S. intelligence agencies had investigated "a vast number of American citizens and domestic organizations." Nearly a quarter of a million first-class letters were opened and photographed "by the CIA between 1953–1973, producing a CIA computerized index of nearly one and one-half million names." An estimated 100,000 individuals were the subject of U.S. Army Intelligence files between the mid 1960s and 1971. The IRS held intelligence files on more than 11,000 individuals between 1969 and

1973, on the basis of political rather than tax criteria. And "at least 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a 'national emergency.'"[22]

In addition to collecting this information, intelligence agencies disrupted the lives and violated the basic human rights of the people targeted. People were discredited, marriages ended, and livelihoods lost. For example,

> [a]n FBI document boasted that a "pretext" phone call to Stokeley Carmichael's mother telling her that members of the Black Panther Party intended to kill her son left her "shocked." The memorandum intimated that the Bureau believed it had been responsible for Carmichael's flight to Africa the following day.[23]

Post-Church

Public reaction to the Church revelations was so strong that sweeping changes in law and policy ensued. A new privacy law, the Privacy Act of 1974, placed limits on the sharing of personal data among U.S. government departments and required the federal government to notify the public of any planned new "system of records." The DoJ initiated new policies that dramatically reduced the FBI's role in domestic intelligence operations,[24] while the DoD announced a similar policy against random spying on American citizens, especially when they were engaged in First Amendment activities such as assembly and protest. As the story is now commonly told, "walls" were placed between government departments and between the policing of crime and the collection of intelligence that significantly limited the flow of information and were intended to prevent the emergence of central federal databases containing comprehensive information on innocent American citizens.

War on Terror

The post-Church status quo was shattered after 11 September 2001, where walls have become nothing more than barriers to "connecting the dots"[25] that might protect America from its next attack. While vestiges of the initial constraints remain, there appears to be an emergent state belief that national security interests justify a basic state right, which citizens should trust them not to abuse, to access, and to produce information on everyone and everything.[26] While the FBI has resumed its earlier (phase 1) role in domestic intelligence, these practices are expanding into the regular police force and, in fact, the broader private workforce.

The report issued by the 9/11 Commission and released to the public in the summer of 2004 faulted the by then decades-old "walls" policy as one of the primary reasons behind the intelligence failure that preceded the September 11 attacks. The commission recommended a dramatic reorganization of the country's intelligence system and the breaking down of existing barriers to information sharing. The "walls" phase was to be replaced by a new culture of information sharing among local, state, and federal agencies. Much of this new culture was introduced with a law passed later that fall, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), sweeping legislation intended to improve coordination between U.S. intelligence agencies and the departments of federal, state, and local governments.[27]

According to the law's preamble, IRTPA was enacted "to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes." As part of the legislation, a new director of national intelligence (DNI) was created to serve as head of the intelligence community and to direct the implementation of the National Intelligence Program.

Section 1016 of the bill called for the implementation of an information sharing environment (ISE). According to the text of the law, "The terms 'information sharing environment' and 'ISE' mean an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section." The law called for the president to designate a program manager for the ISE (PM-ISE) and establish an Information Sharing Council to advise the president and the program manager. The council includes members from the Department of Commerce, the Central Intelligence Agency, Department of Defense, director of national intelligence, Federal Bureau of Investigation, Department of Homeland Security, National Counterterrorism Center, and many other departments with connections to national security.

The PM-ISE lays out the vision of the ISE in its implementation plan:

> We envision a future ISE that represents a trusted partnership among all levels of government in the United States, the private sector, and our

> foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America.[28]

According to the PM-ISE, the primary initiative of the ISE is the National Suspicious Activity Reporting Initiative (NSI). It is important to recognize that the NSI represents far more than a simple plan to share existing information. The NSI is a wholesale expansion of the U.S. domestic intelligence apparatus for which there is no historical precedent.

To make this point clear I will now explore in some detail both the logic and sites of SAR production.

The Logic of Suspicious Activity Reports

Suspicious activity reports are produced by state agents based on a largely top-down logic that is both rigorous and open ended. It is rigorous in the sense that the data format and specific behavioral triggers are explicitly identified in the federal standard. It is open ended in that agents are continually reminded they should call or text in information related to anything they deem "suspicious," whether or not the specific type of behavior is identified in the ISE-SAR standard. Agents are situated within a continuing stream of documents, some produced locally and some by federal agencies, which provide a more variable narrative noting particular kinds of activities that are worthy of special attention. American citizens are also likely to be influenced by popular television culture and programs such as FOX's *24* as to what behavior warrants suspicion.

The raw material for the ISE-SAR comes from a wide range of information streams, including the audio-visual fields of domestic intelligence agents as they go about their day-to-day activities, phone calls, and web submissions from citizens who feel they've seen something out of the ordinary. Generic SARs become ISE-SARs when they are formally vetted and labeled as such by a designated federal intelligence agent, often an FBI agent assigned to a regional fusion center.

SAR Definition and Standard

The ISE-SAR standards document, published by the program manager for the information sharing environment, includes the official definition of a suspicious activity report, guidelines for their production, the vetting procedure required before a generic SAR can become an official ISE-SAR, and a detailed XML schema describing the specific technical standards that ISE-SARs must follow.[29] The ISE-SAR standard is not static. Originally released in January 2008, it was modified in May 2009 after feedback from stakeholders. A further revisions are likely.

The 1.5 revision included a number of significant improvements made at the request of privacy advocates, including the ACLU, that will clearly reduce the possibility for blatant abuse of civil rights and First Amendment freedoms. Specifically, (1) the definition of SAR was narrowed; (2) the list of behavioral targets for SAR production was subdivided into obvious criminal activity and noncriminal activity in which SAR production should proceed only after careful further investigation; (3) the number of data fields that are included under the protected category of PII has grown to reduce the ease of reidentification; and (4) the use of the term *reasonable* was injected into target behavior descriptions to give, at least, some lip service to the reasonableness standard encoded in U.S. federal law (28 CFR Part 23).

The current functional standard defines a SAR as a document chronicling an "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity":

> It is important to stress that this *behavior-focused approach* to identifying suspicious activity requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description).[30]

The specific SAR-triggering criteria listed in the standard are now broken down into two classes of behavior: (1) "defined criminal activity and potential terrorism nexus activity" and (2) potential or noncriminal activity requiring additional fact information during investigation.[31]

The Major Sites of SAR production

Guardian and eGuardian Systems

The two primary technological sites—physical systems of records—where the production of SARs takes place are the Guardian and eGuardian systems maintained by the FBI. Access to the Guardian system is restricted to FBI agents and other authorized personnel, while the eGuardian system is accessible to the broader state and local law enforcement community.[32]

In September 2004, the FBI launched the Guardian system to "facilitate the accurate, complete, and timely reporting on the existence and status of terrorist threats." The system, initially only available on the FBI's intranet, collected reports from FBI agents and legal attaches, who were "required to enter . . . new terrorism threats and suspicious incidents originating in their territory and use it to track resolution." The FBI has reported that agents are expected to draw from multiple sources, including "(1) the general public, (2) other government agency partners, (3) state and local law enforcement, (4) ongoing FBI investigations and intelligence assessments, and (5) FBI Legal Attaches."[33] General threats and suspicious incidents make their way into agent reports via telephone calls, e-mail, mail correspondence, or through the FBI's website. The Guardian system includes classified information up to the level of "secret."

In the fall of 2008, the Guardian system was extended with a web-based component known as eGuardian. Unlike Guardian, eGuardian is restricted to unclassified information. EGuardian draws on a much larger field of people to produce SARs than does the Guardian system. According to the FBI, eGuardian will be "available through our secure Law Enforcement Online Internet portal to more than 18,000 agencies, which will be able to run searches and input their own reports." Data entered into the eGuardian database is immediately accessible at all fusion centers for vetting, where trained personnel decide whether the data will be retained and forwarded to the appropriate FBI task force or simply deleted from the system. According to an FBI web page, Guardian and eGuardian will "work together, feeding each other."

> [E]Guardian entries with a possible terrorism nexus will be pushed to Guardian and out to our task forces, and unclassified threat and suspicious activity information from the FBI housed in Guardian will be pushed to eGuardian and out to the entire law enforcement community. It's an effective one-two punch.[34]

Richard Beauchamp, the FBI's interim information technology portfolio manager at the chief information officer's office in late 2007, explained that the eGuardian system was an attempt to "try to understand whether it is feasible to capture all suspicious activity data in a single repository or whether we need a distributed approach using Web services."[35]

While the FBI were the sole state agents responsible for entering and vetting suspicious activity reports within the Guardian system, the unclassified eGuardian system connected more than 800,000 local police officers into the Department of Homeland Security's extended domestic intelligence network. On 10 June 2008, the Major Cities Chiefs Association, which as of June 2009 included sixty-three cities with populations over half a million, released a formal resolution endorsing the "Findings and Recommendations" and calling for the adoption of suspicious activity reporting practices in police departments nationwide. According to the "Findings and Recommendations," local police departments are advised to incorporate SAR reporting into their existing activities, for example, by simply adding a SAR checkbox to forms and paperwork. By the end of 2009, pilot SAR production systems were being tested in Florida; New York; Virginia; Boston; Miami-Dade; Chicago; Los Angeles; Seattle; Houston; Las Vegas; Washington, D.C.; and Arizona.[36]

Fusion Centers

Fusion centers serve as the primary institutional locale for the vetting of generic SARs and the official production of ISE-SARs. They can be considered an extension of an initiative to "fuse" intelligence information that began with the establishment of the National JTTF in July 2002. The National Joint Terrorism Task Force (NJTTF) and the now more than 100 local JTTFs in more than 100 cities nationwide have been the initial points of fusion for once "walled" intelligence agencies to share and analyze information. The NJTTF, as of 2004, consisted of fifty-seven people from thirty-eight U.S. agencies (law enforcement, intelligence, diplomatic, defense, public safety, and homeland security).[37] Ken Love, acting chief of the NJTTF in July 2004, describes its basic function:

> It's a pretty simple concept: we bring together people from every U.S. agency that collects and processes terrorist intelligence; we put them in one room and hook them into their own and into our FBI intelligence databases; and all of a sudden we have the universe of terrorist intelligence on the table—to share, to query, to coordinate, to answer questions, and to give direction and support to the 84 Joint Terrorism Task Forces (JTTFs) around the country that function under us. "Fusion" means that terrorist intelligence is instantly shared vertically from HQ to our JTTFs and horizontally to all NJTTF agencies.[38]

Local JTTF offices have been in existence since 1980, but they have grown in number and become much more important since the 9/11 attacks. A fusion center can be considered a more general class of the JTTF, which involves state, local, and private institutions as well. The DoJ's official *Fusion Center Guidelines* describe the broad reach of data collection accompanying fusion center charters:

> There is no single source for terrorism-related information. It can come through the efforts of the intelligence community; local, state, tribal, and federal law enforcement authorities; other government agencies (e.g., transportation and health departments); the private sector; and the general public.[39]

Although some fusion centers were in operation before the 9/11 attacks, they were not widely deployed nationally until early 2005. In December 2004 the president's Homeland Security Advisory Council recommended that "each State should establish an information center that serves as a 24/7 'all-source,' multi-disciplinary, information fusion center."[40] Between 2004 and 2007, the Department of Homeland Security dispersed $254 million in support of the centers, while the FBI and other federal law enforcement agencies have personnel on-site. Fusion centers are generally led by local law enforcement chapters such as the state police or the FBI, but they also regularly work with DoD personnel and the U.S. Northern Command.

All-Crimes Approach

Because fusion centers are officially administered by the state, not the federal government, they are not subject to federal privacy laws and have developed in different ways. Although most early fusion centers began with a focus on counterterrorism, the role of fusion centers has tended to expand over time to a broader orientation toward general criminality.[41]

A major concern about the fusion centers raised by civil liberties groups such as EPIC and the ACLU is the way in which they appear to fall through the cracks of the country's legal infrastructure for privacy protection. Although the DoJ's guidelines on fusion centers include a section on privacy and civil liberties and fusion centers are recommended to follow the principles of Fair Information Practices, these are voluntary guidelines, not legal mandates. EPIC has called for formal oversight of fusion centers.[42]

The *Denver Post* reported in the summer of 2008 that fusion centers across the country were beginning to deploy terrorist liaison officers (TLOs) to generate reports of suspicious activity within their communities. In Colorado, as of July 2008, 181 police, firefighters, paramedics, and even utility workers had been trained and were deployed after FBI-led training.[43] *Progressive* reporter Matthew Rotchschild, who located a TLO position announced for East Bay, San Francisco, noted that in addition to locations around the waterfront, TLOs might be situated on the campuses of universities.[44] TLOs report to FBI representatives at their local fusion center.

InfraGard

An increasing number of private sector professionals are being recruited to serve as additional channels of domestic intelligence production in the FBI-sponsored InfraGard program. The ACLU has compared the program to Ashcroft's TIPS program:

> There is evidence that InfraGard may be closer to a corporate TIPS program, turning private-sector corporations—some of which may be in a position to observe the activities of millions of individual customers—into surrogate eyes and ears for the FBI.[45]

First formed in Cleveland in 1996, the FBI made and promoted a national template for the program in January 2001. By March, 518 companies, including Coca-Cola and Delta, had joined the program. By November of that year, InfraGard totaled 1,700 members. Total membership exceeded 23,000 members by January 2008.[46] An FBI web page describes the program:

> It's the twenty-first century: a globalized, systems-driven, networked age. Our job is to prevent attacks—both physical and electronic—against critical infrastructure: banks . . . hospitals . . . telecommunications systems . . . emergency services . . . water and food supplies . . . the Internet . . . transportation networks . . . postal services . . . and other major industries that have a profound impact on our lives. . . .
>
> The essence of the partnership is information and intelligence sharing. FBI Agents assigned to each chapter bring meaningful news and information to the table: threat alerts and warnings, vulnerabilities, investigative updates, overall threat assessments, case studies, and more. Our private sector partners—who own and operate some 85 percent of the nation's critical infrastructures—share expertise, strategies, and most importantly, leads and information that help us track down criminals and terrorists.[47]

InfraGard members can share information via a secure, exclusive network or in person during special meetings and seminars. Members of the InfraGard are trained to supply raw suspicious activity reports to their FBI contacts, who may then enter this information into a threat-reporting system such as Guardian as a formal SAR. InfraGard members are given legal immunity for information that they choose to supply and, in return, may be rewarded with insider information that even high-level government officials may not have access to.

> On November 1, 2001, the FBI had information about a potential threat to the bridges of California. The alert went out to the InfraGard membership. Enron was notified, and so, too, was Barry Davis, who worked for Morgan Stanley. He notified his brother Gray, the governor of California.
>
> "He said his brother talked to him before the FBI," recalls Steve Maviglio, who was Davis's press secretary at the time. "And the governor got a lot of grief for releasing the information. In his defense, he said, 'I was on the phone with my brother, who is an investment banker. And if he knows, why shouldn't the public know?'"[48]

Discussion

In his epic work, *Age of Surveillance*, Frank J. Donner reflects on the role of intelligence in the state:

> "Intelligence" is best understood as a sequential process, which embraces the selection of the subject (an organization or individual) for surveillance, the techniques, both overt and clandestine, used in monitoring the subject or target, the processing and retention of the information collected (files and dossiers), and its evaluation in the light of a strategic purpose (the intelligence mission). Intelligence also includes an activist or aggressive aspect, specifically designed to damage or harass the target. But whether formally classified as passive data collection or aggressive intelligence, the intelligence function is dominated by a punitive or proscriptive purpose. Even the selection of a target embodies a judgment of deviance from the dominant political culture.[49]

Donner's conclusion was based on extensive research into U.S. domestic intelligence history from the 1920s to the 1970s. Although his argument is controversial and perhaps dated, there have been instances in the past decade where domestic intelligence agents, including those in the FBI and DoD, have collected information on U.S. persons for political reasons.[50]

In the discussion that follows I will emphasize the significance of the changes being ushered in by the NSI, not just the rise in information sharing, but the emergence of new sites and logics of production, and explore risks to both civil liberties and national security. I conclude with a few recommendations.

Business as Usual?

In DoJ public relations material about the SAR initiative, a common statement is that the nation's police are not being asked to do anything new. The SAR simply standardizes existing police practices, thus facilitating the sharing of information. Producing a SAR in a local police precinct may only be a matter of checking a new box on an existing form. Certainly, they argue, it is not a central, federal database of suspicious, but not necessarily criminally charged, American citizens. Senior policy advisors for the Bureau of Justice Assistance (BJA) stress that the SAR initiative is focused on what officers are already doing, that the national SAR initiative

> focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime and establishing a process whereby information can be shared to detect and prevent criminal activity, including that associated with domestic and international terrorism.[51]

Paul Garrett, from the Office of the Chief Information Officer at the U.S. DoJ, has stressed that the NSI is simply a standardization of practices at the local level to facilitate sharing.

> What it is not!
>
> A big federal database for "domestic spying"
>
> –We are leveraging and standardizing the information collected by 18K LEAs every day.
>
> –Implementing Information Led Policing in a federated model.[52]

The Rise of Intelligence-Led Policing

While it is true that the current ISE-SAR guidelines let police agencies add SAR checkboxes to existing criminal documentation forms,[53] the logic of production has clearly changed dramatically. In particular, the law enforcement community is being trained with a new philosophy of "intelligence-led policing" (ILP). ILP is based on the core assumption that "a principal task of the police is to prevent and detect crime rather than simply to react to it."[54]

The Practical Guide to Intelligence Led Policing, published by the Center for Policing Terrorism for the New Jersey police, notes that a radical shift in practice is necessary:

> For operators it requires becoming both better data collectors and better consumers of intelligence related products. This means shifting from emphasizing post-event evidence collection to constantly gathering all relevant data and ensuring it is provided for entry into appropriate databases, as well as drawing from the intelligence analysts and relevant databases all the information that is needed to support ongoing operations.[55]

The proto institution that serves as the focal point of ISE-SAR production, the fusion center, is itself a dramatic reconceptualization of state bureaucracy:

> Contrary to intuition, the fusion process (developing intelligence from diverse resources) and the creation of fusion centers (the physical plant) is more involved than merely changing organizational functions of an existing law enforcement intelligence unit. It typically involves either the re-engineering of the entire conceptual framework of the intelligence function in an agency or the creation of an entirely new entity. It requires engaging a wide array of people and organizations to be contributors and consumers of the intelligence function; it involves changing attitudes and processes of personnel; it requires establishing new functional and information sharing processes among state, county, municipal, tribal and federal law enforcement partners; it involves the development of new agreements and functional relationships; the development of new policies and processes; and the inculcation of the Intelligence Led Policing Philosophy.[56]

An earlier document published by the Royal Canadian Mounted Police, but with several U.S. contributors, notes how dramatic a change this approach is from traditional policing techniques:

> Whatever form it takes, intelligence-led policing requires commitment. Police managers must be prepared to stand away from traditional police philosophies and methodologies; to believe that operations can and should be driven by intelligence; to act rather than to react. They must be prepared to have faith in the intelligence process and in the judgements and recommendations of their intelligence staff. It may be a difficult, even painful, step, but it is a necessary one.[57]

Not only does the NSI promote a new culture for the U.S. domestic police force, but also, as David Heyman has noted, an ongoing change in the post-Church FBI culture from "reaction" to "prevention." The FBI has returned to its former role in U.S. domestic intelligence and serves as the primary vetting institution for SARs.[58]

Dangers of Overproduction

That intelligence data can be too voluminous, creating a signal-to-noise problem, is well understood within intelligence circles. Several years into a similar, but more strictly controlled, system of suspicious activity reporting under the Banking Secrecy Act, many analysts began to call attention to damage caused by information overload.[59] Colin Woodcock, head of the fraud section for the UK's Serious Organized Crime Agency (SOCA), expresses the concern succinctly: "If the police or anybody really were expected to act on everything that is suspicious, we would be bogged down in the first five seconds of operation."[60]

An investigative report by Tony Kovaleski of the Denver television station KMGH found that federal air marshals in Las Vegas, Nevada, were regularly generating false surveillance detection reports (SDRs) simply to meet quotas set by the managers, with the impression that the quota "'directly reflects on (their) performance evaluations'" and on "'how much money they make.'" Air marshals interviewed in the course of investigation identified specific instances when innocent air travelers had their names entered into a report just to meet quotas.[61]

Over the course of 2005, more than 51,000 individual reports were entered into the Guardian system. By November of 2007, the database contained approximately 108,000 reports on "terrorism-related threats . . . suspicious activity or watch list encounters."[62] With over 120,000 users and continued expansion, the amount of data stored by the system was exploding.[63] Not only had the FBI been overwhelmed by the volume of data entered into the system; much of it was incomplete or inaccurate.

According to the DoJ inspecter general, 28 percent of field offices participating in the Guardian system in 2006 were not properly deleting "temporary files."[64] Temporary files are important in that, according to federal guidelines, they may be "collected" by government agencies without satisfying the precondition of "reasonableness." Agencies are allowed to store this data with the caveat that it will be deleted within some specified period, usually thirty to ninety days, if it has not yet been connected to a specific criminal or terrorist investigation.

SAR Guidance, "Extremism," and the Watch List

While some significant victories appear to have been won by the privacy community in changing language in the ISE-SAR standard to be more sensitive to potential civil rights violations, its role in determining local SAR reports is not nearly as significant as the regular bulletins and other reports by individual states and the federal government that put the domestic threat in continuing narrative form. *Extremism* is a key word in much of this guidance. It refers to ideologies that are heavily correlated with terrorism, enough to warrant increased attention from the intelligence community. Guidance produced by the Department of Homeland Security has identified opponents of genetically modified organisms[65] and gun rights activists[66] as extremists. Leaked documents at the state level have shown that support for independent political candidates like Ron Paul have been targeted and linked to extremist movements.[67]

It seems likely that those Americans who hold certain beliefs identified as part of an "extremist" ideology will receive greater attention, will have a greater number of SARs referring to them, and, for this reason, will be more likely to appear on U.S. government watch lists. Watch lists, reasonable in moderation (the "10 most wanted"), are distinctly undemocratic in character as they grow in use. Since one's presence on a list does not necessarily indicate conviction or indictment for a crime, it is not subject to judicial review. The more that the names comprising a given watch list are determined by the flow of suspicious activity reports, the less government actions will be constrained by law. Presence on a watch list can mean the individual will be mildly inconvenienced, deprived of their First Amendment rights to assemble and associate, denied credit or a job, or even be subject to physical abuse and harm, all without clear rights to challenge.

SARs and Personally Identifying Information

Given that SARs are, by design, behavior focused, it is important to point out that not all, and very possibly the majority of SARs produced today likely do not, contain personally identifying information. Although it is difficult to make specific estimates from publicly available information, we do know that the ISE-SAR data standard contains multiple fields for PII and that related record systems have been shown to have PII in roughly one out of three documents. In the DoD's now shuttered TALON reporting system, of 1,131 reports reviewed by the inspector general, 334, or 30 percent, contained U.S. person information.[68] It is certainly possible that this is not a representative subset and the overall rate is much lower, but it is also clear that this rate will fluctuate over time and will depend in part on specific technological and policy conditions. For example, one could imagine that in U.S. border areas where many people carry the enhanced driver's license (EDL), the percentage of SARs with PII could be much higher. Federal air marshals carry hand devices to generate SARs in the field,[69] and the read range of the EDL is up to forty feet. The carrier's identity could be captured automatically and entered into the appropriate SAR fields.

Recommendations

As this country's information systems evolve to adjust to a changing threat matrix, it is imperative that we protect the basic rights and freedoms that have defined our nation for more than 230 years. We must keep in mind that the post-Church policy period was a response to a period of domestic intelligence abuse of which most Americans remain unfamiliar. Unless the public at large pays more attention to the suspicious activity reporting phenomenon, there remains the possibility that the gross abuses of an earlier era will return.

Given the Guardian system's central role in SAR management and circulation, it is critical that storage standards designed to minimize the potential for the accretion of noncriminal, politically motivated dossiers are followed. As many have noted, intelligence records have a tendency to persist far longer than the files of standard criminal investigations.

Without clear, specific, and forceful limitations on the production of SARs, there is every reason to believe that the number of SARs will increase dramatically over the coming years, retracing the kind of growth curves that have been seen with banking SARs. SAR standards, even if version 2.0 contains another set of privacy enhancements, will not be sufficient to prevent political abuse. There needs to be more transparency in how SAR guidance is formulated and diffused through the national domestic intelligence system.

Notes

1. William Matthews, "Ashcroft: No Central Database for Citizen Tips," *Federal Computer Week*, 29 July 2002, http://www.fcw.com/print/8_30/news/77288-1.html?page=1 (accessed 2 April 2008).

2. William Safire, "You Are a Suspect," *New York Times*, 14 November 2002, http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html?pagewanted=1 (accessed 1 May 2010).

3. Lisa Bowman, "Is Your Cable Guy a Spy?" CNET, 17 July 2002, http://news.cnet.com/2100-1023-944555.html (accessed 12 December 2009).

4. It is important to distinguish here between the financial SAR that is defined under the Banking Secrecy Act, which populates the Department of the Treasury's (DoT) Financial Crimes Enforcement Network (FinCEN), from the broader ISE-SAR initiative. While one could reasonably include the FinCEN SAR as a class of ISE-SARs, the FinCEN SAR is distinct in that it is subject to federal regulation. While the ISE-SAR initiative can trace its origins back to the ISE defined in the Intelligence Reform and Terrorism Prevention Act (IRTPA) 2004, it is never specifically identified in the law. Although a federal standard exists for their production, legal constraints are local rather than federal. In the author's personal experience, much of the privacy and surveillance studies community is only aware of SARs in the narrower financial sense. And as of late April 2010, the Wikipedia entry on SARs defines them only in this narrow financial context.

5. Government documents included statutory and case law, federal standards, executive orders, congressional testimony, systems of records notices (SORNs) in the Federal Register, Privacy Impact Assessments (PIAs) produced under the E-Government Act of 2002, IG reports from agencies including the Department of Justice (DoJ) and Department of Defense (DoD), DoJ PowerPoint presentations, and leaked internal circulation publications of terror guidance published by a number of state fusion centers. Among the most critical government documents for this research include many reports and bulletins published by the newly established office of the Program Manager for the Information Sharing Environment (PM-ISE).

6. Sherri J. Conrad, "Note: Executive Order 12,333: 'Unleashing' the CIA Violates the Leash Law," *Cornell Law Review* 70 (June 1965): 968.

7. Office of the Director of National Intelligence, Civil Liberties and Privacy Office, "Revision of Executive Order 12333: Privacy and Civil Liberties Information Paper," 4, http://fas.org/irp/dni/12333civillib.pdf (accessed 30 April 2010).

8. See section 2.3.

9. As defined in the order, "intelligence" consists of "foreign intelligence" and "counter intelligence." Foreign intelligence means "infor-

mation relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists," while "counter intelligence" means "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities." Intelligence activities are "all activities that agencies within the Intelligence Community are authorized to conduct" pursuant to the order. What ultimately comprises the intelligence community is left to the discretion of the president and the director of national intelligence.

10. While the order dictates specific limitations on "collection," it never explicitly defines its meaning. In its implementation of the order, the DoD offers an explicit definition of the term:

> Collection. Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form. (DoD Directive 5240.1-R Procedure 2, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982, http://atsdio.defense.gov/documents/5242.html [accessed 15 April 2010].)

11. Anne Salmond, "Theoretical Landscapes: A Cross-cultural Conception of Knowledge," 75, in *Semantic Anthropology*, ed. D. J. Parkin (London and New York: Academic Press, 1982), 65–82.

12. Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004), 108.

13. David Lyon, "New Directions in Theory," in *Surveillance Society: Monitoring Everyday Life* (Buckingham, England, and Philadelphia: Open University, 2001), 2.

14. Gary T. Marx, "Surveillance and Society," *Encyclopedia of Social Theory*, 2005, http://web.mit.edu/gtmarx/www/surandsoc.html (accessed 12 August 2009).

15. Ludwik Fleck, *Genesis and Development of a Scientific Fact* (Chicago: University of Chicago Press, 1979), 42.

16. Bruno Latour and Steve Woolgar, *Laboratory Life: The Construction of Scientific Facts* (Princeton, NJ: Princeton University Press, 1986).

17. Jan Golinski, *Making Natural Knowledge: Constructivism and the History of Science* (Chicago: University of Chicago Press, 2005), 32.

18. See Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, 1st ed. (Garden City, NY: Doubleday, 1966).

19. Marilyn Peterson, "Intelligence-Led Policing: The New Intelligence Architecture," September 2005, report NCJ 21068, Bureau of Justice Assistance, http://www.ncjrs.gov/pdffiles1/bja/210681.pdf (accessed 22 January 2010).

20. Gregory F. Treverton, "Reorganizing U.S. Domestic Intelligence: Assessing the Options," report, RAND Corporation, Homeland Security Program and Intelligence Policy Center, 2008, 15, http://www.rand.org/pubs/monographs/MG767/ (accessed 22 March 2010).

21. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities. United States Senate, 94th Congress, 2nd Session, April 26 (legislative day, 14 April 1976 [aka "Church Committee Report"]. Archived on COINTELPRO sources website, http://www.icdc.com/~paulwolf/cointelpro/cointel.htm (accessed 7 March 2009).

22. Final Report of the Select Committee, Book II, section 1, intro and summary.

23. Ibid., section I.C.3, 9.

24. See the Levi Guidelines, discussed in chapter 2 of September 2005 DoJ Inspector General Special Report, the Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines (Redacted), http://www.justice.gov/oig/special/0509/chapter2.htm (accessed 8 February 2010).

25. This was a "mantra" of the 9/11 Commission Report, a phrase that underlined its most forceful recommendation, that the barriers to information sharing imposed on state agencies and departments in the mid 1970s be dissolved within a new information sharing environment (ISE). After all, it was a failure to "connect the dots" that had blinded the U.S. government to the attacks.

26. See, for example, Dr. Donald Kerr, "Remarks and Q&A by the Principal Deputy Director of National Intelligence," 2007 GEOINT Symposium, Henry B. Gonzalez Convention Center, San Antonio, Texas, 23 October 2007, available at http://www.wired.com/images_blogs/threat-level/files/20071023_speech.pdf (accessed 30 April 2010).

27. PL 108-458.

28. Thomas E. McNamara, "Information Sharing Environment Implementation Plan," xiii, report, U.S. Information Sharing Environment, http://www.ise.gov/docs/ISE-impplan-200611.pdf (accessed 1 April 2010).

29. PM-ISE, Information Sharing Environment Functional Standard Suspicious Activity Reporting, Version 1.5, 21 May 2009, 4, http://www.ncirc.gov/sar/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued.pdf (accessed 12 January 2010).

30. Ibid., 7.

31. Among the behaviors in this second category that can trigger the production of a SAR are Eliciting Information: questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person; Photography: taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person; Observation/Surveillance: demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious; Acquisition of Expertise: attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.

32. A third system of records, the Tactical Information Sharing System (TISS), is maintained by the Federal Air Marshals Service (FAMS) under the TSA. Reports in this system are called surveillance detection reports (SDRs), but they are simply another form of SAR.

33. U.S. Department of Justice (DoJ), Office of the Inspector General, "The Federal Bureau of Investigation's Terrorist Threat and Suspicious Incident Tracking System," November 2008, No. 09-02, http://www.usdoj.gov/oig/reports/FBI/a0902/final.pdf (accessed 2 February 2009).

34. "Connecting the Dots Using New FBI Technology," FBI web page, 2008, http://www.fbi.gov/page2/sept08/eguardian_091908.html (accessed 7 January 2010).

35. Jason Miller, "DOJ Tests Suspicious Activity Reporting System," *Federal Computer Week*, 10 December 2007, http://fcw.com/articles/2007/12/10/doj-tests-suspiciousactivity-reporting-system.aspx (accessed 14 October 2009).

36. J. H. Burch II. "From the Acting Director: The Bureau of Justice Assistance: The DOJ's Global Initiative and Partnerships as the Keys to Success," *Police Chief Magazine*, 12 December 2009, http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1962&issue_id=122009 (accessed 8 February 2010).

37. "A Closer Look at the FBI's Joint Terrorism Task Forces," FBI web page, 4 December 2004, http://www.fbi.gov/page2/dec04/jttf120114.htm (accessed 20 July 2009).

38. "Meet the National Joint Terrorism Task Force," FBI web page, 4 July 2004, http://www.fbi.gov/page2/july04/njttf070204.htm (accessed 21 March 2009).

39. U.S. Department of Justice (DoJ), "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," no date, http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf (accessed 22 February 2009).

40. U.S. Department of Homeland Security (DHS). Homeland Security Advisory Council, Summary of Meeting: December 14, 2004, 4 (published 7 March 2005).

41. Los Angeles Police chief William Bratton, in a 19 March 2008, speech to the National Fusion Center Conference in San Francisco, explained the reasoning for this ongoing transformation:

> Now, let's address the ongoing debate over whether fusion centers should be strictly designed to counter terrorism or whether they should address "all crimes, all hazards."
>
> To advocate the position that fusion centers should be strictly designed around terrorism demonstrates a complete lack of understanding of the public safety risk, threat matrices, and the need to engage the majority of local law enforcement. It also demonstrates a complete lack of understanding about how terrorists are recruited, how terrorists plan and execute their operations and the criminal markets that support terrorist organizations.
>
> The idea of terrorism has come a long way since the days of the Red Brigades. Al Qaeda, FARC and other groups have been successful at exploiting the vulnerabilities of their enemies. In our case, they attacked the arrogance and turf battles that were at the heart of our failure to communicate. As we heard Secretary Chertoff say in this forum last year: "We have to build a network to beat a network." That is precisely what we will do.
>
> My position on the role and operation of fusion centers has been adopted by all the chiefs from America's large cities—intelligence must be gathered on all crimes and fully integrated into the daily operations of the police department. In our view, intelligence should inform and shape the wide range of police services that protect the public. For example, it is critical that we receive timely threat intelligence from the federal government so that we can determine what measures may be taken by police and emergency service agencies.

42. "'National Network' of Fusion Centers Raises Specter of COINTEL PRO." Spotlight on Surveillance, Electronic Privacy Information Center, 2007, http://epic.org/privacy/surveillance/spotlight/0607/ (accessed 12 August 2009).

43. B. Finley, "Terror Watch Uses Local Eyes 181," *Denver Post*, 29 June 2008, http://www.denverpost.com/news/ci_9725077 (accessed 3 March 2009).

44. Matthew Rothschild, "The New Snoops: Terrorism Liaison Officers, Some from Private Sector," *Progressive*, 2 July 2008.

45. Jay Stanley, "The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society," American Civil Liberties Union (ACLU), August 2004.

46. Matthew Rothschild, "The FBI Deputizes Business," *Progressive*, March 2008.

47. "InfraGard: FBI and Private Sector Join to Safeguard Critical Infrastructures," FBI web page, 4 December 2004, http://www.fbi.gov/page2/dec04/infragard121404.htm (accessed 30 June 2009).

48. Rothschild, "The New Snoops."

49. Frank J. Donner, *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System*, 1st ed. (New York: Knopf, 1983), 3.

50. See, for example, Lisa Myers, D. Pasternak, and R. Gardella, "Is the Pentagon Spying on Americans?," MSNBC.com, 14 December 2005, http://www.msnbc.msn.com/id/10454316/ (accessed 18 June 2009), on leaked data from the DoD's Threat and Local Observation Notice (TALON) reporting system; or Matthew Rothschild, "Maryland State Police Infiltrated Groups Opposed to War and the Death Penalty," *Progressive*, 17 July 2008, http://www.progressive.org/mag/mc071708.html (accessed 1 March 2010) on the Maryland State Police scandal.

51. Thomas O'Reilly, David Lewis, and Don Sutherland, "Nationwide Suspicious Activity Reporting (SAR) Initiative," IJIS Institute Winter Briefing, 7–8 January 2009, Herndon, VA, PowerPoint presentation, http://www.kms.ijis.org/db/share/public/Library/Presentations/2009%5fWinter%5fIndustry%5fBriefing/10%5f30%20IJIS%20Industry%20Day%20010708%2dBJA%2dSAR%20Final.ppt (accessed 8 February 2010).

52. Paul Garrett, "IACP-LEIM Briefing," Office of the Chief Information Officer, DoJ, May 2008, PowerPoint presentation, http://www.iacptechnology.org/LEIM/2008Presentations/National%20Strategy%20for%20Information%20Sharing_Garrett.pdf (accessed 10 January 2010).

53. This is suggested in the "Findings and Recommendations" of the SAR Support and Implementation Project, Final Draft, June 2008, 1–2. The SAR Support and Implementation Project was a joint effort of the Department of Justice (DoJ) Bureau of Justice Assistance, the Major Cities Chiefs Association, DoJ's Global Justice Information Sharing Initiative (Global), the Criminal Intelligence Coordinating Council, and DHS to develop recommendations to be used by law enforcement agencies to improve identification and reporting of suspicious activity and the sharing of that information with fusion centers and Joint Terrorism Task Forces.

54. Angus Smith, "Intelligence Led Policing: International Perspectives on Policing in the 21st Century," September 1997, International Association of Law Enforcement Intelligence Analysts, Inc., http://www.ialeia.org/files/other/Intelligence%20Led%20Policing.pdf (accessed 5 April 2010).

55. Joseph R. Fuentes, "Practical Guide to Intelligence Led Policing," September 2006, 3, http://www.cpt-mi.org/pdf/NJPoliceGuide.pdf (accessed 28 January 2010).

56. David L. Carter, "The Intelligence Fusion Process," 1, Intelligence Policy Paper Series, School of Criminal Justice, Michigan State University, https://intellprogram.msu.edu/resources/CARTER_Intelligence_Fusion_Centers.pdf (accessed 7 February 2010).

57. Smith, "Intelligence Led Policing," 3.

58. David Heyman, "Finding the Enemy Within: Towards a Framework for Domestic Intelligence," 159, in *Threats at Our Threshold: Homeland Defense and Homeland Security in the New Century*, ed. Bert B. Tussing (Washington, DC: Center for Strategic and International Studies, 2000), 149–74, http://csis.org/images/stories/HomelandSecurity/071022_Chap4-FindingTheEnemyWithin.pdf (accessed 23 July 2009).

59. Jeremy Kirk, "Fraud Police Buckling under Mountains of Data," *Washington Post*, 26 September 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/26/AR2007092600697.html (accessed 17 January 2010).

60. Ibid., n.p.

61. "Marshals: Innocent People Placed on 'Watch List' to Meet Quota," KMGH Denver, 21 July 2006, http://www.thedenverchannel.com/news/9559707/detail.html (accessed 26 February 2009).

62. U.S. DoJ, November 2008 (see note 23), ii.

63. Miller, "DOJ Tests Suspicious Activity Reporting System."

64. U.S. DoJ, November 2008 (see note 23).

65. U.S. Department of Homeland Security (DHS), Office of Intelligence and Analysis Assessment (OIAA), "Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade (U//FOUO)," 26 January 2009, IA-0141-09, http://www.fas.org/irp/eprint/leftwing.pdf (accessed 3 January 2010).

66. DHS, OIAA, "Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment (U//FOUO)," 7 April 2009, IA-0257-09, http://www.fas.org/irp/eprint/rightwing.pdf (accessed 3 January 2010).

67. Roseann Moring, "Missouri Highway Patrol Rescinds Controversial Militia Report," *St. Louis Post-Dispatch*, 26 March 2009, http://www.stltoday.com/stltoday/news/stories.nsf/missouristatenews/story/A8718605909247EB862575850003B8B4?OpenDocument (accessed 29 March 2009).

68. U.S. Department of Defense (DoD), Office of the Inspector General, "The Threat and Local Observation Notice (TALON) Program," 27 June 2007, No. 07-INTEL-09, http://www.dodig.mil/fo/Foia/TALON%20Rpt%2007-INTEL-09.pdf (accessed 30 April 2010).

69. Thomas D. Quinn, "Tactical Information Sharing System," *Police Chief Magazine*, March 2009, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=810&issue_id=22006 (accessed 30 April 2010).

Dr. Farrall is grateful to the Air Force Office of Scientific Research, ONR BAA 07-036 (MURI), for a grant that has supported this work.