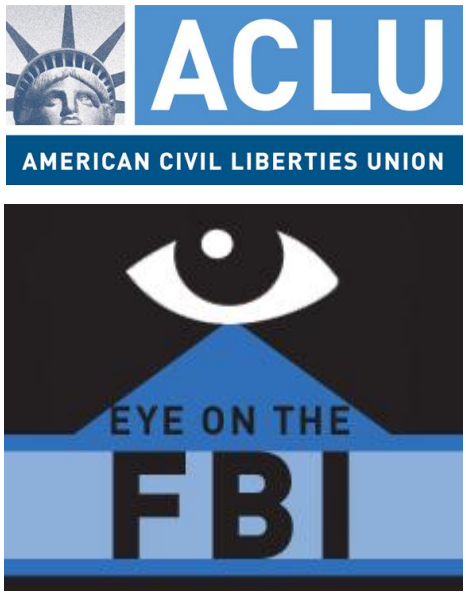

ACLU EYE on the FBI:

Documents Reveal Lack of Privacy Safeguards and Guidance in Government's "Suspicious Activity Report" Systems

---

Government documents obtained by the ACLU show that nationwide programs that collect so-called "Suspicious Activity Reports" provide inadequate privacy safeguards and guidance on the definition of "suspicious activity," leading to violations of Americans' First Amendment and privacy rights, and to racial and religious profiling.

FOIA Lawsuit

In August 2011, the ACLU filed *ACLU v. FBI*, a lawsuit to enforce a Freedom of Information Act (FOIA) request for records about the FBI eGuardian program, a nationwide system of collecting and sharing so-called "suspicious activity reports" ("SARs") from the public and law enforcement and intelligence officials across the country. The Department of Justice (DOJ) and National Security Agency (NSA) initially failed to release any records, and DOJ insisted it had no independent obligation to even search for information because eGuardian is run by the FBI. Although the FBI partially released a handful of records, they represented only a fraction of the FBI's records about this nationwide program.

Through litigation, however, the ACLU secured additional agency searches for eGuardian records. As a result, DOJ identified 13,500 pages of records requiring review. Ultimately, between January 2012 and July 2013, the FBI, DOJ, NSA, and Office of the Director of National Intelligence released in full or in part over 1,900 pages of records to the ACLU, and in August 2013 identified hundreds of additional eGuardian records these agencies sought to keep secret under exemptions to the FOIA.

Documents Reveal Inadequate Privacy Safeguards and Lack of Guidance Over Use of Suspicious Activity Reporting Systems

Although many of the released records are heavily or even entirely redacted, the documents shed important light on eGuardian, a competing suspicious activity reporting program known as the Information Sharing Environment Suspicious Activity Reporting ("ISE-SAR") Shared Spaces, and the Department of Justice's umbrella Nationwide Suspicious Activity Reporting Initiative ("NSI"), of which both systems are a part.

The documents confirm that these programs give extremely broad discretion to law enforcement officials to monitor and collect information about innocent people engaged in commonplace activities, and to store data in criminal intelligence files without evidence of wrongdoing (p. 1). They also demonstrate that several fusion centers and state and local law enforcement agencies have resisted using eGuardian because of concern over whether the system has an approved privacy policy, whether it is adequate in light of state and local laws protecting privacy, the general lack of guidance on the system, and the lengthy retention of data in eGuardian.

For example, in 2009, the New York State Intelligence Center indicated it "would not forward SARs to eGuardian" without confirmation that the system had a DOJ-approved privacy policy. In 2010, an official of the State of Iowa Intelligence Fusion Center (p. 1) complained about the "huge disconnect on how eGuardian is to work" and reported that the "local FBI field office" lacked "guidance on how or when to use eGuardian." In 2011, a number of state and local law enforcement agencies stated they would share Suspicious Activity Reports with the FBI only after controlling "what gets shared consistent with local/state laws, privacy issue [sic] and local expectations of community standards." Similarly, a 2012 email chain shows that the Minnesota Joint Analysis Center (p. 2) reported it would not send Suspicious Activity Reports to eGuardian at all, and that the New Jersey Fusion Center (p. 1) was sharing reports with the FBI only after first vetting reports itself. And a 2011 document (p. 1) demonstrates that "Fusion Center concerns" about using eGuardian prompted the FBI to change the system's data retention policy "from 30 years to 5 years (followed by a 5-year archive period)." Yet, a 2013 Government Accountability Office report recently confirmed that there is continuing cause for concern because even after Suspicious Activity Reports are deleted from eGuardian, the FBI retains the reports for at least an additional 30 years in another location.

The documents obtained by the ACLU further confirm that the Nationwide Suspicious Activity Reporting Initiative, eGuardian, and the Information Sharing Environment Suspicious Activity Reporting Shared Spaces use vague and expansive definitions for "suspicious activity" that have caused persistent confusion among federal, state, and local law enforcement. This confusion underscores the ACLU's concern — shared by some police departments — that Suspicious Activity Reports will be based on racial or religious profiling or the exercise of First Amendment rights, rather than evidence of wrongdoing.

For example, in 2009, the Boston Police Department (p. 81) "recommended that the appropriate threshold be clearly defined for entering a SAR into the ISE-SAR Shared Spaces," cautioned against "the entry of information . . . that is not of value," and emphasized the need to "avoid large volumes of information being 'dumped' into the system." The Miami-Dade Police Department (p. 115) warned that "[t]he NSI needs to stay focused on behaviors and not individuals," suggesting that problems with guidance on what constitutes "suspicious activity" would result in inappropriate profiling. Such confusion over the definition of "suspicious activity" is hardly surprising in light of the government's failure to make clear that 28 C.F.R. Part 23 — a regulation long applied to criminal intelligence information to safeguard privacy, civil rights, and civil liberties — applies to nationwide suspicious activity reporting programs, requiring "reasonable suspicion" of criminal activity to justify the collection, retention, and dissemination of Suspicious Activity Reports about innocent people.

The documents obtained by the ACLU thus heighten concerns previously expressed by the ACLU and others that eGuardian, the Information Sharing Environment, and the broader Nationwide Suspicious Activity Reporting Initiative have opened the door to violations of civil rights and civil liberties across the country. The ACLU of California recently obtained summaries of SARs (pp.3–4) produced by California fusion centers that vindicate these concerns, showing that Suspicious Activity Reports contained no reasonable evidence of criminal activity but were primarily justified based on bias against racial and religious minorities and the exercise of First Amendment rights. Based on the reports obtained thus far, photography and videography are frequently reported without additional facts, rendering these constitutionally-protected activities inherently suspicious.

Additional information from specific documents follows the recommendations below.

Recommendations

The increasingly widespread use of nationwide suspicious activity reporting programs, as revealed by the documents, underscores the serious need for reform. In 2010, the Department of Defense announced that it would participate in the Nationwide Suspicious Activity Reporting Initiative through eGuardian. "As of February 2010, there were more than 560 Federal, state, local, and tribal member agencies with more than 1,800 individual eGuardian users who had reported and shared almost 3,000 incidents." (p. 3) Just six months later, the number of Suspicious Activity Reports in eGuardian had jumped to 5,176 (p.1). And press reports indicate that by December 2010, some 890 state and local agencies had submitted 7,197 reports for inclusion in eGuardian.

The ACLU urges each of the federal agencies involved — the Department of Justice, Federal Bureau of Investigation, Department of Homeland Security, Office of the Director of National Intelligence, National Security Agency, and the Department of Defense — to make public the policy and guideline documents governing nationwide suspicious activity reporting programs, including the Nationwide Suspicious Activity Reporting Initiative, eGuardian, and the Information Sharing Environment Suspicious Activity Reporting Shared Spaces, and to reform these programs to:

1. Require reasonable suspicion of specified criminal activity in order to collect, retain or disseminate SARs containing personally identifiable information, as required by federal regulation 28 C.F.R. Part 23;

2. Clearly and unequivocally prohibit the collection, retention, or dissemination of information about the First Amendment-protected political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless that information directly relates to criminal activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal activity;

3. Remove photography and other activities clearly protected by the First Amendment from inclusion in lists of categories of suspicious activity or other guidance criteria to prevent the unlawful stops, detention, and harassment of photographers; videographers, and journalists;

4. Give agencies contributing Suspicious Activity Reports continuing control over the information in the federal suspicious activity reporting systems to modify, correct, update, and purge data according to state and local laws, regulations, and policies; and

5. Require routine review and re-examination of stored Suspicious Activity Reports to purge any information that is misleading, obsolete, or otherwise unreliable; and require that all Suspicious Activity Reports be purged from all data systems within five years and that all recipient agencies by advised of such changes which involve errors or corrections. No data not leading to an investigation should remain in a suspicious activity reporting system or any other federal database for more than five years.

The Documents

The documents confirm that law enforcement agencies have resisted using eGuardian due to (a) persistent confusion over whether it had a privacy policy, and then, when one was put in place (two years after the program was implemented), (b) persistent confusion over whether that policy adequately protects privacy rights, and (c) a lack of guidance on how to use the system.

- Both eGuardian and the ISE Shared Spaces were first implemented in 2008 (p.8). Yet, a May 18, 2009 email "request[ed] an update on the status of the eGuardian privacy policy," suggesting that the system still lacked one at the time. Although the Nationwide Suspicious Activity Reporting Initiative had promulgated privacy guidelines for entities using Information Sharing Environment Suspicious Activity Reporting Shared Spaces, agencies that participated in the 2009 pilot Nationwide Suspicious Activity Reporting Initiative (p.11–12) expressed concern about the lack of adequate safeguards for privacy rights. The Arizona Counter Terrorism Information Center (p. 76) recommended the creation of "a national legal office . . . to protect the data being collected and to address concerns raised by the American Civil Liberties Union and other privacy advocates." And the New York State Police (p. 121) recommended: "There is a need for a privacy-checklist for analysts to utilize during the initial vetting of the SAR."

- A September 3, 2009 email from an IJIS Institute employee to David Lewis of DOJ reported that two fusion centers had asked "where the FBI stands on their privacy policy" in the context of discussing "forwarding SARs from their Shared Space to eGuardian." An employee of the Institute for Intergovernmental Research responded, "Neither the FBI nor DOJ has promulgated an ISE-SAR specific or other policy that meets the ISE Privacy Guidelines requirements, although the Bureau has promulgated a [Privacy Impact Assessment] for the eGuardian system." The IJIS Institute employee wrote back: "This could be problematic if NY or FL don't like this answer and decide to opt out" of using eGuardian to share SARs. The SAR Manager at the IJIS Institute further surmised, "I suspect that [the New York State Intelligence Center] may not want to get engaged."

- In a September 30, 2009 email, an IJIS employee wrote to DOJ officials that when he was at the New York State Intelligence Center ("NYSIC"), someone "reminded me that his question on

whether eGuardian had an approved privacy policy had not been answered." (The name of the individual who made this reminder is redacted.) The IJIS employee noted: "I believe he indicated that NYSIC would not forward SARs to eGuardian until he knew the answer. The implication was also made that he may not want to provide FBI (or any agency without an approved policy) access to his Shared Space," which would contain the fusion center's Suspicious Activity Reports.

- More than four months later, in a February 5, 2010 email (p. 2), FBI Section Chief J. Roger Morrison wrote that the Deputy Attorney General had approved the DOJ Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment, which "applies immediately to component NSI participants," including eGuardian. He asserted that, "any real or perceived concerns about eGuardian's privacy status can be relaxed."

- In a February 17, 2010 email (p. 1), a special agent in charge of the State of Iowa Intelligence Fusion Center identified "[t]he use of eGuardian as it relates to the SAR initiative" to be one of the "three biggest challenges or opportunities faced by fusion centers in 2010." The agent reported that the fusion center "ha[d] been using eGuardian on a limited basis" and "ha[d] made outreach to our local FBI field office when dealing with eGuardian," but that "[t]he continuous response is that they (FBI) have not been given guidance on how or when to use eGuardian." The agent continued: "There seems to be a huge disconnect on how eGuardian is to work. What role does the FBI play? Who is responsible for running leads out of eGuardian? The question I have is: Has FBI HQ given clear guidance to the field (if so has the field given clear guidance downward) on how to use eGuardian and included in that guidance is the FBI to engage the state fusion center in which the eGuardian entry is made prior to working the lead?" (Emphasis in original.)

- A September 22, 2010 email (p. 1) from Thomas O'Reilly, a DOJ Office of Justice Programs official who served as the director of the Nationwide Suspicious Activity Reporting Initiative, to FBI, DHS and DOJ officials noted that state and local fusion centers had expressed "concerns" regarding eGuardian's relationship to the Nationwide Suspicious Activity Reporting Initiative.

- A September 29, 2010 email (p. 2) from Nancy Libin, the DOJ chief privacy and civil liberties officer, expressed confusion as to why a chart comparing eGuardian and the Information Sharing Environment Suspicious Activity Reporting Shared Spaces "suggests that agencies using eGuardian are not required to have privacy policies. That is absolutely not the case and is not consistent with the DOJ ISE Privacy Policy." In a later email that same day (p.2), Libin wrote: "[T]he DOJ ISE Privacy Policy that went into effect at the beginning of the year (and applies to eGuardian) expressly states that all users must have in place a privacy policy that is at least as comprehensive as the DOJ ISE Privacy Policy." The government has redacted the FBI's "eGuardian Policy Clarification" which responded to Nancy Libin's questions concerning the chart.

- An August 15, 2011 email from Thomas O'Reilly to DOJ officials reported: "There have been at least 4 different meeting [sic] where the S?L [sic] have told the FBI that they will share with the

JTTF but that they also have a responsibility to protect their towns and will share with other cities and states and will control the [sic] what gets shared consistent with local/state laws, privacy issue [sic] and local expectations of community standards." He noted that in one St. Louis meeting involving the FBI and all 12 participants in the pilot Nationwide Suspicious Activity Reporting Initiative (known as the Information Sharing Environment Suspicious Activity Reporting Evaluation Environment), "The total state and local group got up and walked out when Roger Morrison FBI) [sic] told them they had to send everything to the FBI without exercising any review etc."

- A November 3, 2011 email (p.1) from Thomas O'Reilly to various DOJ and DHS officials announced that the FBI had changed its policies as set forth in a Deputy Attorney General letter "outlining new retention schedules for records in the Guardian system" in order to "address Fusion Center concerns about pushing their vetted SAR records to the eGuardian system." A January 17, 2012 email (p. 2) from Nancy Libin referenced these changes when it indicated that "[t]he Guardian retention policy has been changed from 30 years to 5 years (followed by a 5-year archive period)." However, a 2013 Government Accountability Office report (p. 53) confirmed that even after Suspicious Activity Reports are deleted from eGuardian, the FBI retains the reports for at least an additional 30 years in another location.

- A January 5, 2012 email (p. 2) from the Director of the Minnesota Joint Analysis Center (MNJAC) reported that although the fusion center would "continue to share SAR reporting tied to terrorism directly with [its] Minneapolis FBI office and the JTTF and [would] input qualifying SARs to the NSI Shared Space," it would "not be participating in the eGuardian push" because its governing "board recognized the sensitivity in our state to direct input in federal data systems of Minnesota law enforcement data. . . ." In a January 7, 2012 email (p. 1) commenting on that report, Thomas O'Reilly of DOJ indicated, "There is also a mess in NJ right now. The Fusion Center continues to share under first refusal and the JTTF is entering them into Guardian."

The documents confirm that entities are using Nationwide Suspicious Activity Reporting Initiative systems, including eGuardian and the Information Sharing Environment Suspicious Activity Reporting Shared Spaces, without complying with 28 C.F.R. Part 23, which applies to state and local criminal intelligence systems and protects the privacy and civil rights of innocent Americans.

- 28 C.F.R. Part 23 has long prohibited the collection, storage, and dissemination of information about Americans not reasonably suspected of criminal activity in criminal intelligence systems supported by certain federal funds. (*See* 28 C.F.R. §§ 23.3, 23.20.) It has become the "de facto national standard for sharing criminal intelligence information" through widespread voluntary adoption by other agencies. The regulation's "reasonable suspicion" requirement has proven to be an effective standard that allows police to collect and share information where necessary to address threats to public safety, while still requiring a reasonable connection to defined criminal activity to justify collection of personally identifiable information about any individual.

- A consultant to the International Association of Chiefs of Police (IACP) and National Data Exchange Program sent a September 7, 2010 email (p. 2) to DOJ that inquired "if there is a

'definition' of a SAR" and further asked: "Has anyone agreed that it should be considered Intel Subject to 28CFR [sic] part 23 or is it a collection of incidents." In response, David Lewis of the Program Manager Office of the Information Sharing Environment responded (p. 1) : "The Nationwide SAR Initiative is not a 28 CFR Part 23 program since the incidents do not rise to the level of reasonable suspicion, but are incidents *indicative* of criminal activity with the potential nexus to terrorism." (Emphasis in original). A 2011 final report on the pilot Nationwide Suspicious Activity Reporting Initiative (p. 57) further confirmed government officials' refusal to apply 28 C.F.R. Part 23 to nationwide suspicious activity reporting programs: "The ISE-SAR Shared Spaces database is not a criminal intelligence system or database."

- However, as the consultant to the International Association of Chiefs of Police correctly suggested, 28 C.F.R. Part 23 must apply to suspicious activity reporting systems because they contain criminal intelligence information: derogatory information collected by law enforcement and intelligence officials about individuals' "suspicious" activities, which may open them up to further scrutiny and investigation. The very purpose of the regulation is to protect "the privacy and constitutional rights of individuals." 28 C.F.R. § 23.1. In commenting on the 1993 revision of 28 C.F.R. Part 23, the Department of Justice Office of Justice Programs itself recognized that this protection is required "[b]ecause criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete . . . ."

The documents confirm enduring confusion over the definition of "suspicious activity" that may be shared through nationwide suspicious activity reporting programs. This confusion results from a failure to make clear that Suspicious Activity Reports must meet the "reasonable suspicion" requirement of 28 C.F.R. Part 23, and has led to documented abuse.

- Since 2008, participants have been confused about what constitutes "suspicious activity." In September 2008, discussions between fusion centers involved in the pilot Nationwide Suspicious Activity Reporting Initiative (p. 14, 22–23) identified as a key challenge the "[i]nability to vet reports and identify the SAR reports that have a nexus to terrorism and hence need to be forwarded to the ISE-SAR Shared Spaces."

- In January 2008, the program manager of the Information Sharing Environment promulgated the first Information Sharing Environment Suspicious Activity Reporting Functional Standard (p. 8). Its purpose was "to address the privacy and civil liberties issues associated with the NSI, . . . to reduce inappropriate police data gathering and support the training of law enforcement personnel so that they can better distinguish between behavior that is legal or constitutionally protected and that which is potentially associated with criminal activity " (p.10). Accordingly, the Functional Standard (p. 10) "establishes the threshold criteria for what suspicious activity will be considered as having a nexus to terrorism" and "a two-step process to determine whether reports of that activity meet the criteria for being entered into the ISE as a SAR."

- However, even after the 2009 launch of the pilot Nationwide Suspicious Activity Reporting Initiative, confusion remained as to what constitutes "suspicious activity": "At the beginning of the ISE-SAR [Evaluation Environment], there was not a clear agreement on what constituted a terrorism-related suspicious activity. In addition, the level of suspicion needed to classify terrorism-related information as an ISE-SAR that would need to be shared with other law enforcement agencies was not clearly defined." (p. 36) Eventually, "a determination was made that the reasonably indicative standard would be required for this project." In other words, a Suspicious Activity Report would consist of "information that is 'reasonably indicative of terrorism-related activity.'" Even after this clarification, however, pilot program participants requested "specific guidance to future participating agencies concerning the appropriate level of suspicion needed for inclusion of information in the NSI."

- The Information Sharing Environment Suspicious Activity Reporting Functional Standard was subsequently updated to Version 1.5 in May 2009, in the midst of the pilot Nationwide Suspicious Activity Reporting Initiative. It currently defines "suspicious activity" (p. 10) as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Version 1.5 (p. 7) also made clear that "the same constitutional standards that apply when conducting ordinary criminal investigations also apply to local law enforcement and homeland security officers conducting SAR inquiries," including "constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, frisk ("Terry Stop"), request identification, or detain and question an individual." The current functional standard includes a footnote defining photography as First Amendment-protected activity that should not be collected absent articulable facts and circumstances supporting suspicion that the activity is not innocent, but "reasonably indicative of criminal activity associated with terrorism." This language, however, has clearly proven insufficient to prevent improper infringement of photographers' First Amendment rights.

- The failure to clearly state that eGuardian and Information Sharing Environment policy does not authorize the collection, retention, or dissemination of personally identifiable information in violation of 28 C.F.R. Part 23 has led to continued confusion by implying that the "reasonably indicative" requirement is a lower standard than the regulation's "reasonable suspicion" requirement (p. 1).

    - Following the conclusion of the pilot Nationwide Suspicious Activity Reporting Initiative in September 2009, the Boston Police Department (p. 81) reported that "suspicious activity" remained ill defined: "It is recommended that the appropriate threshold be clearly defined for entering a SAR into the ISE-SAR Shared Spaces. During the ISE-SAR EE, there seemed to be a disparate amount of SARs being entered between the agencies." The Department warned of the harm to intelligence gathering from overbroad inclusion of information in suspicious activity reporting systems: "BPD wants to avoid the entry of information into the ISE-SAR Shared Spaces that is not of value and avoid large volumes of information being 'dumped' into the system." The Miami-Dade Police Department recommended (p. 115) that "[t]he NSI needs to stay focused on behaviors and not individuals," suggesting that the lack of adequate guidance concerning the definition of "suspicious activity" would result in inappropriate profiling.

- Confusion about the definition of "suspicious activity" has understandably persisted even following full Nationwide Suspicious Reporting Initiative implementation. In two May 2011 emails, a Lead Intelligence Analyst in the Central California Intelligence Center asked David Lewis of the Office of the Program Manager for the Information Sharing Environment for clarification of the Information Sharing Environment Suspicious Activity Reporting Functional Standard Version 1.5. The analyst wrote (p. 1), "Tom said the functional standards are a 'guideline' and are flexible. [Redacted] Some clarification on these issues would really help us out, as we want to be very clear on it ourselves prior to trying to get all of our analysts on board with these new guidelines." The analyst forwarded his May emails to Lewis on August 12, 2011 and copied Thomas O'Reilly of the Office of the Program Manager for the Information Sharing Environment (p. 1): "You mentioned that your group has come up with answers to the questions below.... I still have not seen them. Can you send them to me please? We are having a statewide meeting in a few weeks, and this is one of the topics of discussion."

- In a January 20, 2012 email, (p. 2) a program supervisor in the Texas Department of Public Safety noted that the Texas Fusion Center submitted non-terrorism related Suspicious Activity Reports to the Nationwide Suspicious Activity Reporting Initiative Information Sharing Environment. In response, an unknown official indicated (p. 1) that "non-terrorism related SARs are approved by the supervisors," and as a result are "put in the queue" for submission "to Common Box" or "eGuardian even though they have not been tagged by the analysts for submission." The author inquired whether that problem "can be corrected easily" or whether the system should stop approving "non-terrorism related for now?" Another document (p. 713) secured by the ACLU confirms that non-terrorism related SARs should not be disseminated to eGuardian because that system is intended to be "an incident reporting system of suspicious terrorism-related activity." (See also: Privacy Impact Assessment for the eGuardian Threat Tracking System.)

- The failure to clearly state that eGuardian and Information Sharing Environment policies do not authorize the collection, retention, or dissemination of personally identifiable information in violation of 28 C.F.R. Part 23 has also led to specific instances of abuse.

  - The American Civil Liberties Union of California obtained summaries of Suspicious Activity Reports produced by fusion centers, which contain no reasonable evidence of criminal activity and demonstrate bias against racial and religious minorities and people exercising their First Amendment rights as the primary justification for the collection of information. In these Suspicious Activity Reports, photography and videography are frequently reported without additional facts that render these constitutionally-protected activities inherently suspicious, despite the footnote in the Information Sharing Environment Suspicious Activity Reporting Functional Standard Version 1.5 indicating that reports of photography should not be collected absent articulable facts and circumstances supporting suspicion that the activity is not innocent, but "reasonably indicative of criminal activity associated with terrorism."

The government's withholding of information is obscuring public understanding of the full scope of the problems with nationwide suspicious activity reporting, including issues with the training of analysts who vet Suspicious Activity Reports for inclusion in eGuardian and the Information Sharing Environment Shared Spaces.

- A February 16, 2011 email (p. 2) from an official of the FBI's Guardian Management Unit provided "information . . . regarding what was observed at the SAR Analyst Training which was deemed inappropriate or misleading." The government redacted five pages of attached information (p. 2–6) on "Potential ISE/eGuardian Problems".

- The government identified a January 31, 2012 email chain communicating feedback to DOJ on issues with the Nationwide Suspicious Activity Reporting Initiative, but redacted all information concerning the content of the feedback itself.

The documents show that the FBI, DOJ, and other agencies possess but continue to withhold policy, guideline, and training documents that would shed additional light on the definition of "suspicious activity" that may be reported in nationwide suspicious activity reporting systems. Without the documents listed below, the public cannot fully understand the system and determine or debate any reforms necessary to ensure that these programs are used consistent with respect for civil rights and civil liberties:

- "Privacy Civil Rights and Civil Liberties Compliance Verification for the Intelligence Enterprise" (p. 2), which serves as a resource to help "agency leadership in determining whether their agency's policies and procedures comprehensively address and implement privacy, civil rights, and civil liberties protections" and provides an appendix "on SAR information and SAR-related policies";

- "ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy Template" (2009) (p.3), which was created by the Program Manager for the Information Sharing Environment "to cover all ISE-SAR [Evaluation Environment] activities conducted by participating pilot sites";

- "Vetting ISE-SAR Data: A Pathway to Ensure Best Practices" (May 2011), a document that provides guidance to fusion center analysts on how to vet the information in Suspicious Activity Reports so that only information that meets Information Sharing Environment Suspicious Activity Reporting Functional Standard Version 1.5 is entered into the system;

- the SAR Vetting Tool (p. 58), which is a "technology" used to vet information in Suspicious Activity Reports to ensure compliance with the Information Sharing Environment Suspicious Activity Reporting Functional Standard Version 1.5;

- SAR Analyst Training materials (p. 4), which address the "review and vetting of information to ensure compliance with the functional standard; privacy and civil liberties protections; terrorism indicators, including recent trends in terrorism, stages of terrorism, and behaviors tied to the ISE-SAR Criteria Guidance";

- Frontline Officer Training materials (p. 20) created by International Association of Chiefs of Police, which consist of an online course addressing the recognition of "those behaviors and incidents that could be indicative precursors to activity related to terrorism";

- Chief Executive Briefing materials (p. 4), which address "executive leadership, policy development and privacy and civil liberties protections; agency training and community outreach";

- Training materials (p. 756) developed following the NSI pilot program for "Continuing Privacy Training," "SAR Vetting Tool User Training," and "First-Line Supervisor/Midlevel Manager Training";

- Training materials on suspicious activity reporting programs for first responders, "public safety/justice professionals," and private-sector personnel dealing with "critical infrastructure" (p. 17);

- The FBI eGuardian Policy Training Guide;

- The FBI eGuardian User's Manual;

- "Frequently Asked Questions on Guardian and eGuardian," "SARS and NSI FAQ," and a "Protecting Privacy—Fact Sheet on Civil Liberties," which DOJ finalized and memorialized in a December 19, 2010 Email (p. 4).