

Federal Election Commission
Office of General Counsel
999 E Street, N.W.
Washington, DC 20463

**VOLUME 1 OF EXHIBITS SUBMITTED IN SUPPORT OF 2016 REQUEST BY THE
SOCIALIST WORKERS PARTY, THE SOCIALIST WORKERS NATIONAL
CAMPAIGN COMMITTEE, AND COMMITTEES SUPPORTING CANDIDATES OF
THE SOCIALIST WORKERS PARTY FOR AN ADVISORY OPINION**

October 31, 2016

Michael Krinsky, Esq.
Lindsey Frank, Esq.
RABINOWITZ, BOUDIN, STANDARD,
KRINSKY & LIEBERMAN, P.C.
61 Broadway, 18th Floor
New York, New York 10006
(212) 254-1111
Attorneys for Requesting Parties

EXHIBIT A



FEDERAL ELECTION COMMISSION
Washington, DC 20463

April 25, 2013

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

ADVISORY OPINION 2012-38

Michael Krinsky, Esq.
Lindsey Frank, Esq.
Rabinowitz, Boudin, Standard, Krinsky & Lieberman, P.C.
45 Broadway, Suite 1700
New York, NY 10006-3791

Dear Messrs. Krinsky and Frank:

We are responding to your advisory opinion request, on behalf of the Socialist Workers Party, the Socialist Workers National Campaign Committee, other Socialist Workers Party committees, and authorized committees of Federal candidates of the Socialist Workers Party (collectively the “SWP” or the “SWP committees”), concerning the application of the Federal Election Campaign Act of 1971, as amended (the “Act”), and Commission regulations to the continuation of a partial reporting exemption for the SWP. The facts presented in this advisory opinion are based on your letter received on November 8, your email received on November 30, 2012, your comment filed on April 18, 2013, as well as publicly available materials.

Based on the long history of systematic harassment of the SWP, including evidence of some harassment after 2009, the Commission is renewing the partial reporting exemption until December 31, 2016.

Background

A. Partial Exemption History

The SWP was first granted a partial reporting exemption in a consent decree that resolved *Socialist Workers 1974 National Campaign Committee v. Federal Election Commission*, Civil Action No. 74-1338 (D.D.C. 1979). In that case, the SWP alleged that certain disclosure provisions of the Act deprived the SWP and its supporters of their First Amendment rights because of the likelihood of harassment resulting from mandatory disclosure of contributors and

vendors. Additionally, the SWP alleged that the governmental interest in obtaining identifying information of contributors and recipients of expenditures was diminished because, as a minor party, the possibility of an SWP candidate winning or influencing an election was remote. The consent decree exempted the SWP from the Act's requirements to disclose: 1) the names, addresses, occupations, and principal places of business of contributors to the SWP committees; 2) other political committees or candidates to which or to whom the SWP committees made contributions; 3) lenders, endorsers, or guarantors of loans to the SWP committees; and 4) persons to whom the SWP committees made expenditures. The consent decree, however, required the SWP to maintain records in accordance with the Act and to file reports in a timely manner. On July 24, 1985, the court approved an updated settlement agreement with these requirements and a partial reporting exemption.¹

In 1990, the SWP sought an extension of the partial reporting exemption through the advisory opinion process in lieu of obtaining a consent decree approved by the court. The Commission granted the same exemption provided by the previous consent decrees. The advisory opinion provided that the exemption would be in effect through December 31, 1996. *See* Advisory Opinion 1990-13 (SWP).

In response to the SWP's subsequent 1996, 2002, and 2008 requests, the Commission again issued advisory opinions renewing these partial reporting exemptions. *See* Advisory Opinion 1996-46 (SWP); Advisory Opinion 2003-02 (SWP); Advisory Opinion 2009-01 (SWP). The current exemptions apply to reports covering committee activity up to December 31, 2012.² *See* Advisory Opinion 2009-01 (SWP).

B. *Factual Update*

1. Electoral Success

Despite proffering a presidential candidate in every election since 1948 and numerous other candidates for Federal, State and local offices, no SWP candidate has ever been elected to public office in a partisan election. Data from elections in 2009-2012 show very low vote totals for SWP presidential and other Federal candidates. The information presented, as well as publicly available information, shows that no SWP candidate has come close to winning a Federal election in the nearly four years since the last exemption was granted. SWP candidates for President received only 10,791 votes in 2004, 9,827 votes (not including write-ins) in 2008, and 3,509 votes in 2012. Further, in 2010 and 2011, none of the three SWP candidates on the ballot for U.S House of Representatives received more than 6,300 votes. The SWP has not had

¹ The 1985 agreement also exempted the SWP from reporting the identification of persons providing rebates, refunds, or other offsets to operating expenditures, and persons providing any dividend, interest, or other receipt.

² Advisory Opinion 2009-01 (SWP) specified that no later than 60 days prior to that date, the SWP could submit a new advisory opinion request seeking another renewal of the partial exemption. On October 31, 2012, the Commission granted an extension of the deadline for applying for a renewal of the partial reporting exemption to November 9 due to difficulties SWP counsel experienced in the wake of Hurricane Sandy. A complete Advisory Opinion Request was received on November 8, 2012.

any candidates on the ballot for the U.S. Senate since 2009. Further, no SWP candidate won a state or local election during the four-year period. *See* Declaration of Chris Hoepfner, Exhibit D, at 1, 4-5 and Supplement to the Request.

2. Financial Activity

Information presented in the request and available on the Commission's website indicates a very low level of financial activity by SWP political committees. As of October 20, 2012, the date of the Declaration submitted by the SWP, only 118 people made contributions to the SWP National Committee in 2012, and, in 2008, only 243 people contributed to the Committee. *See* Declaration of Lea Sherman, Exhibit E, at 1. Commission records reflect that no person contributed over \$200 per calendar year to the Committee during the three-year period from 2009 to 2011. Year-end reports filed with the Commission indicate that the SWP received contributions totaling \$1,222 from 2009 to 2011, and the Committee's last report shows that it had 11 contributors each giving in excess of \$200 in 2012, when the Committee raised approximately \$16,087 in total contributions. The SWP has not received any "bundled" contributions that would require disclosure under the Honest Leadership and Open Government Act (2 U.S.C. 434(i)), and it does not foresee receiving any such contributions. *See* Declaration of Lea Sherman, Exhibit E, at 1.

Unlike committees of other minor parties, the SWP National Campaign Committee has never applied or qualified for national committee status. *See* 2 U.S.C 431(14), 11 CFR 100.13; *cf.* Advisory Opinion 2001-13 (Green Party of the United States); Advisory Opinion 1998-2 (Reform Party USA); Advisory Opinion 1995-16 (U.S. Taxpayers Party). According to Commission records, no SWP party committee other than the National Campaign Committee was registered with the Commission during the 2008 and 2010 election cycles, and only two other SWP party committees, both State committees, were registered during the 2004 cycle. During the 2012 election cycle, no authorized committee of any SWP candidate was registered with the Commission.

3. Harassment

The SWP's current request includes 57 exhibits attesting to some 45 incidents of harassment or intimidation and 12 instances where potential SWP supporters were fearful. Each of the 57 exhibits includes at least one sworn statement from an individual associated with the SWP, sometimes accompanied by news accounts, correspondence received, or other materials. Additionally, the exhibits to the SWP's April 18, 2013, comments describe 12 further incidents of harassment or intimidation and fear, as well as one further explanation of an instance of alleged government surveillance submitted in the SWP's original request.

The statements were made by SWP members, candidates, campaign workers, or supporters from different regions of the United States and generally fall into five categories: (1) statements attesting to the fear that potential SWP supporters have of being identified as an SWP supporter; (2) statements attesting to firings and alleged workplace intimidation; (3) statements and materials attesting to alleged hostility from private parties to SWP activities; (4) statements

and materials attesting to alleged hostility from local government law enforcement sources to SWP activities; and (5) a statement attesting to other alleged governmental information gathering and sharing.³ The requestor states that this compilation of incidents “is not meant to be exhaustive, as acts of intimidation and harassment against the SWP and its supporters are frequent enough that they often go unreported to any central body.”

a. Historical and Current Government Harassment Causing Fears Among Potential SWP Supporters

In its request, the SWP summarizes the history of harassment and disruption by government entities that lasted through the 1970s, and that was the subject of lawsuits as late as the 1980s.⁴ Additionally, the SWP cites recent changes to certain government guidelines and programs for obtaining and maintaining information on U.S. citizens and residents to support the reasonableness of the fear expressed by several potential supporters.⁵

The SWP argues that, along with the lengthy history of governmental harassment and disruption that ended prior to 1990, these recent changes and reported increases in government surveillance could cause any person interested in supporting the SWP to reasonably fear that

³ The SWP’s April 18, 2013, comments contain the following additional statements relating to the five categories described above: (1) two declarations from previous contributors, stating that if their identification must be disclosed for any further contributions, they may no longer contribute to the SWP (*see* Exhibits 58 and 59); (2) a declaration by the editor of *The Militant* newspaper, which has offered editorial endorsement to SWP candidates, describing five incidents in which persons who, having been accurately quoted in the newspaper, requested that their names be removed from the paper’s on-line edition after experiencing difficulty in getting or maintaining employment after employers saw their quotes (*see* Exhibit 62); (3) two declarations describing incidents of alleged hostility from private parties to SWP activities and a declaration from the editor of *The Militant* describing examples of threatening mail, phone calls, and e-mail received by the paper (*see* Exhibits 60 and 61); (4) two declarations from SWP candidates who took part in protests and picket lines sponsored by other organizations, which were later found to have been under surveillance by local and/or federal law enforcement agencies (*see* Exhibits 63 and 64); and (5) a further explanation of a prior statement regarding other alleged governmental information gathering and sharing (*see* Exhibit 66).

⁴ Advisory Opinion 1990-13 (SWP) described FBI investigative activities between 1941 and 1976 that included the extensive use of informants to gather information on SWP activities and on the personal lives of SWP members, warrantless electronic surveillance, surreptitious entry of SWP offices, other disruptive activities including attempts to embarrass SWP candidates and to foment strife within the SWP and between the SWP and others, and frequent interviews of employers and landlords of SWP members. The description of these activities was set out in the Final Report of the Special Master Judge Breitel in *Socialist Workers Party v. Attorney General*, 73 Civ. 3160 (TPG) (S.D.N.Y. Feb. 4, 1980) and *Socialist Workers Party v. Attorney General*, 642 F. Supp. 1357 (S.D.N.Y. 1986); *see also* Advisory Opinion 2003-02 (SWP), n.8, for a description of FBI activities between 1941 and 1976.

⁵ Specifically, the SWP points to alleged relaxation in FBI guidelines concerning investigations and information gathering relating to threats to national security; increased Federal support for, and involvement in, State and local “fusion centers,” described as “a collaborative effort of 2 or more Federal, State, local or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend and respond to criminal or terrorist activity”; and an increase in government surveillance of telephone and electronic communications. Exhibits I, M.

association with the SWP may well subject them to government surveillance and harassment. The SWP, however, does not present evidence that the SWP has been under surveillance under any of these programs.

The SWP's request contains approximately 12 statements by SWP candidates and campaign workers relating to the concerns expressed by potential SWP supporters regarding public identification with the SWP. These include statements by campaign supporters and workers describing their experiences while campaigning and talking with potential supporters, selling subscriptions to the SWP's periodical, *The Militant*, and working to get petition signatures and electors. Individuals have expressed fear that getting involved or placing their names and addresses on subscription lists would result in further scrutiny of them by governmental authorities such as the FBI, the Department of Homeland Security, the Department of Housing and Urban Development (fear of losing housing), and immigration authorities (when applying for citizenship and even when they were legal residents). In addition, some supporters were fearful of being placed on a "government list." *See Exhibits 46-57.*

b. Interactions with Other Governmental Authorities

In addition to the generalized fear of increased government surveillance discussed above, the SWP raises a specific incident of what it believes is "FBI Surveillance and Information Sharing." The incident occurred when the SWP candidate for Vice President was stopped and questioned for over two hours by Canadian immigration authorities. The candidate states that, within seconds of scanning her passport, the Canadian immigration officer was able to review on her computer a "sizeable dossier" concerning the candidate and her prior activities. The SWP asserts that the only possible explanation for this is that the U.S. government has been gathering information and monitoring the SWP and its members and sharing this information with the government of Canada, and possibly other countries. *See Request Exhibits R, 15; SWP Comment Exhibit 66.*

c. Firings and Alleged Workplace Intimidation

The request includes declarations of two SWP candidates and one supporter state that their employment was terminated or that they were laid off and not rehired due to their SWP candidacies and activities. One candidate states that he was fired because of "conversations" and "discussions" the employee was "having with other employees" concerning his candidacy and the SWP ticket. *See Exhibit 4* (quoting his employer). The other candidate states that she was fired in 2010 despite her good work reports. She also states that she was laid off from a different job with other workers during a 2009 work slowdown, but unlike other workers was not rehired. *See Exhibit 1.* Finally, a supporter states that he was fired after going to an establishment frequented by company managers to attend a farewell party for a fellow employee who was an SWP candidate. *See Exhibit 3.*

Other exhibits report instances in which SWP candidates and supporters were subjected to negative actions and abusive behavior by employers and co-workers. In each of these instances, the requestor raises doubts as to the expressed bases for the firings or other adverse

employment actions and raises the possibility that the employee may, in fact, have been terminated or otherwise penalized for SWP-related activities.

d. Hostility from Private Parties

The SWP submitted approximately 22 exhibits consisting of attestations as to incidents of harassment, threats, or violence by private individuals or businesses. Many of these exhibits are described below.

Two exhibits describe face-to-face threats of harm or violence made against SWP workers, property, or materials. According to one exhibit, a person grabbed the clipboard of an SWP supporter collecting signatures on a petition and said that he and his friends would “take care of you,” and then followed the supporters to their car. The SWP supporters believed that they would be “subjected to physical assault” if they did not leave. According to the second exhibit, a man shook the locked SWP headquarters door during an organization meeting and yelled, “If Obama wins I’m going to kill every one of you commie [expletive].” *See Exhibits 11, 12.*

Two other exhibits allege threatening or hostile statements made by mail or by phone.⁶ One phone message threatened to shoot the “president of the campaign” unless he left town immediately, while another stated that “We’re going to shut you down.” *See Exhibits 10, 13.*

Seventeen exhibits describe disruption of SWP workers or candidates while they were distributing SWP literature or attempting to obtain ballot petition signatures. According to the descriptions of some of these incidents, personnel of nearby businesses, including company or store security officers, required SWP campaigners to dismantle or move their tables displaying campaign literature and other party materials or to cease distribution of SWP materials while standing in a certain area. According to the exhibits, these incidents often occurred when the table or the campaigner was not on company premises, but only nearby, or in shopping mall parking lots. The exhibits indicate that, in some cases, company personnel threatened to call the local police, and one individual threatened that the FBI was on the way. *See Exhibits 29 – 45.*

e. Relations with Local Law Enforcement Authorities

The SWP’s request also provides 13 exhibits describing interactions between SWP workers and local law enforcement authorities in seven cities or towns. These often involved police personnel or security police at public institutions who, according to the descriptions in the exhibits, demanded or forced SWP campaigners to remove tables displaying campaign materials and other SWP literature from sidewalks or to cease hand distribution of such materials. Some of the described interactions involved questions as to the content of the literature being displayed

⁶ In a third exhibit, a pro-choice SWP candidate for local office stated that she received at her residence a postcard containing a graphic anti-abortion message. Although the exhibit says that the candidate made the statement in support of SWP’s request for the exemption, there is no allegation that the statement was because the candidate represents the SWP, rather than her position as a pro-choice candidate. Exhibit 14.

or distributed or what appeared to be hostile statements or actions by the police that may have intimidated campaigners and others interested in SWP literature. *See* Exhibits 16 – 28.

For example, after looking through the campaign literature, police officers in Philadelphia, Pennsylvania purportedly warned the SWP workers that “We can put you on the no-fly list. Report you to Homeland Security.” The police officers temporarily took the workers’ identification cards, remained parked, and watched until the workers ended their campaigning.

In some of the situations described, police officers contended that the SWP campaigners needed permits to have a table on the sidewalks or to distribute literature. The SWP asserts, however, that in six of these seven cities or towns, local ordinances did not require a permit and the SWP campaigners’ activities were lawful. The SWP further states that in the one city that did have an ordinance requiring a permit to distribute political materials, the police officers’ actions reveal “anti-SWP animus in the selective application of these code provisions.” *See* Exhibits 16 – 28; *see also* Exhibits T - Y (relevant policies and ordinances). Four of the incidents involving local police resulted in a ticket or summons being issued to SWP workers.

Question Presented

Do the SWP, the Socialist Workers National Campaign Committee, other SWP party committees, and authorized committees of candidates of the SWP qualify for an extension of their previous partial reporting exemption?

I. Legal Analysis and Conclusions

Yes, the SWP, the Socialist Workers National Campaign Committee, other SWP party committees, and authorized committees of candidates of the SWP qualify for an extension of their partial reporting exemption for reports covering activity up to December 31, 2016.

The Act requires political committees to file reports with the Commission that identify individuals and other persons who make contributions over \$200 during the calendar year or election cycle (depending on the type of committee), or who come within various other disclosure categories. 2 U.S.C. 434(b)(3), (5), (6); *see also* 2 U.S.C. 431(13). The Supreme Court has found that under certain circumstances, the Act’s disclosure requirements are unconstitutional as applied to a minor party because the threat to the exercise of First Amendment rights resulting from disclosure outweighs the government’s insubstantial interest in disclosure by that particular entity. *Buckley v. Valeo*, 424 U.S. 1, 71-72 (1976). Reasoning that “[m]inor parties must be allowed sufficient flexibility in the proof of injury to assure a fair consideration of their claim” for a reporting exemption, the Court stated that “[t]he evidence offered need show only a reasonable probability that the compelled disclosure of a party’s contributors’ names will subject them to threats, harassment, or reprisals from either Government officials or private parties.” *Id.* at 74. “The proof may include, for example, specific evidence of past or present harassment of members due to their associational ties, or of

harassment directed against the organization itself. A pattern of threats or specific manifestations of public hostility may be sufficient.” *Id.*

In *Brown v. Socialist Workers '74 Campaign Committee (Ohio)*, 459 U.S. 87 (1982), the Supreme Court reaffirmed and applied the standard set forth in *Buckley* to grant the SWP an exemption from state disclosure requirements, and clarified that the exemption recognized in *Buckley* extended to the names of recipients of disbursements in addition to names of contributors. *See also FEC v. Hall-Tyner Election Campaign Committee*, 678 F.2d 416, 421-22 (2d Cir. 1982).⁷

Following this case law, the Commission must first determine whether the SWP continues to maintain its status as a minor party. *See Buckley*, 424 U.S. at 68-74. Next, the Commission must weigh three factors: (1) the history of violence or harassment, or threats of violence or harassment, directed at the SWP or its supporters by governmental authorities, including law enforcement agencies, or by private parties; (2) evidence of continuing violence, harassment, or threats directed at the SWP or its supporters since the prior exemption was granted; and, balanced against the first two factors, (3) the governmental interest in obtaining identifying information of contributors and recipients of expenditures. The Commission has decided previously that, where the impact of the activities of the SWP and its supporters on Federal elections is minimal because the possibility of an SWP candidate winning an election is remote, the government’s interest in obtaining such information is lessened. Advisory Opinion 2009-01 (SWP); *see also Hall-Tyner Election Campaign Comm.*, 678 F.2d at 422.

A. *Minor Party*

As evidenced by the low vote totals for SWP candidates, the lack of success in ballot access, and the small total amounts of contributions to SWP committees, the Commission concludes that the SWP continues to be a minor party that is out of the mainstream. The SWP is a “small and unpopular political party.” *McArthur v. Smith*, 716 F. Supp. 592, 593 (S.D. Fla. 1989); *cf. also ProtectMarriage.com v. Bowen*, 830 F. Supp. 2d 914, 928 (E.D. Cal. 2011); *Hall-Tyner Election Campaign Comm.*, 678 F.2d at 420.

B. *History of Violence, Threats, and Harassment*

As explained above, there is a long history of threats, violence, and harassment against the SWP and its supporters by Federal and local law enforcement agencies and private parties. The Commission has consistently viewed the SWP’s requests for exemption from the Act’s reporting requirements in light of this “long history of governmental harassment of the SWP.” *See, e.g.*, Advisory Opinion 2009-01 (SWP). Courts have detailed this history. *See generally Socialist Workers Party v. Attorney General*, 642 F. Supp. 1357 (S.D.N.Y. 1986); *Socialist Workers Party v. Attorney General*, 666 F. Supp. 621 (S.D.N.Y. 1987). The Supreme Court has previously referred to “the substantial evidence of both governmental and private hostility

⁷ In discussing disclosure requirements for electioneering communications and possible exemptions to the Act’s disclosure requirements, the Court in *McConnell v. FEC*, 540 U.S. 93, 198-99 (2003), reiterated the standards set forth in *Buckley* and *Brown* that have formed the legal basis for past exemptions for the SWP.

toward and harassment of SWP members and supporters.” *Brown*, 459 U.S. at 98-99 (quoting the underlying district court opinion).

To be sure, the importance of the past history of harassment has diminished as those acts and incidents recede further into the past. FBI surveillance of the SWP lasted for 25 years and ended around 1976, nearly 40 years ago. *Brown*, 459 U.S. at 99. The SWP has provided the Commission with accounts of serious incidents of harassment by private parties over the last several decades, but those have declined over time. *See* Advisory Opinion 2009-01 (SWP) (describing the alleged incidents of violence and harassment from 2003-2008 as “appear[ing] to be of lesser magnitude than those referenced in court opinions and prior AOs granting the exemption”).

But the governmental hostility and public and private harassment against the SWP was pervasive and threatened the group’s existence for decades. It thus continues to provide support for the SWP’s current request for a prospective partial reporting exemption. It is against this historical backdrop that the present evidence presented by the requesters must be considered. *Buckley*, 424 U.S. at 74.

C. Recent Violence, Harassment, and Threats

A review of the information presented in connection with this request indicates that the SWP and persons associated with it have likely experienced harassment from private sources from the end of 2009 to the present. Although some of the alleged incidents of harassment may seem minor or subject to differing interpretations, there are a number of examples, such as firings and instances of workplace intimidation, as well as verbal threats and harassment, that legitimately raise concern by those associated with the SWP, particularly when such examples are taken together.⁸ Considering that these incidents occurred over a four-year span, there are relatively more of them on a per-year basis than incidents that took place during the six-year period before the Commission when it rendered Advisory Opinion 2009-01 (SWP).

Of particular relevance in the SWP’s submissions now before the Commission is the evidence of employment-related repercussions. For example, two SWP candidates were temporary workers released from job placements in circumstances suggesting their party membership may have played a role. *See* Exhibits 1, 4. Though not the exclusive reason given for either firing, references to SWP activities were allegedly made by the employer at various points. *See* Warshell Declaration ¶¶ 3-4, Exhibit 4 (stating that the employer had referred to off-site, off-hours “conversations, discussions you were having with employees” about SWP candidacy as a reason for the termination); Potash Declaration ¶ 1, Exhibit 1 (stating that one management employee said he did not “care if the employee was left or right” and two managers said the company “will make a decision about you within two weeks” following

⁸ Some of the SWP’s alleged incidents merely involve private parties expressing heated disagreement with the SWP’s positions. Such episodes are “typical of any controversial campaign,” and “do not necessarily rise to the level of ‘harassment’ or ‘reprisals.’” *ProtectMarriage.com*, 830 F. Supp. 2d at 934; *see also* Advisory Opinion 2009-01 (SWP) (noting that “insulting messages containing harsh language” are “not out of the ordinary experience of campaigns today”).

publication of the candidate's letter in a newspaper). The SWP alleges that there were at least four terminations involving three SWP supporters in the last four-year period.

There are also allegations of continuing harassment and hostility by local police. Although less frequent, the evidence presented suggests that harassment of the SWP by other governmental entities since 1990 still occurs. Although "[i]t [wa]s not certain that animus against the SWP was the motivating factor" in some situations when local police officers prevented pamphlet distribution, Advisory Opinion 2009-01 (SWP) at 9, the SWP has submitted evidence of two instances of alleged disparate treatment as between SWP workers and the workers of other organizations undertaking the same activity nearby. *See* Exhibits 18 – 19.

In addition, the long history of Federal and local governmental harassment continues to have some present-day chilling effect despite the absence of recent alleged Federal governmental harassment. For example, a number of SWP personnel filed sworn statements that individuals had been reluctant to sign petitions or subscribe to SWP literature for fear of scrutiny by governmental authorities.

The evidence presented does not need to demonstrate to a certainty that harassment would inexorably follow a revocation of the partial reporting exemption. There need be only "a reasonable probability that compelled disclosure" would result in "threats, harassment, or reprisals from either Government officials or private parties." *Buckley*, 424 U.S. at 74. Based on consideration of the evidence from 2009 through 2012, the Commission concludes that there is a reasonable probability that SWP contributors and vendors doing business with the SWP and committees supporting SWP candidates would face threats, harassment, or reprisals if their names and identifying information were disclosed.

D. The Government's Informational Interest

As discussed above, the Commission must weigh against the danger of violence or harassment, or threats of violence or harassment, directed at the SWP or its supporters the governmental interest in obtaining identifying information of contributors and recipients of expenditures. *See Brown*, 459 U.S. at 92.

The governmental interest in obtaining the names, addresses, and other identifying information of SWP contributors and vendors doing business with the SWP committees in connection with Federal elections remains very low and continues to be outweighed by the reasonable probability of threats, harassment, or reprisals resulting from such disclosure. The SWP has experienced a decline in episodes of harassment of serious magnitude, but has submitted some credible evidence of threats and intimidation. When weighed together with the very small amounts of money raised and the significant past history, the recent evidence of harassment thus satisfies the requirement of demonstrating a reasonable probability of harassment.

* * * * *

The Commission thus grants the SWP committees a further continuation of the partial reporting exemption provided for in the consent agreements and continued in previous advisory opinions. As required in previous advisory opinions, each of the SWP committees must assign a code number to each individual or entity from whom or which it receives one or more contributions aggregating in excess of \$200 in a calendar year or applicable election cycle (depending upon the type of political committee).⁹ *See* Advisory Opinion 2009-01 (SWP).

The partial reporting exemption will apply to the following sections of the Act: 2 U.S.C. 434(b)(3) (receipts of a political committee); 434(b)(5) and (6) (expenditures and disbursements by a political committee); 434(e) (reporting by political committees); 434(f) (electioneering communication disclosure); and 434(g) (independent expenditure reporting).¹⁰ Please note that the SWP and the committees supporting SWP candidates must still comply with all other reporting obligations such as electronic filing and reporting their independent expenditures while omitting the names and identifications of contributors, donors, and vendors.

In its request, the SWP also asks for exemptions from “any new, post-2008 reporting and disclosure requirements that might otherwise be applicable.” Since the issuance of Advisory Opinion 2003-02 (SWP), Congress has enacted the Honest Leadership and Open Government Act of 2007 (“HLOGA”), which requires disclosure of the names, addresses, and employers of lobbyists/registrants who provide bundled contributions in excess of \$15,000 (as indexed under 2 U.S.C. 441a(c)) to an authorized committee, leadership PAC, or party committee during a reporting period. *See* 2 U.S.C. 434(i); 11 CFR 104.22. The SWP states that it has not received, and does not anticipate receiving, any such bundled contributions that would require disclosure but nevertheless requested an exemption from this requirement. In the absence of any indication that contributions received by the SWP or committees supporting its candidates would be bundled by lobbyists/registrants and would also reach the current \$16,000 threshold for triggering the requirements of HLOGA, the Commission concludes that the SWP’s need for an exemption from HLOGA’s requirements is hypothetical. *See* Advisory Opinion 2009-01 (SWP).

In sum, based on the record presented, the Commission grants this partial reporting exemption to reports covering through December 31, 2016. *See* Advisory Opinion 2009-01

⁹ Each political committee entitled to the exemption must assign a code number to each individual or entity from whom it receives one or more contributions aggregating in excess of \$200 in a calendar year (if an unauthorized committee) or in excess of \$200 during the election cycle (if an authorized committee). That code number must be included in FEC reports filed by each committee in the same manner that full contributor identification would otherwise be disclosed. Consistent with the requirement that the committees comply with the recordkeeping provisions of the Act, the committee’s records must correlate each code number with the name and other identifying data of the contributor who is represented by that code.

¹⁰ If an SWP committee does not qualify as a political committee and makes an electioneering communication that must be reported under 2 U.S.C. 434(f), it must disclose the name of the broadcasting station even though it would be exempt from disclosing names and addresses of donors and all other vendors. Additionally, the SWP’s request concerns the granting of the partial exemption to both SWP party and candidate committees. The partial exemption does not extend to individual SWP supporters who, as individuals, engage in activity that might require them to file reports of their own, for example, the filing of reports of electioneering communications under 2 U.S.C. 434(f) and independent expenditures under 2 U.S.C. 434(g).

(SWP) (explaining four-year extension). At least 60 days prior to December 31, 2016, the SWP may submit a new advisory opinion request seeking a renewal of the exemption. If a request is submitted, the Commission will consider the factual information then presented as to harassment after December 31, 2012, or the lack thereof, in making a decision regarding renewal.

The Commission emphasizes that the SWP committees must comply with all of the remaining requirements of the Act and Commission regulations. These committees must file reports containing the information required by 2 U.S.C. 434(b) with the exception of the information specifically exempted, and they must keep and maintain records as required under 2 U.S.C. 432 with sufficient accuracy so as to be able to provide information, otherwise exempt from disclosure, in connection with a Commission investigation. In addition to complying with the requirements of the consent decrees, the SWP committees must file all reports required under 2 U.S.C. 434(a) in a timely manner. The SWP committees must also comply with the provisions of the Act governing the organization and registration of political committees. *See, e.g.*, 2 U.S.C. 432-433. Finally, the SWP committees must comply with the Act's contribution limitations, prohibitions, and disclaimer provisions. 2 U.S.C. 441a-441g, 441i.

This response constitutes an advisory opinion concerning the application of the Act and Commission regulations to the specific transaction or activity set forth in your request. *See* 2 U.S.C. 437f. The Commission emphasizes that, if there is a change in any of the facts or assumptions presented, and such facts or assumptions are material to a conclusion presented in this advisory opinion, then the requestor may not rely on that conclusion as support for its proposed activity. Any person involved in any specific transaction or activity which is indistinguishable in all its material aspects from the transaction or activity with respect to which this advisory opinion is rendered may rely on this advisory opinion. *See* 2 U.S.C. 437f(c)(1)(B). Please note that the analysis or conclusions in this advisory opinion may be affected by subsequent developments in the law, including, but not limited to, statutes, regulations, advisory opinions, and case law. The cited advisory opinions are available on the Commission's website, www.fec.gov, or directly from the Commission's Advisory Opinion searchable database at <http://www.fec.gov/searchao>.

On behalf of the Commission,

(signed)

Ellen L. Weintraub
Chair

EXHIBIT B



FEDERAL ELECTION COMMISSION
Washington, DC 20463

March 20, 2009

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

ADVISORY OPINION 2009-01

Michael Krinsky, Esq.
Lindsey Frank, Esq.
Rabinowitz, Boudin, Standard, Krinsky & Lieberman, P.C.
111 Broadway
Eleventh Floor
New York, NY 10006-1901

Dear Messrs. Krinsky and Frank:

We are responding to your advisory opinion request, on behalf of the Socialist Workers Party, the Socialist Workers National Campaign Committee, other Socialist Workers Party committees, and authorized committees of Federal candidates of the Socialist Workers Party (collectively “the SWP” or “SWP committees”), concerning the application of the Federal Election Campaign Act of 1971, as amended (the “Act”), and Commission regulations to the continuation of a partial reporting exemption for the SWP. Based on the long history of systematic harassment of the SWP, and some evidence of harassment after 2002, the Commission is renewing the partial reporting exemption until December 31, 2012.

The facts presented in this advisory opinion are based on your letters received on October 31, 2008, and January 14, 2009, publicly available materials, and telephone conversations with a Commission attorney.

I. Background

A. Socialist Workers Party Litigation

The SWP was first granted a partial reporting exemption in a consent decree that resolved *Socialist Workers 1974 National Campaign Committee v. Federal Election Commission*, Civil Action No. 74-1338 (D.D.C. 1979). In that case, the SWP brought an action for declaratory, injunctive, and affirmative relief, alleging that specific disclosure sections of the Act deprived

the SWP and their supporters of their First Amendment rights because of the likelihood of harassment resulting from mandatory disclosure of contributors and vendors. The consent decree exempted the SWP from the Act's requirements to disclose: (1) the names, addresses, occupations, and principal places of business of contributors to the SWP committees; (2) other political committees or candidates to which the SWP committees made contributions; (3) lenders, endorsers, or guarantors of loans to the SWP committees; and (4) persons to whom the SWP committees made expenditures. It also, however, required the SWP to maintain records in accordance with the Act and to file reports in a timely manner. The decree extended to the end of 1984, and established a procedure for the SWP committees to apply for a renewal of these exemptions.

On July 24, 1985, the court approved an updated settlement agreement with the same requirements and partial reporting exemption.¹ The 1985 court decree extended the exemption until December 31, 1988, and again included a renewal procedure. However, the SWP missed the deadline for reapplication for the exemption.

B. Renewal of SWP's exemptions through advisory opinions

In July 1990, the SWP sought an extension of the partial reporting exemption through the advisory opinion process in lieu of obtaining a court decree. On August 21, 1990, the Commission issued Advisory Opinion 1990-13 (SWP), which granted the same exemption provided by the previous consent decrees. The advisory opinion provided that the exemption would be in effect through the next two presidential election cycles, *i.e.*, through December 31, 1996.

In response to the SWP's subsequent requests in 1996 and 2002, the Commission issued advisory opinions renewing the partial reporting exemptions, each advisory opinion covering the next six years. The Commission granted these renewals after examining the evidence presented in affidavits and other documents describing the continuing harassment of the SWP and its supporters during the six years preceding each request. *See* Advisory Opinions 2003-02 (SWP) and 1996-46 (SWP). The renewed exemption granted in 2003 also reflected amendments to the Act's reporting requirements since Advisory Opinion 1996-46.

The current exemption applies to reports covering committee activity up to December 31, 2008. Advisory Opinion 2003-02 specified that no later than sixty days prior to that date, the SWP could submit a new advisory opinion request seeking another renewal of the exemption.²

¹ The 1985 agreement also exempted the SWP from reporting the identification of persons providing rebates, refunds, or other offsets to operating expenditures, and persons providing any dividend, interest, or other receipt.

² A complete advisory request was received on January 14, 2009. However, SWP's initial submission of October 31, 2008, met the deadline for applying for a renewal of the partial reporting exemption.

II. Case Law

The Act requires political committees to file reports with the Commission that identify individuals and other persons who make contributions over \$200 during the calendar year or election cycle (depending upon the type of committee), or who come within various other disclosure categories listed above in reference to the consent agreements. 2 U.S.C. 434(b)(3), (5), and (6); *see also* 2 U.S.C. 431(13). However, in *Buckley v. Valeo*, 424 U.S. 1 (1976), the United States Supreme Court recognized that, under certain circumstances, the Act's disclosure requirements as applied to a minor party would be unconstitutional because the threat to the exercise of First Amendment rights resulting from disclosure would outweigh the government's insubstantial interest in disclosure by that particular entity. 424 U.S. at 71-72. Reasoning that “[m]inor parties must be allowed sufficient flexibility in the proof of injury to assure a fair consideration of their claim” for a reporting exemption, the Court stated that “[t]he evidence offered need show only a reasonable probability that the compelled disclosure of a party's contributors' names will subject them to threats, harassment, or reprisals from either Government officials or private parties.” *Id.* at 74. The Supreme Court elaborated on this standard, stating:

The proof may include, for example, specific evidence of past or present harassment of members due to their associational ties, or of harassment directed against the organization itself. A pattern of threats or specific manifestations of public hostility may be sufficient.

Id. at 74; *see also McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 356 n.21 (1995).

The Supreme Court reaffirmed this standard in *Brown v. Socialist Workers '74 Campaign Committee (Ohio)*, 459 U.S. 87 (1982), granting the SWP an exemption from State campaign disclosure requirements. The Court noted the evidence of specific incidents of private and government hostility toward the SWP and its members within the four years preceding the trial in that case. The Court also noted the long history of Federal governmental surveillance and disruption of the SWP until at least 1976. 459 U.S. at 99-100. Noting the appellants' challenge to the relevance of evidence of government harassment “in light of recent efforts to curb official misconduct,” the Supreme Court concluded that “[n]otwithstanding these efforts, the evidence suggests that hostility toward the SWP is ingrained and likely to continue.” *Id.* at 101.

The Supreme Court in *Brown* also clarified the extent of the exemption recognized in *Buckley*, stating that the exemption included the disclosure of the names of recipients of disbursements as well as the names of contributors. The Court characterized the view that the exemption pertained only to contributors' names as “unduly narrow” and “inconsistent with the rationale for the exemption stated in *Buckley*.” *Id.* at 95.

The United States Court of Appeals for the Second Circuit also applied the *Buckley* standard in exempting the campaign committee of the Communist Party presidential and vice presidential candidates from the requirements to disclose the identification of contributors and to maintain records of the names and addresses of contributors. *Federal Election Commission v. Hall-Tyner Election Campaign Committee*, 678 F.2d 416 (2d Cir. 1982), *cert. denied*, 459 U.S. 1145 (1983). The court described the applicability of the standard, stating:

[W]e note that *Buckley* did not impose unduly strict or burdensome requirements on the minority group seeking constitutional exemption. A minority party striving to avoid FECA's disclosure provisions does not carry a burden of demonstrating that harassment will certainly follow compelled disclosure of contributors' names. Indeed, when First Amendment rights are at stake and the spectre of significant chill exists, courts have never required such a heavy burden to be carried because "First Amendment freedoms need breathing space to survive." (Citations omitted.) Breathing space is especially important in a historical context of harassment based on political belief. Our examination of the treatment historically accorded persons identified with the Communist Party and a survey of statutes still extant reveal that the disclosure sought by the FEC would have the effect of restraining the First Amendment rights of supporters of the Committee to an extent unjustified by the minimal governmental interest in obtaining the information.

678 F.2d at 421-422.³

The Commission's agreement to the consent decrees granting the previous exemptions to the SWP committees has been based upon the long history of systematic harassment of the SWP and those associating with it and the continuation of harassment. The Commission has required only a "reasonable probability that the compelled disclosure" would result in "threats, harassment, or reprisals from either Government officials or private parties." *Buckley*, 424 U.S. at 74. In addition, the Commission has agreed to the application of this standard to both contributors and recipients of disbursements.

In Advisory Opinions 2003-02, 1996-46, and 1990-13, the Commission noted that, in granting and renewing the exemption, it considered both current and historical harassment. The 1979 Stipulation of Settlement refers to the fact that the Commission had been ordered "to develop a full factual record regarding the present nature and extent of harassment of the plaintiffs and their supporters resulting from the disclosure provisions." 1979 Stipulation of Settlement, p. 2. According to the 1985 Stipulation of Settlement, the renewal was based on evidentiary materials regarding the nature and extent of harassment during the previous five years. The renewals granted in Advisory Opinions 1990-13, 1996-46, and 2003-02 were based, in part, on the evidence of harassment since 1985, 1990, and 1997, respectively. The very nature

³ In *McConnell v. Federal Election Commission*, 540 U.S. 93 (2003), which was issued after Advisory Opinion 2003-02, the Supreme Court addressed the challenge by plaintiffs to certain disclosure requirements for electioneering communications. In discussing the importance of such disclosure and possible exemptions to the Act's disclosure requirements, the Court reiterated the standards set forth in *Buckley* and *Brown* that have formed the legal basis for past exemptions for the SWP. *See McConnell*, 540 U.S. at 198-199.

of the periodic extensions indicates that, after a number of years, it is necessary to reassess the SWP's situation to see if the reasonable probability of harassment still exists.⁴

III. Facts Presented

A. *Status as a Minor Party*

The SWP's current request presents facts demonstrating that it has been a minor party since its founding in 1938. Despite running a presidential candidate in every election since 1948 and numerous other candidates for Federal, State and local offices, no SWP candidate has ever been elected to public office in a partisan election. Data from the 2004, 2006, and 2008 elections show very low vote totals for SWP presidential and other Federal candidates.⁵ Information presented in the request and available on the Commission's website indicates a low level of financial activity by SWP political committees.⁶ Further, unlike committees of several other minor parties, the SWP National Campaign Committee has never applied or qualified for national committee status.⁷ *See* 2 U.S.C 431(14), 11 CFR 100.13; *cf.* Advisory Opinions 2001-13 (Green Party of the United States), 1998-2 (Reform Party USA), and 1995-16 (U.S. Taxpayers Party).

B. *History of government harassment*

The SWP's request for the exemptions must be evaluated in the context of the relationship between the SWP and various Federal, State, and local law enforcement authorities, and private parties. Advisory Opinions 2003-02, 1996-46 and 1990-13 discussed the long

⁴ Similarly, the courts in *Brown* and *Hall-Tyner* rendered their decisions with reference to recent events or factors, as well as a history of harassment, *i.e.*, recent incidents of harassments against the SWP and extant statutes directed against the Communist Party.

⁵ The evidence presented, as well as information publicly available, indicates that no SWP candidate has come close to winning a Federal election in the six years since the last exemption was granted. SWP candidates for U.S. President received only 10,791 votes nationwide in 2004 and 9,827 votes (not yet including write-ins) nationwide in 2008. Further, in 2004, 2006, and 2008, no SWP candidates on the ballot for U.S. Senate (two in 2004 and 2006, and one in 2008) received more than 15,000 votes. Similarly, no SWP candidate on the ballot for the House of Representatives (two in 2004 and 2006, and three in 2008) received more than 4,600 votes in any election during that period. Information on non-Federal elections in 2008 indicates a similar lack of success for SWP candidates. *See* Exhibits D and S.

⁶ A declaration submitted by the treasurer of the SWP's National Campaign Committee states that, up to October 25, 2008, only 243 people had contributed to the committee in 2008, and that, in 2004, 321 people contributed to the committee. Commission records indicate that 26 persons contributed over \$200 per calendar year to the committee in 2007-2008 and that 76 persons contributed over \$200 per calendar year to the committee in 2003-2004. In anticipation of the implementation of the Honest Leadership and Open Government Act of 2007 ("HLOGA"), the committee treasurer stated that the SWP has not received any "bundled" contributions that would require disclosure as such under HLOGA, and does not foresee receiving any such contributions. *See* Exhibit E.

⁷ According to Commission records, no SWP party committee other than the National Campaign Committee was registered with the Commission during the 2006 and 2008 election cycles and only two other SWP party committees, both State committees, were registered during the 2004 cycle. During the 2008 election cycle, no authorized committee of any SWP candidate was registered with the Commission.

history of Federal government harassment of the SWP. Advisory Opinion 1990-13 described FBI investigative activities between 1941 and 1976 that included the extensive use of informants to gather information on SWP activities and on the personal lives of SWP members, warrantless electronic surveillance, surreptitious entry of SWP offices, other disruptive activities including attempts to embarrass SWP candidates and to foment strife within the SWP and between the SWP and others, and frequent interviews of employers and landlords of SWP members. The description of these activities was set out in the Final Report of Special Master Judge Breitel in *Socialist Workers Party v. Attorney General*, 73 Civ. 3160 (TPG) (S.D.N.Y., February 4, 1980) and *Socialist Workers Party v. Attorney General*, 642 F. Supp. 1357 (S.D.N.Y. 1986); *see also* Advisory Opinion 2003-02, n.8, for a description of FBI activities between 1941 and 1976.

The advisory opinions also referred to statements made in affidavits submitted by Federal governmental officials in several agencies expressing the need for information about the SWP based on the officials' unfavorable perceptions of the SWP. These affidavits were submitted in connection with *Socialist Workers Party v. Attorney General*, 666 F. Supp. 621 (S.D.N.Y. 1987), in which the court granted an injunction preventing the Federal government from using, releasing, or disclosing information about the SWP that was unlawfully obtained or developed from unlawfully obtained material, except in response to a court order or a Freedom of Information Act request. The advisory opinions also discussed the statements of SWP workers and candidates and media reports, among other sources, describing incidents of private threats and acts of violence and vandalism, harassment by local police, and difficulties with other governmental authorities experienced by the SWP and those associating with it from 1985 through 2002.

C. *Current evidentiary record*

The SWP's current request includes approximately 90 exhibits attesting to incidents of harassment or intimidation, or fears expressed by potential SWP supporters. Each exhibit includes at least one sworn statement from an individual associated with the SWP, sometimes accompanied by news accounts from the SWP's newspaper, *The Militant*, or from a local newspaper, police reports, correspondence, or other materials. The statements come from SWP members, candidates, campaign workers, or supporters from different regions of the United States and are dated from late 2002 to 2008. Generally, these statements fall into four categories: (1) statements attesting to the fear that potential SWP supporters have of being identified as an SWP supporter; (2) statements and materials attesting to alleged hostility from private parties to SWP activities; (3) statements and materials attesting to alleged hostility from local government law enforcement sources to SWP activities; and (4) statements attesting to other alleged governmental intimidation. The requestor indicates that the compilation of incidents "is not meant to be exhaustive, as acts of intimidation and harassment against the SWP and its supporters are frequent enough that they often go unreported to any central body."

1. Fears expressed by SWP supporters

The SWP's request contains 15 statements (Exhibits 63-71 and 86-90 and Exhibit Q) by SWP candidates and campaign workers relating the concerns expressed by potential SWP supporters regarding public identification with the SWP. These include statements by the 2008

SWP presidential and vice presidential candidates and the National Campaign Committee Chair describing their experiences while campaigning and talking with potential supporters, and statements by SWP workers asking individuals to sign candidate ballot petitions and selling subscriptions to *The Militant*. Individuals expressed fear that putting their names and addresses on public petitions or on subscription lists would result in further scrutiny of them by governmental authorities such as the FBI, the CIA, the Department of Homeland Security, or immigration authorities (even if they were legal residents).

Some of the statements referred to individuals' explicitly stating a concern as to recent increased government surveillance. See Exhibits Q, 65, and 68. In addition, the sworn statement by the National Campaign Committee's Chair (Exhibit Q) indicates that he has met an increasing number of individuals who are attracted to the SWP but are afraid of public involvement for fear of "harassment or victimization by the authorities or right-wing vigilantes." The Chair states that these expressed fears were greater in 2008 than in 2004.⁸

2. Hostility from private parties

The SWP submitted approximately fifty exhibits consisting of attestations as to incidents of harassment, threats, or violence by private individuals or businesses. These exhibits are described below.

Thirteen exhibits described acts of violence or vandalism against SWP workers, property, or materials, including an incident in 2004 when a brick wrapped in incendiary material was thrown through the window of a local SWP headquarters early in the morning, setting the front part of the building on fire and causing considerable damage. See Exhibit 1. Other exhibits described other incidents of violence or vandalism, including pouring paint over an SWP vehicle; racist, anti-gay, or anti-immigrant graffiti on the windows of SWP campaign offices; a threat of imminent bodily harm to SWP campaigners; a physical assault on an SWP worker at a campaign literature table; a piece of concrete thrown through the window of an SWP office in an attempted break-in; extensive egg-throwing at an SWP headquarters on a street where no other businesses or offices were vandalized; and a former head of personnel at a company engaged in disputes with SWP personnel racing his car at an SWP campaigner. See Exhibits 3, 4, 5, 15, 27, 73, 79, 81, 82, and 83.

Several exhibits described more generalized threats of harm made in person to SWP campaigners, such as a statement by an individual to SWP supporters seeking ballot signatures that he wished to "put a bullet in every one of your heads." See Exhibit 8.

⁸ In both the October 2008 and January 2009 letters, and accompanying lettered exhibits, the SWP raises the issue of recent changes in the Attorney General's Guidelines for Domestic FBI Operations. These guidelines, which concern FBI investigations and information gathering relating to threats to national security, are less restrictive than the guidelines issued in the 1970s. The FBI has also recently issued guidance to local law enforcement agencies about "suspicious" activity to be shared with Federal authorities, including information as to "extremist organizations." The SWP notes the general public concern as to the new guidelines and practices, and expresses its concern that the recently expanded governmental authority may lead to the renewal of "the very type of practices and excesses that characterized the FBI's long history of harassment of the SWP." October 30, 2008 Letter, pp. 23-24. See also January 13, 2009 Letter, pp. 14-16, and Exhibits F, G, H, M, N, and O.

Eleven exhibits allege threatening or hostile statements made by mail or by phone. Some of these examples merely involve insulting messages containing harsh language or questioning the SWP's loyalty to the U.S. They are not out of the ordinary experience of campaigns today. However, there are more alarming allegations, such as a threatening letter containing a syringe mailed to an SWP office. There was also a declaration describing a threat by an individual to shoot SWP workers who came to his door. *See Exhibits 7 and 76.*

In four instances, individuals publicly known to be associated with the SWP were terminated from their jobs. Three of these individuals were SWP candidates for public office and one had distributed SWP campaign literature, along with SWP candidates, at the entrance to her company's parking lot after work. In three of the examples, the official basis used by the company to fire the employee was alleged work-related misconduct and did not pertain to SWP-related activities. However, the requestor relies on the circumstances presented in each exhibit to raise doubts as to these official bases and to indicate the possibility that the employee may have been terminated for SWP-related activities. *See Exhibits 20, 21, and 22.* The fourth situation entailed a firing of an SWP candidate for taking three weeks leave to campaign and to attend a youth conference in Venezuela in fulfillment of a campaign promise. The company had refused to grant such leave, and there had been a history of conflict between the company and the SWP. *See Exhibit 74.*

In one described instance, the manager of a bank that was a landlord of an office of the Militant Labor Forum (an SWP entity that sponsors weekly discussion groups on social and political issues) removed a Forum sign from the office's front door and threatened to evict the Forum months before the end of the lease, saying that the Forum was "against a lot of customers that I do business with." (This occurred during a local coal miners' strike in which the Forum was active.) Ultimately, the landlord and the tenant agreed that the tenant would vacate the premises several months before the end of the lease. *See Exhibit 23.*

Nineteen exhibits, some of which are referred to above, describe disruption of SWP workers or candidates while they were distributing SWP literature or attempting to obtain ballot petition signatures. According to the descriptions of some of these incidents, personnel of nearby businesses, including company or store security officers, forced, or attempted to force, SWP campaigners to dismantle or move their tables displaying campaign literature and other party materials, or to cease hand distribution of SWP materials while standing in a certain area. According to the exhibits, these incidents often occurred when the table or the campaigner was not on company premises, but only near it, or in shopping mall parking lots. The exhibits indicate that, in some cases, company personnel referred disparagingly to the political orientation of the literature, although it is also possible that concerns as to any political activity on or near private property may have been the impetus for the disruption in a number of situations. The exhibits also described threats by company personnel to call the local police. *See Exhibits 8, 30, 31, 33, 34, 41, 46, 47, 49, 61, 75, and 83.*

3. Relations with local law enforcement authorities

The SWP also provides sixteen exhibits describing interactions between SWP workers and local law enforcement authorities in eleven cities or towns in the Northeast, the South, and

the Midwest. These often involved police personnel or security police at public institutions who, according to the descriptions in the exhibits, forced SWP campaigners to remove tables displaying campaign materials and other SWP literature from sidewalks or to cease hand distribution of such materials. A substantial number of the described interactions involved questions as to the content of the literature being displayed or distributed, or what appeared to be hostile statements or actions by the police that may have intimidated campaigners and others interested in SWP literature. *See Exhibit J.*

For example, the statement in one exhibit described the police in Phillipi, West Virginia seizing some copies of *The Militant* from SWP workers distributing from house to house, frisking the SWP workers, and then demanding that they leave town or risk arrest. The statement in another exhibit described Toledo, Ohio police hostilely confronting SWP campaigners distributing *The Militant*, forcing them to stop, and demanding that they leave the city, asserting that the campaigners could not distribute such material door-to-door. *See Exhibits 24 and 25.*

It is not certain that animus against the SWP was the motivating factor in these situations. In some of the situations, the police contended that the SWP campaigners needed permits to have a table on the sidewalks or to distribute literature by hand. The SWP asserts that, in seven of these eleven localities, local ordinances did not require a permit and the SWP campaigners' activities were lawful. (Exhibit K includes copies of relevant ordinances from five of the seven localities.)

4. Interactions with other governmental authorities

In the current request, the SWP provides exhibits as to three alleged incidents entailing problems with government officials.⁹ The first consisted of an unannounced visit by FBI agents to the home of an SWP Congressional candidate who had just returned from a book-publicizing trip to Cuba. The candidate's statement indicates that, in questioning him, the FBI agents attempted to "bait [him] with accusations of advocating violence" and asked him other questions about his support of unionization in his workplace. The second incident involved what the SWP considered excessive fines for the posting of Militant Labor Forum event flyers on historic city lampposts. The organizers of the event claimed the posting was done without their knowledge. The third incident concerned the possible placement of an SWP activist on a no-fly list. Whether the individual was on the no-fly list is uncertain from his sworn statement, and the individual was permitted to board his flight. *See Exhibits 19, 58, and 84.*

⁹ In Advisory Opinion 1996-46, the SWP presented evidence of only a few incidents related to SWP interaction with government officials other than local police. The SWP presented only one such situation in Advisory Opinion 2003-02.

IV. Question Presented

Should the SWP, the Socialist Workers National Campaign Committee, other SWP party committees, and authorized committees of candidates of the SWP be granted a continuation of their previous partial reporting exemption?

V. Legal Analysis and Conclusions

Yes, the Commission grants a continuation of the partial reporting exemption for reports covering activity up to December 31, 2012.

In applying the standard established by the court cases and court decrees described above for deciding whether to renew the SWP's partial reporting exemption, the Commission must first determine whether the SWP continues to maintain its status as a minor party. *See Buckley*, 424 U.S. at 68-74. As evidenced by the low vote totals for SWP candidates, the lack of success in ballot access, and the small total amounts contributed to SWP committees, the Commission concludes that the SWP continues to be a minor party.¹⁰

Next, the Commission must weigh three factors in making its determination. The first factor is the history of violence or harassment, or threats of violence or harassment, directed at the SWP or its supporters by governmental authorities, including law enforcement agencies, or by private parties. The second is evidence of continuing violence, harassment, or threats directed at the SWP or its supporters by these same organizations or persons since the end of 2002. These two factors must be balanced against the third factor, which is the governmental interest in obtaining identifying information as contributors and recipients of expenditures. Where the impact of the activities of the SWP and its supporters on Federal elections is minimal because the possibility of winning an election is remote, the government's interest in obtaining such information is diminished. Advisory Opinion 2003-02; *see also Hall-Tyner*, 678 F.2d at 422.

First, as evidenced by the various court cases and the information submitted in previous advisory opinion requests, there is a long history of threats, violence, and harassment against the SWP and its supporters by Federal and local law enforcement agencies and private parties.¹¹ In addition, a review of the information presented in the advisory opinion request indicates that the

¹⁰ In fact, the SWP does not even come close to the level of success necessary for a party to be defined as a "minor party" for the purposes of presidential candidate public financing. According to 26 U.S.C. 9002(7), a "minor party" is a political party whose candidate for president in the preceding presidential election received five percent or more but less than 25 percent of the popular vote.

¹¹ The Commission has consistently viewed the SWP's requests for exemption from the Act's reporting requirements in light of the "long history of governmental harassment of the SWP." Advisory Opinions 2003-02, 1996-46, and 1990-13. Past courts have described in great detail this history of violence, harassment, surveillance and disruption against the SWP. *See generally, Socialist Workers Party v. Attorney General*, 642 F.Supp. 1357 (S.D.N.Y. 1986); *Socialist Workers Party v. Attorney General*, 666 F.Supp. 621 (S.D.N.Y. 1987). The Supreme Court has previously referred to the "substantial evidence of both governmental and private hostility toward and harassment of SWP members and supporters." *Brown v. Socialist Workers '74 Campaign Committee (Ohio)*, 459 U.S. 87, 98-99 (1982) (quoting the underlying district court opinion). It is against this backdrop that the present evidence presented by the requesters must be considered. *See Buckley*, 424 U.S. at 74.

SWP and persons associated with it have likely experienced harassment from private sources from the end of 2002 to the present. Although some of the alleged incidents of harassment may seem minor or subject to differing interpretations based on the circumstances, there are still a number of examples that may legitimately raise concern by those associated with the SWP, particularly when such examples are taken together, rather than viewed in isolation from one another.

There are also some allegations of continuing harassment and hostility by local police toward the SWP based on its political views. The evidence presented suggests that harassment of the SWP by other governmental entities since 1990 still exists but has abated and has been significantly lower than other forms of harassment. Nevertheless, the long history of Federal and local governmental harassment continues to have some present-day chilling effect despite the abatement of Federal governmental harassment.¹²

The Commission notes that the evidence presented does not need to demonstrate a certainty that harassment would follow a revocation of the partial reporting exemption. The standard established in the previous advisory opinions, based on the case law cited earlier, is that there only be “a reasonable probability that compelled disclosure” would result in “threats, harassment, or reprisals from either Government officials or private parties.” *Buckley*, 424 U.S. at 74. Based on its consideration of the evidence from the end of 2002 through 2008, the Commission concludes that there is a reasonable probability that contributors to, and vendors doing business with, the SWP and committees supporting SWP candidates would face threats, harassment, or reprisals if their names and information about them were disclosed.

Information provided by the SWP indicates that the SWP and committees supporting its candidates receive very small total amounts of contributions and its candidates receive very low vote totals in partisan elections. These low vote totals and dollar amounts indicate that the activities of the SWP, its candidates, and committees supporting its candidates have little, if any, impact on Federal elections. The governmental interest in obtaining the names, addresses, and other identifying information of contributors to and vendors doing business with the SWP and committees supporting SWP candidates in connection with Federal elections thus remains very low, and continues to be outweighed by the reasonable probability of threats, harassment, or reprisals resulting from such disclosure.

As a result of its finding that the SWP, the SWP’s party committees, and the authorized committees of SWP candidates have satisfied the factors established in the case law and applied in prior advisory opinions, the Commission grants the SWP, the SWP’s National Campaign Committee, the SWP’s other party committees, and the authorized committees of SWP candidates a further continuation of the partial reporting exemption provided for in the consent agreements and continued in previous advisory opinions. As required in previous advisory opinions, each of the SWP committees must assign a code number to each individual or entity from whom it receives one or more contributions aggregating in excess of \$200 in a calendar

¹² For example, a number of SWP personnel filed sworn statements as to the reluctance of individuals to sign petitions or subscribe to SWP literature for fear of further scrutiny by governmental authorities, and some of these individuals cited concerns as to recent increased government surveillance.

year or applicable election cycle (depending upon the type of political committee).¹³ See Advisory Opinions 2003-02 and 1996-46.

The partial reporting exemption will apply to the following sections of the Act: 2 U.S.C. 434(b)(3) (receipts of a political committee); 434(b)(5) and (6) (expenditures and disbursements by a political committee); 434(e) (reporting by political committees); 434(f) (electioneering communication disclosure); and 434(g) (independent expenditure reporting).¹⁴ Please note that the SWP and the committees supporting SWP candidates must still comply with all other reporting obligations such as electronic filing and reporting their independent expenditures while omitting the names and identifications of contributors, donors, and vendors.

Since the issuance of Advisory Opinion 2003-02, Congress has enacted the Honest Leadership and Open Government Act of 2007 (“HLOGA”) which requires disclosure of the names, addresses, and employers of lobbyists/registrants who provide bundled contributions in excess of \$15,000 (as indexed under 2 U.S.C. 441a(c)) to an authorized committee, leadership PAC, or party committee during a “covered period.” See 2 U.S.C. 434(i); 11 CFR 104.22. The SWP indicates that it has not received, and does not anticipate receiving, any such bundled contributions that would require disclosure, but nevertheless requested an exemption from this requirement. In the absence of any indication that contributions received by the SWP or committees supporting its candidates would be bundled by lobbyists/registrants and would also reach the current \$16,000 threshold for triggering the requirements of HLOGA, the Commission concludes that this question is hypothetical.

Based on the record presented, the Commission grants this partial reporting exemption to reports covering the next four years, *i.e.*, through December 31, 2012, instead of the next six years as had been granted in previous advisory opinions. Although the evidence presented by the requestor demonstrates some continued incidents of violence and harassment, those incidents appear to be of lesser magnitude than those referenced in court opinions and prior AOs granting the exemption. The interest of disclosure, however, is weighed against both the historical and present day evidence of violence and harassment. As the number of severe incidents decline, it may become more difficult for the requestor to demonstrate a “reasonable probability that compelled disclosure” will result in “threats, harassment, or reprisals from either Government

¹³ Each political committee entitled to the exemption must assign a code number to each individual or entity from whom it receives one or more contributions aggregating in excess of \$200 in a calendar year (if an unauthorized committee) or in excess of \$200 during the election cycle (if an authorized committee). That code number must be included in FEC reports filed by each committee in the same manner that full contributor identification would otherwise be disclosed. Consistent with the requirement that the committees comply with the recordkeeping provisions of the Act, the committee's records must correlate each code number with the name and other identifying data of the contributor who is represented by that code.

¹⁴ If an SWP committee does not qualify as a political committee and makes an electioneering communication that must be reported under 2 U.S.C. 434(f), it must disclose the name of the broadcasting station even though it would be exempt from disclosing names and addresses of donors and all other vendors. Additionally, the SWP's request concerns the granting of the partial exemption to both SWP party and candidate committees. The partial exemption does not extend to individual SWP supporters who, as individuals, engage in activity that might require them to file reports of their own, for example, the filing of reports of electioneering communications under 2 U.S.C. 434(f) and independent expenditures under 2 U.S.C. 434(g).

officials or private parties.” *Buckley*, 424 U.S. at 74. The shorter exemption will allow the Commission to reassess the conditions presented by requestors against the interest of disclosure at that time. At least sixty days prior to December 31, 2012, the SWP may submit a new advisory opinion request seeking a renewal of the exemption. If a request is submitted, the Commission will consider the factual information then presented as to harassment after December 31, 2008, or the lack thereof, and will make a decision at that time as to the renewal.

The Commission emphasizes that the SWP committees must still comply with all of the remaining requirements of the Act and Commission regulations. These committees must file reports containing the information required by 2 U.S.C. 434(b) with the exception of the information specifically exempted, and they must keep and maintain records as required under 2 U.S.C. 432 with sufficient accuracy so as to be able to provide information, otherwise exempt from disclosure, in connection with a Commission investigation. In addition to complying with the requirements of the consent decrees, the SWP committees must file all reports required under 2 U.S.C. 434(a) in a timely manner. The SWP committees must also comply with the provisions of the Act governing the organization and registration of political committees. *See, e.g.*, 2 U.S.C. 432 and 433. Finally, the SWP committees must comply with the Act's contribution limitations, prohibitions, and disclaimer provisions. 2 U.S.C. 441a, 441b, 441c, 441d, 441e, 441f, 441g, and 441i.

This response constitutes an advisory opinion concerning the application of the Act and Commission regulations to the specific transaction or activity set forth in your request. *See* 2 U.S.C. 437f. The Commission emphasizes that, if there is a change in any of the facts or assumptions presented, and such facts or assumptions are material to a conclusion presented in this advisory opinion, then the requester may not rely on that conclusion as support for its proposed activity. Any person involved in any specific transaction or activity which is indistinguishable in all its material aspects from the transaction or activity with respect to which this advisory opinion is rendered may rely on this advisory opinion. *See* 2 U.S.C. 437f(c)(1)(B). Please note that the analysis or conclusions in this advisory opinion may be affected by subsequent developments in the law including, but not limited to, statutes, regulations, advisory opinions and case law. All cited advisory opinions are available on the Commission's website at <http://saos.nictusa.com/saos/searchao>.

On behalf of the Commission,

(signed)
Steven T. Walther
Chairman

EXHIBIT C



FEDERAL ELECTION COMMISSION
Washington, DC 20463

April 4, 2003

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

ADVISORY OPINION 2003-02

Michael Krinsky
Jaykumar Menon
Rabinowitz, Boudin, Standard, Krinsky & Lieberman
740 Broadway, Fifth Floor
New York, NY 1002-9518

Dear Mr. Krinsky and Mr. Menon:

This refers to your letters dated October 31, 2002 and February 14, 2003, requesting an advisory opinion concerning the application of the Federal Election Campaign Act of 1971, as amended, ("the Act") and Commission regulations to the continuation of a partial reporting exemption for the Socialist Workers Party National Campaign Committee and committees supporting candidates of the Socialist Workers Party ("SWP").¹

PROCEDURAL BACKGROUND

Judicial origins of the exemption

The SWP National Campaign Committee and committees supporting SWP candidates were first granted a partial reporting exemption in a consent decree, dated

¹ The completed advisory request materials were not received until February 14. However, the date of your initial submission is accepted for purposes of tolling the time for the request of a continuation of the partial reporting exemption.

January 2, 1979, that resolved *Socialist Workers 1974 National Campaign Committee v. Federal Election Commission*, Civil Action No. 74-1338 (D.D.C. 1979). In that case, such committees brought an action for declaratory, injunctive and affirmative relief, alleging that specific disclosure sections of the Act operated to deprive them and their supporters of rights guaranteed by the First Amendment to the Constitution because of the likelihood of harassment resulting from such disclosure. The consent decree required the committees supporting SWP candidates to maintain records in accordance with the Act and to file reports in a timely manner. It also, however, exempted these committees from the provisions requiring the disclosure of: 1) the names, addresses, occupations, and principal places of business of contributors to SWP committees; 2) political committees or candidates supported by SWP committees; 3) lenders, endorsers or guarantors of loans to the SWP committees; and 4) persons to whom the SWP committees made expenditures.² The decree stated that its provisions would extend to the end of 1984, and established a procedure for the SWP committees to apply, prior to that date, for a renewal of the exemptions listed above.

On July 24, 1985, the court approved an updated settlement agreement with the same requirements and partial reporting exemption.³ The court decree extended the exemption until the end of 1988, and again included a renewal procedure. However, the SWP missed the deadline for reapplication for the exemption.

Renewal of the exemptions through advisory opinions

In July 1990, SWP sought an extension of the partial reporting exemption through the advisory opinion process in lieu of obtaining a court decree. On August 21, 1990, the Commission issued Advisory Opinion 1990-13, which granted the same exemption provided for in the previous consent decrees. The advisory opinion provided that the exemption would be in effect through the next two presidential election cycles, i.e., through December 31, 1996. Additionally, the SWP committees could seek a renewal of the exemption by submitting an advisory opinion request by November 1, 1996 to present information as to harassment of SWP, or persons associated with SWP, during the 1990-1996 period. Advisory Opinion 1990-13.

On November 1, 1996, the committees again requested through the advisory opinion process a renewal of the exemption. In Advisory Opinion 1996-46, the Commission agreed to the renewal after examination of the evidence presented in affidavits that described the continuing harassment of SWP and its supporters. However,

² The agreement also stated that if the Commission found reason to believe that the committees violated a provision of the Act, other than those for which an exemption was specified, but needed the withheld information to proceed, the Commission could apply to the court for an order requiring the production of such information.

³ In view of the specific provisions of the 1979 amendments to the disclosure provisions, the agreement also makes reference to an exemption for reporting the identification of persons providing rebates, refunds or other assets to operating expenditures, and persons providing any dividend, interest or other receipts.

the Commission added a new condition to the renewal. This modification required that each committee entitled to the exemption must assign a code number to each individual or entity from whom it receives one or more contributions aggregating in excess of \$200 in a calendar year.⁴ See Advisory Opinion 1996-46. This modified renewal extended the partial reporting exemption for the next six years, i.e., through December 31, 2002. The advisory opinion specified that at least sixty days prior to the expiration date, the requestor could submit a new advisory opinion request seeking another renewal of the exemption.

ACT AND COMMISSION REGULATIONS

The Act requires political committees to file reports with the Commission that identify individuals and other persons who make contributions over \$200 during the applicable time periods, or who come within various other disclosure categories listed above in reference to the consent agreements. 2 U.S.C. 434(b)(3), (5), and (6); see also 2 U.S.C. 431(13). However, in *Buckley v. Valeo*, 424 U.S. 1 (1976), the United States Supreme Court recognized that, under certain circumstances, the Act's disclosure requirements as applied to a minor party would be unconstitutional because the threat to the exercise of First Amendment rights resulting from disclosure would outweigh the insubstantial interest in disclosure by that entity. 424 U.S. at 71-72. Reasoning that "[m]inor parties must be allowed sufficient flexibility in the proof of injury to assure a fair consideration of their claim" for a reporting exemption, the Court stated that "[t]he evidence offered need show only a reasonable probability that the compelled disclosure of a party's contributors' names will subject them to threats, harassment, or reprisals from either Government officials or private parties." *Id.* at 74. The Court elaborated on this standard, stating:

The proof may include, for example, specific evidence of past or present harassment of members due to their associational ties, or of harassment directed against the organization itself. A pattern of threats or specific manifestations of public hostility may be sufficient. New parties that have no history upon which to draw may be able to offer evidence of reprisals and threats directed against individuals or organizations holding similar views.

Id. at 74; see also *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

The Supreme Court reaffirmed this standard in *Brown v. Socialist Workers '74 Campaign Committee (Ohio)*, 459 U.S. 87 (1982), granting SWP an exemption from state campaign disclosure requirements. The Court referred to the introduction of proof of

⁴ The Commission required that the code number must be included in FEC reports filed by each committee in the same manner that full contributor identification would otherwise be disclosed. The committee's records were required to correlate each code number with the name and other identification data of the contributor who is represented by that code.

specific incidents of private and government hostility toward SWP and its members within the four years preceding the trial in that case. The Court also referred to the long history of Federal governmental surveillance and disruption of SWP until at least 1976. *Brown*, 459 U.S. at 99-100. Noting the appellants' challenge to the relevance of evidence of Government harassment "in light of recent efforts to curb official misconduct," the Court concluded that "[n]otwithstanding these efforts, the evidence suggests that hostility toward the SWP is ingrained and likely to continue." *Id.* at 101.

The Supreme Court in *Brown* also clarified the extent of the exemption recognized in *Buckley*, stating that the exemption included the disclosure of the names of recipients of disbursements as well as the names of contributors. The Court characterized the view that the exemption pertained only to contributors' names as "unduly narrow" and "inconsistent with the rationale for the exemption stated in *Buckley*." *Id.* at 95.

The United States Court of Appeals for the Second Circuit also applied the *Buckley* standard in exempting the campaign committee of the Communist Party presidential and vice presidential candidates from the requirements to disclose the identification of contributors and to maintain records of the name and addresses of contributors. *Federal Election Commission v. Hall-Tyner Election Campaign Committee*, 678 F.2d 416 (2d Cir. 1982), *cert. denied*, 459 U.S. 1145 (1983). The court described the applicability of the standard, stating:

[W]e note that *Buckley* did not impose unduly strict or burdensome requirements on the minority group seeking constitutional exemption. A minority party striving to avoid FECA's disclosure provisions does not carry a burden of demonstrating that harassment will certainly follow compelled disclosure of contributors' names. Indeed, when First Amendment rights are at stake and the specter of significant chill exists, courts have never required such a heavy burden to be carried because 'First Amendment freedoms need breathing space to survive.' (Citations omitted.) Breathing space is especially important in a historical context of harassment based on political belief. Our examination of the treatment historically accorded persons identified with the Communist Party and a survey of statutes still extant reveal that the disclosure sought would have the effect of restraining the First Amendment rights of supporters of the Committee to an extent unjustified by the minimal governmental interest in obtaining the information.

678 F.2d at 421-422.

Commission agreement to the consent decrees granting the previous exemptions to the SWP committees has been based upon the long history of systematic harassment of the SWP and those associating with it and the continuation of harassment. The Commission has required only a "reasonable probability that the compelled disclosure" would result in "threats, harassment, or reprisals from either Government officials or

private parties.” *Buckley*, 424 U.S. at 74. In addition, the Commission has agreed to the application of this standard to both contributors and recipients of disbursements.

The Commission in Advisory Opinions 1996-46 and 1990-13 noted that, in agreeing to the granting of the exemption and its renewal, it considered both “present” and historical harassment. The 1985 Stipulation of Settlement refers to the fact that the Commission had been ordered, “to develop a full factual record regarding the present nature and extent of harassment of the plaintiffs and their supporters resulting from the disclosure provisions.” 1985 Stipulation of Settlement, p. 2. According to the 1985 Stipulation of Settlement, the renewal was based on evidentiary materials regarding the nature and extent of harassment during the previous five years. As referred to above, these two Advisory Opinions based their grant, in part, on the evidence of harassment since 1985. The very nature of the periodic extensions indicates that, after a number of years, it is necessary to reassess the SWP's situation to see if the reasonable probability of harassment still exists.⁵

EXAMINATION OF FACTUAL BACKGROUND

Electoral status of SWP

In the request for the exemption granted in the past two advisory opinions and in your present request, you have presented facts indicating SWP's status as a minor party since its founding in 1938. Despite running a presidential candidate in every election since 1948 and numerous other candidates for Federal, State and local offices, no SWP candidate has ever been elected to public office in a partisan election. You have presented data from the 2000 election indicating very low vote totals for SWP presidential and other Federal candidates.⁶ Further, unlike several other minor parties, you state that SWP has never applied or qualified for national committee status. See 2 U.S.C 431(14) and Advisory Opinions 2001-13, 1998-2, 1995-16 and 1992-30.

⁵ In addition, the courts in *Brown* and *Hall-Tyner* rendered their decisions with reference to recent events or factors, as well as a history of harassment, i.e., recent incidents of harassments against the SWP and extant statutes directed against the Communist Party.

⁶ The evidence you present, as well as information publicly available, indicates that no SWP candidate has come close to winning a Federal election in the six years since the last exemption was granted. SWP candidates for U.S. President received only 8,746 votes nationwide in 1996 and only 10,644 votes nationwide in 2000. Further, no SWP candidates on the ballot for U.S. Senate or House of Representatives received more than 15,000 votes in any election during that period, with the vast majority (thirty-five of thirty-seven candidates) receiving not even 5,000 votes. Additionally, the request provides information of a survey conducted by party leadership of the local campaign committees (of which 17 existed) that supported a candidate in 2000. According to this survey, only 354 people nationwide contributed funds to these committees, for an average of approximately twenty contributors per committee. There was only one contribution nationwide to that committee that was over \$300.

History of government harassment

The request for the exemptions must be seen in the context of the relationship between the SWP and various Federal enforcement authorities, as well as SWP's relationship with other enforcement authorities and private parties. It is against this backdrop that the request and the supporting materials can properly be understood. Advisory Opinions 1996-46 and 1990-13 made reference to the long history of governmental harassment of the SWP. The advisory opinions described FBI investigative activities between 1941 and 1976 that included the extensive use of informants to gather information on SWP activities and on the personal lives of SWP members, warrantless electronic surveillance, surreptitious entry of SWP offices, other disruptive activities including attempts to embarrass SWP candidates and to foment strife within SWP and between SWP and others, and frequent interviews of employers and landlords of SWP members.

The advisory opinions also referred to statements made by Federal governmental officials in several agencies expressing the need for information about the SWP based on the officials' unfavorable perceptions of the SWP. These statements were made in affidavits submitted during 1987 in connection with *Socialist Workers Party v. Attorney General*, 666 F. Supp. 621 (S.D.N.Y. 1987), in which the court granted an injunction preventing the government from using, releasing, or disclosing information on the SWP that was unlawfully obtained or developed from unlawfully obtained material, except in response to a court order or a Freedom of Information Act request. The opinion also discussed incidents of private and local governmental harassment of SWP and those associating with it during the period from 1985 through 1996. These included private threats and acts of violence and vandalism, as well as harassment by local police.

Organization of current evidentiary record

In your current request you present over 80 exhibits including statements from various Party members and candidates, sometimes corroborated by local newspaper articles, police reports, court documents or other materials. The statements come from SWP members from different regions of the United States and are dated from 1997 to 2002. These statements are meant to attest to the hostility directed toward the SWP. They can be divided into three categories: 1) statements attesting to the fear possible SWP supporters have of providing identification when expressing SWP support, 2) statements and material attesting to hostility from private parties to SWP activity, and 3) statements and materials attesting to hostility from law enforcement sources to SWP activities.

Fears expressed by party supporters

The request contains eight statements by SWP officials relating the concerns of potential SWP supporters regarding public identification with SWP. These include statements by the 2000 Presidential and Vice Presidential SWP candidates

describing their experiences while campaigning and talking with potential supporters. It also includes statements from SWP workers who sell subscriptions to SWP newspapers. Several of the statements refer to individuals who expressed reluctance to buy subscriptions for fear of finding their names on lists maintained by enforcement authorities such as the FBI. See Exhibits L, M, and N. Your request also notes the refusal in 1997 of the Seattle Elections Commission to grant an exemption from its reporting requirements.⁷ You provide statements from several SWP workers noting that several long-time contributors expressed reluctance to contribute again because now their names, addresses and professions would be public. See Exhibits H and I.

Harassment and violence from private sources

The largest number of exhibits in the request, over forty, consists of examples of harassment of SWP workers and candidates by private individuals and businesses. These are signed statements by SWP workers and candidates that concern their experiences while giving out SWP literature or selling SWP newspapers or gathering signatures for petitions. They include violence and threats of violence directed toward SWP workers and displays. See, for example, Exhibits 4, 19, 20, and 38. The request also includes well-documented accounts of attacks and vandalism against SWP headquarters and property. See Exhibit 5 (District of Columbia); Exhibit 12 (Houston, Texas); Exhibit 22 (Des Moines, Iowa); and Exhibit 50 (San Francisco, California). Your request also describes the receipt of hostile or threatening email, notes or phone messages at various SWP headquarters. See Exhibits 31, 64, and 74.

Additionally, you provide statements of SWP candidates who faced pressure or hostility at the work place once their employers became aware of their political activities. Some of the exhibits involve situations where rules concerning political activity in the workplace were violated. However, in several situations, employees faced sanctions simply because of their affiliation with SWP or their affirmation of its political beliefs. The most striking and well-documented example was the firing in 2001 of the SWP candidate for mayor of Miami. See Exhibit 15.

Relations with law enforcement authorities

The request also includes 25 exhibits describing interactions between SWP workers and local law enforcement authorities. The majority of these involve police or other law enforcement officials forcing SWP personnel to remove campaign and/or literature tables from streets or sidewalks or to cease the hand distribution of campaign or SWP materials. In one instance, local police charged SWP supporters manning a literature table with disorderly conduct and unlicensed vending. A judge later suspended the charges. See Exhibit 24. It is not certain that animus against SWP was the motivating factor in all these situations since it is not clear whether SWP workers were violating the

⁷ Your request includes a 1998 decision of the Washington State Public Disclosure Commission, which by contrast, granted a reporting exemption to the SWP in regard to statewide activity by its sole statewide candidate.

laws of the localities. Nevertheless, prejudice against SWP is indicated in at least some of exhibits since there are cases where SWP activity was, according to evidence provided along with reports of the incidents, legal or protected within the jurisdiction involved. See Exhibits 25, 40, 41, 55, and 70. In one case, SWP successfully challenged in federal district court the constitutionality of a permit regulation as it was applied to SWP activities. See Exhibit 65.

In Advisory Opinion 1996-46, SWP presented less than a handful of incidents that related to SWP interaction with governmental officials other than local police. In your 2002 request, you present only one such situation. Exhibit 43 describes an individual who, as a SWP member and SWP Presidential elector, applied for a position as a census worker and received a very high score in the Census Bureau's standardized test. The SWP member states that his file was forwarded to the FBI for a security evaluation and that other applicants had their files reviewed by the FBI. You assert that he would have been hired but for the lack of action on his file by the FBI because of its stated inability to locate his file. With respect to the incident, you do not present evidence similar to the affidavits submitted by Federal officials with regard to previous determinations. Consequently, it is difficult to assess whether administrative mischance or actual prejudice played a role in the loss of the file. However, it could be seen as significant, in view of past actions by the FBI with regard to the SWP and its supporters.⁸

ANALYSIS AND CONCLUSIONS

In applying the standard established by the court cases and court decrees described above in determining whether to renew the SWP's partial reporting exemption, the Commission must first determine whether SWP continues to maintain its status as a

⁸ Beginning in 1941, the FBI began a generalized investigation of the SWP that was to last at least until 1976. See Final Report of Special Master Judge Breitel in *Socialist Workers Party v. Attorney General*, 73 Civ. 3160 (TPG) (S.D.N.Y., February 4, 1980). Between the years 1960 and 1976, the FBI employed approximately 1300 informants who reported on the activities, discussions and debates of the SWP. In addition to reporting on what the Special Master described, with some qualifications, as "peaceful, lawful political activity" by the SWP and its adjunct, the Young Socialist Alliance ("YSA"), the informants also provided information as to the names, addresses, places and changes of employment of SWP members, and such personal data as information on "marital or cohabitational status, marital strife, health, travel plans, and personal habits." 642 F. Supp. at 1379-1381.

In the 1960's and 1970's, the SWP was the subject of FBI Counterintelligence Programs "designed to disrupt the SWP on a broad national basis." 642 F. Supp. at 1384. The disruption under these programs included attempts to embarrass SWP candidates, foment racial strife within the SWP, and cause strife between the SWP and others in a variety of political movements. 642 F. Supp. at 1385-1389. For a number of years, the FBI also conducted warrantless electronic surveillance of the SWP on an extensive basis and at least 204 surreptitious entries of SWP offices, principally to photograph or remove documents. The court noted that "there is no indication that the FBI obtained any documents showing any violence or any action to overthrow the Government." 642 F. Supp. at 1394.

Over a period of many years, the FBI maintained a list known successively as the Custodial Detention List, the Security Index, and the Administrative Index. The persons on this list were to be considered for apprehension and detention in time of war or national emergency. The FBI intended to include all SWP members on this list. The list was maintained by frequent interviews of landlords and employers of the members. 642 F. Supp. at 1395.

minor party. *See Buckley*, 424 U.S. at 68-74. As evidenced by low vote totals for SWP candidates and the small total amounts contributed to SWP and committees supporting SWP candidates, the Commission concludes that SWP continues to be a minor party. Having satisfied the minor party threshold, the Commission must balance three factors in analyzing your request. The first is the history of violence or harassment, or threats of violence or harassment, directed at the SWP or its supporters by Federal, state, or local law enforcement agencies or private parties. Second is evidence of continuing violence, harassment, or threats directed at the SWP or its supporters by these same organizations or persons since the last advisory opinion in 1996. These two factors must be balanced against the governmental interest in obtaining the information by determining whether the impact of the activities of the SWP and its supporters in connection with Federal elections is diminished by the low probability of the SWP winning an election. *See Hall-Tyner*, 678 F.2d at 422.

As evidenced by the various court cases and the information submitted in connection with previous advisory opinion requests and described briefly above, there is a long history of threats, violence, and harassment against the SWP and its supporters by Federal, state, or local law enforcement agencies and private parties. There is a sufficient record to establish that this history continues to have a chilling effect on possible membership in or association with SWP. One indication of this is the refusal of individuals to purchase or subscribe to SWP literature or circulations for fear of being included in lists maintained by the government identifying them as SWP supporters. *See Exhibits L, M, and N.*

A review of the information you have presented in connection with this AOR indicates that the SWP and persons publicly associated with it have experienced significant harassment from private sources in the 1997-2002 period. Such harassment appears to have been intended to intimidate the SWP and persons associated with it from engaging in their political activities and in expressing their political views. There is also some evidence of continuing harassment by local police, although here the evidence is not as great as that presented for the harassment from private parties and it is more difficult to evaluate. Based on the evidence presented, the hostility from other governmental sources still exists but continues to abate. As indicated above, massive Federal governmental surveillance and disruption were discontinued well before 1990. The incident involving the census position is difficult to assess without complete information, although it does present at least the possibility of a chilling effect on public association with the SWP. However, as stated above, the history of governmental harassment continues to have a present-day chilling effect that is not diminished by the abatement of governmental harassment.

As noted earlier, it must be stressed that the evidence presented in your request does not need to indicate a certainty that harassment would follow a revocation of the partial reporting exemption. The standard established in Advisory Opinions 1990-13 and 1996-46 and based on the case law cited earlier is that there only be "a reasonable probability that compelled disclosure" would result in "threats, harassment, or reprisals

from *either* Government offices *or* private parties” (emphasis added). The Commission considers the totality of the evidence for the 1997-2002 period, especially the evidence of continued harassment from private parties, and concludes that there is a reasonable probability that contributors to and vendors doing business with SWP and committees supporting SWP candidates would face threats, harassment, or reprisal if their names and information about them were disclosed.

Information provided in your request states that SWP and committees supporting its candidates receive very small total amounts of contributions and very low vote totals in partisan elections in which they are candidates. These low numbers indicate that the activities of SWP, its candidates, and committees supporting its candidates have little, if any, impact on Federal elections. Thus the governmental interest in obtaining the names and addresses of contributors to and vendors doing business with SWP and committees supporting SWP candidates in connection with Federal elections is diminished by the low probability of an SWP candidate winning an election.

As a result of its finding that SWP and the committees supporting SWP candidates have satisfied the factors established in the case law and prior advisory opinions, the Commission grants SWP and the committees supporting SWP candidates a further continuation of the partial reporting exemption provided for in the consent agreements as continued by Advisory Opinions 1990-13, and 1996-46. The condition established by the 1996-46 Opinion will also continue with the partial reporting exemption.⁹

Your request notes that the Act was amended in 1999, 2000, and 2002. You ask that the partial reporting exemption be applied to any new reporting obligations arising from these changes that may require SWP or committees supporting SWP candidates to disclose the names of their contributors and vendors. You identify the amended or new provisions as 2 U.S.C. 434(a)(6)(B) (candidate’s notification of expenditure from personal funds), 434(a)(11)(B) (electronic availability of reports), 434(a)(12) (electronic filing standards), 434(e) (reporting by political committees), 434(f) (electioneering communication disclosure), 434(g) (independent expenditure reporting), and 434(h) (inaugural committee reporting). The Commission agrees that the partial exemption applies to SWP and candidate committees to the extent they are required to report the names of contributors and vendors under the amended or new sections of the Act that you

⁹ Therefore, each unauthorized committee entitled to the exemption should assign a code number to each individual or entity from whom it receives one or more contributions aggregating in excess of \$200 in a calendar year. Similarly, each authorized committee of a SWP candidate should assign a code number to each individual or entity from whom it receives one or more contributions aggregating in excess of \$200 during the election cycle. That code number must be included in FEC reports filed by each committee in the same manner that full contributor identification would otherwise be disclosed. Consistent with the requirement that the committees comply with the recordkeeping provisions of the Act, the committee’s records should correlate each code number with the name and other identifying data of the contributor who is represented by that code.

identify¹⁰ except for 2 U.S.C. 434(a)(6)(B)¹¹ and 434(h).¹² Please note that SWP and the committees supporting SWP candidates must still comply with all other reporting obligations such as electronic filing and reporting their independent expenditures while omitting the names and information concerning contributors, donors and vendors.

Consistent with the length of the exemptions granted in 1990 and 1996, this partial reporting exemption applies to reports covering the next six years, i.e., through December 31, 2008. At least sixty days prior to December 31, 2008, the SWP may submit a new advisory opinion request seeking a renewal of the partial reporting exemption. If a request is submitted, the Commission will consider the factual information then presented as to harassment after 2002, or the lack thereof, and will make a decision at that time as to the renewal.

As in Advisory Opinion 1990-13 and 1996-46, the Commission emphasizes that the committees supporting the Federal candidates of the SWP must still comply with all of the remaining requirements of the Act and Commission regulations. The committees must file reports containing the information required by 2 U.S.C. 434(b) with the exception of the information specifically exempted, and the committees must keep and maintain records as required under 2 U.S.C. 432 with sufficient accuracy so as to be able to provide information, otherwise exempt from disclosure, in connection with a Commission investigation. In addition to complying with the requirements of the consent decrees, the committees must file all reports required under 2 U.S.C. 434(a) in a timely manner. The committees must also comply with the provisions of the Act governing the organization and registration of political committees. *See, e.g.*, 2 U.S.C. 432 and 433. Adherence to the disclaimer provisions of 2 U.S.C. 441d is also required. Finally, the committees must comply with the Act's contribution limitations and prohibitions. 2 U.S.C. 441a, 441b, 441c, 441e, 441f, 441g, 441i, and 441k.

¹⁰ If SWP or any committee supporting its candidates do not qualify as political committees and make an electioneering communication that must be reported under 2 U.S.C. 434(f), they must disclose the name of the broadcaster even though they would be exempt from disclosing names and addresses of donors and all other vendors. Additionally, your request concerns the granting of the partial exemption to both SWP and candidate committees. The partial exemption does not extend to individual SWP members who, as individuals, engage in activity that might require them to file reports of their own, for example, the filing of reports of electioneering communications under 2 U.S.C. 434(f) and independent expenditures under 2 U.S.C. 434(g).

¹¹ If a SWP candidate for the United States House of Representative or United States Senate makes sufficient expenditures from personal funds to require disclosure under 2 U.S.C. 434(a)(6)(B), the candidate must file FEC Form 10. This form does not require the candidate to disclose contributors other than the candidate nor does it require disclosure of vendors and therefore, is beyond the scope of the partial reporting exemption. Additionally, it is important for the SWP candidate to file this FEC Form 10 because it affects the opposing candidates' ability to accept contributions in excess of the contribution limitations under the Millionaires' Amendment at 2 U.S.C. 441a(i) and 441a-1.

¹² If the SWP or any candidate of the SWP is in a position to organize an inaugural committee, the analysis, and therefore the conclusion, of this advisory opinion would no longer be applicable.

This response constitutes an advisory opinion concerning the application of the Act and Commission regulations to the specific transaction or activity set forth in your request. *See* 2 U.S.C. 437f.

Sincerely,

(signed)

Ellen L. Weintraub
Chair

Enclosures: AOs 2001-13, 1998-2, 1996-46, 1995-16, 1992-30 and 1990-13

EXHIBIT D



FEDERAL ELECTION COMMISSION
Washington, DC 20463

March 11, 1997

CERTIFIED MAIL,
RETURN RECEIPT REQUESTED

ADVISORY OPINION 1996-46

Michael Krinsky
Rabinowitz, Boudin, Standard,
Krinsky & Lieberman
740 Broadway at Astor Place
New York, NY 10003-9518

Dear Mr. Krinsky:

This responds to your letter dated November 1, 1996, as supplemented by your letter dated January 13, 1997, requesting an advisory opinion concerning the application of the Federal Election Campaign Act of 1971, as amended ("the Act"), and Commission regulations to the continuation of a partial reporting exemption for the Socialist Workers Party National Campaign Committee and committees supporting candidates of the Socialist Workers Party ("SWP").

The SWP National Campaign Committee and committees supporting SWP candidates were first granted a partial reporting exemption in a consent decree, dated January 2, 1979, that resolved *Socialist Workers 1974 National Campaign Committee v. Federal Election Commission*, Civil Action No. 74-1338 (D.D.C.). In that case, such committees brought an action for declaratory, injunctive and affirmative relief, alleging that specific disclosure sections of the Act operated to deprive them and their supporters of rights guaranteed by the First Amendment to the Constitution because of the likelihood of harassment resulting from such disclosure. The decree required the committees supporting SWP candidates to maintain records in accordance with the Act and to file reports in a timely manner. It also, however, exempted the committees from the provisions requiring the disclosure of the names, addresses, occupations, and principal places of business of contributors to SWP committees; of political committees or candidates supported by SWP committees; of lenders, endorsers or guarantors of loans to the SWP committees; and of persons to whom the SWP committees made expenditures.¹ The decree stated that its provisions would extend to the end of 1984, and set out a procedure for the SWP committees to apply, prior to that date, for a renewal of the exemptions.

On July 24, 1985, the court approved an updated settlement agreement with the same requirements and partial reporting exemption.² The court decree extended the exemption until the end of 1988, and again set out a renewal procedure. The SWP missed the deadline for reapplication for the exemption. In lieu of a renewal obtained from the court, the committees, in July 1990, sought a determination from the Commission of entitlement to the partial reporting exemption through the advisory opinion process.

On August 21, 1990, the Commission issued Advisory Opinion 1990-13, which granted the same exemption provided for in the previous consent decrees. The opinion provided that the exemption would last through the next two presidential election cycles, i.e., through December 31, 1996. The SWP committees could seek a renewal of the exemption by submitting an advisory opinion request by November 1, 1996, that would present information as to harassment of the SWP, or persons associated with the SWP, during the 1990-1996 period. Advisory Opinion 1990-13. The Commission received your request for a renewal on that date. You have asked that the exemption period last through the next two presidential election cycles, i.e., until December 31, 2004.

I. Applicable Law

The Act requires political committees to file reports with the Commission that identify individuals and other persons who make contributions over \$200, or who come within various other disclosure categories listed above in reference to the consent agreements. 2 U.S.C. 434(b)(3), (5), and (6). See also 2 U.S.C. 431(13). The United States Supreme Court, however, in *Buckley v. Valeo*, 424 U.S. 1 (1976), recognized that, under certain circumstances, the Act's disclosure requirements as applied to a minor party would be unconstitutional because the threat to the exercise of First Amendment rights resulting from disclosure would outweigh the insubstantial interest in disclosure by that entity. 424 U.S. at 71-72. Asserting that "[m]inor parties must be allowed sufficient flexibility in the proof of injury to assure a fair consideration of their claim" for a reporting exemption, the Court stated that "[t]he evidence offered need show only a reasonable probability that the compelled disclosure of a party's contributors' names will subject them to threats, harassment, or reprisals from either Government officials or private parties." 424 U.S. at 74. The Court elaborated on this standard, stating:

The proof may include, for example, specific evidence of past or present harassment of members due to their associational ties, or of harassment directed against the organization itself. A pattern of threats or specific manifestations of public hostility may be sufficient. New parties that have no history upon which to draw may be able to offer evidence of reprisals and threats directed against individuals or organizations holding similar views.
424 U.S. at 74.

The Court reaffirmed this standard in *Brown v. Socialist Workers '74 Campaign Committee (Ohio)*, 459 U.S. 87 (1982), granting the SWP an exemption from state campaign disclosure requirements. The Court referred to the introduction of proof of specific incidents of private and government hostility toward the SWP and its members within the four years preceding the trial in that case. The Court also referred to the long history of Federal governmental surveillance and disruption of the SWP until at least 1976. 459 U.S. at 99-100. Noting the appellants' challenge to

the relevance of evidence of Government harassment "in light of recent efforts to curb official misconduct," the Court concluded that "[n]otwithstanding these efforts, the evidence suggests that hostility toward the SWP is ingrained and likely to continue." 459 U.S. at 101.

The Court in *Brown* also clarified the extent of the exemption recognized in *Buckley*, stating that the exemption included the disclosure of the names of recipients of disbursements as well as the names of contributors. The Court characterized the view that the exemption pertained only to contributors' names as "unduly narrow" and "inconsistent with the rationale for the exemption stated in *Buckley*." 459 U.S. at 95.

The United States Court of Appeals for the Second Circuit used the *Buckley* standard as a basis for exempting the campaign committee of the Communist Party presidential and vice presidential candidates from the requirements to disclose the identification of contributors and to maintain records of the name and addresses of contributors. *Federal Election Commission v. Hall-Tyner Election Campaign Committee*, 678 F.2d 416 (2d Cir. 1982), *cert. denied*, 459 U.S. 1145 (1983). The court described the applicability of the standard, stating:

[W]e note that *Buckley* did not impose unduly strict or burdensome requirements on the minority group seeking constitutional exemption. A minority party striving to avoid FECA's disclosure provisions does not carry a burden of demonstrating that harassment will certainly follow compelled disclosure of contributors' names. Indeed, when First Amendment rights are at stake and the spectre of significant chill exists, courts have never required such a heavy burden to be carried because 'First Amendment freedoms need breathing space to survive.' (Citations omitted.) Breathing space is especially important in a historical context of harassment based on political belief. Our examination of the treatment historically accorded persons identified with the Communist Party and a survey of statutes still extant reveal that the disclosure sought would have the effect of restraining the First Amendment rights of supporters of the Committee to an extent unjustified by the minimal governmental interest in obtaining the information. 678 F.2d at 421-422.

Commission agreement to the consent decrees granting the previous exemptions to the SWP committees has been based upon the long history of systematic harassment of the SWP and those associating with it and the continuation of harassment. The Commission has required only a "reasonable probability that the compelled disclosure" would result in "threats, harassment, or reprisals from either Government officials or private parties." *Buckley*, 424 U.S. at 74. In addition, the Commission has agreed to the application of this standard to both contributors and recipients of disbursements.

Advisory Opinion 1990-13 noted that, in agreeing to the granting of the exemption and its renewal, the Commission had considered both "present" and historical harassment. The 1979 Stipulation of Settlement refers to the fact that the Commission had been ordered "to develop a full factual record regarding the present nature and extent of harassment of the plaintiffs and their supporters resulting from the disclosure provisions." According to the 1985 Stipulation of

Settlement, the renewal was based on evidentiary materials regarding the nature and extent of harassment during the previous five years. As referred to above, Advisory Opinion 1990-13 based its grant on the evidence of harassment since 1985. The very nature of the periodic extensions indicates that, after a number of years, it is necessary to reassess the SWP's situation to see if the reasonable probability of harassment still exists.³

II. *Facts Presented*

In the request for the exemption granted in Advisory Opinion 1990-13 and in your present request, you have presented facts indicating SWP's status as a minor party since its founding in 1938. Despite running a presidential candidate in every election since 1948 and numerous other candidates for Federal, state, and local offices, no SWP candidate has ever been elected to public office in a partisan election. You have presented data from the 1992 and 1994 elections indicating very low vote totals for SWP presidential and senatorial candidates.

Advisory Opinion 1990-13 discusses the long history of governmental harassment of the SWP. The opinion describes FBI investigative activities lasting from 1941 to 1976 that included the extensive use of informants to gather information on SWP activities and on the personal lives of SWP members, warrantless electronic surveillance, surreptitious entry of SWP offices, other disruptive activity, including attempts to embarrass SWP candidates and to foment strife within the SWP and between the SWP and others, and frequent interviews of employers and landlords of SWP members.⁴

The advisory opinion also referred to statements made by Federal governmental officials in several agencies expressing the need for information about the SWP based on the officials' unfavorable perceptions of the SWP. These statements were made in affidavits submitted during 1987 in connection with *Socialist Workers Party v. Attorney General*, 666 F. Supp. 621 (S.D.N.Y. 1987), in which the court granted an injunction preventing the government from using, releasing, or disclosing information on the SWP unlawfully obtained or developed from unlawfully obtained material, except in response to a court order or an FOIA request.⁵

The opinion also discussed incidents of private and local governmental harassment of the SWP and those associating with it during the period from 1985 through the beginning of 1990. These included private threats and private acts of violence and vandalism, as well as harassment by local police.

As evidence of continuing private and governmental harassment of the SWP and those associated with the SWP during the 1990-1996 period, you have provided descriptions with supporting signed declarations or other documentation as to approximately 70 incidents. Incidents of harassment from private sources included (but were not limited to) acts of vandalism against SWP offices and SWP-related bookstores; threats and acts of violence from persons identifying themselves as members of the Ku Klux Klan; threats and acts of violence by anti-Castro activists; negative actions by, or statements from, employers against persons apparently as a result of those persons' association with the SWP; and abusive behavior toward SWP candidates or other persons publicly associating with the SWP.

Specific examples of the above-described activities area as follows: (1) The windows of SWP headquarters in Detroit, St. Louis, Kansas City, and Chicago were broken, in two cases from thrown objects (a piece of asphalt and a rock). A bullet was fired through the window of the Des Moines headquarters in 1992. A swastika and a "White Power" slogan were spray-painted on the building that housed SWP offices and the Pathfinder bookstore in Birmingham (AL) in 1991. (2) In 1994, the SWP office in Philadelphia (PA) received an abusive letter that was clearly intended to intimidate from a person representing himself as the Grand Dragon of the Pennsylvania KKK (with letterhead stating "The Revolutionary Knights of the Ku Klux Klan," and a mailing address of the state headquarters, as well as a card with the same information). In 1990 and 1991, threatening phone messages were left on the SWP answering machine in Greensboro (NC) by persons identifying themselves as with the KKK. In 1991, two threatening stickers, one purportedly from the KKK, were placed on the entrances of the SWP's Greensboro offices. (3) Anti-Castro activists in Miami overturned SWP informational tables in Miami in 1993 and 1996, and physically assaulted SWP personnel at informational tables in New Jersey in 1995 and 1993. The SWP headquarters in Miami received a number of threatening phone calls in Spanish after radio appearances by SWP candidates in 1993.⁶ (4) In 1995, a woman, who was a politically active socialist and had been an SWP congressional candidate, was denied employment at a mine in Utah. The Employee Relations Director had informed her of his investigation of her socialist political activities, and they appear to have been a disqualifying factor. (5) In several cities, individuals who were known as SWP supporters were subject to insults, written threats, and vandalism, from co-workers, related to their political stances and activities.

Your request includes descriptions and documentation of approximately 20 incidents involving police interactions with SWP workers. Many of these incidents entailed demands by police to remove informational tables or to cease other activities involving petition-signing or the distribution of printed materials in public places. The police would assert that the SWP workers were obstructing pedestrian traffic or acting without a permit or peddler's license. They would sometimes arrest or give citations to the SWP workers. In almost all of those cases, the local prosecutor would drop the charges or the cases would be dismissed. These incidents sometimes appear to involve actions by the police that were apparently motivated by a hostile feeling toward the SWP or the views expressed by the SWP.

Two examples of these cases are as follows: (1) In 1996, three SWP workers who were petitioning for the placement of SWP candidates for president and vice president on the state ballot were taken to the police station by the New York City Parks Department Police and charged with unlawful solicitation and illegal assembly. Their materials, including the petitions, were held by the police for a week and returned after protests by NYCLU and the SWP. The charges were later dismissed in court. (2) According to a 1991 letter from counsel for the New Jersey chapter of the ACLU to the Newark Corporation Counsel, three policemen, two of them mounted, intimidated SWP workers who had set up a literature table outside of local SWP headquarters. The officers blocked access to the table and the book store for over one-half hour and threatened and verbally abused the workers (including comments related to their political views). The workers decided to take down the table.

You present only a few incidents that relate to SWP interaction with governmental officials other than local police. The two most significant events relate to the job status of SWP members: (1) A

civilian employee at the Alameda Naval Aviation Depot was investigated by the Office of Special Counsel (OSC) for violations of the Hatch Act because he ran for the San Francisco Board of Supervisors in 1992, distributed campaign literature for candidates running in partisan elections, and held positions in the SWP. Although candidates for the Board of Supervisors did not run under party labels, OSC noted that the employee accepted the endorsement and support of the SWP. Even though OSC concluded that violations occurred, it decided not to seek disciplinary action against the employee while noting that subsequent violations would be considered knowing and willful. The employee maintained that he should not have been considered a partisan candidate, that the investigation occurred only after his superiors at Alameda became concerned with the content of his views, and that other employees thought to have violated the Hatch Act were merely warned without a referral to OSC. (2) In 1991, the security clearance of an Air Force enlisted man was suspended, and he was transferred from his job as a computer programmer with the nuclear targeting staff to a job as a clerk at the base housing office. The airman was a member of the SWP's affiliate, the Young Socialist Alliance (YSA). The suspension occurred on the day he returned to work from a YSA convention. A subsequent Air Force letter notified the airman of the opening of a security investigation (to resolve the question of his clearance) based on his involvement in socialist organizations, unreported contact with a foreign national (referring to contact at the convention), and perceived questionable loyalty, honesty, and reliability in his previous workcenter. In reply to this letter, the airman disputed the charge as to the foreign national and noted his favorable reviews by supervisors and his initiative on the job. The airman resigned before the end of the investigation as a result of his inability to obtain a promotion in the field under which he enlisted, which would have required regaining his security clearance.

A review of the information presented by you indicates that the SWP and persons publicly associated with it have experienced a significant amount of harassment from private sources in the 1990-1996 period. Such harassment appears to have been intended to intimidate the SWP and persons associated with it from engaging in their political activities and in expressing their political views. There is also evidence of continuing harassment by local police, similar to incidents discussed in the 1990 opinion.

Based on the evidence presented, the hostility from other governmental sources appears to have abated. As indicated above, massive Federal governmental surveillance and disruption was discontinued well before 1990. Moreover, you do not present evidence similar to the affidavits filed by Federal officials in 1987, referred to above, indicating negative attitudes toward the SWP and the need to gather information on it. The incidents involving the naval employee and the airman are difficult to assess without complete information, although the airman's situation presents the possibility of a chilling effect on public association with the SWP.

Nevertheless, the continuation of harassment from private and local police sources during the 1990-1996 period, coupled with the long history of harassment of the SWP, is still sufficient evidence that there is a reasonable probability that the compelled public disclosure of previously exempted information will subject the persons in the exempted categories to threats or harassment from various sources. The Commission, therefore, grants the committees supporting the candidates of the SWP the exemption provided for in the consent agreements and in Advisory Opinion 1990-13, with one new condition described below. Consistent with the length

of the exemption granted in 1990, this exemption is to last for the reports covering the next six years, i.e., through December 31, 2002.⁷ At least sixty days prior to December 31, 2002, the SWP may submit a new advisory opinion request seeking a renewal of the exemption. If a request is submitted, the Commission will consider the factual information then presented as to harassment after 1996, or the lack thereof, and will make a decision at that time as to the renewal.

As in Advisory Opinion 1990-13, the Commission emphasizes that the committees supporting the Federal office candidates of the SWP must still comply with all of the remaining requirements of the Act and Commission regulations. The committees must file reports containing the information required by 2 U.S.C. 434(b) with the exception of the information specifically exempted, and the committees must keep and maintain records as required under 2 U.S.C. 432 with sufficient accuracy so as to be able to provide information, otherwise exempt from disclosure, in connection with a Commission investigation. In addition to complying with the requirements of the decrees, the committees must file all reports required under 2 U.S.C. 434(a) in a timely manner. The committees must also comply with the provisions of the Act governing the organization and registration of political committees. See, e.g., 2 U.S.C. 432 and 433. Adherence to the disclaimer provisions of 2 U.S.C. 441d is also required. Finally, the committees must comply with the Act's contribution limitations and prohibitions. 2 U.S.C. 441a, 441b, 441c, 441e, 441f, and 441g.

As indicated above, the Commission adds one new condition to the reporting requirements. In partial reporting exemptions granted to an SWP campaign committee and various SWP candidates for state or local office, the agencies administering campaign disclosure in the States of Washington and Iowa have required that the committees assign a code number to each contributor whose name and address is not being disclosed. The Iowa agency required that the committee keep books and records that would correlate the code numbers with the names and contributions. The Commission believes that a requirement of assigning a code number for each contributor and reporting that code number when disclosing a contribution by that person would enable a reviewer of that report (i.e., either the Commission staff or a member of the public) to determine whether contributions in excess of the limits of 2 U.S.C. 441a are being made. At the same time, such a requirement would not diminish the anonymity that is already given to contributors under Advisory Opinion 1990-13 and the consent decrees. Therefore, each committee entitled to the exemption should assign a code number to each individual or entity from whom it receives one or more contributions aggregating in excess of \$200 in a calendar year. That code number must be included in FEC reports filed by each committee in the same manner that full contributor identification would otherwise be disclosed. Consistent with the requirement that the committees comply with the recordkeeping provisions of the Act, the committee's records should correlate each code number with the name and other identification data of the contributor who is represented by that code.

This response constitutes an advisory opinion concerning application of the Act, or regulations prescribed by the Commission, to the specific transaction or activity set forth in your request. See 2 U.S.C. 437f.

Sincerely,

(signed)

John Warren McGarry
Chairman

Enclosure (AO 1990-13)

1 Nevertheless, the agreement also stated that if the Commission found reason to believe that the committees violated a provision of the Act, other than those for which an exemption was specified, but needed the withheld information in order to proceed, the Commission could apply to the court for an order requiring the production of such information.

2 In view of the specific provisions of the 1979 amendments to the disclosure provisions, the agreement also makes reference to an exemption for reporting the identification of persons providing rebates, refunds or other offsets to operating expenditures, and persons providing any dividend, interest or other receipt.

3 In addition, the courts in *Brown and Hall-Tyner* rendered their decisions with reference to recent or current events or factors, as well as a history of harassment, i.e., recent incidents of harassment against the SWP and extant statutes directed against the Communist Party.

4 As noted in the opinion, these activities were set out in the Final Report of Special Master Judge Breitel in *Socialist Workers Party v. Attorney General*, 73 Civ. 3160 (TPG) (S.D.N.Y., February 4, 1980) and in *Socialist Workers Party v. Attorney General*, 642 F. Supp. 1357 (S.D.N.Y. 1986), a case in which the Federal District Court awarded judgment against the United States under the Federal Tort Claims Act for disruption activities, surreptitious entries, and use of informants by the FBI.

5 See Advisory Opinion 1990-13 for a further discussion of the implications of the unfavorable statements.

6 You also provide a declaration from an SWP congressional candidate from Florida who noted that some of her airline co-workers asked that SWP newspapers not be delivered to their homes and that they be hand-delivered at work instead, or that the newspapers be mailed in envelopes.

7 As stated above, you have asked for an exemption period that is similar to the previous period because that period was to last through the next two presidential election cycles. Nevertheless, the more important aspect of this exemption is the actual length of time, and that is why six years, not eight, is being granted. Moreover, in view of the apparent abatement in governmental harassment, a longer time interval between the dates when the Commission reviews its grant of the partial exemption is unwarranted.

EXHIBIT E



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 be 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).

UNLEASHED AND UNACCOUNTABLE

The FBI's Unchecked Abuse of Authority



September 2013



Table of Contents

Executive Summary	i
Introduction	1
I. Tension Between Domestic Intelligence and Constitutional Rights.....	2
II. Unleashed: The New Post-9/11 Powers	4
A. Surveillance Powers, Given and Taken	4
1. USA Patriot Act	4
2. Exigent Letters and a Secret OLC Opinion	7
3. Warrantless Wiretapping and the FISA Amendments Act	8
B. Expanding FBI Investigative Authorities	9
1. Ashcroft Attorney General’s Guidelines	9
2. Evidence of FBI Spying on Political Activists	10
3. 2010 Inspector General Report Confirms Spying and Lying	11
4. Mukasey Attorney General’s Guidelines	12
C. FBI Profiling Based on Race, Ethnicity, Religion, and National Origin	13
1. The FBI Domestic Operations and Investigations Guide	14
2. Racial and Ethnic Mapping	15
3. Innocent Victims of Aggressive Investigation and Surveillance	18
D. Unrestrained Data Collection and Data Mining	19
1. eGuardian and “Suspicious” Activity Reports	19
2. Mining Big Data: FTTTF, IDW, and NSAC	20
3. Real Threats Still Slipping Through the Cracks	23
4. Mining Bigger Data: the NCTC Guidelines	27
5. Exploitation of New Technologies	28

6. Secret Spying and Secret Law	28
III. Unaccountable: Evidence of Abuse, Need for Reform	29
A. Shirking Justice Department Oversight	29
B. Suppressing Whistleblowers	30
C. Circumventing External Controls	32
1. Targeting Journalists	32
2. Thwarting Congressional Oversight	33
3. Thwarting Public Oversight with Excessive Secrecy	34
IV. Targeting First Amendment Activity	36
A. Biased Training	36
B. Targeting AMEMSA Communities	39
C. Targeting Activists	41
V. Greater Oversight Needed: The FBI Abroad	43
A. Proxy Detentions	43
B. FBI Overseas Interrogation Policy	45
C. Use of No-fly List to Pressure Americans Abroad to Become Informants	46
VI. Conclusion and Recommendations	48

Executive Summary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

I. Tension Between Domestic Intelligence Activities and Constitutional Rights

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

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

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

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

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

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

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

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

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

A. Surveillance Powers Given and Taken

1. USA Patriot Act

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

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

The Washington Post reported that tens of millions of Verizon customers' records have been seized under this program, and Sen. Dianne Feinstein (D-Calif.) said this order appeared to be "the exact three-month renewal" of similar orders that began in 2006.¹³ With over 200 Section 215 orders issued in 2012, it is very likely that many other telecommunications companies received similar requests for all their customers' metadata as well.¹⁴ And since Section 215 authorizes the government to obtain "any tangible things," it is also likely that the FBI uses the provision to do bulk collection of other types of records. The statute specifically states that FBI agents may seek library circulation and book sales records, medical records, tax returns, and firearms sales records using Section 215, with approval of an FBI Executive Assistant Director.¹⁵

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

[Section 215] allows us to go to the FISA Court and obtain an order to produce records that may be relevant to, say, a foreign intelligence investigation relating to somebody who's trying to steal our secrets or a terrorist. Upon us showing that the records sought are relevant to this particular investigation—a specific showing it is—the FISA Court would issue an order allowing us to get those records. It's been used over 380 times since 2001.¹⁷

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

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

Sen. Wyden and Sen. Mark Udall (D-Colo.) have repeatedly complained over the last several years that Justice Department officials have made misleading public statements about the scope of this authority, even as they refused their demands to declassify this secret interpretation of law so that Americans could understand how the government is using Section 215.¹⁹ It took an unauthorized leak of the FISA Court order to give the public — and many members of Congress — their first glimpse of the government’s overbroad use of this Patriot Act authority.

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

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

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

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

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

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

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

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

2. Exigent Letters and a Secret OLC Opinion

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

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

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

3. Warrantless Wiretapping and the FISA Amendments Act

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

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

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

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

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

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

B. Expanding FBI Investigative Authorities

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

1. Ashcroft Attorney General's Guidelines

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

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

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

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

2. Evidence of FBI Spying on Political Activists

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

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

Rocky Mountain Peace and Justice Center in Colorado, and the Thomas Merton Center for Peace and Justice in Pennsylvania, among many others. In a document that reads as if it were written during the Hoover era, an FBI agent describes the peace group Catholic Worker as having “semi-communistic ideology.”⁵⁸ Environmental activist and self-described anarchist Scott Crow later submitted his own Privacy Act request to the FBI and received 440 pages of materials documenting FBI surveillance directed against him from 2001 through 2008.⁵⁹ The FBI reports exposed the agents’ disdain for the activists they investigated, with one suggesting that non-violent direct action was an “oxymoron” and another stating that attendees at an activist camp “dressed like hippies” and “smelled of bad odor.”⁶⁰

3. 2010 Inspector General Report Confirms Spying and Lying

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

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

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

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

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

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

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

4. Mukasey Attorney General's Guidelines

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

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

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

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

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

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

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

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

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

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

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

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

1. The FBI Domestic Investigations and Operations Guide

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

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

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

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

The FBI unilaterally amended the DIOG in October 2011, giving its agents powers that are not authorized in the current Attorney General's Guidelines issued in 2008.⁸⁸ These new powers include blanket permission for agents to search law enforcement and commercial databases without even opening an assessment on the person searched or documenting why the search was performed. The 2011 DIOG amendments also authorized FBI agents to search peoples' trash during an assessment to find derogatory information to pressure them into becoming informants. Since the 2008 Attorney General's Guidelines did not grant these powers, it is difficult to see where the FBI finds authorization for these activities.

The FBI secretly amended the DIOG again in June 2012.⁸⁹ Only one section of this new guide has been released, pursuant to an ACLU FOIA request regarding the FBI's policy for obtaining stored e-mails. One substantive change from the 2011 DIOG removes the requirement for FBI agents to specify in affidavits submitted to judges for criminal wiretap warrants whether the interception implicates sensitive circumstances, such as whether it targets public officials or religious leaders.⁹⁰ A new subsection requires the agents to discuss the sensitive circumstances with Justice Department prosecutors, but failing to advise the judge evaluating the warrant request would seem to improperly withhold potentially important information that could impact the probable cause determination. It is unknown why this change was made.

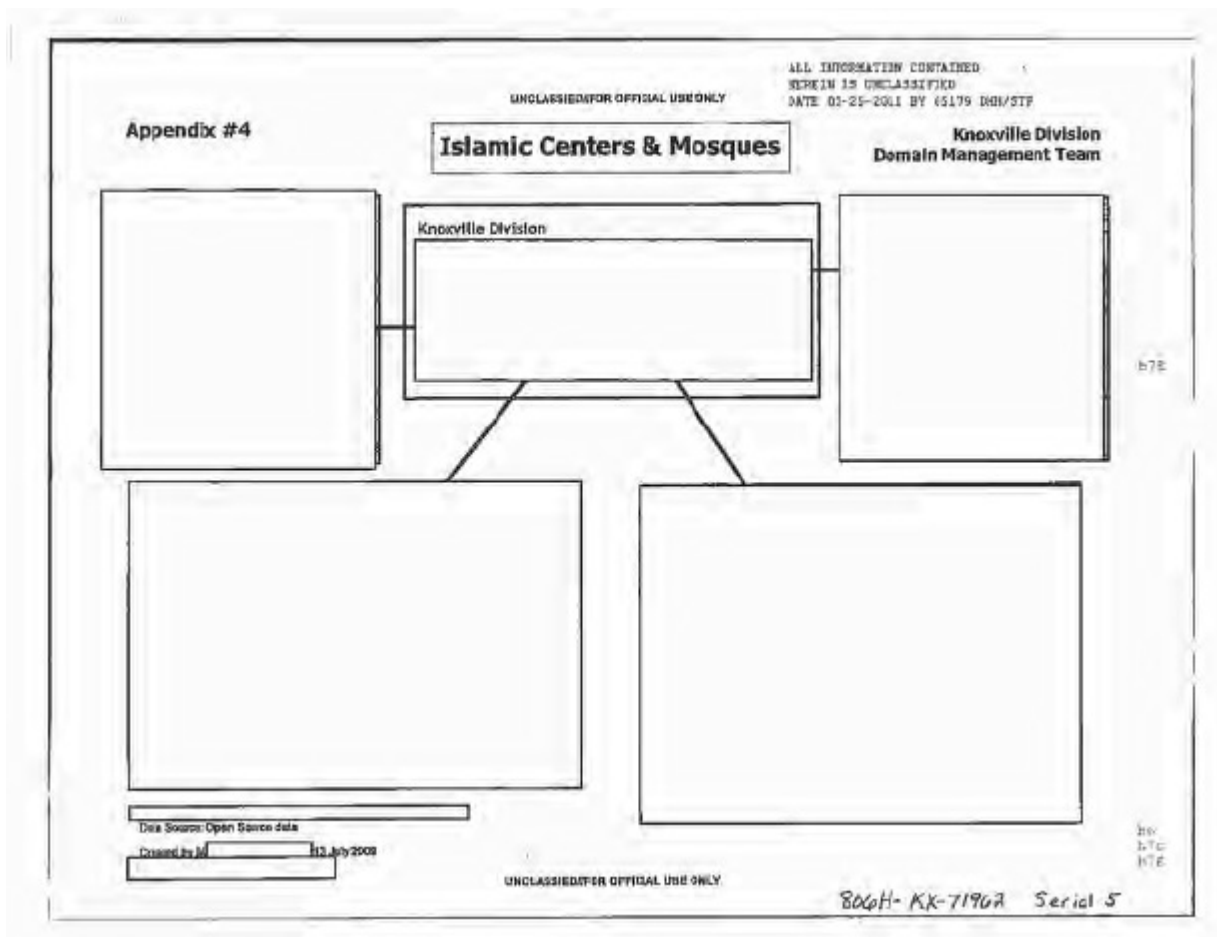
2. FBI Racial and Ethnic Mapping

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

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

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

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



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

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

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

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

3. Innocent Victims of Aggressive Investigation and Surveillance

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

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

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

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

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

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

D. Unrestrained Data Collection and Data Mining

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

1. eGuardian and Suspicious Activity Reports

In 2009, the FBI established a new database called eGuardian to collect reports of “suspicious” behavior generated by state and local law enforcement agencies¹⁰⁶ to be shared broadly with other federal law enforcement agencies, the Department of Homeland Security, and the intelligence community.¹⁰⁷ Like many other suspicious activity reporting (SAR) programs, the standards governing the definition of “suspicious” conduct for reporting to eGuardian are extremely vague and over-broad, making it likely that reports will be based on racial or religious profiling or other bias, rather than objectively reasonable indications of wrongdoing.

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

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

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

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

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

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

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

2. Mining Big Data

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

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

But the FBI had even bigger plans. In 2007, it submitted a budget request seeking \$100 million over three years to establish the National Security Analysis Center, which would combine the Tracking Task Force with the largest FBI data set, the Investigative Data Warehouse.¹²⁴ The Investigative Data Warehouse contains all intelligence and investigative data collected by the FBI across all of its programs, along with “other government agency data and open source news feeds.”¹²⁵ This data includes, for example, well over a million suspicious activity reports filed by financial institutions each year as required by the Bank Secrecy Act, which was expanded by the Patriot Act to include car dealerships, casinos, pawn shops, and even the post office.¹²⁶ The FBI ingests this data directly from the Treasury Department for inclusion in the Investigative Data Warehouse, along with an additional 14 million currency transaction reports submitted annually to document cash transactions over \$10,000.¹²⁷

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

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

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

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

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

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

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

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

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

3. Real Threats Still Slipping Through the Cracks

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

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

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

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

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

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

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

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

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

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

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

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

Perhaps even more troubling, recent media reports indicate Tsarnaev may be implicated in a grisly triple murder in Waltham, Mass., on September 11, 2011, which occurred after the FBI assessment ended but before Tsarnaev travelled to Russia in January 2012.¹⁶⁰ Tsarnaev's potential involvement in serious criminal activity years before the Boston bombing raises additional questions for policymakers about the appropriate distribution of law enforcement resources. According to FBI crime data, in 2011 less than half of the 1.2 million violent crimes in the U.S. were solved through arrest or positive identification of the perpetrator.¹⁶¹ Included in these unsolved crimes were over a third of the murders committed in 2011 and over 58 percent of the forcible rapes.¹⁶² These numbers have remained fairly consistent over the last several years, even as intelligence activities directed against innocent Americans have increased. It is important to recognize that terrorism is a heinous crime with serious emotional and economic consequences, but it is still worth examining whether diverting the resources currently spent on

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

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

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

4. Mining Bigger Data: The NCTC Guidelines

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

5. Exploitation of New Technologies

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

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

6. Secret Spying and Secret Law

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

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

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

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

III. Unaccountable: Evidence of Abuse, Need for Reform

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

A. Shirking Justice Department Oversight

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

The 2008 report on Section 215 of the Patriot Act revealed a troubling incident in which the Foreign Intelligence Surveillance Court rejected an FBI request for a Section 215 order on First Amendment grounds, but the FBI General Counsel ignored this opinion and authorized the issuance of NSLs, which do not require judicial approval, to obtain the same information.¹⁷⁴ That a high-level FBI official would demonstrate such disdain for the court and the law is particularly troubling. The IG also concluded the FBI did not yet fully implement the recommended reforms from 2007, and that it was “too soon to definitively state whether the new system of controls... will eliminate fully the problems with the use of NSLs.”¹⁷⁵ Despite these reports of abuse, Congress failed to narrow the FBI’s powers, or even obtain a public explanation of the government’s interpretation of the scope of its authorities, when the Patriot Act was reauthorized in 2011.¹⁷⁶

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

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

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

B. Suppressing Government Whistleblowers

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

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

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

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

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

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

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

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

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

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

B. Circumventing External Controls

1. Targeting Journalists

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

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

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

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

2. Thwarting Congressional Oversight

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

When Congress debated the first Patriot Act reauthorization in April 2005, FBI Director Robert Mueller testified that he was unaware of any “substantiated” allegations of abuse of Patriot Act authorities.¹⁹⁹ The 2007 IG audit later revealed the FBI self-reported 19 Patriot Act-related violations of law or policy to the Intelligence Oversight Board between 2003 and 2005.²⁰⁰ Though misleading, this testimony was technically accurate because President Bush’s Intelligence Oversight Board did not meet to “substantiate” any reported violations until the spring of 2007.²⁰¹

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

In an FBI oversight hearing in 2008, the late Sen. Arlen Specter criticized FBI Director Mueller for not having told him that President Bush authorized the National Security Agency to eavesdrop on Americans’ communications in violation of the Foreign Intelligence Surveillance Act in 2001.²⁰⁵ Sen. Specter, who had oversight responsibility over the FBI as the Senate Judiciary Committee’s Chairman or Ranking Member during the four years the secret program operated, complained that he only learned about the warrantless wiretapping program when it

appeared in *The New York Times* in late 2005.²⁰⁶ Sen. Specter pointed out that because Director Mueller knew about the program, and knew that the Intelligence Committees had not been briefed as required by the National Security Act of 1947, he had a responsibility to report it. Mueller responded that he “was of the belief that those who should be briefed in Congress were being briefed.”²⁰⁷ Sen. Feinstein, who served on both the Intelligence and Judiciary Committees, said Mueller’s comment that members were fully briefed was “simply not accurate.”²⁰⁸

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

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

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

3. Thwarting Public Oversight with Excessive Secrecy

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

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

judges that are only ever seen by the government agents and telephone and Internet service providers that execute the orders. Judge Smith estimates that magistrate judges seal around 30,000 ECPA orders annually. While these seals are supposed to be temporary, they often effectively become permanent due to inaction by the government.²¹³ In a study in his own division, Judge Smith determined that 99.8 percent of sealed orders from 1995 through 2007 remained sealed in 2008.²¹⁴ Magistrate judges are given little judicial guidance on how to address these requests for secrecy. Because these orders remain sealed they cannot be challenged by the subjects of the surveillance, which in turn deprives the magistrate judges of appellate court decisions that would provide guidance on how to interpret ECPA's complex provisions when evaluating future government secrecy demands under the statute.²¹⁵ The result is less public oversight of law enforcement surveillance activities.

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

Monteilh exposed his role as an FBI informant to the Los Angeles Times in 2009.²²¹ The ACLU of Southern California, the Council on American Islamic Relations of Greater Los Angeles, and the law firm Hadsel, Stormer, Keeny, Richardson & Renick LLP initiated a class action law suit against the FBI on behalf of Southern California Muslims. The suit alleges the FBI unlawfully targeted people based on their religious beliefs in violation of the First Amendment, retained information about their religious practices in FBI files in violation of the Privacy Act, and conducted unreasonable searches in violation of the Fourth Amendment.²²²

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

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

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

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

IV. Targeting First Amendment Activity

A. Biased training

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

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

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

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

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


- Wearing traditional Muslim attire
- Growing facial hair
- Frequent attendance at a mosque or prayer group
- Travel to a Muslim country
- Increased activity in a pro-Muslim social group or cause
- Proselytizing²³¹

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

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

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


But biased training materials were not limited to erroneous information about Muslims. FBI domestic terrorism training presentations on “Black Separatist Extremists” juxtaposed decades-old examples of violence by the Black Panthers and the Black Liberation Army with unorthodox beliefs expressed by a number of different modern groups to suggest, without evidence, that these latter-day groups pose a similar threat of violence.²³⁶ The FBI presentation claims organizations it calls “Black Separatists” have no unifying theme or mission, but “all share racial grievances against the U.S., most seek restitution, or governance base [sic] on religious identity or social principals [sic].”²³⁷ No recent acts of “Black Separatist” terrorism appear in the presentations or in FBI lists of terrorism incidents going back to 1980.²³⁸ FBI domestic terrorism training presentations on “Anarchist Extremists” claim they are “not dedicated to any cause” and merely “criminals seeking an ideology to justify their activities,” yet focus heavily on protest activity, including “‘passive’ civil disobedience.”²³⁹ FBI training presentations on “Animal Rights/Environmental Extremism” list “FOIA Requests” as examples of “Intelligence Gathering,” and another presentation suggests activists are waging a “public relations war.”²⁴⁰




Animal Rights/Eco Extremism Strategy

Public Relations War

- Media is vital part of every action
- Media sometimes slanted in favor of activists
- Celebrities support & fund AR/Eco movement
- Activists spin the truth



UNCLASSIFIED



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

B. Targeting AMEMSA Communities

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Targeting Activists

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

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

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

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

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

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

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

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

V. Greater Oversight Needed: The FBI Abroad

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

A. Proxy Detention

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

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

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

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

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

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

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

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

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

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

B. FBI Overseas Interrogation Policy

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

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

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

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

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

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

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

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

This is particularly true for the No Fly List, which is the smallest subset of the FBI’s massive Terrorist Screening Center watch list (affecting about 21,000 of the 875,000 people on the larger list), but also the most liberty infringing because it bars air travel to or within the U.S.²⁸⁵ The GAO reported in 2012 that the number of U.S. persons on the No Fly List has more than doubled since December 2009.²⁸⁶ In many cases, U.S. citizens and permanent residents only find out that their government is prohibiting them from flying while they are travelling abroad, which all but forces them to interact with the U.S. government from a position of extreme vulnerability, often without easy access to counsel. Many of those prevented from flying home have been subjected to FBI interviews while they sought assistance from U.S. Embassies to return.²⁸⁷ In several documented incidents, the FBI agents offered to take them off the No Fly List if they agreed to become an FBI informant.

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

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

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

The ACLU clients are not the only victims of this practice. In a lawsuit filed in May 2013, American citizen Yonas Fikre alleges that FBI agents from his hometown of Portland, Ore., lured him to the U.S. Embassy in Khartoum under false pretenses while he was travelling in Sudan on business and coerced him into submitting to an interview.²⁹¹ The complaint states that the agents denied Fikre's request for counsel, told him he was on the No Fly List, and interrogated him about the mosque he attended in Portland and the people who went there. They asked him to become an informant for the FBI in Portland, offering to take him off the No Fly List and provide financial compensation if he accepted. He refused. Fikre later traveled to the U.A.E., where in 2011 he was arrested and tortured by security officials. In the lawsuit, Fikre charges that his arrest and interrogation were undertaken at the request of the FBI. U.A.E. officials released Fikre without charge after three months, but were unable to deport him back to Portland because the U.S. still included him on the No Fly List. He applied for political asylum in Sweden.²⁹² In 2012, the U.S. charged Fikre with conspiring to evade financial reporting requirements regarding wire transfers to the Sudan, but made no terrorism allegations against him.²⁹³ And in a more recent case described in *The Huffington Post*, Kevin Iraniha, an American citizen born and raised in San Diego, says he was barred from flying home after graduating with a master's degree in international law from the University of Peace in Costa Rica in June 2012.²⁹⁴ Iraniha submitted to an interview with an FBI agent at the U.S. Embassy, but was told that he would not be allowed to fly into the U.S. and would have to drive or take a boat. Iraniha flew to Tijuana, Mexico, and walked across the border.²⁹⁵

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

VI. Conclusion and Recommendations

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

We offer these recommendations:

RECOMMENDATIONS FOR THE ATTORNEY GENERAL:

1. The AG must revise the Justice Department Guidance Regarding the Use of Race in Federal Law Enforcement to: 1) remove the national security and border integrity exemptions; 2) prohibit profiling by religion or national origin; 3) clarify that the ban on profiling applies to intelligence activities as well as investigative activities; 4) establish enforceable standards that include accountability mechanisms for noncompliance; and 5) make the guidance applicable to state and local law enforcement working on federal task forces or receiving federal funds.
2. The AG must revise the Attorney General's Guidelines to: 1) remove the FBI's authority to conduct "assessments" without a factual predicate of wrongdoing; 2) prohibit racial and ethnic mapping; and 3) prohibit the FBI from undertaking "Preliminary Investigations" unless they are supported by articulable facts and particularized suspicion, and properly limited in time and scope; 4) prohibit the FBI from tasking informants or using undercover agents in Preliminary Investigations.
3. The AG must direct the Justice Department's Civil Rights Division to investigate the FBI's counterterrorism training materials and intelligence products to identify and remove information that is factually incorrect; exhibits bias against any race, ethnicity, religion or national origin; or improperly equates First Amendment-protected activity or non-violent civil disobedience with terrorism.
4. The AG must direct the Civil Rights Division to investigate the FBI's domain management and racial and ethnic profiling programs and determine whether the FBI used these programs to

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

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

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

RECOMMENDATIONS FOR CONGRESS:

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

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

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

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

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

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

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

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

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

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

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

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

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

- Policy Counsel, American Civil Liberties Union), available at <http://www.aclu.org/national-security/aclu-testimony-house-judiciary-subcommittee-constitution-civil-rights-and-civil-li>; and *The Permanent Provisions of the PATRIOT Act: Hearing Before the H. Judiciary Subcomm. on Crime, Terrorism & Homeland Sec.*, 111th Cong. (2011) (statement of Michael German, Senior Policy Counsel, American Civil Liberties Union), available at https://www.aclu.org/files/assets/ACLU_Testimony_Before_the_HJC_Regarding_the_Patriot_Act.pdf.
- ⁴ *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961).
- ⁵ See *Mapp v. Ohio*, 367 U.S. 643 (1961).
- ⁶ Allan M. Jalon, *A Break-In to End All Break-Ins*, L.A. TIMES, Mar. 8, 2006, <http://articles.latimes.com/2006/mar/08/opinion/oe-jalon8>.
- ⁷ S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT ON SUPPLEMENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (BOOK II), S. Rep. No. 94-755, at 6-7 (1976) [hereinafter *Church Comm. (Book II)*].
- ⁸ *Id.*
- ⁹ 50 U.S.C. § 1801 et. seq. (2010).
- ¹⁰ *FBI Statutory Charter: Hearings Before the S. Comm. on the Judiciary*, 95th Cong. Pt. 1, at 22 (1978).
- ¹¹ Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, June 5, 2013, <http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order>.
- ¹² Secondary Order, In Re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Serv., Inc., on Behalf of MCI Commc'n Serv., Inc., D/B/A Verizon Bus. Serv., (U.S. Foreign Intelligence Surveillance Court Apr. 25, 2013), available at <http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order>.
- ¹³ Ellen Nakashima, *Verizon providing all call records to U.S. under court order*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_print.html.
- ¹⁴ Letter from Ronald Weich, Assistant Att'y Gen., Dep't of Justice, to Hon. Joseph R. Biden, Jr., President of the U.S. Senate (Apr. 30, 2012) (on file with author), available at <http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf>.
- ¹⁵ 18 U.S.C. §1861 (2006), available at: <http://www.law.cornell.edu/uscode/text/50/1861>
- ¹⁶ Letter from Rep. Sensenbrenner, to Eric Holder, Att'y Gen., Dep't of Justice (June 6, 2013) (on file with author), available at http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.
- ¹⁷ *Current and Projected Nat'l Sec. Threats to the U.S.: Hearing Before the Sen. Select Comm. on Intelligence*, 112th Cong. (2011) (statement of Robert S. Mueller, III, Dir., Fed. Bureau of Investigation), at 46, available at http://www.fas.org/irp/congress/2011_hr/ssci-threat.pdf.
- ¹⁸ *Current and Projected Nat'l Sec. Threats the the U.S.: Hearing Before the S. Select Comm. on Intelligence*, 112th Cong. (2011) (statement of Sen. Ron Wyden), at 48, available at http://www.fas.org/irp/congress/2011_hr/ssci-threat.pdf.
- ¹⁹ See, Charlie Savage, *Senators Say Patriot Act is Being Misinterpreted*, N.Y. TIMES, May 27, 2011, at A17, available at http://www.nytimes.com/2011/05/27/us/27patriot.html?_r=0; and Letter from Sen. Mark Udall & Sen. Ron Wyden to Eric Holder, Att'y Gen., Dep't of Justice (Sept. 21, 2011) (on file with author), available at <http://www.documentcloud.org/documents/250829-wyden-udall-letter-to-holder-on-wiretapping.html>.
- ²⁰ Press Release, Wyden, Udall Issue Statement on Effectiveness of Declassified NSA Programs (June 19, 2013) (on file with author), available at <http://www.wyden.senate.gov/news/press-releases/wyden-udall-issue-statement-on-effectiveness-of-declassified-nsa-programs>.
- ²¹ *American Civil Liberties Union v. Fed. Bureau of Investigation*, 11 CIV 7562 (S.D.N.Y. Oct. 26, 2011).
- ²² Complaint for Declaratory Judgment and Injunctive Relief, *ACLU v. Clapper*, No.13CIV3994 (S.D.N.Y. June 11, 2013), available at http://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf.
- ²³ OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (2007), available at <http://www.usdoj.gov/oig/special/s0703b/final.pdf> [hereinafter *2007 NSL Report*].
- ²⁴ *Id.* at 104, 84.
- ²⁵ *Id.* at 98.
- ²⁶ OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (2008), available at <http://www.usdoj.gov/oig/special/s0803b/final.pdf> [hereinafter *2008 NSL Report*].
- ²⁷ *Id.* at 9.

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

- ⁵⁵ Michael R. Blood, *FBI Director Defends Use of Informants in Mosques*, ASSOC. PRESS, June 8, 2009, available at <http://www.guardian.co.uk/world/feedarticle/8548433>.
- ⁵⁶ See FBI.gov, Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jtffs (last visited Apr. 9, 2012).
- ⁵⁷ See ACLU.org, FBI/JTTF Spying, <http://www.aclu.org/national-security/fbi-jtff-spying> (last visited July 1, 2013); and ACLU.org, FBI Spy Files Project: ACLU Client List, <http://www.aclu.org/national-security/fbi-spy-files-project-aclu-client-list> (last visited July 1, 2013).
- ⁵⁸ Electronic communication from Fed. Bureau of Investigation Los Angeles, Santa Maria Resident Agency, to Fed. Bureau of Investigation Counterterrorism Div. 3, (May 22, 2001) (on file with author), available at http://www.aclu.org/spyfiles/jtff/672_674.pdf (Summary of case. Report of 05/19/2001 protest. Proposed development of [REDACTED] source).
- ⁵⁹ Scott Shane, *For Anarchist, Details of Life as FBI Target*, N.Y. TIMES, May 29, 2011, at A1, available at <http://www.nytimes.com/2011/05/29/us/29surveillance.html?pagewanted=all>.
- ⁶⁰ *Id.* see also N.Y. Times, From Scott Crow's F.B.I. File, <http://www.nytimes.com/interactive/2011/05/29/us/29surveillance-text.html> (last visited July 1, 2013).
- ⁶¹ Letter from Rep. Zoe Lofgren, to Glenn A. Fine, Inspector Gen., Dep't of Justice (May 18, 2006) (on file with author).
- ⁶² OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S INVESTIGATIONS OF CERTAIN DOMESTIC ADVOCACY GROUPS (2010), <http://www.justice.gov/oig/special/s1009r.pdf> [hereinafter *Review of FBI's Investigations*].
- ⁶³ *Id.* at 186-187.
- ⁶⁴ *Id.*
- ⁶⁵ *Id.*
- ⁶⁶ *Id.* at 186.
- ⁶⁷ *Id.* at 187.
- ⁶⁸ *Id.* at 190.
- ⁶⁹ *Id.* at 183.
- ⁷⁰ *Id.* at 166.
- ⁷¹ *Id.* at 177, 184.
- ⁷² *Id.* at 184.
- ⁷³ MICHAEL B. MUKASEY, DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 17 (2008), <http://www.justice.gov/ag/readingroom/guidelines.pdf> [hereinafter *2008 AGG*].
- ⁷⁴ *Id.* at 20.
- ⁷⁵ Carrie Johnson, *Rule Changes Would Give FBI Agents Extensive New Powers*, WASH. POST, Sept. 12, 2008, http://articles.washingtonpost.com/2008-09-12/news/36900434_1_fbi-agents-criminal-cases-intelligence.
- ⁷⁶ Electronic communication from Fed. Bureau of Investigation Counterterrorism Div., to all field offices (Sept. 24, 2009) (on file with author), available at: <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM004887.pdf> (Counterterrorism Program Guidance, Baseline Collection Plan).
- ⁷⁷ Charlie Savage, *FBI Focusing on Security Over Ordinary Crime*, N.Y. TIMES, Aug. 24, 2011, at A16, available at <http://www.nytimes.com/2011/08/24/us/24fbi.html>.
- ⁷⁸ Fed. Bureau of Investigation Counterterrorism Div., *supra* note 76, at 11.
- ⁷⁹ DEP'T OF JUSTICE, FACT SHEET: RACIAL PROFILING (June 17, 2003), http://www.justice.gov/opa/pr/2003/June/racial_profiling_fact_sheet.pdf.
- ⁸⁰ DEP'T OF JUSTICE, GUIDANCE REGARDING THE USE OF RACE BY FEDERAL LAW ENFORCEMENT AGENCIES (June 2003), http://www.justice.gov/crt/about/spl/documents/guidance_on_race.pdf.
- ⁸¹ Scott Keeter, *Why Surveys of Muslim Americans Differ*, PEW RESEARCH CENTER, Mar. 6, 2009, <http://www.pewresearch.org/2009/03/06/why-surveys-of-muslim-americans-differ/>.
- ⁸² FEDERAL BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE (2008), available at <http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DI0G%29/fbi-domestic-investigations-and-operations-guide-diog-2008-version> [hereinafter *2008 DI0G*].
- ⁸³ *Id.* at 32.
- ⁸⁴ *Id.* at 33-34
- ⁸⁵ *Id.* at 33.

⁸⁶ Al Baker, *FBI Official Faults Police Tactics on Muslims*, N.Y. TIMES, Mar. 8, 2012, at A25, available at <http://www.nytimes.com/2012/03/08/nyregion/chief-of-fbi-newark-bureau-decries-police-monitoring-of-muslims.html>.

⁸⁷ Jason Grant, *Recent NYPD spying uproar shakes FBI's foundations in N.J. terror intelligence*, NEWARK STAR-LEDGER, Mar. 7, 2012, http://www.nj.com/news/index.ssf/2012/03/recent_nypd_spying_uproar_shak.html.

⁸⁸ FEDERAL BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATION AND OPERATIONS GUIDE (2011), available at <http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version> [hereinafter *2011 DIOG*].

⁸⁹ See Nathan Freed Wessler, Staff Att'y, ACLU, *FBI Documents Suggest Feds Read Emails Without a Warrant*, May 8, 2013, <http://www.aclu.org/blog/national-security-technology-and-liberty/fbi-documents-suggest-feds-read-emails-without-warrant>.

⁹⁰ FEDERAL BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATION AND OPERATIONS GUIDE § 18, § 18.7.2.6 (2012), available at <http://www.aclu.org/files/pdfs/email-content-foia/FBI%20docs/June%202012%20FBI%20DIOG.pdf> [hereinafter *2012 DIOG*]; see also *2011 DIOG supra* note 88, at § 18.7.2.10(H).

⁹¹ 2008 DIOG, *supra* note 82, at 32.

⁹² Electronic communication from Fed. Bureau of Investigation, to Detroit field office (July 6, 2009) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM011609.pdf> (Domain Management).

⁹³ Kecia Escoe, *Demographic Makeup of Muslims in Michigan*, Muslim Observer, Mar. 1, 2012, <http://muslimmedianetwork.com/mmn/?p=10258>.

⁹⁴ Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Oct. 7, 2009) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM011454.pdf> (Intelligence Related to the Black Separatist Threat).

⁹⁵ Electronic communication from Fed. Bureau of Investigation, San Francisco, Oakland Resident Agency, to San Francisco (June 8, 2009) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM011495.pdf> (Domain Management – Criminal; Asian-Eurasian Criminal Enterprise).

⁹⁶ *Id.* at 2.

⁹⁷ Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Jan. 21, 2009) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM009170.pdf> (Intelligence Related to Mara Salvatrucha Threat); Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Dec. 15, 2008) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM011388.pdf> (Intelligence Related to MS-13 Threat); Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Sept. 22, 2008) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM008040.pdf> (Intelligence Related to MS-13 Locations); Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Sept. 4, 2008) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM007857.pdf> (Intelligence Related to Mara Salvatrucha (MS-13)).

⁹⁸ Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Sept. 22, 2008) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM008040.pdf> (Intelligence Related to MS-13 Locations); and Fed. Bureau of Investigation, Intelligence Note from Domain Mgmt. (Jan. 21, 2009) (on file with author), available at <http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM009170.pdf> (Intelligence Related to Mara Salvatrucha Threat).

⁹⁹ William J. Broad & Scott Shane, *Anthrax Case Had Costs for Suspects*, N.Y. TIMES, Aug. 10, 2008, at A1, available at <http://www.nytimes.com/2008/08/10/washington/10anthrax.html?pagewanted=1&ref=stevenjhatfill>.

¹⁰⁰ Scott Shane, *FBI vehicle hits Hatfill, but he gets the \$5 ticket*, BALT. SUN, May 20, 2003, http://articles.baltimoresun.com/2003-05-20/news/0305200401_1_clawson-anthrax-fbi-vehicle.

¹⁰¹ See Amy Goldstein, Nelson Hernandez & Annie Hull, *Tales of Addiction, Anxiety, Ranting*, WASH. POST, Aug. 6, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/05/AR2008080503747.html>; and Jerry Markon, *Anthrax report casts doubt on scientific evidence in FBI case against Bruce Ivins*, WASH. POST, Feb. 15, 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021502251.html>.

¹⁰² PADDY HILLYARD, SUSPECT COMMUNITY: PEOPLE'S EXPERIENCE OF THE PREVENTION OF TERRORISM ACTS IN BRITAIN 238, (1993).

¹⁰³ AMERICAN CIVIL LIBERTIES UNION, BLOCKING FAITH, FREEZING CHARITY: CHILLING MUSLIM CHARITABLE GIVING IN THE “WAR ON TERRORISM FINANCING,” (2009), <http://www.aclu.org/human-rights/report-blocking-faith-freezing-charity>.

¹⁰⁴ *Id.* at 72.

¹⁰⁵ THE CREATING LAW ENFORCEMENT ACCOUNTABILITY AND RESPONSIBILITY PROJECT, CUNY LAW SCHOOL, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (2013), <http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf> [hereinafter *Mapping Muslims*].

¹⁰⁶ Fusion centers are state, local and regional information sharing entities which incorporate federal, state and local law enforcement, emergency response and other government agencies and private entities to analyze and disseminate information. For more information see ACLU.org, Spy Files: More About Fusion Centers, <http://www.aclu.org/spy-files/more-about-fusion-centers> (last visited July 1, 2013).

¹⁰⁷ See FED. BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR THE eGUARDIAN THREAT TRACKING SYSTEM (2008), available at <http://www.aclu.org/files/assets/aclueg000047.pdf> [hereinafter *eGuardian PIA*]; and ACLU.org, Spy Files: More About Suspicious Activity Reporting <http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting> (last visited July 1, 2013).

¹⁰⁸ FBI.gov, Connecting the Dots Using New FBI Technology, http://www.fbi.gov/news/stories/2008/september/eguardian_091908 (last visited July 1, 2013).

¹⁰⁹ Daniel Zwerdling, G.W. Schulz, Andrew Becker & Margot Williams, *Mall Counterterrorism Files ID Mostly Minorities*, NAT’L PUB. RADIO, Sept. 8, 2011, <http://www.npr.org/2011/09/08/140262005/mall-counterterrorism-files-id-mostly-minorities>.

¹¹⁰ AMERICAN CIVIL LIBERTIES UNION, NO REAL THREAT: THE PENTAGON’S SECRET DATABASE ON PEACEFUL PROTEST, (2007), http://www.aclu.org/files/pdfs/safefree/spyfiles_norealthreat_20070117.pdf.

¹¹¹ See Press Release, Office of the Assistant Sec’y of Def. (Pub. Affairs), DOD to Implement new Interim Threat Reporting Procedures (Aug. 21, 2007) (on file with author), available at <http://www.defense.gov/releases/release.aspx?releaseid=11251>; and Press Release, Office of the Assistant Sec’y of Def. (Pub. Affairs), DOD to Implement new Suspicious Activity Reporting System (May 21, 2010) (on file with author), available at <http://www.defense.gov/releases/release.aspx?releaseid=13553>.

¹¹² eGUARDIAN PIA, *supra* note 107, at 4, 10.

¹¹³ FRANK J. CILLUFFO, JOSEPH R. CLARK, MICHAEL P. DOWNING & KEITH D. SQUIRES, GEO. WASH. U. HOMELAND SEC. POLICY INSTITUTE, COUNTERTERRORISM INTELLIGENCE: FUSION CENTER PERSPECTIVES 31 (2012), available at <http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf>.

¹¹⁴ Pub. L. 108-458, 118 Stat. 3638 (Dec. 17, 2004).

¹¹⁵ GOV’T ACCOUNTABILITY OFFICE, INFORMATION SHARING: ADDITIONAL ACTIONS COULD HELP ENSURE THAT EFFORTS TO SHARE TERRORISM-RELATED SUSPICIOUS ACTIVITY REPORTS ARE EFFECTIVE 15-17 (2013), available at <http://www.gao.gov/assets/660/652995.pdf>.

¹¹⁶ *Id.* at 16.

¹¹⁷ *Id.* at 17.

¹¹⁸ *Id.* at 33.

¹¹⁹ Letter from Rep. Brad Miller and Rep. James Sensenbrenner, Jr., H. Comm. on Sci. & Tech. Subcomm. on Investigations, to Hon. David Walker, Comptroller of the U.S. (June 5, 2007) (on file with author), available at http://www.securityprivacyandthelaw.com/uploads/file/miller_snsbrnner_walker_GAO_6_5_07.pdf.

¹²⁰ Press Release, Office of the Press Sec’y, White House, Homeland Security Presidential Directive 2 (Oct. 29, 2001) (on file with author), available at <http://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011030-2.html>.

¹²¹ DEP’T OF JUSTICE, REPORT ON “DATA-MINING” ACTIVITIES PURSUANT TO SECTION 126 OF THE USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005 (2007), available at <http://epic.org/privacy/fusion/doj-dataming.pdf>.

¹²² *Id.* at 11.

¹²³ *Id.*

¹²⁴ Letter from Chairman Brad Miller, H. Comm. on Sci. & Tech. Subcomm. on Investigations, to Chairman David Obey, H. Comm. on Appropriations (June 16, 2008) (on file with author), available at http://www.wired.com/images_blogs/dangerroom/files/61608_miller_to_obey.pdf.

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

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

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

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

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

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

¹⁵⁷ Mark Hosenball & Tabassum Zakaria, *U.S. Was Alerted to Bombing Suspect's Travel to Russia*, REUTERS, Apr. 24, 2013, <http://mobile.reuters.com/article/newsOne/idUSBRE93N1EA20130424?irpc=932>; and, Greg Miller, *Anti-terrorism Task Force Was Warned of Tamerlan Tsarnaev's Long Trip to Russia*, WASH. POST, Apr. 25, 2013, http://www.washingtonpost.com/world/national-security/anti-terror-task-force-was-warned-of-tamerlan-tsarnaevs-long-trip-to-russia/2013/04/25/Oed426de-addb-11e2-8bf6-e70cb6ae066e_story.html.

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

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

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

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

¹⁶² *Id.*

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

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

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

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

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

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

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

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

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

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

¹⁷³ *Id.* at 95.

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

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

¹⁹⁹ *USA PATRIOT Act of 2001: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 97, 100 (2005) (statements of Alberto R. Gonzales, Att’y Gen., Dep’t of Justice, & Robert S. Mueller, III, Dir., Fed. Bureau of Investigation).

²⁰⁰ See 2007 NSL REPORT, *supra* note 23, at 75..

²⁰¹ See John Solomon, *Gonzales was told of FBI violations*, WASH. POST, July 10, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/09/AR2007070902065.html>; and John Solomon, *In Intelligence World, a Mute Watchdog*, WASH. POST, July 15, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/14/AR2007071400862.html>.

²⁰² *Hearing On FBI Oversight: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. (2006) (statement of Sen. Patrick Leahy), available at http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da11db40a&wit_id=e655f9e2809e5476862f735da11db40a-0-0.

²⁰³ *Id.*

²⁰⁴ OFFICE OF THE INSPECTOR GEN., DEP’T OF JUSTICE, A REVIEW OF THE FBI’S INVOLVEMENT IN AND OBSERVATIONS OF DETAINEE INTERROGATIONS IN GUANTANAMO BAY, AFGHANISTAN, AND IRAQ (2008), available at <http://www.justice.gov/oig/special/s0805/final.pdf>.

²⁰⁵ *Oversight of the Fed. Bureau of Investigation, Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 14-15 (2008), available at <http://www.gpo.gov/fdsys/pkg/CHRG-110shrg53619/pdf/CHRG-110shrg53619.pdf> [hereinafter 2008 FBI Oversight Hearing].

²⁰⁶ Risen & Lichtblau, *supra* note 38.

²⁰⁷ 2008 FBI OVERSIGHT HEARING, *supra* note 206, at 14.

²⁰⁸ *Id.* at 16.

²⁰⁹ *Oversight of the Fed. Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 24 (2009), available at https://www.fas.org/irp/congress/2009_hr/fbi.pdf.

²¹⁰ Letter from Ronald Welch, Assistant Att’y Gen., Dep’t of Justice, to Chairman Patrick Leahy, S. Comm. on the Judiciary (Sept. 14, 2009) (on file with author), available at https://www.cdt.org/security/20090914_leahy.pdf.

²¹¹ REVIEW OF FBI’S INVESTIGATIONS, *supra* note 62, at 35–59.

²¹² *Id.* at 53 n.79.

²¹³ U.S. Magistrate Judge Stephen W. Smith, *Gagged, Sealed and Delivered: Reforming ECPA’s Secret Docket*, 6 HARV. L. & POL’Y REV. 609 (2012), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2071399.

²¹⁴ *Id.* at 613.

²¹⁵ *Id.* at 603.

²¹⁶ Declarations of Craig Monteilh Submitted by Plaintiffs in Support of Their Opposition to Motions to Dismiss, *Yassir Fazaga v. Fed. Bureau of Investigation*, Case No. SA CV 11-00301, at 6 (C.D.Cal., Jan. 30, 2012), available at <http://www.aclu-sc.org/cases/fazaga/declaration-of-craig-monteilh-re-motion-to-dismiss/>.

²¹⁷ *Id.* at 6-7.

²¹⁸ *Id.* at 12.

²¹⁹ *Id.* at 16.

²²⁰ *Id.* at 23.

²²¹ Teresa Watanbe & Scott Glover, *Man Says He Was an Informant for FBI in Orange County*, L.A. TIMES, Feb. 26, 2009, <http://articles.latimes.com/2009/feb/26/local/me-informant26>.

²²² First Amended Complaint, *Yassir Fazaga v. Fed. Bureau of Investigation*, Case No. SA CV 11-00301, at 6 (C.D.Cal. Jan. 30, 2012), available at <http://www.aclu-sc.org/cases/fazaga/first-amended-complaint/>.

²²³ The state secrets privilege is a long-standing common law privilege that allows the government to block the release of evidence in a lawsuit that would harm national security. The George W. Bush administration increasingly used the privilege to dismiss entire lawsuits at the onset, blocking lawsuits challenging government torture, rendition and warrantless surveillance. The Obama administration’s continuing use of this practice, particularly in a case of domestic law enforcement activities directed at Americans is troubling. See Nancy Goldstein, *The US National Security Smokescreen*, THE GUARDIAN, Dec. 11, 2011, <http://www.theguardian.com/commentisfree/cifamerica/2011/dec/08/us-national-security-smokescreen>.

²²⁴ See Peter Bibring, American Civil Liberties Union of S. Cal., *You Have the Right to Remain Spied On*, (Aug. 16, 2012), <http://www.aclu.org/blog/national-security/you-have-right-remain-spied>.

²²⁵ *Id.*

²²⁶ Spencer Ackerman, *FBI ‘Islam 101’ Guide Depicted Muslims as 7th Century Simpletons*, WIRED, July 27, 2011, <http://www.wired.com/dangerroom/2011/07/fbi-islam-101-guide/>; Spencer Ackerman, *FBI Teaches Agents:*

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

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

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

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

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

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

²³² *Id.* at 6.

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

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

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

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

²³⁷ *Id.*

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

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

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

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

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

²⁶⁷ Maxine Bernstein, *Two Portland Residents Facing Federal Grand Jury Subpoena from Seattle Vow They Won't Cooperate*, THE OREGONIAN, Aug. 1, 2012, http://www.oregonlive.com/pacific-northwest-news/index.ssf/2012/08/two_portland_residents_facing.html.

²⁶⁸ *Id.*

²⁶⁹ Radley Balko, *Swat Officer Killed by Non-Lethal Flash-Bang Grenade*, Reason (Mar. 8, 2011), <http://reason.com/blog/2011/03/09/swat-officer-killed-by-non-let>.

²⁷⁰ See Dep't of State, *Arrest or Detention of an American Citizen Abroad*, http://travel.state.gov/travel/tips/emergencies/arrest/arrest_3879.html (last visited Apr. 9, 2013).

²⁷¹ 22 USC §1732.

²⁷² See Press Release, American Civil Liberties Union, *ACLU Lawsuit Charges U.S. Officials Illegally Detained American Citizen* (Nov. 10, 2009) (on file with author), available at <http://www.aclu.org/national-security/aclu-lawsuit-charges-us-officials-illegally-detained-american-citizen>.

²⁷³ See Anna Louie Sussman, *Naji Hamdan's Nightmare*, THE NATION, Mar. 22, 2010, <http://www.thenation.com/article/naji-hamdans-nightmare#>.

²⁷⁴ Mark Mazetti, *Detained American Says He Was Beaten in Kuwait*, N.Y. TIMES, Jan. 6, 2011, at A10, available at http://www.nytimes.com/2011/01/06/world/middleeast/06detain.html?_r=2&hp&.

²⁷⁵ *Id.*

²⁷⁶ Nick Baumann, *Lawyer: FBI Illegally Interrogating Gulet Mohamed*, MOTHER JONES, Jan. 12, 2011, <http://www.motherjones.com/politics/2011/01/gulet-mohamed-fbi-illegal-interrogation>.

²⁷⁷ Email from redacted FBI officials to Nick Baumann, Mother Jones magazine (July 8, 2011, 04:39 PM) (on file with author), available at <https://s3.amazonaws.com/s3.documentcloud.org/documents/235035/fbistatementtomotherjones.pdf>; see also Nick Baumann, *Locked Up Abroad for the FBI*, MOTHER JONES, Sept.-Oct. 2011, available at <http://www.motherjones.com/politics/2011/08/proxy-detention-gulet-mohamed?page=1>.

²⁷⁸ AUTHOR'S NAME REDACTED, FED. BUREAU OF INVESTIGATION, CROSS CULTURAL, RAPPORT-BASED INTERROGATION, VERSION 5 (Feb. 23, 2011), available at <http://www.aclu.org/files/fbimappingfoia/20120727/ACLURM036782.pdf>.

²⁷⁹ *Id.* at 7-8.

²⁸⁰ *Id.* at 8. See also PHYSICIANS FOR HUMAN RIGHTS & HUMAN RIGHTS FIRST, *LEAVE NO MARKS: ENHANCED INTERROGATION TECHNIQUES AND THE RISK OF CRIMINALITY* 31 (2007); and NAT'L DEF. INTELLIGENCE COLLEGE, *EDUCING INFORMATION: INTERROGATION: SCIENCE AND ART* 138 (2006), available at http://www.pegc.us/archive/DoD/DIA_EI_rpt_200612.pdf.

²⁸¹ FED. BUREAU OF INVESTIGATION, *LEGAL HANDBOOK FOR FBI SPECIAL AGENTS* 90 (2003), available at <http://vault.fbi.gov/Legal%20Handbook%20for%20FBI%20Special%20Agents>; *Haley v. State of Ohio*, 332 U.S. 596 (1948).

²⁸² Letter from Laura W. Murphy, Director of the Washington Legislative Office, American Civil Liberties Union, & Devon Chaffee, Legislative Counsel, American Civil Liberties Union, to FBI Director Robert Mueller, III, (Aug. 2, 2012) (on file with author), available at <http://www.aclu.org/national-security/letter-director-fbi-regarding-interrogation-primer>.

²⁸³ See GOV'T ACCOUNTABILITY OFFICE, *REP. TO CONGRESSIONAL REQUESTERS: TERRORIST WATCH LISTS SHOULD BE CONSOLIDATED TO PROMOTE BETTER INTEGRATION AND SHARING*, GAO-03-322 (2003); OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., *DHS CHALLENGES IN CONSOLIDATING TERRORIST WATCH LIST INFORMATION*, OIG-04-31 (2004); OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, *REVIEW OF THE TERRORIST SCREENING CENTER (REDACTED FOR PUBLIC RELEASE)*, AUDIT REPORT 05-27 (2005); OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, *REVIEW OF THE TERRORIST SCREENING CENTER'S EFFORTS TO SUPPORT THE SECURE FLIGHT PROGRAM (REDACTED FOR PUBLIC RELEASE)*, AUDIT REPORT 05-34 (2005); OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, *FOLLOW-UP AUDIT OF THE TERRORIST SCREENING CENTER (REDACTED FOR PUBLIC RELEASE)*, AUDIT REPORT 07-41 (2007); OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, *AUDIT OF THE U.S. DEPARTMENT OF JUSTICE TERRORIST WATCHLIST NOMINATION PROCESSES*, AUDIT REPORT 08-16 (2008); OFFICE OF THE INSPECTOR GEN., U.S. JUSTICE DEP'T, *THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES*, AUDIT REPORT 09-25 (2009); OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., *EFFECTIVENESS OF THE DEPARTMENT OF HOMELAND SECURITY TRAVELER REDRESS INQUIRY PROGRAM*, OIG-00-103 (2009).

²⁸⁴ OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, *THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES*, at iv (2009), available at <http://www.justice.gov/oig/reports/FBI/a0925/final.pdf>.

²⁸⁵ See, Mark Hosenball, *Number of Names on U.S. Counter-terrorism Database Jumps*, REUTERS, May 2, 2013, <http://www.reuters.com/article/2013/05/03/us-usa-security-database-idUSBRE94200720130503>; and, Eileen Sullivan, *US No-Fly List Doubles in 1 Year*, ASSOCIATED PRESS, Feb. 2, 2012, <http://www.foxnews.com/us/2012/02/02/ap-exclusive-us-no-fly-list-doubles-in-1-year/>.

²⁸⁶ GOV'T ACCOUNTABILITY OFFICE, ROUTINELY ASSESSING IMPACTS OF AGENCY ACTIONS SINCE THE DECEMBER 25, 2009, ATTEMPTED ATTACK COULD HELP INFORM FUTURE EFFORTS (2012), available at <http://www.gao.gov/assets/600/591312.pdf>.

²⁸⁷ See Shirin Sadeghi, *U.S. Citizen Put on No-Fly list to Pressure Him Into Becoming Informant*, HUFFINGTON POST, June 7, 2012, http://www.huffingtonpost.com/shirin-sadeghi/kevin-iraniha-no-fly-list_b_1579208.html.

²⁸⁸ Complaint for Injunctive and Declaratory Relief, Latif, et al., v. Holder, No. 10-cv-750 (BR) (D.Or. June 29, 2010), available at <http://www.aclu.org/files/assets/2010-6-30-LatifvHolder-Complaint.pdf>.

²⁸⁹ *Id.*, see also ACLU.org, Latif, et al. v. Holder, et al. – ACLU Challenge to Government No Fly List, <http://www.aclu.org/national-security/latif-et-al-v-holder-et-al-aclu-challenge-government-no-fly-list> (last visited July 1, 2013).

²⁹⁰ Memorandum of Points and Authorities in Opposition to Defendant's Motion for Partial Summary Judgment, Latif, et al. v. Holder, No. 10-cv-750 (BR), at 25 n25 (D.Or. Mar. 22, 2013), available at http://www.aclu.org/files/assets/nfl_sj_opp.pdf.

²⁹¹ Yonas Fikre v. The Fed. Bureau of Investigation, Civil No. 3:13-cv-000899, (D.Or. May 30, 2013), available at <https://s3.amazonaws.com/s3.documentcloud.org/documents/705673/yonas-fikre-lawsuit.pdf>. See also Nigel Duara & Malin Rising, *Yonas Fikre, US Muslim, Claims He Was Tortured At FBI's Behest In United Arab Emirates*, ASSOC. PRESS, Apr. 18, 2012, available at http://www.huffingtonpost.com/2012/04/18/us-muslim-tortured_n_1434664.html.

²⁹² Kari Huus, *American Seeks Political Assylum in Sweden, Alleging Torture, FBI Coercion*, MSNBC, Apr. 18, 2012, http://usnews.nbcnews.com/_news/2012/04/18/11266018-american-seeks-political-asylum-in-sweden-alleging-torture-fbi-coercion?lite.

²⁹³ Nick Baumann, *U.S. Charges Yonas Fikre, American Who Claimed Torture, With Conspiracy*, MOTHER JONES, May 3, 2012, <http://www.motherjones.com/mojo/2012/05/yonas-fikre-american-who-claimed-torture-indicted-conspiracy-charges>.

²⁹⁴ Shirin Sadeghi, *U.S. Citizen Put on No-Fly List to Pressure Him Into Becoming FBI Informant*, HUFFINGTON POST, June 7, 2012, http://www.huffingtonpost.com/shirin-sadeghi/kevin-iraniha-no-fly-list_b_1579208.html.

²⁹⁵ Ashley McGlone & Susan Shroder, *San Diego Man on No-Fly List Returns Home*, SAN DIEGO UNION TRIB., June 7, 2012, <http://www.utsandiego.com/news/2012/Jun/06/no-fly-list-keeps-sdsu-grad-grounded-in-costa-rica/>.

²⁹⁶ NRC REPORT, *supra* note 134.

EXHIBIT G

DECLARATION

I, John Studer, make this declaration in support of the application to the Federal Election Commission for an advisory opinion that the SWP, the SWP's National Campaign Committee, and the committees supporting the candidates of the SWP are entitled to an exemption from certain disclosure provisions of the Federal Election Campaign Act.

I make this statement on the basis of my personal knowledge.

1. I am the 2016 campaign director for the Socialist Workers Party and I am familiar with the campaigns, candidates, ballot status and election results for SWP candidates over the last six years.
2. The Socialist Workers Party has not won any election in the last four years. The party has never won an election for any federal, state or municipal office.
3. In 2013, the Socialist Workers party fielded candidates for municipal offices in Atlanta, Ga.; Des Moines, Ia.; Houston, Tx.; Los Angeles, Ca.; Miami, Fl.; New York, NY; Omaha, Ne.; Philadelphia, Pa.; San Francisco, Ca.; Seattle, Wa.; and Minneapolis, Mn.
4. In 2014, the SWP ran for statewide gubernatorial offices in California, Florida, Georgia, Illinois, Massachusetts, Minnesota, Nebraska, New York, Pennsylvania and Texas. The party also ran for Lt. Governor in California, Georgia and New York. The SWP also ran one candidate for Congress, in Washington state, and a candidate for Mayor of Washington, D.C. None of these candidates were on the ballot.
5. In 2015, the SWP ran five election campaigns, one for Congress in New York and four for municipal offices — for Mayor in Chicago, Illinois; for Mayor and City Council-at-large in Philadelphia, Pennsylvania, and for city council in Washington, D.C. The total number of votes recorded for these candidates was 4,315.
6. In 2016, the SWP is running candidates in the U.S. presidential election, Alyson Kennedy for president and Osborne Hart for vice-president. The SWP calls for a vote for its presidential ticket in all 50 states, and is on the ballot in Colorado, Louisiana, Minnesota, New Jersey, Tennessee, Utah, and Washington.
7. The SWP is also running for U.S. Senate in California, Florida, Georgia, Illinois, Miami, New York, Pennsylvania, and for U.S.

House of Representative seats in California, Illinois, Minnesota and Washington, D.C. None of these candidates are on the November ballot. In Washington, the party is running a campaign for governor and the candidate is not on the ballot.

8. Attached is a list of party candidates from 2013 - 2016.

I declare under penalty of perjury that the foregoing is true and correct. Executed in New York City, New York, October 21, 2016.

A handwritten signature in blue ink that reads "John Studer". The signature is fluid and cursive, with a long horizontal stroke at the end.

John Studer
October 21, 2016

Socialist Workers Presidential Ticket

2016

Alyson Kennedy for president

Osborne Hart for vice-president

- On the ballot in 7 states: Colorado, Louisiana, Utah, Tennessee, Washington, Minnesota and New Jersey

Other federal candidates (None were on the ballot):**2013**

None.

2014

U.S. Congress	State
Mary Martin	Washington, 9 th C.D.

2015

U.S. Congress	State
Margaret Trowe	New York, 11 th C.D,

2016

U.S. Senate	State
Jacob Perasso	New York
Sam Manuel	Georgia
Cynthia Jacquith	Florida
Dan Fein	Illinois
David Rosenfeld	Minnesota
John Staggs	Pennsylvania

(In California, SWP U.S. Senate candidate Eleanor Garcia was on the 2016 California all-candidate primary ballot in June, receiving 65,084 votes. However she was not listed with any party designation.)

U.S. Congress

Jeff Powers	California
Betsy Farley	Illinois
Glova Scott	Washington, D.C.

State and Municipal offices, mostly write-in. Candidates on the ballot are indicated by an asterisk (*):

2013

Georgia: Atlanta mayor, Atlanta city council; **Iowa:** City Council At-Large and Wars 1, 3; **Texas:** Houston Mayor, City Council At-Large Positions 1,2; **Florida:** Miami Mayor; **New York:** New York City Mayor, Comptroller, Public Advocate, Bronx Borough President; **Nebraska:** Omaha Mayor*, City Council District 4*; **California:** Los Angeles Mayor, School Board; San Francisco City Attorney, Treasurer; **Pennsylvania:** Philadelphia City Controller, District Attorney; **Washington:** Seattle Mayor, City Council Position 6, Port Commissioner Position 2; **Minnesota:** Minneapolis Mayor, City Council Ward 2.

2014

California: Governor, Lt. Governor; **Florida:** Governor; **Georgia:** Governor, Lt. Governor; **Illinois:** Governor; **Massachusetts:** Governor; **Minnesota:** Governor; **Nebraska:** Governor; **New York:** Governor, Lt. Governor; **Pennsylvania:** Governor; **Texas:** Governor; **Washington, D.C.:** Mayor.

2015

Illinois: Chicago Mayor; **Pennsylvania:** Osborne Hart for Philadelphia Mayor*, John Staggs for Philadelphia City Council At-Large* (Hart received 1,234 votes, 0.5% of the total vote; Staggs received 3,028 votes, 0.3% of the total vote)

2016

Washington: Mary Martin for Governor.

EXHIBIT H

DECLARATION

I, Lea Sherman, make this declaration in support of the application to the Federal Election Commission for an advisory opinion that the SWP, the SWP's National Campaign Committee, and the committees supporting the candidates of the SWP are entitled to an exemption from certain disclosure provisions of the Federal Election Campaign Act.

I make this statement on the basis of my personal knowledge.

1. I am the current treasurer of the Socialist Workers National Campaign Committee and have been its treasurer since October, 2007.
2. I reviewed the number of contributors to the committee and the total number of contributors of \$300 or more, a randomly low dollar amount, for the 2016 presidential campaign until October 20, 2016.
3. So far in 2016, 406 people contributed funds to the committee. There were 47 contributions over \$300 to the committee.
4. The Socialist Workers Party has not received any "bundled" contributions that would require disclosure, and does not foresee receiving any such contributions. A bundled contribution is a contribution to a candidate committee or party committee or a leadership PAC that is either forwarded to the committee from a contributor by a registered lobbyist (or a PAC controlled by a registered lobbyist), or is received from a contributor but credited to a registered lobbyist (or a PAC controlled by a registered lobbyist). The law requires a committee to disclose the name, address and employer of each person who made two or more bundled contributions in an aggregate amount of more than \$15,000.
5. The Socialist Workers Party does not have any registered lobbyist. It never has had any registered lobbyists nor does it plan to.

I declare under penalty of perjury that the foregoing is true and correct. Executed on October 21, 2016, in New York City, New York.



Lea Sherman
October 21, 2016

RECEIVED

By Office of General Counsel at 4:26 pm, Nov 14, 2016

DECLARATION

I, Lea Sherman, make this declaration in support of the application to the Federal Election Commission for an advisory opinion that the SWP, the SWP's National Campaign Committee, and the committees supporting the candidates of the SWP are entitled to an exemption from certain disclosure provisions of the Federal Election Campaign Act.

I make this statement on the basis of my personal knowledge.

1. I am the treasurer of the Socialist Workers National Campaign Committee. I have served as the treasurer since 2007. I have reviewed the records of contributions to the Committee from 2009 through 2016.
2. 86 of the 406 contributions in 2016 were over \$200.
3. There were no contributions over \$200 in 2013, 2014 or 2015.
4. 11 of the 118 contributions in 2012 were over \$200.
5. There were no contributions over \$200 in 2009, 2010 or 2011.

I declare under penalty of perjury that the foregoing is true and correct. Executed in New York City, New York, November 13, 2016.



Lea Sherman
New York
November 13, 2016

EXHIBIT I

N.Y. / REGION

Old New York Police Surveillance Is Found, Forcing Big Brother Out of Hiding

By JOSEPH GOLDSTEIN JUNE 16, 2016

From the mid-1950s to the early 1970s, police surveillance of political organizations in New York was extensive enough to require more than half a million index cards, simply to catalog and cross-reference the many dossiers. But over the ensuing decades, the dossiers themselves were presumed missing or lost. Police Department lawyers said they had no idea where the files had gone.

Now, a significant portion of the missing files have been discovered during what the city said on Thursday was a routine inventory of a Queens warehouse, where archivists found 520 brown boxes of decades-old files, believed to be the largest trove of New York Police Department surveillance records from the era.

“It’s the whole mother lode,” said Gideon Oliver, a civil rights lawyer who two years ago filed a lawsuit on behalf of a historian seeking records about a group that was a target of surveillance.

The boxes, according to a written index, contain extensive files about the Black Panthers, the Nation of Islam and the Young Lords, as well as public demonstrations and civil unrest. Files on individuals are also among the documents; at least 15 boxes primarily contain photographs, Mr. Oliver said.

The city’s Records Department, in a statement, said it was working to develop rules regarding public access to the documents, though no timetable or process has been set.

The files are bound to resonate not only among those subjected to surveillance decades ago, but also among current activists and organizations that have faced police surveillance and infiltration in the years since Sept. 11, 2001.

After the terrorist attacks, the Police Department bolstered its spying capabilities; Muslim organizations and mosques in particular reported extensive surveillance. Others, including activists associated with causes ranging from the antiwar movement to cycling, have also found themselves watched.

The files discovered in Queens are from a secretive police unit that began as the anti-Communist “Red Squad.” During the 1960s, it was called the Special Services Division. Today it is called the Intelligence Division.

Its activities are subject to rules intended to limit the circumstances under which the police can begin investigating political groups, or maintain surveillance files that capture political activity. The rules, put in place in the 1980s and modified after Sept. 11, emerged from a long-running lawsuit brought by political activists.

Pablo Guzman, an early member of the Young Lords, said he hoped to have a chance to inspect the Police Department’s records on the group, which was the target of extensive surveillance and infiltration, he said.

“We would be most interested in discovering who they sent in to infiltrate us — who were the undercovers and who was subverting what we were doing?” Mr. Guzman, a longtime television reporter in New York, said. “But we’re not going to find out who the turncoats were, who the agents were. They’re going to redact all that.”

For the past 30 years, the files were supposed to be open to the public, as part of the settlement of the lengthy lawsuit. The

city had agreed to release portions to people who asked to see their own file, one of the lawyers, Jethro Eisenstein, recalled. But a significant number of those who sought access were rebuffed, he said. By the time the files were to be made public they were in disarray, rendering the indexing system useless.

Civil rights lawyers claimed it reflected a clear effort on the part of the Police Department to stymie public access. "They scrambled the entire system, so it was impossible to find anything," Mr. Eisenstein said.

But the index-card filing system, described in various old court documents, offers insight into the extent of surveillance.

A court filing from 1989 provides a sampling of the material in the dossiers. One card referred to signers of a Communist Party petition, while another mentioned a Catholic lay teacher who was involved in labor negotiations with the archdiocese. There are index cards for those who spoke at rallies against the Vietnam War. There is an index card for the person "seated at Table 8 in Albert Ballroom, Americana Hotel, paying \$15 for dinner held by Emergency Civil Liberties Committee 12/15/62."

For years the files were believed to have been stored in two rooms at Police Headquarters. The rooms, A10 and 1206, became a topic of fascination and frustration for civil rights lawyers. Over time the files were said to become increasingly disorganized. Ultimately, they disappeared.

In affidavits from the past two years, the current occupants of those two rooms, or the detectives who searched them, reported finding none of the surveillance files.

New York Today

Sign up to receive the latest on local news, arts, sports, dining, style and more, delivered to your inbox every morning.

Receive occasional updates and special offers for The New York Times's products and services.

I'm not a robot

reCAPTCHA
Privacy - Terms

[See Sample](#)

[Manage Email Preferences](#)

[Privacy Policy](#)

"Throughout the '80s we were pressing for this stuff," Mr. Eisenstein recalled. "And then it fell from view."

Over time, he said, "the people who were concerned about what was written about them in the '60s were onto other stuff."

When the documents resurfaced this week, among the first to learn of the discovery was Johanna Fernandez, a professor at Baruch College who is writing a book on the Young Lords, a Puerto Rican organization that began as a reformed street gang in Chicago before evolving into a radical social justice movement. She had requested surveillance files relating to the organization from the Police Department as well as from the Federal Bureau of Investigation, which she said was far more responsive in providing records.

In 2014, she sued the city to gain access, after years of letter writing had yielded little.

In court affidavits, police officials said they found little, despite searches lasting more than 100 hours. The judge, Alice Schlesinger, dismissed the lawsuit in May, expressing frustration at the outcome.

In an interview, Professor Fernandez said she had been told by the Records Department that the documents would soon be made accessible not only to scholars but also to the public at large.

Taken together, she said, the files tell "the story of thousands of people and organizations in New York City who fought to

make the city more just and democratic and were systematically obstructed by the police.”

Her own book is largely written, but she said she hoped to incorporate the records into an epilogue.

A version of this article appears in print on June 17, 2016, on page A23 of the New York edition with the headline: Decades Later, Big Brother Comes Out of Hiding.

© 2016 The New York Times Company

EXHIBIT J

BRENNAN

CENTER

FOR JUSTICE

NATIONAL SECURITY
AND LOCAL POLICE

Michael Price

ABOUT THE BRENNAN CENTER FOR JUSTICE

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

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

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

ABOUT THE BRENNAN CENTER'S PUBLICATIONS

Red cover | Research reports offer in-depth empirical findings.

Blue cover | Policy proposals offer innovative, concrete reform solutions.

White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

ABOUT THE AUTHOR

Michael Price serves as counsel for the Brennan Center's Liberty and National Security Program, which seeks to ensure that our government respects human rights and fundamental freedoms in conducting the fight against terrorism. Before joining the Brennan Center, Mr. Price was the National Security Coordinator for the National Association of Criminal Defense Lawyers, where he provided legal assistance for the defense of detainees in the military commissions at Guantanamo Bay. Mr. Price also engaged in litigation and public advocacy on issues related to privacy, electronic searches and surveillance, and government secrecy. Mr. Price was the student research director for NYU's Center on Law and Security, an intern with the Department of Justice Civil Rights Division, a symposium editor for the *Journal of International Law and Politics*, and a student advocate in NYU's International Human Rights Clinic, where he represented two Yemeni nationals detained and tortured in secret CIA "black sites." He holds a J.D. from NYU School of Law and a B.A. from Columbia University in Political Science and Middle East & Asian Languages and Cultures.

ACKNOWLEDGEMENTS

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

The author would like to thank Emin Akopyan, Sadia Ahsanuddin, R. Kyle Alagood, Emanuel Arnaud, Jeremy Carp, Michael Eggenberger, Lena Glaser, Elizabeth Goitein, Elizabeth Hira, Seth Hoy, John Kowal, Rachel Levinson-Waldman, Kimberly Lubrano, Jim Lyons, Eric Opsal, Shannon Parker, Faiza Patel, Jeanine Plant-Chirlin, Desiree Ramos Reiner, Frederick A.O. Schwarz, Jr., Jeramie Scott, Madeline Snider, Amos Toh, and Michael Waldman for their invaluable input and assistance. In addition, the author greatly benefited from the advice and comments of Kara Dansky, Michael German, Patrick O'Hara, Stephen Schulhofer, Matthew Waxman, and members of the Muslim American Civil Liberties Coalition.

TABLE OF CONTENTS

Introduction	1
I. New Roles For Local Law Enforcement: Philosophy, Organization, and New Rules	6
Philosophy: Toward “Intelligence-Led Policing”	7
Organization: Counterterrorism Intelligence Units	9
New Rules: Untethering Intelligence Activities from the Reasonable Suspicion Requirement	11
Consent Decrees: New York, Chicago, and Los Angeles	11
Suspicious Activity Reports	12
Why Reasonable Suspicion?	14
II. Information Sharing: Fusion Centers and Joint Terrorism Task Forces	17
Fusion Centers	17
Fusion Center Overview	18
The Information Sharing Environment	21
Joint Terrorism Task Forces	22
Guardian and eGuardian	22
Quality Control and Civil Liberties	23
The History of 28 CFR 23	27
III. Local Law Enforcement Oversight Mechanisms	29
Review and Appellate Model	30
Investigative and Quality Assurance Models	31
Evaluative and Performance-Based Model	32
IV. Fusion Center Oversight	35
V. Joint Terrorism Task Force Oversight	37
VI. Conclusion and Recommendations	39
Substantive Recommendations	39
Oversight Recommendations	40
Endnotes	41

*Stamp's Law: "The Government are very keen on amassing statistics – they collect them, add them, raise them to the n th power, take the cube root and prepare wonderful diagrams. But what you must never forget is that every one of those figures comes in the first instance from the chowky dar (village watchman), who just puts down what he damn pleases."*¹

INTRODUCTION

Since the attacks of September 11, 2001, many state and local law enforcement agencies have assumed a critical but unfamiliar role at the front lines of the domestic fight against terrorism. The federal government has encouraged their participation, viewing them as a tremendous “force multiplier”² with approximately 800,000 officers nationwide.³ Indeed, by collecting and sharing information about the communities they serve, police departments have been able to significantly increase the data accessible to members of the federal intelligence community.⁴ At the same time, however, the headlong rush into counterterrorism intelligence has created risks for state and local agencies, with too little attention paid to how to manage them.

Although prevention of terrorist attacks is often described as a new, post-9/11 paradigm for law enforcement, the prevention of all crime has been a central tenet of modern policing since its debut nearly 200 years ago.⁵ Intelligence activities, including the use of surveillance, undercover officers, and informants, have helped fulfill this mandate. But due to the potential for abuse that came to light during the 1960s and 70s, many courts and legislatures placed checks on police intelligence operations. Most importantly, they required officers engaged in intelligence activities to have reasonable suspicion that a person or group is involved in criminal activity before collecting, maintaining, or sharing information about them. Of course, this rule does not apply to most other police activities. Officers responding to an emergency, for example, may record a victim’s statement or document an eyewitness account without suspecting either individual of wrongdoing. But for many police departments, reasonable suspicion became a prerequisite for creating intelligence files.⁶

Since 9/11, some police departments have established counterterrorism programs to collect and share intelligence information about the everyday activities of law-abiding Americans, even in the absence of reasonable suspicion.⁷ This information is fed into an array of federal information sharing networks, creating mountains of data.⁸ Whether these practices have made us safer is debatable.⁹ What is clear is that they raise issues of accountability and oversight in ways that have not been given sufficient attention.

The centerpiece of this new counterterrorism architecture is a national information sharing network connecting police departments and federal agencies, known as the Information Sharing Environment (ISE). But there is little consistency regarding the types of information that local law enforcement agencies collect and share with their federal counterparts. The policies and procedures governing such activities are often opaque or unavailable to the public, while a deliberately decentralized system produces rules that vary considerably across the country. Inconsistent rules jeopardize the quality of shared intelligence and raise serious civil liberties concerns. In some jurisdictions, for example, police have used aggressive information-gathering tactics to target American Muslim communities without any suspicion of wrongdoing. Such practices have not generated investigative leads or proven especially useful in preventing potential terrorist attacks.¹⁰ But they have strained community relations with law enforcement, thereby jeopardizing the very terrorism prevention mission they are intended to accomplish.¹¹

Many state and local intelligence programs lack adequate oversight. While federal agencies operate under the watch of independent inspectors general, there is often no equivalent for state and local information sharing ventures. Very few local governments have built the kind of oversight structures that should accompany such a significant expansion of police functions.

Joint Terrorism Task Forces (JTTFs) are teams of counterterrorism investigators, analysts, and experts culled from dozens of law enforcement and intelligence agencies, including state and local police departments.¹²

Fusion centers are regional or statewide hubs where federal, state, and local agencies come together to collect and share information about national security and other threats.¹³

Local police departments often run regional fusion centers covering major urban areas while state police operate statewide fusion centers. JTTFs tend to focus on investigative work while fusion centers are geared towards information collection and analysis, but their missions are intimately related and often overlapping.

This report surveys the following police departments, fusion centers, and JTTFs:

Police Departments

- New York City Police Department (NYPD)
- Chicago Police Department (CPD)
- Los Angeles County Sheriff's Department (LASD)
- Los Angeles Police Department (LAPD)
- Philadelphia Police Department (PPD)
- Houston Police Department (HPD)
- Metropolitan Police Department (MPDC)
- Miami -Dade County Police Department (MDPD)
- Detroit Police Department (DPD)
- San Francisco Police Department (SFPD)
- Seattle Police Department (SPD)
- Miami Police Department (MPD)
- Portland Police Bureau (PPB)
- Minneapolis Police Department (MPD)
- St. Paul Police Department (SPPD)
- Dearborn Police Department (DPD)

Fusion Centers

- New York State Intelligence Center
- [Chicago] Crime Prevention and Information Center
- Illinois Statewide Terrorism and Intelligence Center
- Los Angeles Joint Regional Intelligence Center
- California State Terrorism Threat Assessment Center
- Delaware Valley Intelligence Center [Philadelphia]
- Pennsylvania Criminal Intelligence Center
- Houston Regional Intelligence Service Center
- Texas Fusion Center
- Washington [DC] Regional Threat and Analysis Center
- Southeast Florida Fusion Center [Miami-Dade]
- Florida Fusion Center
- Detroit and Southeast Michigan Information and Intelligence Center
- Michigan Intelligence Operations Center
- Northern California Regional Intelligence Center [San Francisco]
- Washington State Fusion Center
- Oregon Terrorism Information Threat Assessment Network
- Strategic Information Center [Minneapolis-St. Paul]
- Minnesota Joint Analysis Center

JTTFs

- New York City JTTF
- Chicago JTTF
- Los Angeles JTTF
- Philadelphia JTTF
- Houston JTTF
- Washington, DC JTTF
- Miami JTTF
- Detroit JTTF
- San Francisco JTTF
- Seattle JTTF
- Portland JTTF
- Minneapolis JTTF

At the state and local level, the intelligence architecture has developed along two main tracks: Joint Terrorism Task Forces (JTTFs) led by the Federal Bureau of Investigation (FBI) and “fusion centers” funded by the Department of Homeland Security (DHS) and Department of Justice (DOJ).

There is no shortage of reports describing particular aspects of this system,¹⁴ but the overall enterprise – which includes approximately 14,600 different sub-federal law enforcement agencies,¹⁵ 78 regional and state-run fusion centers,¹⁶ and 103 JTTFs¹⁷ – is difficult to map fully. This report seeks to fill this gap by describing and assessing the role played by state and local law enforcement in counterterrorism intelligence activities through the prism of 16 major police departments, 19 affiliated fusion centers, and 12 JTTFs.

The 16 police departments selected for study are among the largest in the United States. The Brennan Center chose them on the basis of three factors that made it likely that they would be most involved in the counterterrorism enterprise: (1) the number of terrorism prosecutions in their federal judicial districts; (2) the size of their American Muslim communities (which have been subject to intensive law enforcement scrutiny since 9/11) in their jurisdiction; and (3) their history of law enforcement intelligence activities. Some smaller cities, like Portland, Oregon, and Dearborn, Michigan, are included because they have large Muslim communities. The Eastern District of Michigan, which covers Dearborn and Detroit, also has the most federal terrorism indictments of any jurisdiction in the country.

The Brennan Center examined the 19 fusion centers that work with these police departments, focusing on their policies and procedures for collecting and sharing intelligence information. We also sought to understand the relationship between police departments and JTTFs, particularly where local participants were subject to different laws and policies than their federal colleagues. In addition to reviewing federal, state, and local laws, as well as departmental policies and procedures, the Brennan Center made extensive use of freedom of information requests, analyzed budgets, audits, and grant applications, conducted fusion center site visits in New York and California, and interviewed dozens of community leaders, state and local police, and fusion center officials.

We sought clarity about how state and local agencies are actually functioning in the domestic intelligence architecture. What we found was organized chaos: a federally subsidized, loosely coordinated system for sharing information that is collected according to varying local standards with insufficient quality control, accountability, or oversight.

Understanding this new system requires a brief examination of the evolution of state and local law enforcement agencies in the 12 years since 9/11, which is set out in Section I. This section shows that while no two police departments are the same, most departments covered in this survey have, to a greater or lesser extent, incorporated an “intelligence-led” approach to policing and have adopted rules to allow the collection and sharing of information through federal networks and databases. Only a handful of jurisdictions, however, have taken steps to minimize the risk to civil liberties and community relations posed by their intelligence operations.

Section II identifies the new web of information-sharing relationships among these police departments and thousands of other federal, state, and local agencies. It demonstrates that this web operates with a range of state and local rules about inputs, potentially compromising both the quality of information and constitutionally protected rights.

The Boston Marathon Bombing

The Brennan Center did not conduct an extensive review of the Boston Police Department because Boston did not meet the initial selection criteria for this survey. Nonetheless, the April 2013 Boston Marathon bombing naturally raised questions about the effectiveness of existing information sharing networks. The FBI is conducting its own investigation of the matter and Congress too has expressed concerns. As of the writing of this report, it cannot be said for certain whether the system worked as intended. Many questions relevant to such an evaluation remain unanswered. It is clear that the FBI conducted an assessment of one of the suspects, Tamerlan Tsarnaev, prior to the attack, based on a tip from Russian authorities that he planned to travel to Russia and join “underground” groups.¹⁸ The FBI closed its assessment in June 2011, concluding that Tamerlan did not warrant further investigation. But just three months later, Tamerlan was implicated in a gruesome triple homicide occurring on September 11, 2011.¹⁹ Were police investigators aware that the FBI had conducted an assessment of Tamerlan? Was the FBI aware of the murder investigation? Tamerlan’s name was also included on a travel watch list as a result of the Russian tip. When he flew to Russia in 2012 and returned six months later, officials at the Boston Joint Terrorism Task Force received alerts. Should the FBI have reopened its assessment or questioned Tamerlan when he returned? Did the four Boston police officers assigned to the JTTF have access to the FBI’s information about Tamerlan? Should the FBI have done more to bring it to their attention?²⁰ More broadly, were there gaps in the intelligence sharing system, or does the system need to be better tuned?²¹

Oversight of the system is spotty at the state, local, and federal levels. Section III analyzes the types of oversight models employed by police departments, concluding that most are ill suited to monitoring counterterrorism intelligence activities. A few police departments are subject to independent oversight by special counsels or inspectors general, which offer the best potential to fill this role at the municipal level. As discussed in Section IV, fusion centers have almost no independent oversight at the state or federal level. And as described in Section V, local police officers serving on JTTFs regularly operate under vague rules, often without police supervisors or local elected officials aware of their activities.

The push to increase information sharing among all levels of government was intended to safeguard the country against terrorism. But there is little data to gauge whether the system, as currently structured, has contributed to our safety.²² DHS has spent nearly \$1.4 billion on fusion centers, but it has not collected information to determine how these funds are utilized.²³ Likewise, the FBI does not track whether the information it receives from state and local agencies has helped deter terrorist threats or led to arrests and convictions.²⁴ At the same time, advocates have reported an increasing number of privacy and civil rights abuses.²⁵ And last year, a bipartisan, two-year Senate investigation concluded that fusion centers have routinely produced “irrelevant, useless or inappropriate” intelligence that endangers civil liberties and have not contributed to disrupting a single terrorist plot.²⁶ These revelations call into question the value of fusion centers as currently structured and, at minimum, point to the need for clearer rules on information sharing and greater oversight of state and local intelligence operations, including funding streams.

A systematic view of the involvement of local law enforcement agencies in counterterrorism operations reveals three problems that present significant challenges and potential costs from both a security and a civil liberties perspective:

- Most existing police oversight mechanisms are not equipped to monitor intelligence activities or weigh the impact of such operations on civil liberties or police-community relations.
- Information sharing among federal, state, and local agencies occurs under inconsistent rules and procedures that create a patchwork intelligence system with little in the way of quality controls or civil liberties protections.
- Independent oversight of fusion centers is virtually non-existent and compounds the risks of the decentralized form that information sharing has taken.

Section VI offers a number of recommendations for reform. Substantively, the Brennan Center recommends that state and local police departments tighten standards for collecting and sharing intelligence information in order to ensure that their efforts provide quality data and mitigate harm to community relations and civil liberties and civil rights. The various federal agencies that provide funding for these departments should encourage better standards by tying future financial assistance to reform. To ensure compliance with applicable rules, the Brennan Center recommends strengthening oversight of state and local intelligence activities at the state and local level. Additionally, fusion centers should be required to commission or consent to regular independent audits in order to verify compliance with applicable laws and policies. These reforms will help ensure that local intelligence efforts generate quality counterterrorism information while taking care not to jeopardize critical police-community relations or civil liberties and civil rights.

I. NEW ROLES FOR LOCAL LAW ENFORCEMENT: PHILOSOPHY, ORGANIZATION, AND NEW RULES

The attacks of September 11, 2001, sparked a massive overhaul of the federal intelligence and counterterrorism infrastructure. Terrorism was not a new problem, but it had not been a domestic priority until 2001,²⁷ especially for state and local law enforcement agencies. The 9/11 Commission Report emphasized that prevention of future attacks would require effective sharing of information throughout all levels of law enforcement: federal, state, and local.²⁸

In response, Congress combined 22 federal agencies to form the Department of Homeland Security,²⁹ now the third largest agency in the federal government.³⁰ The FBI recast its priorities as well: preventing terrorism took precedence over its regular crime fighting responsibilities.³¹ The Attorney General paved the way for more terrorism-related intelligence work by easing restrictions on the gathering of information about religious and political activities.³² By 2004, the newly minted Office of the Director of National Intelligence (ODNI) was responsible for coordinating the entire intelligence community, consisting of 17 separate federal agencies, including the Central Intelligence Agency (CIA), the FBI, and parts of DHS and the Department of Defense.³³ At the same time, Congress created the National Counterterrorism Center (NCTC) to begin integrating information from all sources.³⁴

As part of this transformation, the federal government sought to “leverage” the information gathering abilities of state and local law enforcement.³⁵ A flood of money flowed from the federal government to support local police in their new and unfamiliar job as the “eyes and ears” of the U.S. intelligence community.³⁶ Major cities such as New York and Los Angeles, which faced a heightened risk of attack, significantly altered the mission and structure of their police departments.³⁷ Smaller departments were equally eager to receive federal funding and build their intelligence capacities, even if counterterrorism was not a local priority.

As a result, many police departments changed the way they did business. Philosophically, there was a shift toward “intelligence-led policing,” which seeks to collect information about possible perpetrators and intervene *before* a crime is committed.³⁸ In the counterterrorism context, proponents of intelligence-led policing believe that analyzing even innocuous or disparate pieces of information can help “connect the dots” and reveal potential terrorist plots.³⁹ According to David Cohen, the NYPD’s Deputy Commissioner of Intelligence, “to wait for an indication of crime before investigating is to wait far too long.”⁴⁰ Consequently, increased resources were devoted to intelligence gathering, especially by larger police departments. Rules, or the interpretation of them, were changed to permit greater latitude in the collection, storage and sharing of intelligence reports.

The utility of this approach is hotly debated.⁴¹ What is not debatable is that police departments, and the local lawmakers charged with their supervision, have not always paid sufficient attention to the risks associated with this turn towards counterterrorism intelligence. As a result, reports of abuses have emerged, including departments accused of targeting American Muslim communities⁴² and social protest movements, such as Occupy Wall Street and its local manifestations.⁴³

But violations of civil rights are not the only risks posed by these changes. Losing the trust of its community is easy for a police department that strays far from its longstanding mission of serving the public. This can be counterproductive for both crime fighting and counterterrorism.

Community cooperation is essential to both. According to a 2010 study by the Institute for Homeland Security Solutions, tips from the public accounted for nearly a third of all actionable information leading to foiled terrorist plots.⁴⁴ Decades of policing research show that perceptions of fairness directly influence the willingness of communities to cooperate with the police. But community resentment and distrust can build if local law enforcement trawls for information with little rationale, discouraging engagement with the police. This is especially true where intelligence operations single out ethnic or religious communities for scrutiny. A study recently cited by the Department of Justice⁴⁵ found that individuals with potentially valuable information will be more reluctant to engage with police, even though they may be staunchly opposed to violence to achieve political ends.⁴⁶ And, as intelligence experts have concluded, sweeping surveillance programs will almost inevitably produce a mountain of irrelevant information that makes identifying genuine threats more difficult.⁴⁷ Like a Google search, the results are only as good as the query. If police officers do not have a focused and well-founded reason for collecting and sharing information, the resulting “white noise” may complicate and distort the intelligence process.⁴⁸

Philosophy: Toward “Intelligence-Led Policing”

When it comes to fighting terrorism, many local law enforcement agencies have adopted the idea of “intelligence-led policing.”⁴⁹ There are differing definitions of the term,⁵⁰ but a central tenet is the collection and analysis of information, often covertly, for the purpose of top-down decision-making aimed at crime prevention.⁵¹

The Brennan Center’s research found that 12 of the 16 police departments surveyed utilize elements of an intelligence-led approach.⁵² The extent to which a police department embraces this philosophy depends on many factors, including the perceived likelihood of a terrorist attack; force size; funding; and the opportunity cost of shifting resources to counterterrorism.

No department has embraced intelligence-led policing as fully as the New York City Police Department (NYPD).⁵³ In the aftermath of 9/11, Police Commissioner Raymond Kelly dedicated 1,000 officers to counterterrorism duties and recruited David Cohen, a 35-year CIA veteran, to run the Intelligence Division.⁵⁴ The NYPD’s intelligence operations extend to bordering states as well as overseas.⁵⁵ No other local police department has a comparable program.

The NYPD’s intelligence operations have been highly controversial. A 2011 Pulitzer Prize-winning Associated Press (AP) investigation documented the NYPD’s surveillance of Muslim communities because of their religion.⁵⁶ In brief, documents released by the AP show: the police “Demographics Unit” mapped and monitored New York’s Muslim neighborhoods;⁵⁷ the NYPD sent informants and undercover officers into mosques to listen in on religious and political discussions, which were then recorded in police files;⁵⁸ and the NYPD routinely monitored the activities of Muslim Student Associations at colleges and universities in New York, New Jersey, Connecticut, and Pennsylvania.⁵⁹ These activities are the basis of three ongoing federal lawsuits challenging their legality.⁶⁰ The approach has

also come at the cost of community trust, which experts agree is essential to the success of counterterrorism efforts.⁶¹ Since the extent of the NYPD's intelligence operations became public, there has been a noticeable cooling of relations between the police and many community leaders. Muslims have boycotted "outreach" events hosted by the city,⁶² protested against the NYPD, and organized reform efforts.⁶³

Other police departments that are also strong proponents of intelligence-led policing have rejected some of the tactics used by the NYPD. For example, in 2007, the Los Angeles Police Department (LAPD) dropped a plan to "map" Muslim communities following grave concerns expressed by religious and civil rights groups.⁶⁴ And after details of the NYPD's surveillance operations emerged in 2011, the Chicago police chief (who previously served in the NYPD) affirmed that his department "does not and will not conduct blanket surveillance and profiling of any community in the city of Chicago."⁶⁵ The Chicago police also promptly expanded prohibitions against "bias-based policing" and religion-based intelligence investigations.⁶⁶

This does not mean, however, that either Los Angeles or Chicago does not collect intelligence. Indeed both police forces operate broad counterterrorism intelligence programs that are permitted to collect information even where there is no suspicion of criminal or terrorist activity. Nonetheless, publically available information suggests that neither department targets particular religious or ethnic groups for active, wholesale surveillance. Rather, both departments rely heavily on their officers reporting "suspicious activity" that they encounter in the course of their normal duties. This information is then shared with state and regional "fusion centers," as detailed in Section II.

The Los Angeles County Sheriff's Department (LASD), the fourth largest local law enforcement agency in the country, follows a somewhat different approach. While it collects intelligence, it prohibits its officers from retaining any intelligence files unless they contain reasonable suspicion that an individual or group is involved in criminal activity.⁶⁷ It also employs a robust community outreach strategy, but segregates outreach programs from police counterterrorism or intelligence units.⁶⁸

All of the police departments in this survey (and others like them) conduct community outreach. Some combine community outreach with intelligence collection, while others keep the two ventures separate. The LASD, for example, says it does not provide outreach information to counterterrorism or intelligence units, focusing instead to build "long-term, trusted relationships" with the community.⁶⁹ Muslim community leaders in Los Angeles take a generally positive view of the LASD's outreach efforts and do not believe local police are being duplicitous, although some lament that the relationship is based on homeland security concerns.⁷⁰ By contrast, many Muslim New Yorkers suspect that the NYPD uses outreach activities such as youth cricket leagues and mosque visits as a cover for intelligence collection.⁷¹ As a result, prominent community leaders have developed a pronounced distrust of NYPD outreach efforts, perceiving them as little more than a public relations tool for the department.⁷²

Overall, many police departments have strengthened their intelligence collection operations and explicitly shifted toward intelligence-led strategies in the years since 9/11. There are, however, significant variations in how police view this mission. While some, such as the NYPD, have whole-heartedly embraced an aggressive approach, others have sought to balance counterterrorism imperatives with their traditional mandate to serve and build trust with communities.

Organization: Counterterrorism Intelligence Units

The Brennan Center's review of 16 police departments shows a direct correlation between the overall size of a department, the degree to which it relies on intelligence-led policing, and the amount of resources it has devoted to counterterrorism intelligence units. Intelligence-led counterterrorism strategies require additional resources because local police departments cannot simply abandon their obligation to fulfill traditional law enforcement responsibilities such as crime investigation and neighborhood patrols.⁷³ Consequently, many police departments have found ways to incorporate counterterrorism intelligence responsibilities into more traditional police operations. Department missions to preserve "homeland security" often describe a diverse set of functions, by no means limited to (or even explicitly inclusive of) counterterrorism. In this context, counterterrorism intelligence may be secondary to broader "criminal intelligence" responsibilities geared toward prevention and interdiction of a range of threats to public safety.⁷⁴

Before 9/11, police intelligence units fought organized crime, narcotics, and gangs. Only New York, which had a terrorist attack in 1993, and Los Angeles had dedicated counterterrorism personnel.⁷⁵ Today, more than 80 percent of the departments in this report have sworn personnel with specific counterterrorism intelligence duties, not including officers assigned to state or federal operations.⁷⁶ Seven of these departments have officers whose sole function is counterterrorism while six have more generalized intelligence units that include counterterrorism in their mandate. Only cash-strapped Detroit,⁷⁷ which has been forced to trim its police force despite having one of the nation's highest violent crime rates,⁷⁸ and the community policing bastions of Dearborn⁷⁹ and Portland,⁸⁰ do not have any such personnel.

As noted, the NYPD has developed a vast and unique counterterrorism apparatus. It has devoted approximately 1,000 officers to the Counterterrorism Bureau and the Intelligence Division with annual combined budget of more than \$100 million.⁸¹ The Intelligence Division receives approximately two-thirds of these resources.⁸² Funding for the department's counterterrorism operations comes not only from the city, state, and federal governments, but also from two private foundations. The New York City Police Foundation pays for the NYPD's overseas intelligence operations, which span 11 locations around the world.⁸³ The NYPD Counter-Terrorism Foundation raised nearly \$300,000 to pay Marc Sageman, a former CIA officer, to become the department's first "scholar-in-residence."⁸⁴

Police departments outside of New York spend far less on counterterrorism intelligence operations. The LAPD formed a Counterterrorism and Special Operations Bureau to house its long-standing Anti-Terrorist Intelligence Section, which is responsible for receiving, analyzing, and disseminating information about potential terrorist activity.⁸⁵ The entire Bureau consists of five divisions, with 750 people and has an annual budget of approximately \$77 million.⁸⁶ While official figures are unavailable, news reports indicate that it devotes roughly 300 people and \$24 million to counterterrorism.⁸⁷ Similarly, the D.C. police department created a Homeland Security Bureau with a total budget of \$53 million and roughly 300 officers, 63 of which are responsible for intelligence work at a cost of \$7 million.⁸⁸ In addition, in late 2011, Chicago began the process of reorganizing its police department, consolidating counterterrorism functions under a single unit.⁸⁹ In 2012, the Chicago Police Department employed 327 counterterrorism officers in 6 sections with a combined budget of \$25 million.⁹⁰ But by 2013,

Chicago moved its counterterrorism intelligence operations under the command of a new “Office of Crime Control Strategies,” reduced their budget to approximately \$8 million, and cut the number of officers to 100.⁹¹ Given that the city recorded a shocking 506 murders during 2012,⁹² the Chicago police have naturally been keen to focus their resources on more traditional policing.⁹³

The LASD is one of six police departments in this survey that has officers with counterterrorism intelligence duties but does not have a dedicated counterterrorism intelligence unit. Instead, counterterrorism is the responsibility of the Major Crimes Bureau, which is also charged with investigating a host of other offenses ranging from organized crime to gang activity to health care fraud.⁹⁴ Similarly, the Miami Police Department has an Intelligence and Terrorism Unit that provides protection for visiting dignitaries and is responsible for investigating organized crime and money laundering in addition to terrorism.⁹⁵

This division of resources is typical of mid-sized police departments that do not follow a strict intelligence-led philosophy. Fiscal constraints have also prompted some departments to reconsider and curtail their counterterrorism intelligence operations to instead fund routine crime prevention and investigation.⁹⁶ Without dedicated counterterrorism intelligence units, these departments often rely on regional or state-run fusion centers and federal Joint Terrorism Task Forces, as discussed in Section II.

Departments without a dedicated counterterrorism intelligence unit or full-time counterterrorism intelligence officers can still play a critical role in identifying and protecting critical infrastructure, educating and increasing community awareness about potential threats, conducting outreach to vulnerable segments of the population, and preparing emergency response plans.⁹⁷ Unlike covert intelligence operations, protecting critical infrastructure and building partnerships with local businesses and communities is in line with traditional policing priorities and poses far fewer risks to civil liberties and community relations. Officers assigned to ports and airports, for example, can simultaneously protect against terrorism, improve drug interdiction capabilities, and decrease other crime.⁹⁸ In fact, the Miami-Dade Police Department reported a “spillover effect” due to increased police presence at the airport resulting in an 80 percent reduction in theft over time.⁹⁹

As a result of this dynamic, many of the smaller departments studied by the Brennan Center, and particularly those that emphasize community policing, have focused almost entirely on what DHS calls “hometown security,” also known as community protection.¹⁰⁰ The Dearborn Police Department exemplifies this approach, tending to view the primary responsibility for counterterrorism intelligence as the province of state and federal agencies. In addition to its community outreach work, Dearborn focuses on preventive patrols for possible terrorist targets (i.e., increased police presence in strategic locations), general target hardening (i.e., increased physical security at vulnerable locations), investigating suspicious packages, and improving emergency response capabilities.¹⁰¹ Such activities are often outside the mandate of federal authorities but are particularly well suited to local law enforcement agencies because of their presence in the community and their preexisting patrol and response capacity.¹⁰²

Overall, only large police departments facing a significant threat of terrorism may be able to afford big, dedicated counterterrorism intelligence units. However, such an approach carries known risks. Without sufficient rules and oversight, these units risk violating civil rights and civil liberties and can alienate large swaths of the community, which in turn may prove counterproductive. They also detract

resources from traditional crime fighting obligations. Smaller police departments do not have personnel dedicated to counterterrorism intelligence, but their day-to-day criminal intelligence work will often include a counterterrorism component. An emphasis on community outreach and partnership can also enhance public trust and open lines of communication, although it is important not to exploit this relationship or to substitute it for actionable intelligence. Moreover, when police intelligence efforts support patrols, target hardening, and the investigation of “precursor” crimes, they are likely to mitigate the danger of abuse and the deterioration of community relations while performing critical counterterrorism functions.

New Rules: Untethering Intelligence Activities from the Reasonable Suspicion Requirement

The decentralized nature of American policing has allowed for the proliferation of an array of philosophies and structures. This has produced wildly different rules on how police departments collect, store, and share intelligence information. Until 9/11, police departments had limited authority to gather information on innocent activity, such as what people say in their houses of worship or at political meetings. Police could only examine this type of First Amendment-protected activity if there was a direct link to a suspected crime. But the attacks of 9/11 led law enforcement to turn this rule on its head.¹⁰³ Some departments, such as New York and Chicago, loosened restrictions for monitoring First Amendment-protected activity, under the theory that acts of terrorism are preceded by many legal activities that could be detected by giving police freedom to spy on religious or political organizations.¹⁰⁴ Others started participating in Suspicious Activity Reporting (SAR) programs, which are based on the premise that police officers may come across activity that is not indicative of a crime, but is still “suspicious” and should be recorded. Notably, some police departments decided that they could prevent terrorism perfectly well under existing rules and did not embrace these changes. These choices have tremendous implications for the liberty and security of everyone in the United States.

Consent Decrees: New York, Chicago, and Los Angeles

In theory, the authority of local law enforcement agencies to conduct intelligence operations rests entirely on their statutory mandate to enforce criminal law.¹⁰⁵ It follows that there should be some criminal predicate, some fact-based reason to suspect criminal activity, to justify intelligence gathering activities by local police.¹⁰⁶ In 1968, the Supreme Court established this basic principle – the “reasonable suspicion” requirement – to govern “stop and frisk” encounters.¹⁰⁷ Today, cadets in every police academy in the United States learn it. To satisfy the requirement, “an officer ‘point[s] to specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch of criminal activity.’”¹⁰⁸

The reasonable suspicion standard is not a particularly high bar to clear. But history shows that when police departments deviate from this principle, there are abuses. In the 1960s and 70s, for example, the NYPD engaged in widespread surveillance of political activists and organizations, including anti-war demonstrators, gay rights advocates, and other “activist” groups.¹⁰⁹ In Chicago, the police operated a “Red Squad” that monitored political and social activities for decades, targeting everyone from alleged anarchists and communists to the American Civil Liberties Union (ACLU) and the National Association for the Advancement of Colored People (NAACP).¹¹⁰ And in Los Angeles, the police department’s Public

Disorder Intelligence Division infiltrated anti-war groups, monitored unions and student groups, spied on the city's mayor, and reported on City Council members who criticized the LAPD.¹¹¹

Subsequent lawsuits led to court orders, known as consent decrees, requiring these police departments to demonstrate reasonable suspicion of criminal conduct in order to collect intelligence involving lawful First Amendment activities.¹¹² The NYPD, in particular, remains subject to a consent decree stemming from a 1971 lawsuit called *Handschu v. Special Services Division*.¹¹³ The decree consists of a set of guidelines, known as the Handschu Guidelines (Guidelines), which regulate NYPD investigations related to political activity. Initially, the Guidelines prohibited the NYPD from investigating a person or group engaged in political activity unless it had “specific information” that the person or group was involved in criminal conduct.¹¹⁴ However, after 9/11, the NYPD won permission to loosen this restriction for the purpose of combating terrorism, as did the LAPD and Chicago police.¹¹⁵

The NYPD now claims the authority to collect information through informants and undercover officers, attend public events without disclosing their presence as police officers, and conduct general topical and online research, all without reasonable suspicion of criminal activity.¹¹⁶ The most restrictive remaining element of the Guidelines is a prohibition on keeping information obtained at public events that does not relate to unlawful activity.¹¹⁷ But in a recent deposition, Assistant Chief Thomas Galati cast doubt on whether the Intelligence Division has been following even this rule.¹¹⁸ Galati testified that none of the information collected and maintained by the Demographics Unit has given rise to an indication of unlawful or terrorist activity that would trigger an investigation,¹¹⁹ suggesting that the information retained by the NYPD is not about criminal activity and is likely a violation of the *Handschu* consent decree.¹²⁰ In February 2013, counsel for *Handschu* plaintiffs sought to enjoin the NYPD's surveillance of Muslim communities and install a court-appointed monitor to oversee NYPD compliance with the consent decree.¹²¹ A declaration by Paul Chevigny, an attorney for the *Handschu* plaintiffs, stated that the NYPD continues to violate the rule against keeping information unrelated to criminal activity as well as rules governing the use of informants to infiltrate and investigate organizations.¹²² The litigation is ongoing.

Suspicious Activity Reports

After public criticism caused the LAPD to abandon its plans for NYPD-style community mapping,¹²³ the department developed a new theoretical construct. Known as a Suspicious Activity Report (SAR), its central feature is information generated from observations by police officers in the normal course of their duties. In other words, police compile information not through targeted surveillance or informants, but from what they see or hear while conducting their usual work. Given the rarity of terrorist attacks in the United States, this may well reflect a pragmatic choice about best practices for resource allocation. Nevertheless, this model too carries risks. Vague and expansive definitions of “suspicious activity” can open the door to a flood of irrelevant information. They can also lead to bias-based reporting as well as an influx of reports on political and religious activity protected by the First Amendment.

From a law enforcement perspective, the appeal of SARs is obvious. A SAR program reduces the opportunity costs of intelligence-led counterterrorism work because officers on the street continue to perform their traditional crime-fighting duties. They can follow protocols for reporting suspicious activity that is potentially related to threats with no substantial diversion from their “core mission of

providing emergency and non-emergency services in order to prevent crime, violence and disorder.”¹²⁴ SARs also reinforce the notion that every cop is the “eyes and ears” of the national counterterrorism effort. Consequently, both the Justice Department and DHS have encouraged police to adopt standardized SAR programs through the National SAR Initiative (NSI).¹²⁵

Although the notion of SARs has proliferated, only seven of the 16 police departments in the Brennan Center survey have established a formalized SAR program through the NSI. Departments that do not have an official SAR program still collect terrorism-related “tips and leads” and may share that information with a JTTF or fusion center that participates in the NSI. The NYPD, for example, does not participate in the NSI, but it certainly collects “suspicious” information. It has also implemented a public “See Something, Say Something” campaign and has enlisted private businesses in a counterterrorism information-sharing network dubbed “NYPD SHIELD.”¹²⁶

Figure 1 identifies which police departments have signed on to participate in the NSI and whether their local rules require officers to suspect wrongdoing before generating intelligence files.

Figure 1. Police Department Involvement in SAR Initiative and Reasonable Suspicion Requirement

Police Departments	Nationwide SAR Initiative Participants ¹²⁷	Reasonable Suspicion Requirement ¹²⁸
New York City		
Chicago	✓	
Los Angeles County		✓
City of Los Angeles	✓	
Philadelphia	✓	✓
Houston	✓	
Washington, D.C.	✓	
Miami-Dade County	✓	
Detroit		✓
San Francisco		✓
Seattle	✓	✓
City of Miami		
Portland		✓
Minneapolis		✓
St. Paul		Conflicting
Dearborn		✓

Just as intelligence-led policing means different things to different departments, what is considered “suspicious activity” also varies by jurisdiction. While the federal government actively promotes SAR programs through the NSI, it has not been effective in promoting uniformity among police departments with respect to which activities they consider suspicious. Departments do not have consistent rules about whether and when the reasonable suspicion standard is required, and the federal government has not been anxious to clarify its position.¹²⁹ As a result, the police in Washington, D.C., use one list of suspicious activities while the police in Los Angeles use another. Meanwhile, the Houston police have their own criteria, which are so broad as to include “any suspicious person or event ... determined as suspicious or worthy of reporting by an officer or supervisor.”¹³⁰

In Los Angeles, police use SARs to “document any reported or observed behavior/activity that may reveal a nexus to foreign or domestic terrorism.”¹³¹ But, as is true with the more intensive intelligence collection practice of New York, the “suspicious activity” recorded need not be linked to any specific plot or target. The LAPD’s list of suspicious activities includes some common sense indicators such as the theft of badges or uniforms, presenting false identification, breaching protected facilities, and making threats.¹³² However, it also includes such innocuous and non-criminal activities as photography, looking through binoculars, and taking notes.¹³³ With such a broad view of terrorism-related activities, officers are more likely to stop, detain, and report individuals exercising their First Amendment rights based on bias, which in turn increases the likelihood that irrelevant information will enter the system.¹³⁴

The LAPD acknowledges that the First Amendment may protect these “non-criminal” behaviors, but it instructs officers to report them anyway if they are “reasonably indicative of suspicious activity associated with terrorism.”¹³⁵ The “reasonably indicative” standard is not well understood, and it has been interpreted as less stringent than the “reasonable suspicion” standard, a well-established rule requiring officers to suspect criminal activity before conducting a *Terry* stop (“stop and frisk”).¹³⁶ The first-ever audit of the LAPD’s SAR program in 2013 defined “reasonably indicative” as “the totality of the circumstances which creates in the mind of the reasonable observer an articulable concern that the observed behavior is terrorism-related.”¹³⁷ But with such an expansive list of “terrorism-related” behaviors, this standard offers little comfort or clarification.¹³⁸

Why Reasonable Suspicion?

The absence of a reasonable suspicion requirement for documenting and sharing counterterrorism information for SARs can render a department’s intelligence activities rudderless. As described by former CIA assistant director Mark Lowenthal, the operating philosophy is very often “don’t let bad things happen,” which is “hardly a compelling analytical doctrine.”¹³⁹ If there is no suspicion of criminal activity – past, present, or future – then the basic rationale and natural focus for local police intelligence fades away. In its place are often vague or misguided conceptions of the threat posed by terrorism.¹⁴⁰

In Los Angeles, for example, the city’s regional fusion center determined that only 2 percent of the SARs generated by the LAPD between 2008 and 2010 had an articulable connection to terrorism.¹⁴¹ Nonetheless, the LAPD retained 98 percent of the SARs in its intelligence files, purging just 66 of 2,734 records.¹⁴²

Such broad standards can also open the door to racial and religious profiling. The ACLU raised this concern in a letter to LAPD Chief Charlie Beck, noting that “the SAR program invites officers to use their own hunches and subjective judgments about which photographers might be terrorists, judgments that will necessarily be informed by biases, even if unconsciously formed.”¹⁴³ And in New York, there are now three federal lawsuits involving allegations that the NYPD’s intelligence program singled out American Muslims for scrutiny for no reason other than their religion.¹⁴⁴

The NYPD maintains that its surveillance of Muslims is justified because the “majority of recent terror plots have either been carried out or planned by Islamists who have been radicalized to violence.”¹⁴⁵ But a landmark ruling against the department on its controversial “stop and frisk” program casts doubt on this defense. In the stop and frisk case, the NYPD said it encouraged officers to stop young black and Hispanic young men because doing so was consistent with the racial composition of crime suspects.¹⁴⁶ The court found that this program was a form of racial profiling and that it is “impermissible to subject all members of a racially defined group to heightened police enforcement because some members of that group are criminals.”¹⁴⁷ Instead, the court reiterated that police must base their stops on reasonable suspicion, which works to remove bias from the equation by requiring officers to have “a minimal level of objective justification” for their activity.¹⁴⁸ One’s race or religion, without more, is insufficient.

Intelligence-led policing does not – and should not – necessitate targeting communities or beliefs. The LASD, for example, relies on “criminal based intelligence.”¹⁴⁹ According to the department’s intelligence guidelines, officers cannot collect information about “political, religious, social views, associations or activities” unless it is “related directly to the criminal predicate which is the basis for focusing on the individual or group.”¹⁵⁰

The intent of this rule is not to hamstring law enforcement. The reasonable suspicion standard does not prevent police from responding to emergency calls or following up on the tips and leads they receive. It does not prevent officers from retaining information identifying witnesses, victims, or the location of crimes, assuming there is a criminal predicate.¹⁵¹ It also does not apply to other types of records regularly maintained by police departments such as accident reports or 911 calls. It simply directs officers not to create or share intelligence files when the inquiry is unmoored from any suspicion of criminal activity.

Given their mandate to enforce the criminal law, this baseline requirement makes sense for state and local police departments. In fact, congressional research suggests that of all the counterterrorism roles that law enforcement agencies can play, “identifying terrorist precursor crimes is perhaps the most natural.”¹⁵² Irrespective of ideology, terrorist groups engage in a series of *illegal* activities to sustain themselves and plan attacks.¹⁵³ These crimes include “various fraud schemes, petty crime, identity and immigration crimes, the counterfeit of goods, narcotics trade, and illegal weapons procurement.”¹⁵⁴ Local law enforcement agencies are in a good position to identify these precursor crimes, and the reasonable suspicion requirement is a fitting guide. Moreover, pursuing these offenses and sharing information about them will have the added benefit of reinforcing traditional law enforcement functions.

In short, the reasonable suspicion requirement serves an important function. Like a compass, it directs scarce resources away from conjectural or unsubstantiated threats. It separates the wheat from the chaff, preventing irrelevant or useless information from “clogging the system.”¹⁵⁵ It is a standard to embrace, not an obstacle to overcome.¹⁵⁶

* * *

Overall, although about half of the police departments in this survey use the reasonable suspicion standard quite successfully, there is no overall agreement among departments about what information to collect and share. This is deeply problematic given the overall trend toward intelligence-led policing and the national push to share information broadly. If the ultimate goal is to create a system in which law enforcement agencies at all levels of government share terrorism-related information, there must be clear rules that all participants can embrace. The reasonable suspicion standard is that well-established common denominator.

II. INFORMATION SHARING: FUSION CENTERS AND JOINT TERRORISM TASK FORCES

There are two primary institutions for sharing counterterrorism information among federal, state, and local law enforcement agencies: “fusion centers” funded by the Department of Justice and DHS, and Joint Terrorism Task Forces (JTTFs) led by the FBI. These entities work closely with one another, often located in the same building. They also have some overlapping responsibilities that can create competition for information, promote confusion about the rules, and lead to the proliferation of bad data without adequate oversight.

The mission of fusion centers, most of which did not exist until 2006, is not uniform or particularly well defined.¹⁵⁷ According to guidelines issued by the DOJ and DHS, a fusion center is a “collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.”¹⁵⁸ State or local agencies are responsible for establishing fusion centers, but they receive significant funding from the federal government and representatives from all levels of law enforcement participate in them (Wyoming is the lone holdout).¹⁵⁹ Since 2001, 49 states, 3 territories, and 26 major urban centers have created fusion centers.¹⁶⁰

JTTFs are FBI-led partnerships among federal, state, and local agencies whose primary mission is to detect, prevent, and investigate acts of terrorism within their jurisdiction. JTTFs operate locally and serve as a conduit for the federal government to exchange information with state and local law enforcement.¹⁶¹ There are now 103 JTTFs, including 71 established after 9/11.¹⁶² Although a comprehensive assessment of JTTF operations is beyond the scope of this report, it is important to recognize the prominence of the FBI’s “eGuardian” information sharing system, which competes with the national network of fusion center “Shared Spaces” and operates according to different rules.

From a state and local perspective, fusion centers and JTTFs serve as critical links to the federal intelligence community. However, the decentralized structure of these partnerships, combined with a distinct oversight deficit, poses significant concerns. Weak standards and inconsistent rules for collecting and sharing information produce inconsistent and poor-quality intelligence, much of which targets non-criminal activities. Untethered from the reasonable suspicion requirement, fusion centers may report “suspicious” activities to their local JTTF for investigation, including activities protected by the First Amendment, often on the basis of misguided notions about the role of race, ethnicity, religion, or political ideology as a terrorism indicator.

Fusion Centers

Although fusion centers were started with federal funding, they are not under federal government control. The state or local agency that establishes a fusion center determines its policies and purpose. The federal government takes the view that it cannot directly control fusion centers for the same reason it cannot directly control a local police department: the Constitution prohibits federal “commandeering” of state resources.¹⁶³ This doctrine may also preclude the federal government from directly setting rules for fusion centers – except, of course, through federal funding requirements. Notably, the federal government has not aggressively pursued the latter option. On the contrary, it seems to have deliberately

taken a back seat, failing to track how federal grants are allocated and spent, and leaving fusion centers to their own devices in ensuring compliance with federal privacy guidelines.¹⁶⁴ Federal funds for fusion centers simply flow to state legislatures, which allocate them as they see fit. This positions the federal government at arm's length from fusion centers. It has also generated great confusion when it comes to determining which rules apply and how.

Fusion Center Overview

The first National Criminal Intelligence Sharing Plan, issued in 2003, emphasized the new role of state and local law enforcement in domestic intelligence. This plan was the basis for the 2006 federal fusion center guidelines.¹⁶⁵ The guidelines called for the creation of “a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety agencies, and the private sector.”¹⁶⁶ They also instructed fusion centers to “[l]everage the databases, systems, and networks available via participating entities,” including “driver’s license information, motor vehicle registration data, location information, law enforcement and criminal justice systems or networks, and correctional data.”¹⁶⁷

With the exception of large cities such as New York and Los Angeles, state police usually play the lead role in sub-federal homeland security initiatives.¹⁶⁸ As a result, fusion centers have been the primary vehicles for state contributions to counterterrorism intelligence. Although there is no uniformity, fusion centers usually include officers from state and local law enforcement agencies, the DHS Office of Intelligence and Analysis, the FBI Field Intelligence Group (FIG) and JTTF, and the National Guard, as well as civilian analysts, members of the military, and private companies. Beginning with a pilot program in Los Angeles, many local law enforcement agencies have also designated Terrorism Liaison Officers (TLOs) to serve as the primary point of contact for terrorism information sharing with fusion centers and to relay information, such as SARs, between the police, fusion center, and JTTF.¹⁶⁹

Some city police departments have established their own fusion centers to cover their jurisdictions, such as Los Angeles, Chicago, Houston, and Miami-Dade. These “regional” fusion centers typically serve as “nodes” that are responsible for major urban areas and work closely with their state-run counterparts.¹⁷⁰ Figure 2 (opposite) lists the fusion centers associated with police departments in the Brennan Center survey.

Technically, each fusion center operates according to the laws of the state and municipality where it is located. Each fusion center is therefore unique, and each has developed its own rules for the collection, storage, and sharing of intelligence information. Some state or local laws are more protective of civil rights and civil liberties than the rules applied in other jurisdictions, or even federal rules. Some agencies require reasonable suspicion to collect intelligence on religious and political activities while others do not. Some utilize the SAR reporting process while others do not. Some share information automatically with FBI, while others seek to retain control of their data.¹⁷¹

Figure 2. Police Departments and Affiliated Fusion Centers

Police Departments	Regional (Recognized) Fusion Center	State (Primary) Fusion Center
New York City*	-	New York State Intelligence Center
Chicago	Crime Prevention and Information Center	Illinois Statewide Terrorism and Intelligence Center
Los Angeles County	Los Angeles Joint Regional Intelligence Center	California State Terrorism Threat Assessment Center
City of Los Angeles	Los Angeles Joint Regional Intelligence Center	California State Terrorism Threat Assessment Center
Philadelphia	Delaware Valley Intelligence Center	Pennsylvania Criminal Intelligence Center
Houston**	Houston Regional Intelligence Service Center	Texas Fusion Center
Washington, D.C.	Washington Regional Threat and Analysis Center	-
Miami-Dade County	Southeast Florida Fusion Center	Florida Fusion Center
Detroit	Detroit and Southeast Michigan Information and Intelligence Center	Michigan Intelligence Operations Center
San Francisco	Northern California Regional Intelligence Center	California State Threat Assessment Center
Seattle	-	Washington State Fusion Center
City of Miami	-	Florida Fusion Center
Portland	-	Oregon Terrorism Information Threat Assessment Network
Minneapolis	Strategic Information Center	Minnesota Joint Analysis Center
St. Paul	Strategic Information Center	Minnesota Joint Analysis Center
Dearborn	-	Michigan Intelligence Operations Center

* DHS will only recognize fusion centers that have been formally “designated” as such by their state governors. See *Fusion Centers and Contact Information*, U.S. DEPT OF HOMELAND SEC., <http://www.dhs.gov/fusion-center-locations-and-contact-information> (last visited Mar. 7, 2013). Although the NYPD’s Intelligence Division functions like a fusion center, it has not been designated by New York State as a fusion center. It is therefore not recognized by DHS as part of the nationwide fusion center structure. See Dan Verton, *Is It Time for the Federal Government to Rein in the NYPD?*, AOL GOV’T (Oct. 13, 2011), <http://gov.aol.com/2011/10/13/is-it-time-for-the-feds-to-rein-in-the-nypd/>. As a consequence, the NYPD is not bound by federal privacy requirements that apply to “recognized” fusion centers receiving federal funding through the Homeland Security Grant Program. See Nat’l Criminal Intelligence Res. Ctr., DHS/DOJ Fusion Process Technical Assistance Program and Services 2 (n.d.), available at http://ise.gov/sites/default/files/Fact_Sheet_Enhancing_the_Privacy_for_State_and_Major_Urban_Area_FCs.pdf.

** Many of the regional fusion centers evolved out of local intelligence units. For example, the Homeland Security Bureau of the Miami-Dade Police Department is the Southeast Florida Fusion Center. Similarly, the Houston Regional Intelligence Service Fusion Center grew out of an intelligence unit in the Houston Police Department (HPD) that later became the HPD’s Intelligence Division.

This uneven foundation has introduced a degree of disorder into the domestic intelligence structure built upon it. Because of different rules and practices about what information to collect, any effort to “fuse” this information will have variable results. A recent Senate investigation concluded that the quality of information produced by fusion centers has generally been shoddy.¹⁷² Moreover, the investigation found that police have often needlessly intruded into Americans’ privacy and impinged upon First Amendment-protected activity in the process.¹⁷³ Fusion centers are also increasingly under pressure as federal funds dry up and state legislatures seek to cut fat from their budgets. At least two fusion centers covered by this survey, Oregon and Texas, have been on the cusp of closing due to fiscal constraints and concerns about effectiveness.¹⁷⁴

In reality, the overwhelming majority of fusion center staff does not even believe counterterrorism is their primary function. According to a 2012 survey of fusion center employees, only 28 percent said counterterrorism was their most important activity.¹⁷⁵ Instead, most fusion centers now have a broader purpose: to fight “all crimes” or coordinate and consolidate information and action on “all hazards,” including, for example, disasters such as tornadoes or hurricanes.

This expansion is pragmatic. Simply put, there is not enough terrorism-related work for fusion centers. Sacramento police Lieutenant Milton Nenneman, who conducted a DHS-funded study of fusion centers at the Naval Postgraduate School, concluded that there is “insufficient purely ‘terrorist’ activity to support a multi-jurisdictional, multi-governmental level fusion center that exclusively processes terrorist activity.”¹⁷⁶ In fact, with a counterterrorism-only diet, intelligence “analysts’ skills would atrophy, as would their interest, from a lack of relevant work,” Nenneman found. Since terrorism is relatively rare, an expanded mission increases possible funding sources and additional rationales for their continued operation.

From a national security perspective, however, broadening fusion centers’ missions has the potential to dilute their potency as a counterterrorism tool. Information-sharing specific to terrorism may become less robust,¹⁷⁷ or lead to information overload, in which data is insufficiently scrutinized before is distributed. In fact, some say poor analysis is already a problem. A 2012 study by the Homeland Security Policy Institute concluded, “fusion centers excel at the dissemination of information, yet lack the analytical capabilities needed to fulfill their mandate to assess the local implications of threats.”¹⁷⁸

The Information Sharing Environment

In 2007, Congress passed the 9/11 Commission Act, which called for the creation of a new computer system to share information.¹⁷⁹ This network, the Information Sharing Environment (ISE), links fusion centers to the federal government and to each other. From the federal perspective, fusion centers help “connect the dots” by aggregating state and local counterterrorism information in searchable form on the ISE. The ISE links state and local law enforcement databases nationwide with various federal agencies and is intended to foster exchange of terrorism-related intelligence among all levels of government.

The ISE consists of “Shared Spaces” that are roughly analogous to personal folders on a shared computer server. Although accessible to other users, each individual is responsible for the contents of his or her own folder. Each fusion center has at least one Shared Space and can query other Shared Spaces, such as those operated by federal agencies and other fusion centers.¹⁸⁰ At the urging of the federal government,¹⁸¹ 68 fusion centers have developed the ability to contribute and share SAR information through their Shared Spaces on the ISE.¹⁸² This expands the reach of the National SAR Initiative to “over 14,000 law enforcement agencies in 46 states, including the District of Columbia.”¹⁸³

A “Functional Standard” developed at the national level dictates what information should be shared on the ISE. Under its provisions, SARs are included on ISE if they have a “potential nexus to terrorism.” Fusion center officials determine whether their SARs meet this standard based on a list of 16 “suspicious activities” that include both criminal and non-criminal activities as well as some activities protected by the First Amendment.¹⁸⁴ A SAR that satisfies the Functional Standard is known as an “ISE-SAR.”¹⁸⁵ SARs that do not satisfy the Functional Standard are not supposed to be shared on the ISE. However, what police departments do with the leftover information depends entirely on their local laws, policies, and procedures. Some departments will segregate the deficient reports on an internal database for further review. Some will not keep them at all. Others will bypass the Functional Standard and share the information directly with the FBI, which operates its own information sharing networks, “Guardian” and “eGuardian.” As a result, there is still considerable variation in the types of SAR information collected and shared, subverting the purpose of a national standard and making quality control far more difficult.

A key feature of the ISE is that information stored on a Shared Space, *e.g.*, an ISE-SAR, is supposed to be under the control of the agency that produced it. In theory, this means the facts will remain accurate and up to date. If an ISE-SAR is no longer accurate or relevant, the agency has a responsibility to correct it or purge it from the ISE in order to ensure that bad data does not generate poor intelligence.¹⁸⁶ In practice, however, information updates may not happen for years.¹⁸⁷ Divergent rules and a lack of independent oversight also create wide variation in the quality and usefulness of the information shared.¹⁸⁸ Indeed, the ISE operates on the premise that fusion centers and law enforcement agencies will generate SARs based on their own laws and policies. The ISE is simply a platform to share and disseminate information that meets a minimum standard.¹⁸⁹

The concern with such a decentralized system is that the participants are all playing by their own rules, or at least their own interpretation of them. A 2008 survey sponsored by DOJ and DHS concluded that among the Los Angeles, Chicago, Boston, and Miami-Dade police departments:

Each agency employed different intake and preliminary review procedures to determine whether a report actually had a “potential” connection with terrorist activity subject to special treatment. In addition, ... each agency varied in the determination of when or if SARs are passed or made available to an external agency or system such as a JTTF or fusion center. More important, each agency described slightly different decision processes that would determine when SAR information actually became intelligence and subsequently subject to [the reasonable suspicion requirement].¹⁹⁰

This is still true today. In the absence of any significant federal, state, or local oversight, fusion centers continue to play by their own rules.¹⁹¹

Some police departments clearly collect intelligence information about constitutionally protected activities without a criminal predicate. Some have collected this information based on religion and ethnicity. And some fusion centers may share this information in the ISE. Intentionally or not, the federal government has facilitated this situation and has not fulfilled its obligation to prevent it from continuing to happen.

Joint Terrorism Task Forces

Unlike fusion centers, JTTFs conduct their own terrorism investigations and federal agents may collect their own intelligence according to federal guidelines. But police officers assigned to a JTTF must serve two masters. They remain bound by state and local laws while operating in a unit that follows FBI rules. In addition to the concern that state and local laws may conflict with the federal rules, the secrecy surrounding JTTF operations limits the ability of police officers to raise concerns with local supervisors, which undermines local oversight. Moreover, JTTFs duplicate some of the functions of fusion centers without heeding state and local privacy laws. Many JTTFs receive the same reports that fusion centers post on ISE Shared Spaces. But unlike information stored on a Shared Space, the FBI copies fusion center data, keeps it for longer than state or local laws might otherwise permit, and limits a fusion center’s ability to update or correct bad information.¹⁹²

JTTFs include more than 4,400 federal, state, and local officials from over 600 different agencies.¹⁹³ They also include analysts from Field Intelligence Groups (FIGs) at each of the FBI’s 56 field offices who help direct JTTF efforts by assessing “raw” intelligence gleaned from FBI sources and case files.¹⁹⁴ According to a 2012 study by the Homeland Security Policy Institute, JTTFs were the second most important source for counterterrorism information for fusion center staffers, preceded only by local law enforcement. Some JTTFs are even “co-located” with fusion centers, meaning that they operate out of the same physical office or building.¹⁹⁵

Guardian and eGuardian

The FBI has created its own information sharing networks, known as “Guardian” and “eGuardian,”¹⁹⁶ which operate in addition to (and often compete with) the ISE Shared Space system.¹⁹⁷ eGuardian is an unclassified network designed to receive SARs directly from fusion centers and convey them to the appropriate JTTF,¹⁹⁸ regardless of whether they meet the ISE Functional Standard requirements.¹⁹⁹

Guardian is a classified version of the network that copies fusion center data from eGuardian.²⁰⁰ Fusion centers have the option of sharing SAR information through an ISE Shared Space, eGuardian, or both.²⁰¹

Paradoxically, eGuardian is both independent from and a part of the ISE. It exists as a stand-alone FBI database, accessible to fusion centers and JTTFs through its own web portal, Law Enforcement Online (LEO).²⁰² At the same time, the FBI has also configured eGuardian to operate on the ISE as if it were a Shared Space, allowing other fusion centers and JTTFs to search its records and upload ISE-SARs. However, unlike other ISE Shared Spaces, all of the reports submitted to eGuardian are copied to the classified Guardian database, thereby maintaining the data wholly within the Bureau's control. Even reports with no nexus to terrorism may be retained in eGuardian for 180 days, after which they are "deleted" and moved to the Guardian system, where they are kept for at least five years.²⁰³ And after the record is "deleted" from Guardian, it is retained for another 30 years in the FBI's case management system.²⁰⁴

This data retention policy limits the ability of fusion centers to control information they share on the ISE, to update it, correct it, purge it, or limit access to it. It also raises serious concerns about the persistence of inaccurate or outdated information and presents a legal conflict for fusion centers, which are subject to state and local laws requiring police to maintain control of the intelligence information they share.²⁰⁵

It is important to recognize that the FBI uses its own criteria to determine whether to share information on the ISE through its eGuardian Shared Space. All other participants in the ISE must adhere to the Functional Standard, but eGuardian follows its own set of rules based on FBI investigative guidelines.²⁰⁶ It defines "suspicious activity" as "behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention."²⁰⁷ Although the FBI contends that this rule is "generally consistent" with the Functional Standard,²⁰⁸ it is in fact much broader. According to FBI officials, "certain terrorism-related activities – such as those related to terrorist financing, known terrorism subject location, and past terrorism event information – currently are not among the behavior-based criteria in the Functional Standard but would meet the FBI's guidelines."²⁰⁹ Moreover, some JTTFs have explicitly told fusion centers to "provide all potentially terrorism-related information and not just ISE-SARs that [meet] the Functional Standard."²¹⁰ As a result, there is growing concern that Guardian and eGuardian networks provide an end-run around the Functional Standard, lowering the bar for sharing information on the ISE.

In sum, it is clear that eGuardian is competing with the ISE Shared Space system initially promoted by DHS.²¹¹ A 2013 report from the Government Accountability Office found that the two systems offer "duplicative services," warning that information could inadvertently fall through the cracks.²¹² Another concern is, of course, that duplicate systems with different rules sows confusion and results in a lack of transparency about how information is being shared among law enforcement agencies.

Quality Control and Civil Liberties

It is beyond question that there is a need to coordinate counterterrorism intelligence information. However, the standards for collecting and disseminating that information are so lax and variable that they not only endanger civil liberties, but risk hobbling the entire enterprise.²¹³ Harold "Skip" Vandover, the former DHS official in charge of reviewing fusion center reports, could not have been blunter when he told the Senate Homeland Security Committee "a bunch of crap is coming through."²¹⁴

The Senate Homeland Security Committee published a bipartisan report in 2012 that supported Mr. Vandover's assessment, determining that many of the reports produced by fusion centers have been useless and potentially illegal.²¹⁵ This finding is reminiscent of the Church Committee report on intelligence abuses nearly 40 years ago. The Church Committee reached the conclusion that "the dissemination of large amounts of relatively useless or totally irrelevant information has reduced the efficiency of the intelligence process."²¹⁶ It also noted that "the dissemination practices of some local law enforcement agencies" resulted in federal agencies accumulating "inherently inaccurate and distortive data."²¹⁷

Part of the problem today is the use of vague and poorly understood standards for placing information on the ISE. In order for a fusion center to share a report on the ISE, the Functional Standard requires that information have a "potential terrorism nexus."²¹⁸ Of course, virtually all information has a *potential* link to terrorism, including everyday activities such as taking photographs or dining out with a group of friends. More specifically, information posted to the ISE must be "*reasonably indicative* of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism."²¹⁹

While the Functional Standard appears to narrow the window for inclusion, in practice there is no requirement that the information be related to an actual or planned crime. According to the DOJ, information that flows through the ISE need "not be indicative of a potential crime," provided that it might help prevent a potential act of terrorism "when collated and analyzed with correlating pieces of data from other sources."²²⁰ Consequently, there has been a regular problem with reporting and improperly characterizing First Amendment-protected activities without a nexus to violence or criminality.²²¹

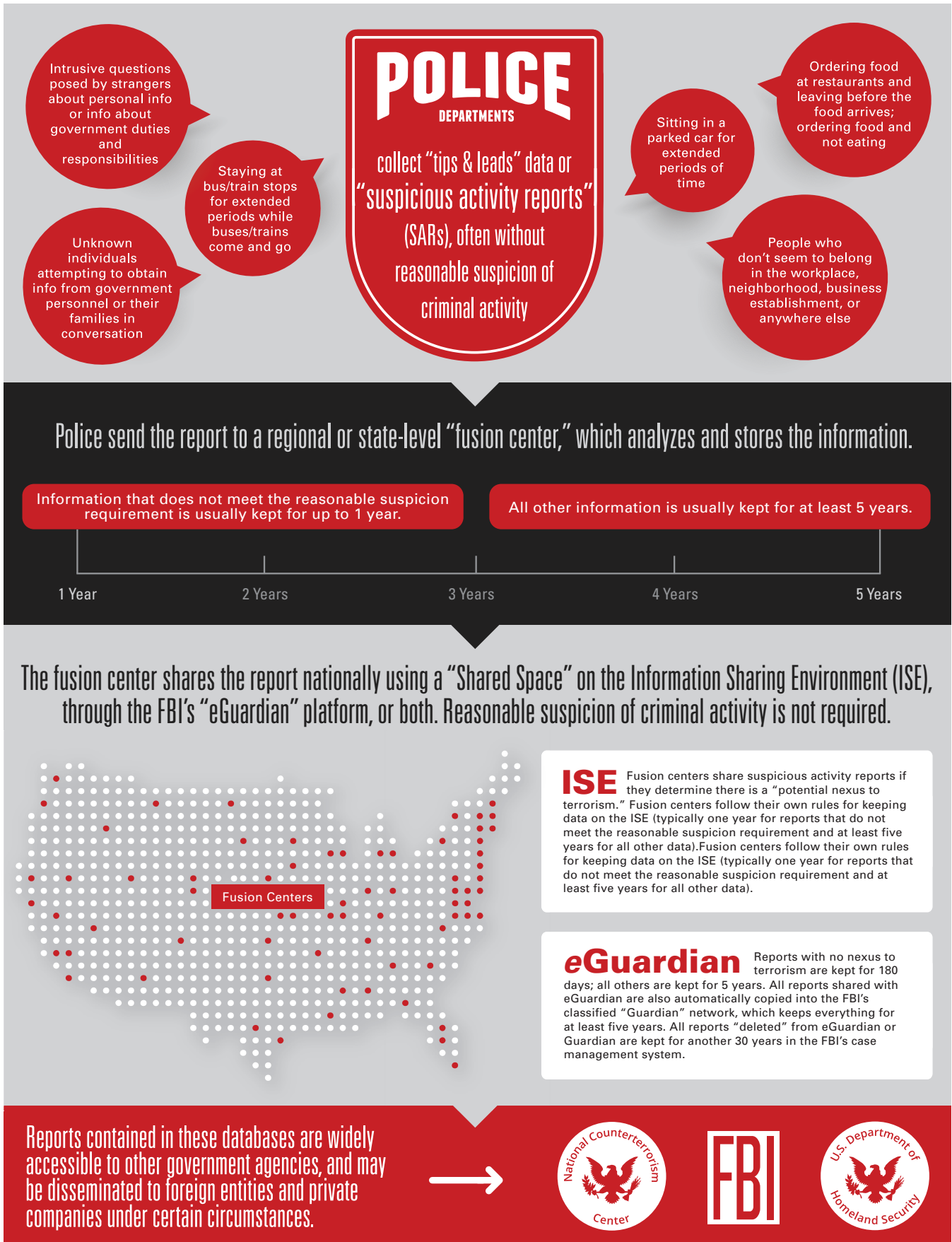
After a revision in 2009, the Functional Standard won some praise from civil liberties groups.²²² For one thing, it now includes a footnote recognizing that "[r]ace, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion."²²³ It also acknowledges that First Amendment protected behaviors such as photography and asking questions require some articulable facts that support a connection to terrorism.²²⁴ Nonetheless, it explicitly instructs state and local law enforcement that SARs shared on the ISE "may or may not meet the reasonable suspicion standard for criminal intelligence information."²²⁵

The difference between the "reasonably indicative" standard used in the Functional Standard and the "reasonable suspicion" standard used in typical criminal investigations is larger than it appears. Since the Supreme Court decided *Terry v. Ohio* in 1968, "reasonable suspicion" has become a fixture in police vocabulary.²²⁶ By contrast, there is no common definition of the "reasonably indicative" standard. While there is little public information about individual SARs shared through the ISE or eGuardian, there is ample evidence that fusion centers continue to collect personal information without a criminal predicate.

For example, even with the revised Functional Standard in place, police officers throughout California have been encouraged to document and immediately report suspicious "surveillance activities." From the LAPD's *Characteristics of Terrorists Surveillance*,²²⁷ police officers should report:

- Individuals who stay at bus or train stops for extended periods while buses and trains come and go;

Figure 3. State and Local Information Sharing Network



- Individuals who carry on long conversations on pay or cellular telephones;
- Individuals who order food at a restaurant and leave before the food arrives or who order without eating; and
- Joggers who stand and stretch for an inordinate amount of time.

Such activities may be “evidence of pre-operational planning related to terrorism”²²⁸ or evidence of a sore hamstring, but in either case, they do not amount to reasonable suspicion of criminal activity.

In an interview with the Brennan Center, Mike Sena, director of the Northern California Regional Intelligence Center (NCRIC), confirmed that SARs shared on the ISE or eGuardian may not meet the reasonable suspicion requirement. Sena, who is also the president of the National Fusion Center Association, added that the NCRIC does not include personally identifiable information in such reports, but recognized that other fusion centers do include this information.²²⁹ Indeed, the Functional Standard does not require fusion centers to omit personal information from SARs when there is insufficient evidence of a terrorism-related crime, leaving it up to each fusion center or police department to apply its own rules.²³⁰

Centers as careful about information sharing as the NCRIC appear to be the exception and not the rule. According to the 2012 Senate report, DHS employees shared information about reading suggestions by a Muslim community group, information about a motorcycle club leaflet advising what to do if pulled over by police, and information about a U.S. citizen lecturing at a mosque.²³¹ Also included was a report on a Muslim organization hosting a daylong seminar on marriage.²³²

Some officials have decried the reasonable suspicion requirement as an impediment to effective counterterrorism intelligence, citing the need to “connect the dots” or create a “mosaic” of all available threat information in order to unearth terrorist plots.²³³ But the Senate report found that this approach has “yielded little, if any, benefit to federal counterterrorism efforts.” Reviewing 13 months worth of fusion center reporting, the Senate determined that “DHS-assigned detailees to the centers forwarded ‘intelligence’ of uneven quality – oftentimes shoddy, rarely timely, sometimes endangering citizens’ civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism.”²³⁴

There is also no official data on the effectiveness of the FBI’s eGuardian network, which employs a rule for sharing information that is even more permissive than the Functional Standard.²³⁵ Two government surveys have found that eGuardian is the preferred platform among fusion centers,²³⁶ but the Justice Department has not even attempted to track the role of SARs in deterring terrorist activities. In short, there are no means for establishing the efficacy of the eGuardian system.²³⁷ The most detailed figures available indicate that of the thousands of suspicious activity reports generated by police departments and fusion centers, just 4.8 percent of ISE-SARs result in FBI investigations.²³⁸ There is no data on whether these investigations led to arrests or convictions.²³⁹ This modest figure suggests a proliferation of innocuous information, a profound lack of manpower, or some combination of the two.

The History of 28 CFR 23

More than 30 years ago, policymakers recognized the significance of the reasonable suspicion requirement, making it the touchstone for a set of guidelines on sharing criminal intelligence information among law enforcement agencies. A 1980 federal regulation, *Criminal Intelligence Systems Operating Policies*, prohibits collecting or retaining “criminal intelligence information” that does not meet the reasonable suspicion threshold.²⁴⁰ Codified at 28 CFR 23, it specifically prohibits collecting or retaining First Amendment activities information “about the political, religious or social views, associations, or activities of any individual or any group . . . unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.”²⁴¹

Even though the information they collect and retain is precisely the type of information that should be kept out of federal intelligence sharing networks, fusion centers and JTTFs have been able to sidestep the constraints of 28 CFR 23 in two ways. First, 28 CFR 23 only applies to networks that receive funding from the Omnibus Crime Control and Safe Streets Act of 1968, which the ISE and eGuardian do not.²⁴² Fusion centers receive federal funds through other grant programs, such as the State Homeland Security Program and the Urban Areas Security Initiative. Second, the government has essentially defined away the problem. Official guidance from the Department of Justice asserts that 28 CFR 23 applies only to “criminal intelligence” information, which supposedly does not include “tips and leads” data such as SARs.²⁴³ A 2007 “Tips and Leads Issue Paper” published by the Justice Department, claims that “tips and leads” that do not rise to level of reasonable suspicion may be recorded and maintained “in a secure system similar to data that rises to the level of reasonable suspicion.”²⁴⁴

Police officers have always collected “tips and leads.” Dubbed “temporary” or “working” files, officers would conduct a quick follow-up to determine whether further investigation was warranted, and if not – if there was still no reasonable suspicion of criminal activity – they would discard the information.²⁴⁵ Today, however, these records frequently find their way into the ISE and eGuardian despite fusion center privacy policies professing compliance with 28 CFR 23. In fact, the FBI has actively encouraged fusion centers to disseminate “tips and leads” information that does not meet the reasonable suspicion requirement. FBI documents distributed at the 2009 National Fusion Center Conference make the dubious claim that “[i]nformation that is deemed inconclusive will be maintained in eGuardian for a maximum of five years in accordance with [28 CFR 23].”²⁴⁶ But 28 CFR 23 does not mention “tips and leads” and explicitly prohibits retaining records for any length of time that do not meet the reasonable suspicion standard.²⁴⁷

Consequently, fusion centers operate in a “gray area” of the law²⁴⁸ – freed from compliance with the reasonable suspicion requirement of 28 CFR 23 while subject to state and local laws that vary considerably. To its credit, DHS has used grant-funding requirements to mandate that fusion centers establish privacy policies consistent with federal guidelines.²⁴⁹ Indeed, almost all fusion centers have now established privacy policies stating they comply with 28 CFR 23 “as applicable.” However, in light of the Justice Department’s guidance, which states that 28 CFR 23 is inapplicable to “tips and leads,” this statement is more form than substance.

Fusion centers have embraced the idea that “tips and leads” data (including SARs) is not criminal intelligence as defined by 28 CFR 23.²⁵⁰ In Los Angeles, for example, the LAPD may report individuals for taking photographs of national landmarks, regardless of whether there is reasonable suspicion of criminal activity. The resulting SAR is shared with the Joint Regional Intelligence Center (JRIC), the regional fusion center for Los Angeles. In theory, the JRIC unequivocally adheres to 28 CFR 23.²⁵¹ But as is true of every fusion center in California, it also permits “temporary files” to be maintained for up to one year and shared as an ISE-SAR during that time.²⁵² Houston’s fusion center, the Houston Regional Intelligence Service Center (HRISC), also professes to follow to 28 CFR 23.²⁵³ But it too maintains intelligence information that does not meet the reasonable suspicion threshold for one year.²⁵⁴ Moreover, if shared with the FBI’s eGuardian network, the bureau can keep any of this information for at least five years.²⁵⁵

The Origins of 28 CFR 23

28 CFR 23 derives from a set of guidelines first developed in 1978 by the now-defunct Law Enforcement Assistance Administration (LEAA), an arm of the Department of Justice that administered the first federally funded criminal intelligence networks. The express purpose of the LEAA guidelines was to mitigate “the potential privacy violations surrounding the collection of criminal intelligence information.”²⁵⁶ Specifically, the guidelines sought to address such “basic concerns” by requiring intelligence information to “be relevant to criminal activity” and not “collected or stored in violation of First Amendment rights.”²⁵⁷

In 1980, the LEAA guidelines were codified as 28 CFR 23.²⁵⁸ According to the Justice Department’s own position in 1993, “the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation [28 CFR 23].” The Department also noted that “the quality and utility of ‘hits’ in an information system is enhanced by the reasonable suspicion requirement,” adding that “[s]carce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural.”²⁵⁹

As a practical matter, this approach to processing tips and leads data has considerable appeal. Police officers who receive a tip or lead must have an opportunity to conduct a limited inquiry to determine if further investigation is necessary. But extending this concept to a networked system of maintaining and sharing files, encouraging law enforcement agencies to maintain and disseminate such “temporary” files as if they were predicated criminal intelligence records, is antithetical to both the history and purpose of 28 CFR 23. It is also harmful to both national security and civil liberties. It is not a coincidence that the reports produced by fusion centers have been full of irrelevant information. Indeed, there is mounting evidence that the deluge of information may be overwhelming analysts rather than helping them “connect the dots.”²⁶⁰ The reasonable suspicion standard is as much a bulwark against abuse as it is a filter for bad information. All levels of government should embrace it and establish robust oversight mechanisms to enforce it.

III. LOCAL LAW ENFORCEMENT OVERSIGHT MECHANISMS

To have a full appreciation of the mechanics of police oversight, a little history is in order. Although the U.S. adopted some precepts of the British model of policing, a significant difference is that local law enforcement in America is highly decentralized and an extension of municipal politics. As policing expert Cynthia Brown has noted, “Initially, the police were an extension not of local government, but of the different political factions that made up municipal government. It was the local political leaders in a particular ward or precinct that recruited and selected police officers.”²⁶¹ Not surprisingly, this patronage led to selective enforcement and corruption. From about 1920 to 1960, police departments underwent a wave of reform, replacing the political model with a “professional” and “legalistic” one. This transformation, which also ushered in the era of community policing, brought oversight along with it. Nonetheless, an absence of uniformity remains. Each jurisdiction sets its own policies. Generally, but not always, the intensity of oversight seems to be a function of past police department abuses.

None of the current oversight mechanisms, however, are especially well suited to monitoring state and local counterterrorism intelligence activities. Merrick Bobb, Special Counsel to the LASD Board of Supervisors and court-appointed monitor for the Seattle Police Department,²⁶² has explained that police oversight can be divided into three categories: (1) the review and appellate model; (2) the investigative and quality assurance model; and (3) the evaluative and performance-based model.²⁶³ The table below uses these categories to show the oversight mechanisms of the departments in the Brennan Center survey. Some departments fall into more than one category.

Figure 4. Oversight Models by Police Department

Police Departments	Review and Appellate	Investigative and Quality Assurance	Evaluative and Performance-Based
New York City		✓	
Chicago	✓	✓	
Los Angeles County	✓	✓	✓
City of Los Angeles		✓	✓
Philadelphia		✓*	
Houston	✓		
Washington, D.C.		✓	
Miami-Dade County**			
Detroit		✓	
San Francisco		✓	
Seattle	✓	✓	✓
City of Miami		✓	
Portland	✓	✓	
Minneapolis		✓	
St. Paul	✓		
Dearborn***			

* Police Advisory Commission. Note that the Commission includes an Integrity and Accountability Office that shares some features with the evaluative and performance-based model. It is directed by an employee of the police department and has produced only seven reports since 1997, the last of which was published in 2004.

** The Miami-Dade Police Department used to have an Independent Review Panel that followed the Review & Appellate Model. However, it was eliminated in 2009 due to countywide budget cuts, leaving the police department without any form of external civilian oversight.

*** The Dearborn Police Department has no civilian oversight body, relying only on its Internal Affairs Unit to investigate civilian complaints.

Review and Appellate Model

Departments that use the review and appellate oversight model typically rely on boards to review internal investigations of individual complaints. These boards, often composed of civilians and police officers, generally lack the authority to receive complaints or conduct their own investigations. Subpoena power is also rare. The boards are usually limited to recommending whether to sustain, reverse, or remand for additional investigation an internal police probe.²⁶⁴

The Houston Independent Police Oversight Board is typical of this approach. This 20-member civilian board, appointed by the mayor, reviews all major internal investigations to “determine if the investigation was sufficient and the conclusions were correct.”²⁶⁵ It can make nonbinding disciplinary recommendations or request additional investigation by the police, and if necessary, by the city’s Inspector General.²⁶⁶ The board is new, created in 2011 after the disclosure of video showing four Houston police officers beating a 15-year old burglary suspect. Although intended to operate independently from the police, its lack of subpoena power and investigative authority has raised concerns about its effectiveness.²⁶⁷ The board also has no authority to sit in on questioning during an Internal Affairs investigation.

Other examples of the review and appellate models include: the Los Angeles County Ombudsman;²⁶⁸ the St. Paul Police-Civilian Internal Affairs Review Commission;²⁶⁹ the Portland Citizen Review Committee;²⁷⁰ and the Seattle Office of Professional Accountability Auditor.²⁷¹ Like Houston’s Independent Police Oversight Board, many of these bodies were corrective measures taken in the wake of high-profile episodes of police violence and criticism that the police could not adequately discipline its personnel.²⁷²

The review and appellate oversight model has had a mixed record of success, due in large part to the focus on individual incidents instead of systemic problems.²⁷³ It is not, however, a good option for intelligence oversight. Whatever the merits of a particular review board, the potential complainant must at least be aware that they have encountered law enforcement. Unlike a traffic stop, for example, virtually all counterterrorism intelligence gathering is covert; subjects are unlikely to be in a position to identify and report misconduct. Even if evidence of abuse came to light, police reluctance to cooperate with investigators could cripple any review.

Additionally, review bodies do not have the power to evaluate underlying policies or procedures that may be indicative of a systemic problem. They “do not, as a rule, look at the department as a whole or search for patterns and practices of police misconduct.”²⁷⁴ While some panels may have limited authority to issue policy recommendations, their focus on discrete instances of misconduct ensures that they do not exercise this power with any frequency.²⁷⁵

Lack of access to adequate staff and resources often plagues review boards.²⁷⁶ While this problem can affect every model of oversight, the process of reviewing individual cases is particularly resource-intensive. At minimum, inadequate funds result in a large backlog of unresolved cases.²⁷⁷ At worst, fiscal constraints can cause elimination of the board altogether, as was the case in Miami-Dade when budget cuts in 2009 abolished the Independent Review Panel, the department’s only form of external civilian oversight.²⁷⁸

Investigative and Quality Assurance Models

Departments using the investigative and quality assurance model seek to supplement the internal police disciplinary process, usually called Internal Affairs, by giving investigative authority to an outside entity, such as a civilian board, a group of lawyers/investigators, or an individual.²⁷⁹ Unlike the appellate and review models, this body can investigate police misconduct on its own and is not limited to reviewing an Internal Affairs investigation.²⁸⁰ In theory, subpoena power and independent investigative authority provide “teeth” to civilian review of Internal Affairs investigations.²⁸¹ This arrangement is often a second stage in the quest for effective oversight, deployed by jurisdictions dissatisfied with a review board.²⁸²

For counterterrorism intelligence, however, this model has many of the same limitations as the appellate and review model: the boards are generally restricted to oversight of specific cases where there is known misconduct. While some may have the power to address policy issues, they rarely do; and insufficient resources and departmental resistance can hamper their work.²⁸³

New York City’s Civilian Complaint Review Board (CCRB) is a prominent example of the limitations of this brand of oversight. The CCRB devotes almost all of its resources to investigating specific complaints against individual officers and making disciplinary recommendations to the Police Commissioner, who frequently ignores them.²⁸⁴ It has the power to subpoena documents and witnesses,²⁸⁵ and the City Charter requires the NYPD to cooperate with CCRB investigations.²⁸⁶ In practice, however, the CCRB does not issue subpoenas to the NYPD. It relies instead on the cooperation of the NYPD through an officer assigned to assist the board.²⁸⁷ Consequently, the CCRB has had difficulty obtaining information from the NYPD about particularly sensitive incidents. One striking example is the CCRB inquiry into allegations of police misconduct surrounding the arrest of 247 demonstrators during the 2004 Republican National Convention. The NYPD refused to cooperate with the investigation and high-ranking officers simply ignored requests to appear before the CCRB.²⁸⁸ According to one former CCRB supervisor, the board has “broadcast its irrelevance” through its “near total absence” from controversial issues such as “stop and frisk, invasive surveillance of Muslim communities, and deliberate heavy-handedness in the policing of public demonstrations.”²⁸⁹

It is also rare for the CCRB to make policy recommendations. Over the past 20 years, the CCRB has issued just a handful of recommendations to the NYPD, most of which concerned the use of force and relied on expert testimony rather than an examination of police records.²⁹⁰ According to a 12-year survey by the New York Civil Liberties Union, “The CCRB has failed to discover, or has ignored, patterns of police misconduct; and the NYPD has therefore failed to adopt reforms – in police training, tactics, policies and practices – that could prevent foreseeable risks of harm.”²⁹¹

Investigative and quality assurance models are the most common form of oversight found in the Brennan Center survey, utilized by 12 out of 16 police departments.²⁹² Unfortunately, the problems that have beset New York City’s CCRB are true elsewhere as well. For example, a 2012 editorial in *The Philadelphia Inquirer* lamented that the Police Advisory Commission is “underfunded and lacks authority,” and called for an independent office that would “identify trends in policing, and made recommendations for strengthening the department.”²⁹³ One bright spot is the San Francisco Office of

Citizen Complaints, which conducts annual First Amendment compliance audits of police intelligence files, but this function is more frequently associated with evaluative and performance-based oversight mechanisms, as described below.²⁹⁴

Evaluative and Performance-Based Model

This model places discipline for misconduct entirely in the hands of a department's Internal Affairs unit, and focuses instead on accountability throughout the chain of command.²⁹⁵ According to Merrick Bobb, the evaluative component considers “a police department in its entirety” with the goal of publicly assessing “how well it minimizes the risk of police misconduct, identifies and corrects patterns and practices of unconstitutional and illegal behavior, and finds solutions to systemic failures.”²⁹⁶ The performance-based component “examines how individual officers perform, how supervisors and executives respond, and how the institution as a whole manages the risk that its employees engage in unconstitutional or illegal behavior.”²⁹⁷

Three police departments in the Brennan Center survey use this approach: the Los Angeles Police Department (Office of the Inspector General); the Los Angeles Sheriff's Department (Special Counsel); and the Seattle Police Department (Office of Professional Accountability Review Board). These entities are empowered to address big picture issues and foster systemic change. Although such oversight may be rare at the state or local level, it is the norm in the federal government. All major intelligence agencies – including the FBI and CIA – operate with inspectors general.²⁹⁸ As an earlier Brennan Center report explained, this system of oversight has increased transparency and the permitted independent review of controversial policies while allowing intelligence professionals to do their jobs and making their agencies more effective.²⁹⁹

The impetus to follow this model came from blue ribbon panels formed in the wake of highly publicized incidents of police misconduct that revealed the insufficiency of existing oversight mechanisms. In Los Angeles, for example, the 1991 beating of Rodney King led to the Christopher Commission, which in turn recommended the creation of an Inspector General to oversee the LAPD.³⁰⁰ In Los Angeles County, four controversial police shootings prompted the LASD Board of Supervisors to hire a “special counsel” to investigate and make recommendations for reform.³⁰¹ The position was later made permanent,³⁰² and the county is now in the process of hiring a full-time inspector general following the recommendation of a blue ribbon commission on jail violence.³⁰³ In Seattle, the mayor convened a panel in 1999 to evaluate mechanisms for investigating police misconduct after eight officers failed to report allegations that a veteran homicide detective stole \$10,000 from a crime scene.³⁰⁴ The panel recommended a “hybrid” approach that employs all three models of oversight.³⁰⁵

The common denominator among the LAPD Inspector General, the LASD Special Counsel, and Seattle's Review Board is that they have a mandate to look beyond the four corners of a complaint. They are empowered to determine whether the police's own machinery of oversight is operating effectively. Moreover, because their work is not case-dependent, they tend to assume a more flexible and policy-oriented role. According to University of Nebraska Emeritus Prof. Samuel Walker, an expert on police accountability, this approach may succeed where others fail because it is “focused on organizational

change” and because it has the authority to “probe deeply into departmental policies and procedures with an eye toward correcting them and reducing future misconduct.”³⁰⁶ These bodies also have the “capacity for sustained follow-up” to determine whether their recommendations have been followed.³⁰⁷ The Seattle Review Board, for example, assesses departmental policies and practices and reports its recommendations to the City Council. Instead of investigating individual complaints of police misconduct,³⁰⁸ it reviews audits about how the police handle complaints and community outreach, and researches national trends and best practices in police oversight and accountability.³⁰⁹ Seattle also has a civilian Police Intelligence Auditor (distinct from the Office of Professional Accountability Auditor) dedicated to ensuring the department does not run afoul of its longstanding “Intelligence Ordinance,” which prohibits the police from collecting information about a person’s political or religious associations, activities, beliefs, or opinions without reasonable suspicion of criminal activity.³¹⁰ If the Auditor has a reasonable belief that the police have violated the Ordinance, he or she must notify the person who is the subject of the breach.³¹¹ The Ordinance also permits the subject of a violation to sue the city for redress.³¹²

The evaluative and performance-based approach may be the most conducive to monitoring a department’s intelligence activities. For example, the LAPD Inspector General has published three audits since the department established the Anti-Terrorism Intelligence Section (ATIS) in 2003.³¹³ The audits evaluate the Section’s compliance with guidelines governing intelligence investigations, including a reasonable suspicion requirement for maintaining intelligence files. In a 2012 report, the Inspector General found that ATIS was in “substantial compliance” with the guidelines, but that it did not adequately document the necessary reasonable suspicion before starting an investigation. As a result, ATIS personnel received training to ensure that intelligence reports demonstrate reasonable suspicion.³¹⁴ In 2013, the Inspector General completed an audit of the LAPD’s SAR program for the first time.³¹⁵ While the audit report found the department in compliance with its own SAR policy, it unfortunately did not scrutinize the policy itself or express an opinion on the broad categories of “suspicious activities.”³¹⁶ Nonetheless, the report serves a valuable transparency function and represents one of the few available data points on the operation of police SAR programs.

Such intelligence oversight is extremely uncommon at the state and local level. Only 5 of the 22 police oversight bodies examined by the Brennan Center have conducted intelligence audits: San Francisco, Los Angeles, Washington, D.C., Seattle, and Chicago.³¹⁷ Moreover, many of these inquiries have been cursory or incomplete. In Washington, D.C., for example, the District Council passed a 2004 law requiring annual audits of investigations and inquiries involving First Amendment activity. However, there has been just one audit in the past nine years. Worse still, it failed to report any information about the most sensitive issue: the use of “preliminary inquiries,” which do not require reasonable suspicion of criminal activity.³¹⁸ In Seattle, the Police Intelligence Auditor conducts frequent audits, as required by local ordinance,³¹⁹ but the reports offer little detail beyond conclusory statements that all information has been appropriately collected, distributed, and/or maintained.³²⁰ In Chicago, a 1982 consent decree mandated independent audits every five years, but the department has not established audit procedures following dissolution of the decree in 2009.³²¹

In sum, the evaluative and performance-based model appears best positioned to conduct meaningful oversight of police intelligence operations, but it is important to recognize its limitations. It is susceptible

to funding cuts as well as the willingness of police departments to embrace oversight and participate in the process. Still, this model has worked relatively well for federal oversight of the FBI and CIA, which depends on reports from independent inspectors general to inform congressional supervision.³²² For cities with large police departments and significant intelligence operations, it may be the best hope for effective local oversight.

IV. FUSION CENTER OVERSIGHT

Despite modest encouragement from DHS, many fusion centers operate with minimal oversight, or no oversight whatsoever. Moreover, the oversight that does exist can hardly be described as independent. Designated privacy officers are usually fusion center employees while representatives from the participating agencies populate the governing boards. Of the 19 centers in the Brennan Center survey, only five mandate independent audits of the information they retain, and it is often unclear when or whether such audits have actually been conducted. Indeed, the ISE’s 2013 Annual Report to Congress recognizes that there is no “effective ISE-wide performance measurement for internal agency compliance, oversight, and accountability mechanisms to ensure consistent application of [privacy, civil rights, and civil liberties] protections.”³²³

Figure 5. Independent Oversight of Regional and State Fusion Centers ³²⁴

Police Departments	Regional (Recognized) Fusion Center	Independent Oversight?	State (Primary) Fusion Center	Independent Oversight?
New York City	—	—	New York State Intelligence Center	No
Chicago	Crime Prevention and Information Center	No	Illinois Statewide Terrorism & Intelligence Center	No
Los Angeles County	Los Angeles Joint Regional Intelligence Center	No	California State Terrorism Threat Assessment Center	No
City of Los Angeles	Los Angeles Joint Regional Intelligence Center	No	California State Terrorism Threat Assessment Center	No
Philadelphia	Delaware Valley Intelligence Center	No	Pennsylvania Criminal Intelligence Center	No
Houston	Houston Regional Intelligence Service Center	No	Texas Fusion Center	No
Washington, D.C.	Washington Regional Threat and Analysis Center	Yes	—	—
Miami-Dade County	Southeast Florida Fusion Center	No	Florida Fusion Center	Yes
Detroit	Detroit and Southeast Michigan Information and Intelligence Center	Yes	Michigan Intelligence Operations Center	Yes
San Francisco	Northern California Regional Intelligence Center	No	California State Threat Assessment Center	No
Seattle	—	—	Washington State Fusion Center	No
City of Miami	—	—	Florida Fusion Center	Yes
Portland	—	—	Oregon Terrorism Information Threat Assessment Network	No
Minneapolis	—	—	Minnesota Joint Analysis Center	Yes
St. Paul	—	—	Minnesota Joint Analysis Center	Yes
Dearborn	—	—	Michigan Intelligence Operations Center	No

As early as 1977, experts in the government recognized that regional intelligence sharing networks focused on organized crime and drug trafficking could slip through the cracks of federalism and operate without adequate oversight. A study from the time warned that regional systems “operate across political boundaries and are therefore not subject to continued review, funding and control by a State legislature,” adding that they “could operate outside the scope of normal channels of legislative control and oversight.”³²⁵ Fusion centers magnify these concerns; they not only operate outside normal channels of oversight but can also share exponentially more information than the regional networks of the 1970s. Efforts by the federal government to address this oversight gap have been half-hearted and ineffective. State and local governments have not stepped into the breach.

As a condition of continued funding, DHS has required each fusion center to craft a privacy policy and encouraged each of them to designate a “privacy officer” to ensure compliance.³²⁶ DHS has also provided model language setting out the duties of privacy officers, which include resolving complaints and reviewing reports of alleged privacy policy violations.³²⁷ The Chicago, Detroit, Houston, Los Angeles, Miami-Dade, and San Francisco fusion centers have all incorporated these provisions into their privacy policies. But in each instance, the privacy officer is a fusion center employee.³²⁸

Annual audits of intelligence files are required in nearly 90 percent of the centers surveyed.³²⁹ But with staff or supervisors conducting the audits at 13 of the 17 fusion centers, they are hardly independent.³³⁰ One of the few centers that uses an outside auditor (and equally important, publicly discloses its findings) is the Minnesota Joint Analysis Center.³³¹ The Florida Fusion Center also provides for regular independent audits by the Florida Office of the Inspector General.³³² Privacy policies require independent audits for the Michigan state fusion center as well as the Detroit and Washington, D.C., regional centers, but our research has found no public record of these audits, including when they happened, who conducted them, what they found, or whether the fusion center has taken action to correct any problems.³³³

Regular independent audits are especially important for fusion centers because the information they disseminate has such a wide audience – more than 14,000 law enforcement agencies in 49 states as well as the District of Columbia, Puerto Rico, and the Virgin Islands.³³⁴ Sharing biased, inaccurate, or irrelevant information through the ISE magnifies the harm to civil liberties as well as national security. According to the former director of DHS’s Collection and Requirements Division, the agency has been “flooded” with inappropriate reporting from state and local fusion center officials.³³⁵

If the tried and true framework of 28 CFR 23 were applied, the federal government would be responsible for conducting regular compliance audits to ensure that the data shared by fusion centers through the ISE meets the reasonable suspicion standard and other federal requirements.³³⁶ But because federal agencies maintain that 28 CFR 23 is not applicable to the ISE or eGuardian, there is no federal audit process in place for fusion centers.³³⁷ As a result, there are often significant differences in the quality of information shared by state and local law enforcement agencies on the ISE.

Without federal audits at the fusion center level, the quality of state and local intelligence information shared through the ISE will continue to depend on the inner workings of each fusion center. In order to ensure that the information collected and shared by fusion centers is both actionable and respectful of civil liberties, fusion centers should embrace the reasonable suspicion requirement and encourage independent audits of their files.

V. JOINT TERRORISM TASK FORCE OVERSIGHT

The most significant oversight problem with assigning police officers to JTTFs is that there is no mechanism geared towards ensuring compliance with state and local laws. This problem is exacerbated by the fact that rules relating to how police officers should act in the event of a conflict between their federal and state/local obligations are sometimes unknown and almost always unclear. Several municipalities and government reports have expressed concern that local officers assigned to JTTFs may be asked to engage in activities not permitted under state and local rules.

A 2005 report by the DOJ Inspector General found that the FBI did not have signed memoranda of understanding (MOUs) addressing these matters with many of the agencies participating in JTTFs.³³⁸ While 88 percent of the police departments in the Brennan Center survey now have MOUs, the language of these documents is ambiguous and provides little concrete guidance.*

For example, the Houston MOU cites the FBI guidelines as a “controlling document” with only a caveat that any conflict with state or local law “will be jointly resolved.”³³⁹ This hedging provides Houston officers with little practical instruction as to what to do in case of conflicts. In Detroit’s case, the police department signed an MOU with the JTTF but, disturbingly, it does not appear to have retained a copy.³⁴⁰

There is also an ongoing concern that the JTTF structure undermines state and local supervision of personnel and information. The FBI Special Agent in Charge of a JTTF supervises assigned police personnel.³⁴¹ These officers, deputized as United States Marshals, must obtain high-level security clearances.³⁴² But because JTTF operations are often classified, police commanders and city officials who commonly do not hold federal security clearances are unable to supervise and oversee the work of their own officers who are detailed to the JTTF.

The experiences of the Portland and San Francisco police departments demonstrate the problems police personnel can encounter when working on JTTFs. Oregon state law is stricter than the federal guidelines, and requires a criminal predicate before collecting information about political, religious, or social views.³⁴³ Recognizing this discrepancy, MOUs between the Portland Police Bureau and the FBI were (uncharacteristically) clear that should a conflict between the federal and local directives arise, Portland officers must comply with Oregon law.³⁴⁴ But the MOUs did not provide for any mechanism to review the work of Portland police assigned to JTTFs.³⁴⁵ Moreover, officers uncertain about their authority were not

* The NYPD and Dearborn Police Department are the only two local law enforcement agencies surveyed that claim not to have an MOU with the JTTF. *See* Letter from Richard Mantellino, Records Access Officer, N.Y.C. Police Dep’t, to Faiza Patel, Co-Director, Liberty & Nat’l Sec. Program, Brennan Ctr. for Justice (Mar. 2, 2012) (on file with the Brennan Center) (“A thorough and diligent search was conducted for Memorandums of Understanding between the NYPD and the FBI concerning the Joint Terrorist Task Force. However, no responsive records were located pursuant to our search.”); Letter from Office of the Corporate Counsel, City of Dearborn Mich., to Michael Price, Counsel, Brennan Ctr. for Justice (Mar. 21, 2012) (on file with the Brennan Center) (“There is no current MOU presently in force and copies of a past MOU are not available.”). *But see* Memorandum from Michael Jacobson, Assistant Gen. Counsel, Fed. Bureau of Investigation 4 (Sep. 5, 2003), available at <http://www.scribd.com/doc/61419208/FBI-NYPD-Joint-Terrorism-Task-Force-Dysfunction> (“There is a new updated MOU on D’Amuro’s desk which is very different from the previous MOUs. The previous MOUs were 3 pages, and this is a booklet, with a far different tone.”).

permitted to consult with the City Attorney to obtain legal advice about compliance with Oregon law.³⁴⁶ The FBI refused to allow the City Attorney to apply for the necessary security clearance or to assure the mayor and police chief that they would have access to the same information as their officers serving on the JTTF.³⁴⁷ Consequently, Portland withdrew from the JTTF in 2005, agreeing instead to work with the FBI on a case-by-case basis, if and when there was sufficient criminal predicate.³⁴⁸

The Portland Police Bureau rejoined the JTTF in 2010. The following year, the City Council passed a resolution clearly delineating the circumstances under which an officer could be detailed to a JTTF and providing for stronger oversight.³⁴⁹ The police chief can now assign officers to a JTTF on an as-needed basis but only for investigations “of suspected terrorism that have a criminal nexus.”³⁵⁰ In other words, the investigation must meet the reasonable suspicion requirement. Both the police chief and the Commissioner-in-Charge are to receive security clearances and the City Attorney is supposed to have access to classified information when necessary.³⁵¹ This would leave the FBI in control of JTTF investigations but permit supervisors to understand the context of their officers’ actions. Any officer asked to do something in violation of Oregon law must report the incident immediately to the police chief.³⁵² Finally, the police chief must provide an annual public report about Portland officers’ work for JTTFs.³⁵³

San Francisco confronted many of the same issues following a lengthy February 2011 report by the San Francisco Human Rights Commission. The study questioned whether San Francisco’s association with the JTTF compromised compliance with police policy,³⁵⁴ which requires reasonable suspicion of criminal activity before monitoring First Amendment-protected activity.³⁵⁵ Indeed, without informing the Police Commission or the public, the police department signed a revised MOU in 2007 that eliminated all provisions ensuring the full application of local rules to San Francisco officers participating in the JTTF.³⁵⁶ The MOU did not become public until 2011. The San Francisco Board of Supervisors responded by adopting an ordinance that requires local participation in the JTTF to be consistent with state and local privacy laws as well as department policies, procedures, and orders.³⁵⁷ The ordinance also mandates that any MOU with the JTTF be open to public notice and comment and that the police chief provide annual public reports on the police department’s work with the JTTF.³⁵⁸

Portland and San Francisco are national leaders in a “legislative approach” to defining local law enforcement participation in JTTFs. Other agencies surveyed still rely on MOUs that are not publicly debated and might perpetuate uncertainty about the law and create barriers to effective supervision and oversight of local officers.³⁵⁹ Five police departments have agreements like the 2007 San Francisco MOU that eliminate restrictions based on local laws.³⁶⁰

By passing local legislation, Portland and San Francisco provided clear, practical guidance to ensure that officers dispatched to JTTFs comply with state and local laws. These lawmakers set out procedures for annual audits and public reports. Local legislators, especially in jurisdictions with strong state privacy laws or local rules that require a criminal predicate before conducting intelligence activities, may do well to follow the examples of these two West Coast cities.

VI. CONCLUSION AND RECOMMENDATIONS

The need to adapt to new threats with speed and agility has fueled the transformation of state and local law enforcement since 9/11. But in the race to improve intelligence sharing across all levels of government, oversight and accountability have not kept pace. The entire homeland security enterprise runs on disparate and ambiguous rules about what intelligence information can or should be collected, maintained, and shared. The result has been a great deal of confusion, serious infringements on civil rights and civil liberties, and a pile of useless information.

We must recognize that giving local police broad new powers requires, at the very least, consistent rules and robust oversight. We would not set up a federal intelligence agency today without such safeguards, and it is dangerous to do so at the state and local level. Concrete steps to alleviate these concerns – at the federal, state, and local levels – are set out below.

Substantive Recommendations

When engaged in intelligence operations, law enforcement agencies should create, maintain, or share records of personal information only if there is reasonable suspicion of criminal activity and the information is relevant and material to that criminal activity.

- There must be a consistent, transparent standard for state and local intelligence activities. The Brennan Center believes that the reasonable suspicion standard is both consistent with our nation's core constitutional values and flexible enough to allow law enforcement to identify and investigate potential threats. State and local governments should require their police forces to adopt the reasonable suspicion standard for creating, maintaining, or sharing any intelligence records containing personal information. When the information contained in a record concerns First Amendment-protected activities, it must also directly relate to the suspected criminal activity.
- State and local governments should expressly prohibit the collection, maintenance, or dissemination of information that relies on race, ethnicity, national origin, or religious affiliation as a factor in establishing reasonable suspicion (except as part of a specific suspect description).

Fusion centers should not disseminate information that does not meet the reasonable suspicion requirement on any federally funded intelligence network.

- The Program Manager for the ISE should amend the Functional Standard to require reasonable suspicion of criminal activity, consistent with 28 CFR 23.
- The FBI should amend its eGuardian guidelines to require reasonable suspicion of criminal activity, consistent with 28 CFR 23.
- The DOJ should revise its guidance to clarify that sharing “temporary files,” “tips and leads” information, or SARs without reasonable suspicion of criminal activity is not permissible under 28 CFR 23.

Oversight Recommendations

Strengthen oversight of state and local intelligence activities with independent police monitors tasked with reviewing intelligence files and local supervision of officers working with federal agencies.

- Although the extent of oversight needed will depend on the size of the police department and the scope of its activities, the inspector general model has worked well for federal intelligence agencies and is most likely to produce the best oversight of state and local intelligence activities. Complaint-driven models – such as civilian complaint boards – are likely to prove ineffective due to the secretive nature of intelligence work.
- If a police department participates in a JTTF, the state or local legislature should require a publicly available, written MOU that preserves local supervision and includes clear rules for resolving any legal conflicts.

Require regular independent audits for fusion centers to ensure compliance with applicable laws and policies.

- As a condition of continued grant funding, DHS should require all fusion centers to fully implement their privacy policies and demonstrate compliance through regular independent audits available to the public.
- State and local governments that have created fusion centers should empower an independent auditor to review the center's files for compliance and publish a report of the findings.

The United States has a long and sordid history of spying on people with unpopular beliefs – a tragically predictable cycle of fear, excess, reprimand, and relapse that has threatened our liberty and our security time and again. We can do better. We must praise the good, but we must learn from our mistakes. We must strive to make the state and local role in national security more effective, rational, efficient, and fair. We must get smart on surveillance.

ENDNOTES

- 1 JOSIAH STAMP, SOME ECONOMIC FACTORS IN MODERN LIFE 258-59 (1929).
- 2 THE WHITE HOUSE, NATIONAL STRATEGY FOR COUNTERTERRORISM 11 (2011), available at http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf; see also Michael P. Downing, Commanding Officer, Counter-Terrorism/Criminal Intelligence Bureau, L.A. Police Dep't, Remarks at the Washington Institute: Counterterrorism and Crime Fighting in Los Angeles 6 (Oct. 22, 2009), available at <http://www.washingtoninstitute.org/html/pdf/LAPD-Stein.pdf>.
- 3 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-233, INFORMATION SHARING: ADDITIONAL ACTIONS COULD HELP ENSURE THAT EFFORTS TO SHARE TERRORISM-RELATED SUSPICIOUS ACTIVITY REPORTS ARE EFFECTIVE 32 (2013) [hereinafter "GAO-13-233"], available at <http://www.gao.gov/assets/660/652995.pdf>.
- 4 See *Law Enforcement and the Intelligence Community: Hearing Before the Nat'l Comm'n on Terrorist Attacks Upon the U.S.* (2004) (statement of John Brennan, Director, Terrorist Threat Integration Center), available at https://www.cia.gov/news-information/speeches-testimony/2004/brennan_testimony_04142004.html.
- 5 Sir Robert Peel famously proclaimed that the basic mission for which police exist is to "prevent crime and disorder as an alternative to the repression of crime and disorder by military force and severity of legal punishment." See CHARLES REITH, A SHORT HISTORY OF THE BRITISH POLICE 64 (1948).
- 6 See generally Paul G. Chevigny, *Politics and Law in the Control of Local Surveillance*, 69 CORNELL L. REV. 735, 768-775 (1984). For a detailed discussion of the history and substance of intelligence rules governing the police departments in this survey, see *infra*, notes 105-122, 128.
- 7 The FBI also loosened its investigative rules through repeated modifications to the Attorney General Guidelines. Compare RICHARD THORNBURGH, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS § III (1989), available at <http://www.justice.gov/ag/readingroom/generalcrimea.htm>, with JOHN ASHCROFT, U.S. DEPT' OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS § III.A.2.a (2002), available at <http://www.fas.org/irp/agency/doj/fbi/generalcrimes2.pdf>. For concerns raised by these new powers, see EMILY BERMAN, BRENNAN CTR. FOR JUSTICE, DOMESTIC INTELLIGENCE: NEW POWERS, NEW RISKS 26-37 (2011), available at <http://www.brennancenter.org/publication/domestic-intelligence-new-powers-new-risks>.
- 8 PERMANENT SUBCOMM. ON INVESTIGATIONS OF THE S. COMM. ON HOMELAND SEC. AND GOVERNMENTAL AFFAIRS, 112TH CONG., FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 2 (2012) [hereinafter 2012 SENATE HSGAC FUSION CENTER REPORT], available at <http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04>.
- 9 *Id.*; GAO-13-233, *supra* note 3, at 33-38.
- 10 See, e.g., MATT APUZZO AND ADAM GOLDMAN, ENEMIES WITHIN 89 (2013) (Chronicling how "[a]fter years of raking, the NYPD knew where New York's Muslims were ... [but] [t]hey still didn't know where the terrorists were. And they didn't know a thing about [Najibullah] Zazi," an al-Qaeda-trained U.S. citizen convicted of plotting to bomb the New York subway system. The NYPD had files on the restaurants in Zazi's neighborhood, on his mosque, and on the travel agency where he bought his plane tickets to Pakistan - none of which offered any early warning of the plot or proved useful in locating Zazi.).
- 11 Michael B. Ward, the special agent in charge of the FBI's Newark office, explained: "People are concerned that they are being followed, ... that they can't trust law enforcement, and it's having a negative impact." Al Baker, *F.B.I. Official Faults Police Tactics on Muslims*, N.Y. TIMES, Mar. 7, 2012, available at <http://www.nytimes.com/2012/03/08/nyregion/chief-of-fbi-newark-bureau-decries-police-monitoring-of-muslims.html>; Jason Grant, *Recent NYPD Spying Uproar Shakes FBI's Foundations in N.J.* *Terror Intelligence*, N.J. STAR-LEDGER, Mar. 7, 2012, available at http://www.nj.com/news/index.ssf/2012/03/recent_nypd_spying_uproar_shak.html.
- 12 *Joint Terrorism Task Force*, U.S. DEP'T OF JUSTICE, <http://www.justice.gov/jttf/> (last visited Feb. 28, 2012).
- 13 *State and Major Urban Area Fusion Centers*, U.S. DEP'T OF HOMELAND SECURITY, <http://www.dhs.gov/state-and-major-urban-area-fusion-centers> (last visited July 12, 2013).

- 14 See, e.g., CONSTITUTION PROJECT, RECOMMENDATIONS FOR FUSION CENTERS: PRESERVING PRIVACY & CIVIL LIBERTIES WHILE PROTECTING AGAINST CRIME & TERRORISM (2012) [hereinafter RECOMMENDATIONS FOR FUSION CENTERS], available at <http://www.constitutionproject.org/pdf/fusioncenterreport.pdf>; Milton Nenneman, An Examination of State and Local Fusion Centers and Data Collection Methods 78-86 (Mar. 2008) (unpublished thesis, Naval Postgraduate School), available at <https://www.fas.org/irp/eprint/fusion.pdf>; David Thacher, *The Local Role in Homeland Security*, 39 LAW & SOC'Y REV. 635 (2005); John G. Comiskey, Effective State, Local, and Tribal Police Intelligence: The New York City Police Department's Intelligence Enterprise – A Smart Practice 13-19 (Mar. 2010) (unpublished thesis, Naval Postgraduate School), available at http://edocs.nps.edu/npspubs/scholarly/theses/2010/Mar/10Mar_Comiskey.pdf.
- 15 *Crime in the United States: Full-time Civilian Law Enforcement Employees by Population Group, Percent of Total, 2011*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2011/crime-in-the-u.s.-2011/tables/table_75_full-time_civilian_law_enforcement_employees_by_population_group_percent_of_total_2011.xls (last visited Mar. 1, 2013).
- 16 GAO-13-233, *supra* note 3, at 10.
- 17 INFO. SHARING ENV'T, ANNUAL REPORT TO THE CONGRESS 7 (2013) [hereinafter ISE ANNUAL REPORT], available at www.ise.gov/sites/default/files/2013_ISE_Annual_Report_Final.pdf.
- 18 Press Release, Fed. Bureau of Investigation, 2011 Request for Information on Tamerlan Tsarnaev from Foreign Government (Apr. 19, 2013), available at <http://www.fbi.gov/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government>.
- 19 See Michael Rezendes, *Bombing Case Casts Shadow Over Waltham Triple Murder*, BOSTON GLOBE (Jun. 8, 2013), available at <http://www.bostonglobe.com/metro/2013/06/07/waltham-triple-homicide-raises-troubling-question-about-marathon-bombing/mj2MwjWEZnZqYPRDixQX4I/story.html>; Margaret Hartmann, *Police Let Tsarnaev Get Away With 2011 Murder, or Had No Evidence*, N.Y. MAGAZINE (Jul. 11, 2013), available at <http://nymag.com/daily/intelligencer/2013/07/did-officials-fail-to-nab-tsarnaev-for-murder.html>; Michael Daly, *How Local Police Missed a Chance to Stop Tamerlan Tsarnaev in 2011*, DAILY BEAST (Jul. 12, 2013), available at <http://www.thedailybeast.com/articles/2013/07/12/how-local-police-missed-a-chance-to-stop-tamerlan-tsarnaev-in-2011.html>.
- 20 See Paul Lewis, *Boston Police Urge FBI to Share Intelligence as Tsarnaev Is in Court*, GUARDIAN, Jul. 10, 2013, available at <http://www.theguardian.com/world/2013/jul/10/boston-police-fbi-tsarnaev-court>.
- 21 See Michael Isikoff, *Unaware of Tsarnaev Warnings, Boston Counterterrorism Unit Tracked Protesters*, NBC NEWS (May 10, 2013), available at <http://investigations.nbcnews.com/news/2013/05/10/18152849-unaware-of-tsarnaev-warnings-boston-counterterrorism-unit-tracked-protesters>.
- 22 See LOIS M. DAVIS ET AL., RAND CORP., LONG-TERM EFFECTS OF LAW ENFORCEMENT'S POST-9/11 FOCUS ON COUNTERTERRORISM AND HOMELAND SECURITY 107-11 (2010) [hereinafter 2010 RAND REPORT], available at http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG1031.pdf.
- 23 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 3 (“The Subcommittee investigation also found that DHS failed to adequately police how states and municipalities used the money intended for fusion centers. The investigation found that DHS did not know with any accuracy how much grant money it has spent on specific fusion centers, nor could it say how most of those grant funds were spent, nor has it examined the effectiveness of those grant dollars.”).
- 24 GAO-13-233, *supra* note 3, at 35.
- 25 See e.g., RECOMMENDATIONS FOR FUSION CENTERS, *supra* note 14, at 9-11; AM. CIVIL LIBERTIES UNION, SPYING ON FIRST AMENDMENT ACTIVITY – STATE-BY-STATE (2011), available at http://www.aclu.org/files/assets/policingfreepresspeech_20111103.pdf; Adam Goldman & Matt Apuzzo, *With CIA Help, NYPD Moves Covertly in Muslim Areas*, ASSOCIATED PRESS (Aug. 23, 2011), available at <http://ap.org/Content/AP-In-The-News/2011/With-CIA-help-NYPD-moves-covertly-in-Muslim-areas>.
- 26 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 2.
- 27 Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. NAT'L SECURITY L. & POL'Y 377, 380-81 (2009).

- 28 NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT: FINAL REPORT OF THE
NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 427 (2004) [hereinafter 9/11 REPORT],
available at <http://www.9-11commission.gov/report/911Report.pdf>.
- 29 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (establishing the Department of Homeland
Security). Congress tasked DHS with commissioning an independent study on the feasibility of creating a domestic
intelligence agency. The RAND Corporation conducted the study and published its findings in 2009, assessing the merits
of various configurations, but Congress ultimately took no action. See RAND CORP., CONSIDERING THE CREATION OF
A DOMESTIC INTELLIGENCE AGENCY IN THE UNITED STATES: LESSONS FROM THE EXPERIENCES OF AUSTRALIA, CANADA,
FRANCE, GERMANY, AND THE UNITED KINGDOM (Brian A. Jackson, ed. 2009), available at [http://www.rand.org/
content/dam/rand/pubs/monographs/2009/RAND_MG805.pdf](http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG805.pdf); see also 9/11 REPORT, *supra* note 28, at 423-424.
- 30 See U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES: 2012, FEDERAL CIVILIAN EMPLOYMENT
BY BRANCH AND AGENCY: 1990 TO 2010 (2012), available at [http://www.census.gov/compendia/statab/2012/
tables/12s0499.pdf](http://www.census.gov/compendia/statab/2012/
tables/12s0499.pdf).
- 31 Robert Mueller, Dir., Fed. Bureau of Investigation, Address at Stanford Law School: Terrorism in a Post-9/11 World (Oct.
19, 2002), available at <http://www.fbi.gov/news/speeches/terrorism-in-a-post-9-11-world> (“Of course, we will continue
to investigate criminal cases and are proud of our work in such areas as violent crime, organized crime, financial fraud,
civil rights, and public corruption. But in the wake of September 11th, our first and abiding priority, plain and simple,
is counterterrorism. That priority is to stop another attack like we saw on September 11th. To do that, we have to enter
into an age of preventive investigation. At the heart of our attack on counterterrorism is this massive redeployment of
Agents from other programs.”). See also FED. BUREAU OF INVESTIGATION, U.S. DEP’T OF JUSTICE, REPORT TO NATIONAL
COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES: THE FBI’S COUNTERTERRORISM PROGRAM SINCE
SEPTEMBER 2001 12 (2004), available at http://www.fbi.gov/stats-services/publications/fbi_ct_911com_0404.pdf.
- 32 BERMAN, *supra* note 7, at 17.
- 33 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1021(3)(d), 118 Stat. 3638,
3673.
- 34 *Id.*
- 35 OFFICE OF JUSTICE PROGRAMS, U.S. DEP’T OF JUSTICE, THE NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN 43-
46 (2003) [hereinafter NCISP 2003], available at <http://www.fas.org/jrp/agency/doj/ncisp.pdf> (“Recommendation
22: Interoperability with existing systems at the local, state, tribal, regional, and federal levels with the RISS/
LEO communications capability should proceed immediately, in order to leverage information sharing systems
and expand intelligence sharing.”); Deborah J. Daniels, *From the Assistant Attorney General: Increasing Information
Sharing to Help Reduce Crime and Respond to Emergencies*, 71 THE POLICE CHIEF, no. 10, Oct., 2004, available
at [http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1402&issue
id=102004](http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1402&issue
id=102004).
- 36 DAVID L. CARTER, LAW ENFORCEMENT INTELLIGENCE: A GUIDE FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT
AGENCIES 344 (Office of Cmty. Oriented Policing Servs., U.S. Dep’t of Justice, 2nd ed. 2009), available at [www.
it.ojp.gov/docdownloader.aspx?ddid=1133](http://www.
it.ojp.gov/docdownloader.aspx?ddid=1133).
- 37 CHRISTOPHER DICKEY, SECURING THE CITY: INSIDE AMERICA’S BEST COUNTERTERROR FORCE—THE NYPD 99-
216 (Simon & Schuster 2009) [hereinafter SECURING THE CITY]; LEONARD LEVITT, NYPD CONFIDENTIAL: POWER
AND CORRUPTION IN THE COUNTRY’S GREATEST POLICE FORCE 232-83 (Thomas Dunne Books 2009); *Preliminary
Budget Hearing for Fiscal Year 2013 and the Fiscal Year 2012 Mayor’s Management Report: Hearing Before the N.Y.C.
Council Pub. Safety Comm.* 21-25 (2012) (testimony of Raymond Kelly, Chief, New York City Police Department),
available at [http://legistar.council.nyc.gov/View.ashx?M=F&ID=1828553&GUID=FD7A13D2-9BF4-4898-
8309-8BADF961BB38](http://legistar.council.nyc.gov/View.ashx?M=F&ID=1828553&GUID=FD7A13D2-9BF4-4898-
8309-8BADF961BB38); George L. Kelling & William J. Bratton, *Policing Terrorism*, CIVIC BULLETIN, Sept. 2006,
at 5-6, available at http://www.manhattan-institute.org/pdf/cb_43.pdf.
- 38 CARTER, *supra* note 36, at 80.
- 39 MARILYN PETERSON, INT’L ASS’N OF CHIEFS OF POLICE, INTELLIGENCE-LED POLICING: THE NEW INTELLIGENCE
ARCHITECTURE 3-4 (2005), available at <https://www.ncjrs.gov/pdffiles1/bja/210681.pdf>.
- 40 The NYPD, for example, asserts that it has thwarted or helped thwart at least 14 terrorist plots against New
York City. But a widely-cited investigation by ProPublica found that the figure “overstates both the number of
serious, developed terrorist plots against New York and exaggerates the NYPD’s role in stopping attacks.” Justin

- Elliott, *Fact-Check: How the NYPD Overstated Its Counterterrorism Record*, PROPUBLICA (July 10, 2012, 9:33 AM), <http://www.propublica.org/article/fact-check-how-the-nypd-overstated-its-counterterrorism-record>. See also *All Things Considered: Counterterrorism and the NYPD*, NAT'L PUB. RADIO (Jul. 15, 2012), available at <http://www.npr.org/2012/07/15/156815759/counterterrorism-and-the-nypd>; Leonard Levitt, *Lone Wolves or Sheep?*, NYPD CONFIDENTIAL (Mar. 19, 2012), <http://nypdconfidential.com/columns/2012/120319.html>; CTR. FOR HUMAN RIGHTS AND GLOBAL JUSTICE, *TARGETED AND ENTRAPPED: MANUFACTURING THE "HOMEGROWN THREAT" IN THE UNITED STATES* 38 (2011), available at <http://chrgj.org/wp-content/uploads/2012/07/targetedandentrapped.pdf>. The Senate Homeland Security Committee and the Government Accountability Office have also raised serious concerns about the quality of intelligence generated by fusion centers and Suspicious Activity Reporting programs. See 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 2; GAO-13-233, *supra* note 3, at 33-38.
- 41 Declaration of Deputy Commissioner David Cohen at ¶ 52, *Handschu v. Special Servs. Div.*, 273 F. Supp. 2d 327 (S.D.N.Y. 2003) (No. 71 Civ. 2203).
- 42 See generally FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, *RETHINKING RADICALIZATION* (2011), available at <http://www.brennancenter.org/publication/rethinking-radicalization>.
- 43 Colin Moynihan, *Wall Street Protesters Complain of Police Surveillance*, N.Y. TIMES, Mar. 11, 2012, available at <http://www.nytimes.com/2012/03/12/nyregion/occupy-wall-street-protesters-complain-of-police-monitoring.html>.
- 44 KEVIN STROM, ET AL., INST. FOR HOMELAND SEC. SOLUTIONS, *BUILDING ON CLUES: EXAMINING SUCCESSES AND FAILURES IN DETECTING U.S. TERRORIST PLOTS, 1999-2009* 12 (2010), available at http://sites.duke.edu/ihss/files/2011/12/Building_on_Clues_Strom.pdf. Only federal law enforcement sources (30 percent) rival the importance of public tips (29 percent) in foiling terrorist plots. *Id.* Moreover, the vast majority of initial clues – 78 percent – did *not* come from local law enforcement. *Id.*
- 45 Statement of Interest of the United States at 10, *Floyd v. City of New York*, 2013 WL 4046209 (S.D.N.Y. 2013) (No. 08 Civ. 1034).
- 46 Stephen J. Schulhofer, Tom R. Tyler & Aziz Z. Huq, *American Policing at a Crossroads: Unsustainable Policies and the Procedural Justice Alternative*, 101 J. OF CRIM. L. & CRIMINOLOGY 335, 369 (2011); see also MUSLIM AM. CIVIL LIBERTIES COAL. ET AL., *MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS* 32-28 (2013) [hereinafter *MAPPING MUSLIMS*], available at <http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf>.
- 47 See, e.g., FINAL REPORT OF THE WILLIAM H. WEBSTER COMMISSION ON THE FEDERAL BUREAU OF INVESTIGATION, COUNTERTERRORISM INTELLIGENCE, AND THE EVENTS AT FT. HOOD, TEXAS, ON NOVEMBER 5, 2009, 88 (2012) (finding that the “exponential growth in the amount of electronically stored information” posed a critical challenge to the FBI in its assessment of Nidal Hasan, creating “relentless” demands on a limited number of personnel), available at <http://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission>.
- 48 FRANK J. CILLUFFO ET AL., THE GEO. WASH. UNIV. HOMELAND SEC. POLICY INST., *COUNTERTERRORISM INTELLIGENCE: FUSION CENTER PERSPECTIVES* 31 (2012), available at <http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf> [hereinafter 2012 HSPI REPORT].
- 49 See generally PETERSON, *supra* note 40.
- 50 See, e.g., NCISP 2003, *supra* note 35, at viv (“the primary purpose of intelligence-led policing is to provide public safety decision makers the information they need to protect the lives of our citizens.”); Jerry H. Ratcliffe, *Intelligence-Led Policing*, in ENVIRONMENTAL CRIMINOLOGY AND CRIME ANALYSIS 263, 268 (Richard Wortley & Lorraine Mazerolle eds., 2008) (“Intelligence-led policing is a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders.”); GLOBAL JUSTICE INFO. SHARING INITIATIVE, U.S. DEP’T OF JUSTICE, *NAVIGATING YOUR AGENCY’S PATH TO INTELLIGENCE-LED POLICING* 3 (2009), available at <http://www.it.ojp.gov/docdownloader.aspx?ddid=1082> (“Intelligence-led policing (ILP) is a business process for systematically collecting, organizing, analyzing, and utilizing intelligence to guide law enforcement operational and tactical decisions.”).
- 51 2010 RAND Report, *supra* note 22, at 4.

52 The Brennan Center characterized the police departments in this report based in large part on self-identifying statements in annual reports and internal strategy documents. A handful of departments do not describe their overall approach as “intelligence-led” but explicitly use elements of the philosophy in officer training or specific programs. The Los Angeles and Minneapolis Police Departments ascribe to “predictive policing,” which is a variant of intelligence-led policing.

53 SECURING THE CITY, *supra* note 37, at 171-72.

54 *Hearing Before the Nat’l Comm’n on Terrorist Attacks Upon the U.S.* 2-3 (2004) (testimony of Raymond Kelly, Chief, New York Police Department) [hereinafter *Kelly May 18, 2004 Testimony*], available at http://www.globalsecurity.org/security/library/congress/9-11_commission/040518-kelly.pdf; see also Charlie Savage, *C.I.A. Report Finds Concerns With Ties to New York Police*, N.Y. TIMES, Jun. 26, 2013, available at <http://www.nytimes.com/2013/06/27/nyregion/cia-sees-concerns-on-ties-to-new-york-police.html>.

55 *International Liaison Program*, NEW YORK CITY POLICE FOUND., <https://www.nycpolicefoundation.org/netcommunity//Page.aspx?pid=639> (last visited April 21, 2013).

56 *See generally Highlights of AP’s Pulitzer Prize-Winning Probe Into NYPD Intelligence Operations*, ASSOCIATED PRESS, <http://www.ap.org/media-center/nypd/investigation> (last visited Feb. 28, 2012); *AP’s Probe Into NYPD Intelligence Operations*, ASSOCIATED PRESS, <http://www.ap.org/Index/AP-In-The-News/NYPD#tpHdr> (last visited Feb. 28, 2012).

57 N.Y. POLICE DEP’T, INTELLIGENCE DIVISION 18-26 (n.d.) [hereinafter *NYPD DEMOGRAPHICS UNIT DOCUMENT*], available at <http://enemieswithinbook.com/documents/Analytical%20Units%20PowerPoint.pdf>.

58 Confidential informants and undercover officers were sent to monitor so-called “hot spots” by eavesdropping and noting “extremist” literature or rhetoric. *Id.* at 2. The NYPD formed teams to collect this information, using one detective “handler” to supervise undercover officers called “rakers.” *Id.* at 7. The “rakers” would visit communities “consistent with their ethnicity and or language” and report information on a daily basis. *Id.*; see also Apuzzo & Goldman, *supra* note 25. At businesses, officers were instructed to “determine the ethnicity of the owner,” “gauge sentiment” by “interacting, observing and conversing with owners and patrons,” “[p]urchase extremist literature or paraphernalia” and determine if the business is “facilitating criminal acts which may be enablers of terrorism” such as untaxed cigarettes, narcotics, or sales of fraudulent identity documents. *NYPD DEMOGRAPHICS UNIT DOCUMENT*, at 23. The Intelligence Division also deploys informants known as “mosque crawlers” to monitor sermons and conversations among congregants. Apuzzo & Goldman, *supra* note 25. It has created an intelligence file for every mosque within 100 miles of New York City, *id.*, and prepared analytical reports on the reaction to news events such as a Danish newspaper’s publication of 12 cartoons depicting the Prophet Mohammed or the shooting death of Sean Bell, an African American man who died in a hail of police bullets outside a Queens nightclub. N.Y. POLICE DEP’T, *NYPD INTELLIGENCE NOTE: NYC MOSQUE STATEMENTS ON DANISH CARTOON CONTROVERSY* (2006), available at http://hosted.ap.org/specials/interactives/documents/nypd/nypd_cartoons.pdf; INTELLIGENCE DIVISION, N.Y. POLICE DEP’T, *DEPUTY COMMISSIONER’S BRIEFING* (2008) [hereinafter *APRIL 25, 2008 BRIEFING*], available at <http://hosted.ap.org/specials/interactives/documents/nypd/dci-briefing-04252008.pdf>.

59 N.Y. POLICE DEP’T, *WEEKLY MSA REPORT 3* (2006), available at <http://hosted.ap.org/specials/interactives/documents/nypd-msa-report.pdf>. In one highly publicized incident, the NYPD infiltrated a student whitewater-rafting trip using an informant who reported on how often the students prayed and the religious content of their conversations. *APRIL 25, 2008 BRIEFING*, *supra* note 58, at 3-4.

60 *See* Declaration of Paul Chevigny at ¶ 4, *Handschu v. Special Servs. Div.*, No. 71 Civ. 2203 (S.D.N.Y. Feb. 4, 2013) (on file with the Brennan Center); First Amended Complaint at 21-22, *Hassan v. New York*, No. 12-03401 (D.N.J. Oct. 3, 2012), available at http://www.ccrjustice.org/files/10_First%20Amended%20Complaint.10.3.2012.pdf; Complaint at 1, *Raza v. New York*, No. 13 Civ. 03448 (E.D.N.Y., Jun. 18, 2013), available at http://www.aclu.org/files/assets/nypd_surveillance_complaint_-_final_06182013_0.pdf.

61 *See* David A. Harris, *Law Enforcement and Intelligence Gathering in Muslim and Immigrant Communities After 9/11*, 34 N.Y.U. REV. L. & SOC. CHANGE 123, 161-168 (2010); David H. Bayley & David Weisburd, *Cops and Spooks: The Role of the Police in Counterterrorism*, in *TO PROTECT AND TO SERVE: POLICING IN AN AGE OF TERRORISM* 94-95 (David Weisburd et al. eds., 2009), available at <http://www.scribd.com/doc/97752927/Policing-in-Age-of-Terrorism> (“The problem is that a single episode of thoughtlessness or overreaching may undermine public trust. Perception is everything. The loss of public confidence is especially costly for the success of counterterrorism itself if it increases the alienation of minority and immigrant communities.”).

- 62 Letter from Imam al-Hajj Talib ‘Abdur-Rashid, Imam, The Mosque of Islamic Brotherhood, et al., to Michael Bloomberg, Mayor of the City of New York (Dec. 29, 2011), *available at* <http://interfaithletter.wordpress.com/>; *Some Local Muslims Boycott NYPD’s Annual Pre-Ramadan Conference*, NY1 (Jul. 11, 2012), http://manhattan.ny1.com/content/top_stories/164630/some-local-muslims-boycott-nypd-s-annual-pre-ramadan-conference; *Muslims to Boycott NY Mayor’s Interfaith Breakfast*, MSNBC.COM (Dec. 29, 2011, 5:29 PM), http://www.msnbc.msn.com/id/45814786/ns/us_news-life/t/muslims-boycott-ny-mayors-interfaith-breakfast/; MAPPING MUSLIMS, *supra* note 46, at 37.
- 63 Chris Hawley, *Muslim Groups Hold Rally After NYPD Intel Report*, WABC-TV N.Y.C. (Feb. 3, 2012), http://abclocal.go.com/wabc/story?section=news/local/new_york&cid=8530224; Samantha Gross & Tom Hays, *Muslims Call for NYPD Chief to Resign Over Movie*, WALL ST. J., Jan. 26, 2012, *available at* <http://online.wsj.com/article/APbe6d40631fdb4cc89bc868e32ba0aace.html>; *New York Muslims to rally against NYPD*, PRESS TV (Feb. 1, 2012), <http://presstv.com/detail/224295.html>; Christie Thompson, *Momentum Builds in the Fight Against Stop-and-Frisk*, THE NATION, Oct. 31, 2012, *available at* <http://www.thenation.com/article/170944/momentum-builds-fight-against-stop-and-frisk>.
- 64 Richard Winton & Teresa Watanabe, *LAPD’s Muslim mapping plan killed*, L.A. TIMES, Nov. 15, 2007, *available at* <http://articles.latimes.com/2007/nov/15/local/me-muslim15>; *The Role of Local Law Enforcement in Countering Violent Islamic Extremism: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. 7 (2007) (statement of Michael P. Downing, Commanding Officer, Counter-Terrorism/Criminal Intelligence Bureau, Los Angeles Police Department), *available at* <http://www.lapdonline.org/assets/pdf/Michael%20DowningTestimonyfortheU.S.Senate-Final.PDF>; Letter from Ranjana Natarajan, Staff Attorney, Am. Civil Liberties Union of S. Cal., to Michael P. Downing, Commanding Officer, Counter-Terrorism/Criminal Intelligence Bureau, L.A. Police Dep’t (Nov. 8, 2007) (on file with the Brennan Center) (“In addition to constitutional concerns that such a practice would violate equal protection and burden the free exercise of religion, religious profiling engenders fear and distrust in the community that hampers law enforcement efforts. A mapping project that aims only to gather intelligence and identify ‘risk factors’ unfairly targets members of the Muslim community based on their religion and ethnicity, and also increases the inaccurate perception among the larger community that Muslims are doing something suspicious that merits investigation.”).
- 65 Hugh Dellios, *Garry McCarthy, Chicago Police Chief, Pledges No NYPD-esque Spying on Muslims*, HUFFINGTON POST (Mar. 4, 2012, 4:04 PM), http://www.huffingtonpost.com/2012/03/04/chicago-police-chief-pled_0_n_1319515.html.
- 66 CHI. POLICE DEP’T, GENERAL ORDER G02-04: PROHIBITION REGARDING RACIAL PROFILING AND OTHER BIAS-BASED POLICING I(B) (2012), *available at* <http://directives.chicagopolice.org/directives/data/a7a57be2-1287e496-14312-87ee-0dae86849cf9f737.html>.
- 67 EMERGENCY OPERATIONS BUREAU, L.A. CNTY. SHERIFF’S DEP’T, UNIT ORDER NO. 5: INTELLIGENCE GUIDELINES 2 (n.d.) (on file with the Brennan Center).
- 68 *The Extent of Radicalization in the American Muslim Community and the Community’s Response: Hearing Before the H. Comm. On Homeland Sec.*, 112th Cong. 2 (2011) [hereinafter Baca Testimony 2011] (statement of Leroy Baca, Sheriff, L.A. Sheriff’s Dep’t), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Baca_0.pdf.
- 69 *Id.*
- 70 The Brennan Center conducted interviews with over a dozen Arab and South Asian community leaders and advocates in Los Angeles for this report. Two of them were willing to go on the record. Personal Interview with Personal Interview with Zohab Munshi, Founding Member, Young Muslim American Leaders Advisory Council (Sept. 20, 2013); Personal Interview with Ameena Qazi, Deputy Executive Director and Staff Attorney, Council on American Islamic Relations (CAIR) of Los Angeles, Feb. 22, 2013. In the wake of the July 7, 2005 London bombings, the LASD partnered with members of the Muslim American community to establish a “Muslim American Homeland Security Congress” (MAHSC) that includes the Council on American Islamic Relations (CAIR), the Islamic Shura Council of Southern California, the Muslim Public Affairs Council, and the Muslim American Society. *Muslim American Homeland Security Congress (MAHSC)*, FACEBOOK, <http://www.facebook.com/pages/Muslim-American-Homeland-Security-Congress-MAHSC/199844210096880?id=199844210096880&sk=info> (last visited Mar. 4, 2013); The group facilitates dialogue and partnership between law enforcement and the Muslim community through town hall meetings, trainings, seminars and presentations. Hussam Ayloush, the

- executive director of CAIR-Los Angeles, called the relationship “an example for the rest of the nation to emulate.” CAIR-LA, *Calif. Muslims Hold Law Enforcement Training Conference*, FACEBOOK, <http://www.facebook.com/notes/cair/cair-la-calif-muslims-hold-law-enforcement-training-conference/10150936570909442> (last visited Mar. 4, 2013). See also Laurie Goodstein, *Police in Los Angeles Step Up Efforts to Gain Muslims’ Trust*, N.Y. Times, Mar. 9, 2011, available at <http://www.nytimes.com/2011/03/10/us/10muslims.html>.
- 71 Dave Zirin, *Not a Game: How the NYPD Uses Sports for Surveillance*, THE NATION, Sept. 10, 2013, available at <http://www.thenation.com/blog/176082/not-game-how-nypd-uses-sports-surveillance#>; see also N.Y. POLICE DEPT., SPORTS VENUE REPORT 2 (n.d.), available at <http://s3.documentcloud.org/documents/779743/demographics-sports-venues.pdf>.
- 72 Personal Interview with Debbie Almontaser, President, Muslim Consultative Network (Mar. 29, 2013). Furthermore, according to a former member of the NYPD’s Muslim Advisory Council, established in 2012, the NYPD’s willingness to receive and engage feedback from Muslim leaders has been lackluster at best. Personal Correspondence with Asim Rehman, President, Muslim Bar Association of New York (Jun. 27, 2013). Following revelations that the NYPD is using “terrorism enterprise investigations” to put entire mosques and Muslim non-profit organizations under intensive surveillance, Dr. Ahmad Jaber, another member of the NYPD’s Advisory Council, resigned in protest. Documents indicated that the NYPD had attempted to place an informant on the board of the Arab American Association of New York, a Brooklyn-based social services organization; Dr. Jaber is the organization’s president. Mary Murphy, *Muslim Doctor Resigns from NYPD Advisory Board after Alleged Secret Investigations*, PIX 11, Aug. 29, 2013, available at <http://pix11.com/2013/08/29/muslim-doctor-resigns-from-nypd-advisory-board-as-backlash-grows/>; Kerry Burke and Tina Moore, ‘New NYPD Low’: Muslims Outraged by ‘Terror Enterprise’ Mosque Probes, N.Y. DAILY NEWS, Aug. 28, 2013, available at <http://www.nydailynews.com/new-york/new-nypd-muslims-outraged-terror-enterprise-mosque-probes-article-1.1439951>.
- 73 See Patrick A. Burke, *Collecting and Connecting the Dots: Leveraging Technology to Enhance the Collection of Information and the Dissemination of Intelligence* 29-30 (Sept. 2009) (unpublished thesis, Naval Postgraduate School), available at <https://www.hsdl.org/?view&did=33358>. To the extent that a shift towards intelligence-led policing also entails the redistribution of personnel and resources, it may disrupt more traditional police functions. According to a 2010 study by the RAND Corporation, a 1% reduction in sworn personnel devoted to routine crime fighting would result in at least \$4.7 million in crime costs and an additional two homicides per year. 2010 RAND Report, *supra* note 22, at 99. While this cost might be reasonable compared to the cost of another successful terrorist attack, it is not at all clear that “community mapping” or eavesdropping at cafes are effective means of preventing a terrorist incident. Indeed, NYPD Assistant Chief Thomas Galati testified in 2012 that the Demographics Unit has produced no actionable intelligence in at least the past six years, and perhaps longer. Transcript of Examination Before Trial at 124, *Handschu v. Special Servs. Div.*, 273 F.Supp.2d 327 (S.D.N.Y. June 28, 2012) (No. 71 Civ. 2203) (testimony of Thomas Galati, Assistant Chief, NYPD), available at http://www.nyclu.org/files/releases/Galati_EBT_6.28.12.pdf.
- 74 Officers tasked with guarding transportation infrastructure, such as ports or airport terminals, may well have counterterrorism responsibilities even if they are not described as counterterrorism personnel. In Seattle, for example, one assistant chief is responsible for overseeing “the day to day operations of the Traffic Section, Parking Enforcement, Homeland Security, the Intelligence Section and the Metropolitan Section (SWAT, Canine, Mounted, Crisis Intervention, and Harbor Patrol).” *Seattle Police Chief Diaz Reorganizes Command Structure*, W. SEATTLE HERALD, Sept. 15, 2010, <http://www.westseattleherald.com/2010/09/15/news/seattle-police-chief-diaz-reorganizes-command-str>.
- 75 See Greg Krikorian, *Terrorism Early Warning Group Works to Keep L.A.’s Guard Up*, L.A. TIMES, Nov. 7, 2004, available at <http://articles.latimes.com/2004/nov/07/local/me-terror7>. The LAPD had an “Anti-Terrorist Division” pre-9/11, “formed prior to 1984 Summer Olympics in the aftermath of the 1983 dismantling of the department’s scandal-ridden Public Disorder Intelligence Division.” William Overend, *Schlei Bids a Tearful Farewell to LAPD*, L.A. TIMES, Sept. 21, 1988, available at http://articles.latimes.com/1988-09-21/local/me-2305_1_tearful-farewell; see generally L.A. TERRORISM EARLY WARNING GRP., TERRORISM EARLY WARNING: 10 YEARS OF ACHIEVEMENT IN FIGHTING TERRORISM AND CRIME (John P. Sullivan & Alain Bauer eds., 2008), available at http://file.lacounty.gov/lasd/cms1_144939.pdf.
- 76 This is consistent with the national trend, identified by the DOJ in a 2007 report, which determined that more than 90% of local police departments serving a population of 500,000 or more have such personnel. BRIAN A.

- REAVES, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, LOCAL POLICE DEPARTMENTS, 2007, at 32 (2010), available at <http://www.bjs.gov/content/pub/pdf/lpd07.pdf>. It is also consistent with recommendations from the International Association of Chiefs of Police and the National Criminal Intelligence Sharing Plan. See INT'L ASS'N OF CHIEFS OF POLICE & OFFICE OF CMTY. ORIENTED POLICING, NATIONAL PLAN FOR INTELLIGENCE-LED POLICING AT THE LOCAL, STATE AND FEDERAL LEVELS vii, 9-10 (2002), available at http://www.ncirc.gov/documents/public/supplementaries/intel_sharing_report.pdf; NCISP 2003, *supra* note 35, at 21-22.
- 77 The DPD appears to have devoted little of its own resources to counterterrorism intelligence work. Instead, the city and state stepped in to fill this role. The City of Detroit formed an Office of Homeland Security, which is responsible for counterterrorism planning and operations, emergency management, and the protection of critical infrastructure and resources. According to the city's 2012-2013 budget, the Office of Homeland Security will be consolidated under the control of the DPD. However, it is comprised of just two employees (a director and an emergency management specialist) whose counterterrorism intelligence duties remain unclear. See BUDGET DEP'T, CITY OF DETROIT, *Detroit Office of Homeland Security*, in EXECUTIVE BUDGET 46-1, 46-5 (2012), available at http://www.detroitmi.gov/Portals/0/docs/budgetdept/2012-13%20Budget/Executive%20Budget/46%20EB%2012-13%20Detroit%20Office%20of%20Homeland%20Security_stamped.pdf; BUDGET DEP'T, CITY OF DETROIT, EXECUTIVE BUDGET SUMMARY A8, B43 (2012), available at http://www.detroitmi.gov/Portals/0/docs/budgetdept/2012-13%20Budget/Executive%20Summary/Budget_2012-13%20OVERVIEW.pdf; see also BUDGET DEPARTMENT, CITY OF DETROIT, *Departmental Budget Information: Detroit Office of Homeland Security*, in EXECUTIVE BUDGET 46-1, 46-2 (2007), available at http://www.detroitmi.gov/Portals/0/docs/budgetdept/2007-08_Budget/Summary/EBS_46_HOMELAND%20SECURITY_07-08.pdf. The Office has worked closely with the state to establish a regional fusion center called the "Detroit and Southeast Michigan Information and Intelligence Center" (DSEMIIC), which adopts an "all crimes, all hazards" approach that includes terrorism. See DETROIT & SE. MICH. INFO. CTR., PRIVACY POLICY 4 (n.d.) (discussion draft), available at <http://www.nfcausa.org/files/DDF/DetroitPrivacyPolicy.pdf>; IJIS INST., TA REPORT ABSTRACT: DETROIT AND SOUTHEASTERN MICHIGAN INFORMATION AND INTELLIGENCE CENTER (DSEMIIC) REVIEW AND ASSESSMENT I (2007), available at http://www.kms.ijis.org/db/share/public/Library/TA%20Abstracts/ijis_ta_abstract_detroit_fusion_20080902.pdf.
- 78 Daniel Fisher, *Detroit Tops The 2012 List Of America's Most Dangerous Cities*, FORBES, Oct. 18, 2012, available at <http://www.forbes.com/sites/danielfisher/2012/10/18/detroit-tops-the-2012-list-of-americas-most-dangerous-cities/>.
- 79 Dearborn has not created a special unit to handle counterterrorism-related work. When it announced in 2002 that it would establish a "Homeland Security" unit to spearhead counterterrorism efforts, there was widespread community suspicion over fears of government surveillance. Thacher, *supra* note 14, at 662-63. As a result, the city quickly renamed the unit the "Office of Community Preparedness" in an effort to demonstrate that the police would be focused on community protection and not new surveillance efforts. David Thacher recounts one city official's view of the episode: "We got hung for that one. The federal government can call it homeland security, the state can call it homeland security. Dearborn says, "OK, we've got a homeland security [office]." "Why? Have you got terrorists in your town?" No, that's not what we said! ... It was [just] a nice name because it was consistent with the federal government and the state. And of course we quickly changed that name to community preparedness coordinator just so there wouldn't be any more [criticism]. To quiet the ... perception that we had a terrorist problem in Dearborn. Because that's what everyone said, "You're doing this because you must have this problem." *Id.* Indeed, re-naming the office appears to have been more than a symbolic act. While at least one member of the Office is assigned to the local Joint Terrorism Task Force, its activities continue to be centered on increasing coordination with regional and state emergency management. In 2010, it was primarily responsible for administering federal grants related to emergency response programs. CITY OF DEARBORN, *Dearborn Police Department Annual Report*, in ADMINISTRATIVE REPORT 2009/2010, at 531, 607-608 (2010), available at http://www.cityofdearborn.org/documents/doc_view/721-annual-administrative-report-fy10. It also operates a "Buffer Zone Protection Program" and a public-private partnership called the "Critical Incident Protocol" program. *Id.*
- 80 The Portland Police Bureau has a Criminal Intelligence Unit (CIU) that recently reestablished ties to the local JTTF and assigns personnel to JTTF activities at the case-by-case discretion of the Chief. As of February 2012, only two officers had been detailed. See Memorandum from Mike Reese, Chief, Portland Police Bureau, to Portland City Council 2 (Feb. 28, 2012), available at www.portlandonline.com/shared/cfm/image.cfm?id=386900. The CIU collects its own criminal intelligence, but Portland's policy is that "it is the responsibility of the Federal Bureau of Investigation (FBI) to prevent, investigate, and respond to terrorism in the United States." See PORTLAND POLICE BUREAU, CRIMINAL INTELLIGENCE UNIT STANDARD OPERATING PROCEDURE #23, at 1 (2011) (on file with the Brennan Center). Consequently, Portland does not have a dedicated counterterrorism intelligence unit.

- 81 *Hearing Before the Comm'n on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism*, (2008) (statement of Michael R. Bloomberg, Mayor, N.Y.C) [hereinafter Bloomberg Sept. 10, 2008 Testimony], available at http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2008b%2Fpr351-08.html&cc=unused1978&rc=1194&ndi=1; see also *Homeland Security: The Next Five Years: Hearing Before the S. Comm. On Homeland Sec. & Governmental Affairs*, 109th Cong. 3-4 (2006) (statement of Richard A. Falkenrath, Deputy Comm'r for Counterterrorism, N.Y. Police Dep't), available at <http://www.investigativeproject.org/documents/testimony/259.pdf> (testifying that in 2006 the NYPD budget for counterterrorism and intelligence was some \$200 million).
- 82 FIN. DIV., N.Y.C COUNCIL, HEARING ON THE MAYOR'S FISCAL 2013 PRELIMINARY BUDGET & THE FISCAL 2012 PRELIMINARY MAYOR'S MANAGEMENT REPORT : POLICE DEPARTMENT 7 (2012), available at <http://council.nyc.gov/downloads/pdf/budget/2013/056%20Police%20Department.pdf>.
- 83 Raymond W. Kelly, *9/11: 10 Years Later*, THE POLICE CHIEF, Sept. 2011, at 20, available at http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2473&issue_id=92011; *International Liaison Program*, *supra* note 55. The NYPD has also signed international cooperation agreements, which are historically (and constitutionally) the province of the President of the United States. See Jaime Sinapit, *PNP Links up with NYPD to Combat Terrorism*, *International Crime*, INTERAKSYON (Nov. 3, 2012), <http://www.interaksyon.com/article/47111/npn-links-up-with-nypd-to-combat-terrorism-transnational-crimes> (agreement between the NYPD and the Philippines National Police); see also U.S. CONST. art. II, § 2, cl. 2 (Treaty Clause).
- 84 Leonard Levitt, *The NYPD's "Privately" Funded War on Terrorism*, NYPD CONFIDENTIAL (Nov. 7, 2011), <http://nypdconfidential.com/columns/2011/111107.html>.
- 85 L.A. POLICE DEP'T BD. OF POLICE COMM'RS, INTELLIGENCE GUIDELINES FOR MAJOR CRIMES DIVISION: ANTI-TERRORISM INTELLIGENCE SECTION 2 (2012) [hereinafter LAPD INTELLIGENCE GUIDELINES 2012], available at <http://www.lapdonline.org/assets/pdf/INTELLIGENCE%20GUIDELINES%20FOR%20MAJOR%20CRIMES%20DIV.pdf>. The Board of Police Commissioners recently approved sweeping new guidelines for the Anti-Terrorism Intelligence Section, whose objective is the "detection, collection, analysis and dissemination of information for the purpose of developing a strategy for crime prevention." *Id.* at 2. The unit produces "link charts, timelines, financial analysis, etc." to reveal terrorist trends, networks, and tactics. COUNTER-TERRORISM AND CRIMINAL INTELLIGENCE BUREAU, L.A. POLICE DEP'T, COUNTER-TERRORISM AND CRIME-FIGHTING IN LOS ANGELES 4, available at <http://lapdblog.typepad.com/files/ctcib-approach-and-summary.pdf>; LAPD INTELLIGENCE GUIDELINES 2012, at 12. ATIS personnel may open counterterrorism investigations on the basis of tips and leads, including "suspicious activity reports," without reasonable suspicion of criminal activity. *Id.* at 14. Such initial lead investigations may involve photo or video monitoring, the use of informants, or other clandestine surveillance methods. *Id.* at 15-16. But unlike the NYPD, the primary intent of such activities must be to "corroborate information," not to "map" neighborhoods or "bait" community members in an effort to gin up new leads. *Id.* at 16.
- 86 Email from Michael Downing, Commanding Officer, Counter-Terrorism and Special Operations Bureau to the Brennan Ctr. (Nov. 27, 2012) (Note: The Bureau's \$77 million budget covers salaries only and does not include operating expenses or any additional grant funding.).
- 87 See Frank Stoltze, *LAPD Key Player in Preventing Attacks*, *Chief Says*, S. CAL. PUB. RADIO (Sept. 11, 2011), <http://www.scp.org/news/2011/09/11/28770/lapd-key-player-in-preventing-terrorist-attacks-ch/>; Judith Miller, *On the Front Line in the War on Terrorism*, CITY JOURNAL, Summer 2007, available at http://www.city-journal.org/html/17_3_preventing_terrorism.html.
- 88 2 DIST. OF COLUMBIA, *Agency Budget Chapters—Part I*, in FY 2013 PROPOSED BUDGET AND FINANCIAL PLAN A1, C-6, C-8 (2012), available at http://cfo.dc.gov/sites/default/files/dc/sites/ocfo/publication/attachments/ocfo_fy2013_volume_2_chapters_part_1.pdf; YOLANDA BRANCH, OFFICE OF THE D.C. AUDITOR, AUDIT OF THE METROPOLITAN POLICE DEPARTMENT'S INVESTIGATIONS AND PRELIMINARY INQUIRIES INVOLVING FIRST AMENDMENT ACTIVITIES 11 (2012), available at <http://dcauditor.org/sites/default/files/DCA232012.pdf> (Of the 63 intelligence officers, 36 work for the Criminal Intelligence Branch, which includes two undercover officers assigned to conduct First Amendment investigation and three staff members to monitor websites, manage investigations, and write annual reports on First Amendment investigation activities).
- 89 David Lepaska, *Preparing for 2012, Police Create Counterterrorism Unit*, N.Y. TIMES, Sept. 8, 2011, available at <http://www.nytimes.com/2011/09/09/us/09cncpolice.html>.

- 90 The “Counterterrorism and Intelligence Division,” now defunct, consisted of six sections: the Airport Law Enforcement; the Bomb and Arson Section; the Deployment Operations Center; the Intelligence Section; the Predictive Analytics Group; and the Public Transportation Section. See OFFICE OF BUDGET MGMT., CITY OF CHI., 2012 BUDGET RECOMMENDATIONS 218-219 (2011), available at http://www.cityofchicago.org/dam/city/depts/obm/supp_info/2012%20Budget/2012MayorsRecommendation.pdf; CHI. POLICE DEP’T, GENERAL ORDER G01-02: DEPARTMENT ORGANIZATION FOR COMMAND, attachment 2.5 (2009), available at http://directives.chicagopolice.org/attachments/G01-02_Att1.pdf; see also RESEARCH AND DEV. DIV., CHI. POLICE DEP’T, ANNUAL REPORT 2010: A YEAR IN REVIEW 52 (2011), available at <https://portal.chicagopolice.org/portal/page/portal/ClearPath/News/Statistical%20Reports/Annual%20Reports/10AR.pdf>.
- 91 OFFICE OF BUDGET MGMT., CITY OF CHI., 2013 BUDGET RECOMMENDATIONS 155 (2012), available at http://www.cityofchicago.org/content/dam/city/depts/obm/supp_info/2013%20Budget/2013BUDGETRECFINAL.pdf (listing the Deployment Operations Section under the aegis of the new Office of Crime Control Strategies); CHI. POLICE DEP’T, DEPARTMENT NOTICE D12-01: ORGANIZATIONAL CHANGES, attachment 2 (2012), available at <https://portal.chicagopolice.org/portal/page/portal/ClearPath/About%20CPD/CPD%20Organization/DeptOrgChartMar12.pdf>.
- 92 Jeremy Gorner & Robert McCoppin, *Police: Chicago Ends 2012 with 506 Homicides*, CHICAGO TRIBUNE, Jan. 2, 2013, available at http://articles.chicagotribune.com/2013-01-02/news/ct-met-chicago-homicides-2012-20130102_1_homicide-surge-homicide-toll-chicago-homicide-victims.
- 93 See Whet Moser, *Garry McCarthy’s New Chicago Crime Strategy: Social Networks, ‘Hot People’*, CHIAGOMAG.COM (Oct. 1, 2012), <http://www.chicagomag.com/Chicago-Magazine/The-312/October-2012/Garry-McCarthy’s-New-Chicago-Crime-Strategy-Social-Networks-Hot-People/>; *Chicago Shootings: Garry McCarthy Defends Police Strategies as Weekend Gun Violence Continues*, HUFFINGTON POST (Aug. 26, 2012, 11:05 AM), http://www.huffingtonpost.com/2012/08/26/chicago-shootings-garry-m_n_1831254.html. As the Chicago Police Department determined in 2004, “Concern about terrorism is real, although what this city can do about it is not clear. Recent attention to violent crime has taken its share of energy that could be directed at responding to some of the program’s weak spots.” CHI. CMTY. POLICING EVALUATION CONSORTIUM, COMMUNITY POLICING IN CHICAGO, CAPS AT TEN ix (2004), available at <https://portal.chicagopolice.org/i/cpd/clearpath/Caps10.pdf>.
- 94 L.A. CNTY. SHERIFFS DEP’T, MANUAL OF POLICIES AND PROCEDURES § 2-05/090.00 (2009) (on file with the Brennan Center). The Emergency Operations Bureau is also responsible for collecting “criminal intelligence in support of the overall mission of the department to protect the public health through suppression of criminal activity.” EMERGENCY OPERATIONS BUREAU, *supra* note 67.
- 95 *Intelligence and Terrorism*, MIAMI POLICE DEP’T (n.d.), http://www.miami-police.org/intelligence_terrorism.html. According to the department’s 2010 annual report, “[o]ne of the most significant investigations involved a multi-million dollar Ponzi scheme which resulted in the prosecution of individuals who defrauded over \$35 million from investors and pocketed about \$7 million in fraudulent business loans.” MIAMI POLICE DEP’T, MIAMI POLICE DEP’T ANNUAL REPORT 10-11 (2010), available at http://www.miami-police.org/docs/PD_Annual_Report_10.pdf.
- 96 Christopher J. Brown, *Countering Radicalization: Refocusing Responses to Violent Extremism within the United States* 44 (Dec. 2011) (unpublished thesis, Naval Postgraduate School), available at www.hsdl.org/?view&did=699530 (“A drawback to this approach is that police departments must carry out normal duties while working to prevent terrorism and meeting the intelligence and agenda requirements of higher agencies.”); see also RENEE GRAPHIA JOYAL, *STATE FUSION CENTERS: THEIR EFFECTIVENESS IN INFORMATION SHARING & INTELLIGENCE ANALYSIS* 19-20 (2012) (discussing organizational obstacles to allocating resources for counterterrorism units).
- 97 Waxman, *supra* note 27, at 383-84; Bayley & Weisburd, *supra* note 61, at 87 (“Besides collecting intelligence and undertaking preventive actions, counterterrorism involves limiting the damage from terrorism and investigating, arresting, and prosecuting those who have done it. It is important to remember that all terrorist attacks are local. This means that although some counterterrorism functions can be the responsibility of dedicated units deployed and centralized levels of organization, police on the ground will necessarily become involved wherever terrorism strikes or is likely to strike.”).
- 98 2010 RAND REPORT, *supra* note 22, at 82, 97.
- 99 *Id.* at 97.
- 100 See generally Janet Napolitano, *Homeland Security Begins with Hometown Security*, U.S. DEP’T OF HOMELAND SEC. (Aug. 3, 2010, 6:35 PM), <http://www.dhs.gov/blog/2010/08/03/homeland-security-begins-hometown-security>;

- Thacher, *supra* note 14, at 635.
- 101 Thacher, *supra* note 14, at 637-38; Douglas Page, *Community Policing or Homeland Security: Sophie's Choice For Police?*, OFFICER.COM (Sept. 12, 2011), <http://www.officer.com/article/10325312/community-policing-or-homeland-security-sophies-choice-for-police>.
- 102 Thacher, *supra* note 14, at 637-38.
- 103 See, e.g., *The Role of Local Enforcement in Countering Violent Islamic Extremism: Hearing Before the S. Comm. on Homeland Sec. and Gov'tal Affairs*, 110th Cong. (2007) (statement of Lawrence H. Sanchez, Assistant Comm'r, N.Y.C. Police Dep't) ("The key to it was . . . to start appreciating what most people would say would be non-criminal would be innocuous looking behaviors that could easily be argued in a Western Democracy especially in the United States to be protected by First and Fourth Amendment rights but not to look at them in the vacuum but to look across to them as potential precursors to terrorism"), available at <http://votesmart.org/public-statement/301624/hearing-of-the-senate-committee-on-homeland-security-role-of-local-law-enforcement-in-countering-violent-islamist-extremism-panel-1>.
- 104 See Declaration of Paul Chevigny at ¶ 46, *Handschu v. Special Servs. Div.*, No. 71 Civ. 2203 (S.D.N.Y. Feb. 4, 2013) (on file with the Brennan Center).
- 105 CARTER, LAW ENFORCEMENT INTELLIGENCE, *supra* note 36, at 134 ("It must be emphasized that law enforcement authority to perform any kind of intelligence activity is based solely in the statutory authority to enforce the criminal law, hence the obligation to follow the law of criminal procedure. As such, collecting and retaining information about citizens without an articulable criminal nexus is improper.").
- 106 In *Laird v. Tatum*, 408 U.S. 1, 5-6 (1972), the Supreme Court suggested that police departments may use informants and undercover officers to attend public events and gather intelligence concerning First Amendment activities in order to detect or prevent crime. However, it also recognized that "constitutional violations may arise from the deterrent, or 'chilling,' effect" of such political surveillance. *Id.* at 11. The same can be said about the role of the Equal Protection Clause and constitutional violations that may arise out of discriminatory intelligence gathering. See, e.g., Complaint at 21-22, *Hassan v. New York*, No. 12-03401 (D.N.J. Oct. 3, 2012), available at http://www.ccrjustice.org/files/10_First%20Amended%20Complaint.10.3.2012.pdf. Consequently, many courts have required police to demonstrate – at minimum – that they have a "legitimate law enforcement purpose" that outweighs the potential harm to constitutional interests. See, e.g., *United States v. Mayer*, 503 F.3d 740, 753 (9th Cir. 2007); *United States v. Aguilar*, 883 F.2d 662, 703 (9th Cir. 1989); *Anderson v. Davila*, 125 F.3d 148, 161 (3d Cir. 1997) ("[W]here the First Amendment is concerned, the motives of government officials are indeed relevant, if not dispositive, when an individual's exercise of speech precedes government action affecting that individual."). Following this logic, courts in New York, Los Angeles, and Chicago have found it reasonable to require police departments to demonstrate "reasonable suspicion" of criminal conduct in order to collect intelligence on otherwise lawful political activities. See *infra*, note 112.
- 107 See *Terry v. Ohio* 392 U.S. 1, 30 (1968).
- 108 *United States v. Mason*, 628 F.3d 123, 128 (4th Cir. 2010) (quoting *United States v. Branch*, 537 F.3d 328, 336 (4th Cir. 2008)).
- 109 *Handschu v. Special Servs. Div.*, 349 F.Supp. 766, 768-70 (S.D.N.Y. 1972); *Civil Rights Implications of Post-September 11 Law Enforcement Practices in New York: Hearing Before N.Y. Advisory Comm. to the U.S. Comm. on Civil Rights* (March 2004) (statement of Arthur N. Eisenberg, New York Civil Liberties Union), available at <http://www.nyclu.org/content/testimony-police-surveillance-of-political-activity-history-and-current-state-of-handschu-de> ("[T]he renewed political energy and activity of the 1960's served as a catalyst for the renewed activity of the police intelligence unit in New York City. Accordingly, '[d]uring the sixties, the unit launched a yearly average of one thousand intensive political investigations of dissident groups and individuals and about six hundred lesser probes.' The targets of such police investigations included the NAACP, the ACLU, CORE, the Fifth Avenue Peace Parade Committee, and the Lower East Side Mobilization for Peace Action."); see also Chris Hawley, *Barbara Handschu Likens NYPD Spying on Muslims to Spying on Free Speech Advocates*, HUFFINGTON POST (Nov. 17, 2011, 7:53 AM), http://www.huffingtonpost.com/2011/11/17/in-nypd-spying-a-yippie-l_n_1099479.html.
- 110 *Alliance to End Repression v. City of Chicago*, 742 F.2d 1007, 1009 (7th Cir. 1984).
- 111 Jim Newton, *LAPD Pushing to Relax Limits on Undercover Probes*, L.A. TIMES, Oct. 11, 1996, available at http://articles.latimes.com/1996-10-11/news/mn-52716_1_police-department.

- 112 See Stipulated Consent Decree and Judgment at § IV.A, *Coalition Against Police Abuse v. Bd. of Police Comm'rs*, No. 243-458 (L.A. Cnty. Ct. Feb. 22, 1984) (permitting preliminary investigations based “upon reasonable and articulated suspicion . . .”); *Alliance to End Repression v. City of Chicago*, 561 F.Supp. 537, 564 (N.D. Ill. 1982) (§ 3.2 requires “reasonable suspicion” that evidence of criminal conduct will be obtained); *Handschu v. Special Servs. Division*, 605 F.Supp. 1384, 1421 (S.D.N.Y. 1985) (requiring “specific information” that the person or group was linked to criminal conduct.). See also 69 CORNELL L. REV. at 768-775.
- 113 *Handschu v. Special Servs. Div.* 273 F.Supp.2d 327, 329 (S.D.N.Y. 2003); see also Christopher Dunn, *Balancing the Right to Protest in the Aftermath of September 11*, 40 HARV. C.R.-C.L. L. REV. 327, 339 (2005).
- 114 *Handschu*, 605 F.Supp. at 1421.
- 115 *Handschu*, 273 F.Supp.2d at 333-35, 349. The Los Angeles and Chicago consent decrees were eventually both dissolved. The Los Angeles decree expired in 1996 and the LAPD won changes to the rules that relaxed the threshold for engaging in investigative activities. See Newton, *supra* note 111. No longer bound by the decree, the LAPD eliminated the reasonable suspicion requirement and increased its authority to conduct undercover probes in the name of counterterrorism. *Id.* The Chicago decree remained in force as originally written until 2001, when the CPD successfully moved a federal court to eliminate the need to demonstrate indicia of past, present, or imminent future criminal conduct – i.e., the reasonable suspicion requirement. *Alliance to End Repression*, 237 F.3d 799, 802 (7th Cir. 2001). Judge Posner, writing for the Seventh Circuit, noted that the nature of the issue had changed, with the targets of police investigation being terrorist groups rather than political dissidents. *Id.* The decree was entirely dissolved in 2009 and has not been replaced, although portions of it survive as a part of the department’s own rules. See *Alliance to End Repression*, 328 Fed.Appx. 339, 340 (7th Cir. 2009).
- 116 Under the terms of the revised 2003 Handschu Guidelines, the NYPD may use undercover officers and confidential informants during a “preliminary inquiry,” which does not require any “reasonable indication” of criminal activity. *Handschu v. Special Servs. Div.*, 288 F.Supp.2d 411, 423 (S.D.N.Y. 2003) (Appendix A, § V(B)(5)); see also Raymond Kelly, Commissioner, N.Y. Police Dep’t, Remarks to Fordham Law School Alumni (Mar. 3, 2012), available at http://www.nyc.gov/html/nypd/html/pr/pr_2012_03_03_remarks_to_fordham_law_school_alumni.shtml (“This is what Handschu says about the broadest form of intelligence gathering: ‘The NYPD is authorized to visit any place and attend any event that is open to the public’ and ‘to conduct online search activity and to access online sites and forums on the same terms... as members of the public.’ The department is further authorized to, ‘prepare general reports and assessments... for purposes of strategic or operational planning.’ Anyone who intimates that it is unlawful for the Police Department to search online, visit public places, or map neighborhoods has either not read, misunderstood, or intentionally obfuscated the meaning of the Handschu Guidelines.”).
- 117 N.Y. POLICE DEP’T, NYPD PATROL GUIDE, 2011-A EDITION § 212-72 (2011); *Handschu v. Special Servs. Div.*, 288 F.Supp.2d 411, 430-31 (S.D.N.Y. 2003) (Appendix A, § IX).
- 118 Transcript of Examination Before Trial, *supra* note 73, at 124.
- 119 *Id.*
- 120 See *Handschu*, 288 F.Supp. 2d 411, 430-31 (Appendix A, § IX). Moreover, the Demographics Unit’s ongoing investigation and infiltration of Muslim organizations in the absence of indications of unlawful terrorist activity also appears to violate sections V(B), (C) and (D) of the *Handschu* Guidelines, which still require some criminal predicate. Declaration of Paul Chevigny, *supra* note 104, at ¶ 4.
- 121 Declaration of Paul Chevigny, *supra* note 104, at ¶ 8.
- 122 *Id.*
- 123 See generally *supra* note 64.
- 124 L.A. POLICE DEP’T, SPECIAL ORDER NO. 11 (2008) [hereinafter LAPD SPECIAL ORDER 11], reprinted in SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT, FINDINGS AND RECOMMENDATIONS OF THE SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT app. B, at 36 (2008), available at <http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf>.
- 125 See generally *The Nationwide SAR Initiative (NSI)*, NATIONWIDE SAR INITIATIVE, <http://nsi.ncirc.gov/> (last visited Mar. 5, 2013).
- 126 See generally *NYPD Shield*, N.Y.C. POLICE DEP’T, <http://www.nypdshield.org/public/about.aspx> (last visited Mar. 6, 2013).

127 As of 2011, the Nationwide SAR Initiative (NSI) was under various stages of implementation at 33 sites, covering two thirds of the US population. See *Understanding the Homeland Threat Landscape—Considerations for the 112th Congress: Hearing Before the H. Comm. On Homeland Security*, 112th Cong. 13 (2011), available at <http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72212/pdf/CHRG-112hhrg72212.pdf>. Chicago, LAPD, Houston, DC, Miami-Dade, and Seattle began participating in the NSI as part of a 2009 pilot program. See U.S. DEP'T OF JUSTICE ET AL., FINAL REPORT: INFORMATION SHARING ENVIRONMENT (ISE) - SUSPICIOUS ACTIVITY REPORTING (SAR) EVALUATION ENVIRONMENT 2 (2010) [hereinafter EVALUATION ENVIRONMENT 2010], available at http://nsi.ncirc.gov/documents/NSI_EE.pdf; NATIONWIDE SAR INITIATIVE, U.S. DEP'T OF JUSTICE, NATIONWIDE SUSPICIOUS ACTIVITY REPORTING (SAR) INITIATIVE (NSI) 4 (2009), available at www.it.ojp.gov/docdownloader.aspx?ddid=1229. A 2012 map of participating sites includes Philadelphia. *Implementation Map*, NATIONWIDE SAR INITIATIVE (Oct. 4, 2012), http://nsi.ncirc.gov/implementation_map.aspx. See also PHILA. POLICE DEP'T, DIRECTIVE 126, COLLECTION AND DISSEMINATION OF PROTECTED INFORMATION POLICY V (on file with the Brennan Center) (delineating the process for reporting and sharing homeland security information, including SARs). Also note that the NYPD does not participate in the NSI, although the New York State Police have been participants since 2009. EVALUATION ENVIRONMENT 2010, at 2.

128 **NYPD:** The NYPD is bound by a federal consent decree, which was modified in 2003 to remove the criminal predicate requirement for various types of investigative activity targeting First Amendment activities. See *supra* notes 113-117.

Chicago: According to a 2012 order issued by Superintendent Garry McCarthy, Chicago police may conduct an investigation implicating First Amendment rights for any “reasonable law enforcement purpose,” including “public safety issues, whether they amount to criminal conduct or not.” CHI. POLICE DEP'T, GENERAL ORDER GO2-02-01, INVESTIGATIONS DIRECTED AT FIRST AMENDMENT-RELATED INFORMATION A(2)(b) (2012), available at <http://directives.chicagopolice.org/directives/data/a7a57be2-12936eaa-d1812-9373-a45df889893a9f52.html>.

LA Sheriff: A set of intelligence guidelines prohibits LASD officers from retaining intelligence files unless they contain reasonable suspicion that an individual or group is suspected of being or having been involved in criminal activity. EMERGENCY OPERATIONS BUREAU, *supra* note 67, at 3. It also prohibits sorting intelligence about “political, religious, or social views, associations, or activities” unless it is “related directly to the criminal predicate which is the basis for focusing on the individual group.” *Id.* at 2.

LAPD: See *infra*, notes 131-137; L.A. POLICE DEP'T, SPECIAL ORDER No. 1, at 2-3 (2012) [hereinafter LAPD SPECIAL ORDER 1], available at <http://stoplapdspying.org/wp-content/uploads/2012/04/SO-1.pdf>. In April 2012, the LAPD reportedly agreed to collect SARs only where there is reasonable suspicion of criminal activity, but according to Deputy Chief Michael Downing, who commands the LAPD's Counterterrorism and Special Operations Bureau, “All we did was put the ODN [Office of the Director of National Intelligence] definition of SAR in the order and separated the 9 non-criminal behaviors from the 6 criminal behaviors and included an indented note about Terry vs Ohio. ... There is no real substantive change.” Matthew Harwood, *LAPD Agrees to Suspicious Activity Reporting Reforms*, SECURITY MANAGEMENT (Apr. 18, 2012), <http://www.securitymanagement.com/news/lapd-agrees-suspicious-activity-reporting-reforms-009873?page=0%2C0>; see also Press Release, Stop LAPD Spying Coalition, Stop LAPD Spying Coalition Continues to Demand Answers from LAPD About Suspicious Activity Reporting Program (May 22, 2012), available at <http://stoplapdspying.org/2012/05/beware-of-misleading-stories/>. Moreover, the Board of Police Commissioners approved sweeping new guidelines for the Anti-Terrorism Intelligence Section in late 2012, permitting officers to use informants and engage in surveillance for up to 180 days without reasonable suspicion of criminal activity. See LAPD INTELLIGENCE GUIDELINES 2012, *supra* note 85, at 5, 15-16 (“The Initial Lead Investigation threshold need not rise to the reasonable suspicion standard ...”).

Philadelphia: See PHILA. POLICE DEP'T, *supra* note 127, at 3 (requiring reasonable suspicion of criminal activity in order to collect information about First Amendment conduct and other personal information); see also PHILA. POLICE DEP'T, DIRECTIVE 122, RACE, ETHNICITY, AND POLICING 1 (2011) (requiring reasonable suspicion to engage in a temporary investigatory detention of an individual and prohibiting the use of race/ethnicity in determining whether there is reasonable suspicion) (on file with the Brennan Center). Pennsylvania state law also requires reasonable suspicion to collect or maintain “protected information,” which includes “concerning the habits, practices, characteristics, possessions, associations or financial status of any individual compiled in an effort to anticipate, prevent, monitor, investigate or prosecute criminal activity.” See 18 PA. CONS. STAT. § 9106 (Westlaw through 2012 legislation); LINDA L. KELLY ET AL., OFFICE OF THE ATTORNEY GEN., COMMONWEALTH OF PA., CRIMINAL HISTORY RECORD INFORMATION HANDBOOK 3 (6th ed. 2012), available at <http://www.attorneygeneral>.

[gov/uploadedfiles/crime/chria.pdf](#). However, both the regional and state-run fusion centers have privacy policies that appear to conflict with this rule, explicitly permitting the centers to “retain protected information that is based on a level of suspicion that is less than ‘reasonable suspicion,’ such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy.”). PA. CRIMINAL INTELLIGENCE CTR., PA. STATE POLICE, PRIVACY POLICY 4 (n.d.), available at http://www.nfcausa.org/files/DDF/PennsylvaniaPaCICApprovedPrivacyPolicy02-11_3.pdf; DEL. VALLEY INTELLIGENCE CTR., PRIVACY POLICY 6 (2011) (on file with the Brennan Center).

Houston: See HOUS. POLICE DEP’T, GENERAL ORDER 800-07: CRITERIA FOR SUBMITTING INCIDENT REPORTS 2-3 (2007) (on file with the Brennan Center) (requiring officers to report “suspicious persons, vehicles, or activities involved in videotaping, photographing, sketching, drawing ... or asking detailed questions regarding buildings”; “a person or event associated with suspicious possession of ... suspicious posters, fliers, or other publications”; “any protest or demonstration associated with terrorism, acts of war, attacks, [or] unusual suspicious activity ...”; and “any suspicious person or event not listed in the above categories but determined as suspicious or worthy of reporting by an officer or supervisor.”).

Washington, D.C.: See DC CODE § 5-333.06(a) (permitting “preliminary inquiries” involving First Amendment activities where the police have “information or an allegation the responsible handling of which requires further scrutiny,” but “does not justify opening a full investigation because it does not establish reasonable suspicion that persons are planning or engaged in criminal activity.”). When conducting a preliminary inquiry, DC police may examine government records and open sources, conduct surveillance, and utilize informants as well as undercover officers. DC CODE § 5-333.07(c)-(d). DC models its SAR criteria on an old version of the LAPD’s list. Compare METRO. POLICE DEP’T, GO-HSC-802.06, § III.A.7 (2011), available at <https://go.mpdconline.com/GO/GOHSC80206.pdf>, with L.A. POLICE DEP’T, SPECIAL ORDER 11, *supra* note 124. The fusion center serving the D.C. region, known as the Washington Regional Threat & Analysis Center, also explicitly permits officers to “retain protected information that is based on a level of suspicion that is less than ‘reasonable suspicion,’ such as tips and leads or suspicious activity report (SAR) information.” WASH. REGIONAL THREAT AND ANALYSIS CTR., PRIVACY POLICY 3 (2010) (on file with the Brennan Center).

Miami-Dade: Miami-Dade’s Homeland Security Bureau (HSB) doubles as a regional fusion center, known as the Southeast Florida Fusion Center (SEFFC). The HSB Standard Operating Procedure recognizes that some databases are subject to the reasonable suspicion requirement in 28 C.F.R. § 23. See HOMELAND SEC. BUREAU, MIAMI-DADE POLICE DEP’T, STANDARD OPERATING PROCEDURE 67-69. But the rules do not specify whether it applies this requirement to sharing SARs as part of the NSI. On the contrary, the SEFFC privacy policy states that officers will seek and retain information if it is “based on (a) a criminal predicate *or* (b) a possible threat to public safety, including potential terrorism-related conduct.” SE. FLA. FUSION CTR., SEFFC ISE-SAR EE PRIVACY POLICY: ISE-SAR EVALUATION ENVIRONMENT INITIATIVE PRIVACY, CIVIL RIGHTS AND CIVIL LIBERTIES PROTECTION POLICY 3 (n.d.) (emphasis added), available at http://iwatchmiamidade.com/Documents/SEFFC_ISE_SAR_EE_PrivacyPolicy0811.pdf. This policy is consistent with other SAR programs examined by the Brennan Center, including the state-run Florida Fusion Center, which has established a privacy policy that is binding on all participating state and local agencies. FLA. FUSION CTR., PRIVACY POLICY VERSION 3.0 3 (2010), available at <http://www.fdle.state.fl.us/Content/Florida-Fusion-Center/Menu/Privacy-Policy.aspx>. Like the SEFFC, the Florida Fusion Center does not have a firm reasonable suspicion requirement, instead permitting officers to seek and retain information that constitutes “a potential threat to public safety,” is “relevant” to an ongoing investigation, or is “reasonably believed to be reliable.” *Id.* at 6.

Detroit: The Detroit Police Department has a blanket policy forbidding the “collection, indexing, maintenance, or dissemination of information dealing with beliefs, opinions, associations, or expressions of any individual, group, or organization” unless connected to valid law enforcement activities. DETROIT POLICE DEP’T, DIRECTIVE 203.6-2(1) (2008) (on file with the Brennan Center). Any surveillance which has the purpose of gathering the “beliefs, opinions, attitudes, statements, associations and activities of persons, groups or organizations” is prohibited unless the target is violating the law or under reasonable suspicion of violating or conspiring to violate the law. *Id.* at 203.6-2(2). The Chief of Police is responsible for ensuring adherence to the policy and must provide the Board a quarterly report on compliance. *Id.* at 203.6-3.

San Francisco: See S.F. POLICE DEP’T, DEPARTMENT GENERAL ORDER 8.10: GUIDELINES FOR FIRST AMENDMENT ACTIVITIES I (2008) [hereinafter SFPD DGO 8.10], available at <http://www.sf-police.org/modules/>

[ShowDocument.aspx?documentid=24722](#) (“The Department may conduct a criminal investigation that involves the First Amendment activities of persons, groups or organizations where there is an articulable and reasonable suspicion to believe that: 1) They are planning or are engaged in criminal activity ... and 2) The First Amendment activities are relevant to the criminal investigation.”).

Seattle: See SEATTLE MUN. CODE § 14.12.150(C) (requiring reasonable suspicion of criminal activity in order to collect information about a person’s political or religious associations, activities, beliefs, or opinions); see also SEATTLE POLICE DEP’T, PROCEDURES AND TACTICS PUBLICATION: 024 (2007) [hereinafter PROCEDURES AND TACTICS PUBLICATION] (implementing SEATTLE MUN. CODE § 14.12.150(C)) (on file with the Brennan Center); SEATTLE POLICE DEP’T, POLICIES & PROCEDURES: 5.140 – UNBIASED POLICING at § I(C)(2) (2011) (requiring reasonable suspicion to engage in investigative stops and prohibiting the use of race or ethnicity as a motivating factor in establishing reasonable suspicion) (on file with the Brennan Center); SEATTLE POLICE DEP’T, SEATTLE POLICE MANUAL § 1.110 IV(B)(1) (2009) (requiring reasonable suspicion of criminal activity for the collection and analysis of information on individuals and groups by the department’s Special Investigations Squad and Organized Crime Intelligence Squad).

Miami: Standard operating procedures for Miami’s Intelligence and Terrorism Unit (ITU) expressly permit officers to conduct “preliminary inquiries” where “there is not yet a ‘reasonable indication’ of criminal activities.” INTELLIGENCE & TERRORISM UNIT, MIAMI POLICE DEP’T, *General Principles of Investigations, in* STANDARD OPERATING PROCEDURE 2 (2012) (on file with the Brennan Center). The ITU may use a preliminary inquiry to investigate a “sensitive criminal matter” such as “the activities of a religious organization or a primarily political organization, or the related activities of any individual prominent in such organizations.” *Id.* at 2-3. Such an inquiry may include database queries, the use of previously established informants and confidential sources, interviews, and physical or photographic surveillance. *Id.* at 5. The ITU maintains information generated during these inquiries, including those that have been closed. *Id.* The procedures are silent on when information obtained during an inquiry may be shared or disseminated. Information obtained pursuant to a full investigation based on reasonable suspicion may be disseminated if it “may assist in preventing a crime or the use of violence or any other conduct dangerous to life.” *Id.* at 15.

Portland: See OR. ADMIN. RULES § 137-090-0060 (2013) (defining a criminal intelligence file as stored information about the activities and associations of individuals or groups that is based upon reasonable suspicion of criminal activity); OR. ADMIN. RULES § 137-090-0070 (2013) (“No information will be collected or maintained about the political, religious, racial, or social views, sexual orientation, associations or activities of any individual, group, association organization, corporation, business or partnership unless information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of information is, or may be, involved in criminal conduct.”).

Minneapolis: See STRATEGIC INFO. CTR., POLICY & PROCEDURE, MINNEAPOLIS POLICE DEP’T at § 2(2)(B) & (E) (n.d.) (“Information gathering for intelligence purpose[s] shall be premised on circumstances that provide a reasonable suspicion ... that specific individuals or organizations may be planning or engaging in criminal activity.”) (“Criminal intelligence information shall not be collected or maintained about the political, religious, social views, associations or activities of any individual or any group, association, ... or other organization, unless there is reasonable suspicion that the subject or information is or may be involved in criminal conduct or activity.”) (on file with the Brennan Center).

St. Paul: St. Paul’s policies and procedures on collecting information for intelligence purposes are ambiguous at best, if not outright contradictory. The department manual states that only information “related to” criminal activities may be retained, but there is a large gap between “reasonable suspicion of criminal activity” and “related to” criminal activity. ST. PAUL POLICE DEP’T, ST. PAUL POLICE DEPARTMENT MANUAL 154 (n.d.) (on file with the Brennan Center). Unfortunately, the department has heavily redacted portions of the manual, including entire sections on the use of informants and intelligence information, making it difficult to tell how officers are to implement this rule. *Id.* at 257-60, 263. The manual adds that information will not be gathered about groups or organizations unless they are “known or reasonably suspected of involvement in criminal activities,” but there is no similar requirement for personal information. *Id.* at 153. A set of guidelines for the Special Investigation Unit, while unredacted, is equally vexing. With respect to First Amendment activities, the guidelines state that investigations or information gathering operations must be based on “an existing criminal predicate or the reasonable suspicion that unlawful

acts have occurred or may occur.” St. PAUL POLICE DEP’T, SIU POLICY AND GUIDELINES FOR INVESTIGATIONS AND INFORMATION GATHERING OPERATIONS INVOLVING FIRST AMENDMENT ACTIVITY 1 (2008) (on file with the Brennan Center). But at the same time, they explicitly permit the use of undercover officers and existing informants at the “preliminary inquiry” stage of investigation, where there “is not yet reasonable suspicion of unlawful activity.” *Id.* at 4-5. Using language similar to the modified *Handschu* guidelines that govern the NYPD, reasonable suspicion is required only for “full investigations.” *Id.* at 5. Moreover, the guidelines permit officers to seek and maintain information about individuals or organizations based *solely* on the individual’s or group’s race, ethnicity, and First Amendment-protected activities, provided it is “relevant” to whether an individual or organization is engaged in criminal activity. *Id.* at 2. Corresponding policy in the department manual is redacted.

Dearborn: The City of Dearborn denied the Brennan Center’s request for the Dearborn Police Department’s policies and procedures for investigations and information collection related to First Amendment activities. However, in a personal interview with the Brennan Center, Chief Ronald Haddad confirmed that Dearborn police officers must have reasonable suspicion of criminal activity in order to collect information about lawful First Amendment activities. Telephone Interview with Dearborn Police Department Chief Ronald Haddad, Dep’t Chief, Dearborn Police Dep’t (Feb. 26, 2013). It remains unclear, however, whether the reasonable suspicion requirement applies to the collection of intelligence information about activities that are not specifically protected by the First Amendment.

129 *See infra*, notes 244-251.

130 In Houston, officers are required to report: “suspicious persons, vehicles, or activities involved in videotaping, photographing, sketching, drawing ... or asking detailed questions regarding buildings”; “a person or event associated with suspicious possession of ... suspicious posters, fliers, or other publications”; “any protest or demonstration associated with terrorism, acts of war, attacks, [or] unusual suspicious activity ...”; and “any suspicious person or event not listed in the above categories but determined as suspicious or worthy of reporting by an officer or supervisor.” HOUS. POLICE DEP’T, *supra* note 128, at 2-4.

131 LAPD SPECIAL ORDER 1, *supra* note 128, at 1 (revising and renaming LAPD SPECIAL ORDER 11, *supra* note 124, which established the LAPD SAR program in 2008).

132 *Id.* at 1-3.

133 *Id.*

134 Yaman Salahi, *Beware of Photographers, Note-Takers and Protesters*, HUFFINGTON POST (Sept. 4, 2012, 10:37 AM), http://www.huffingtonpost.com/yaman-salahi/lapd-counter-terrorism_b_1847961.html.

135 L.A. POLICE DEP’T, DEPARTMENTAL MANUEL: VOLUME IV § 271.46 (2012), available at http://www.lapdpolice.com.lacity.org/082812/BPC_12-0358.pdf.

136 RECOMMENDATIONS FOR FUSION CENTERS, *supra* note 14, at 12-13; THOMAS CINCOTTA, POLITICAL RESEARCH ASSOCS., PLATFORM FOR PREJUDICE: HOW THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE INVITES RACIAL PROFILING, ERODES CIVIL LIBERTIES, AND UNDERMINES SECURITY 19 (2010), available at http://www.publiceye.org/liberty/matrix/reports/sar_initiative/sar-full-report.pdf; see also STOP LAPD SPYING COALITION, TO OBSERVE AND TO SUSPECT: A PEOPLE’S AUDIT OF THE LOS ANGELES POLICE DEPARTMENT’S SPECIAL ORDER 1, at 4 (2013), available at <http://stoplapdspying.org/wp-content/uploads/2013/03/PEOPLES-AUDIT-FINAL.pdf>.

137 ALEXANDER A. BUSTAMANTE, OFFICE OF THE INSPECTOR GENERAL, L.A. POLICE COMM’N, SUSPICIOUS ACTIVITY REPORTING SYSTEM AUDIT 2 n. 4 (2013) [hereinafter LAPD SAR AUDIT], available at http://www.lapdpolice.com.lacity.org/031913/BPC_13-0097.pdf.

138 *See, e.g., Selected Suspicious Activity Reports from the Central California Intelligence Center and Joint Regional Intelligence Center*, AM. CIVIL LIBERTIES UNION (Sept. 19, 2013), https://www.aclunc.org/sites/default/files/asset_upload_file470_12586.pdf.

139 Mark Lowenthal, President, Intelligence & Security Acad., Remarks at the Ctr. for Strategic and Int’l Studies Panel: Homeland Security Intelligence Analytic Tradecraft 8 (Sept. 7, 2011), available at http://csis.org/files/attachments/110907_hs_intelligence_analytic_tradecraft_transcript.pdf.

140 PATEL, *supra* note 42, at 10-11.

141 Letter from Peter Bibring et al., Senior Staff Attorney, Am. Civil Liberties Union of S. Cal., to Charlie Beck, Chief,

L.A. Police Dep't, and Michael Downing, Deputy Chief, L.A. Police Dep't 3 (Mar. 2, 2012), available at <http://www.chirla.org/sites/default/files/20120312SARSACLUCHIRLA.pdf>.

142 *Id.*

143 *Id.* at 4.

144 Complaint at 22, Hassan v. New York, No. 2:12-cv-03401 (D.N.J. Oct. 3, 2012), available at http://www.ccrjustice.org/files/10_First%20Amended%20Complaint.10.3.2012.pdf.

145 Defendant's Brief in Opposition to Class Counsel's Motion for Injunctive Relief and Appointment of a Monitor 6, No. 71 Civ. 2201 (S.D.N.Y. May 17, 2013) (on file with the Brennan Center).

146 Floyd v. City of New York, No. 08 Civ. 1034, 2013 WL 4046209, at *6, 22-23 (S.D.N.Y. Aug. 12, 2013).

147 *Id.* at *6.

148 *Id.* at *10. According to Sheriff Leroy Baca of the LASD, the reasonable suspicion requirement keeps law enforcement agencies from "shotgunning societies or groups of people as a general strategy," a strategy that is ineffective to say the least. Leroy Baca, Sheriff, L.A. Sheriff's Dep't, Remarks on Panel 1 at Brennan Center for Justice Symposium: Intelligence Collection and Law Enforcement: New Roles, New Challenges, YOUTUBE.COM (Mar. 20, 2011), <http://www.youtube.com/watch?v=Op1TgEGVuso>.

149 Leroy Baca, *supra* note 144, at 8.

150 EMERGENCY OPERATIONS BUREAU, *supra* note 67.

151 See BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUSTICE, 1998 POLICY CLARIFICATION 20 (1993), available at http://www.it.ojp.gov/documents/28cfr_part_23.pdf ("Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23.").

152 SIOBHAN O'NEIL, CONG. RESEARCH SERV., RL340114, TERRORIST PRECURSOR CRIMES: ISSUES AND OPTIONS FOR CONGRESS 25 (2007).

153 *Id.* at 1.

154 *Id.*

155 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 27.

156 Cf. INFO. SHARING ENV'T, A LEGAL AND POLICY APPROACH FOR RESPONSIBLE INFORMATION SHARING: THE ROLE OF THE INFORMATION SHARING ENVIRONMENT (ISE) 3 (2012), available at http://ise.gov/sites/default/files/Legal_and_Policy_Approach_White_Paper.pdf (encouraging state and local agencies to overcome "legal problems" that limit data sharing and change "overly restrictive" interpretations of laws designed to protect privacy and civil liberties).

157 See Beth Sheridan & Spencer S. Hsu, *Localities Operate Intelligence Centers To Pool Terror Data*, WASH. POST, Dec. 31, 2006, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/12/30/AR2006123000238.html> (reporting 37 fusion centers in existence at the end of 2006).

158 GLOBAL JUSTICE INFO. SHARING INITIATIVE, U.S. DEP'T OF JUSTICE, ET AL., FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA 2 (2006) [hereinafter FUSION CENTER GUIDELINES], available at http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

159 Janet Napolitano, Dep't of Homeland Sec., Address at the National Fusion Center Conference (Mar. 11, 2009), available at http://www.dhs.gov/ynews/speeches/sp_1236975404263.shtm.

160 *The National Preparedness Report: Assessing the State of Preparedness: Hearing Before the Subcomm. on Emergency Preparedness, Response, and Comm'ns of the H. Comm. on Homeland Sec.*, 112th Cong. 2 (2012) (statement of Mike Sena, President, National Fusion Center Association), available at <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Sena.pdf> (counting 77 fusion centers in 2012); GAO-13-233, *supra* note 3, at 10 (counting 78 fusion centers). In addition to the presence of fusion centers in the two U.S. territories listed by Mike Sena in his 2012 testimony, the GAO told the Brennan Center that fusion centers are now present in a total of three

- U.S. territories, with the newest center having been established in the U.S. territory of Guam. Telephone Interview with Eileen R. Lawrence, Director, Homeland Sec. and Justice, U.S. Gov't Accountability Office (May 21, 2013).
- 161 JEROME P. BJELOPERA, CONG. RESEARCH SERV., R4178, THE FEDERAL BUREAU OF INVESTIGATION AND TERRORISM INVESTIGATIONS 13 (2013), available at <http://www.fas.org/sgp/crs/terror/R41780.pdf>.
- 162 *Id.*
- 163 See generally *Printz v. United States*, 521 U.S. 898, 919-22 (1997); *New York v. United States*, 505 U.S. 144, 176 (1992).
- 164 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 27, 35-36, 61.
- 165 GLOBAL INFO. SHARING INITIATIVE, U.S. DEP'T OF JUSTICE, THE NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN (2003), available at http://www.au.af.mil/au/awc/awcgate/doj/nat_crim_intel_share_plan2003.pdf.
- 166 FUSION CENTER GUIDELINES, *supra* note 158, at 29.
- 167 *Id.* at 33.
- 168 Council of State Gov'ts & E. Ky. Univ., The Impact of Terrorism on State Law Enforcement: Adjusting to New Roles and Changing Conditions 7 (June 2006) (unpublished report), available at <https://www.ncjrs.gov/pdffiles1/nij/grants/216642.pdf> (estimating that approximately three-quarters of state law enforcement agencies serve as their "state's leader for gathering, analyzing and sharing terrorism-related intelligence."). The study also found that 92% of state law enforcement agencies allocated substantial resources for intelligence gathering, analysis, and sharing since 9/11. *Id.* at 24.
- 169 See Nenneman, *supra* note 14, at 78-86; see also CHI. POLICE DEP'T, SPECIAL ORDER 05-08-03: TERRORISM LIAISON OFFICER (TLO) PROGRAM (2009) (on file with the Brennan Center).
- 170 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-223, INFORMATION SHARING: DHS COULD BETTER DEFINE HOW IT PLANS TO MEET ITS STATE AND LOCAL MISSION AND IMPROVE PERFORMANCE ACCOUNTABILITY 19 n.33 (2010), available at <http://www.gao.gov/new.items/d11223.pdf> ("Of the 72 designated fusion centers, 50 (one in each state) are considered the primary designated state fusion centers. The remaining 22 centers are "secondary designated" fusion centers. Secondary fusion centers are located in cities that receive Urban Area Security Initiative funding—grants administered by the Federal Emergency Management Agency to state, local, tribal jurisdictions, and urban areas to build and sustain national preparedness capabilities—and agree to work in conjunction with the primary fusion center."); INFO. SHARING ENV'T, ISE-G-112, INFORMATION SHARING ENVIRONMENT GUIDANCE (ISE-G): FEDERAL RESOURCE ALLOCATION CRITERIA (RAC) 3 (2011), available at http://www.ise.gov/sites/default/files/RAC_final.pdf.
- 171 GAO-13-233, *supra* note 3, at 24-25.
- 172 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 27.
- 173 *Id.* at 36-38, 57-59; see also Michael Price, *Senate to DHS: No Tanks, Thanks*, THE HILL (Dec. 6, 2012, 4:00 PM), <http://thehill.com/blogs/congress-blog/economy-a-budget/271511-senate-to-dhs-no-tanks-thanks>.
- 174 Due to anticipated reductions in federal grant funding, the Oregon Terrorism Information Threat Assessment Network reported in December 2012 that Oregon may become the "first state in the nation to close the doors on its fusion center." Queenie Wong, *Budget Cuts May Close Salem Terrorism Center*, STATESMAN JOURNAL, Dec. 4, 2012. The Texas state legislature has also taken steps to close the state-level Texas Fusion Center due to concerns that it has been expensive and ineffective. Brenda Bell, *Budget Conferees Vote Not to Fund DPS Fusion Center*, AUSTIN AMERICAN-STATESMAN, May 14, 2003, available at <http://www.mystatesman.com/news/news/budget-conferees-vote-not-to-fund-dps-fusion-cente/nXrPx/>. See also Jonathan Tamari, *Federal Report Cites Unfinished Philadelphia Counterterrorism Center as Flawed*, PHILA. INQUIRER, Oct. 5, 2012, available at http://articles.philly.com/2012-10-05/news/34261225_1_regional-intelligence-center-federal-money-fusion-centers (cataloguing the sluggish and expensive operation underway in Philadelphia to house its regional fusion center in a new facility).
- 175 2012 HSPI Report, *supra* note 48, at 27.
- 176 Nenneman, *supra* note 14, at 2-3.
- 177 2010 RAND Report, *supra* note 22, at 52.
- 178 2012 HSPI Report, *supra* note 48, at 1.

179 See Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458 § 1016, 118 Stat. 3638, 3664 (as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, §§ 501-504); see also 9/11 REPORT, *supra* note 28, at 427 (“The FBI is just a small fraction of the national law enforcement community in the United States, a community comprised mainly of state and local agencies. The network designed for sharing information, and the work of the FBI through local Joint Terrorism Task Forces, should build a reciprocal relationship, in which state and local agents understand what information they are looking for, and, in return, receive some of the information being developed about what is happening, or may happen, in their communities. In this relationship, the Department of Homeland Security will also play an important part.”).

180 OFFICE OF THE PROGRAM MANAGER FOR THE INFO. SHARING ENV’T ET AL., SUSPICIOUS ACTIVITY REPORTING FUNCTIONAL STANDARD AND EVALUATION ENVIRONMENT: INITIAL PRIVACY AND CIVIL LIBERTIES ANALYSIS 6 (2008) [hereinafter INITIAL PRIVACY AND CIVIL LIBERTIES ANALYSIS], available at http://www.ise.gov/sites/default/files/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf.

181 GLOBAL JUSTICE INFO. SHARING INITIATIVE, U.S. DEP’T OF JUSTICE, BASELINE CAPABILITIES FOR STATE AND MAJOR URBAN AREA FUSION CENTERS: A SUPPLEMENT TO THE *FUSION CENTER GUIDELINES* 15 (2008), available at www.it.ojp.gov/documents/baselinecapabilitiesa.pdf.

182 NATIONWIDE SAR INITIATIVE, U.S. DEP’T OF JUSTICE, ANNUAL REPORT 2011 3 (2012), available at http://nsi.ncirc.gov/documents/NSI_Annual_Report_2011.pdf.

183 *Id.*

184 INFO. SHARING ENV’T, ISE-FS-200, INFORMATION SHARING ENVIRONMENT (ISE) FUNCTIONAL STANDARD (FS): SUSPICIOUS ACTIVITY REPORTING (SAR) 9, 29-30 (2009) [hereinafter ISE-SAR Functional Standard], available at <http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise-appendix.pdf>.

185 *Id.* at 2.

186 *Id.* at 26 (recognizing that purge policies vary from jurisdiction to jurisdiction).

187 See *infra*, notes 252-257.

188 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 27.

189 INITIAL PRIVACY AND CIVIL LIBERTIES ANALYSIS, *supra* note 180, at 15.

190 SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT, FINDINGS AND RECOMMENDATIONS OF THE SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT 30 (2008), available at <http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf>.

191 *Are We Safer?: Interview of Michael German*, PBS (Nov. 18, 2010), <http://www.pbs.org/wgbh/pages/frontline/are-we-safer/interviews/michael-german.html#2>.

192 GAO-13-233, *supra* note 3, at 22-25.

193 JEROME B. BJELOPERA, CONG. RESEARCH SERV., R41780, THE FEDERAL BUREAU OF INVESTIGATION AND TERRORISM INVESTIGATIONS 13 (2011), available at <http://www.fas.org/sgp/crs/terror/R41780.pdf>.

194 *Id.* at 15.

195 Three of the 19 fusion centers surveyed in this report are known to be co-located with their local JTTF: the Los Angeles Joint Regional Intelligence Center, the Northern California Regional Intelligence Center, and the Washington State Fusion Center.

196 In addition to the eGuardian and Guardian networks, the FBI also operates the Law Enforcement Regional Data Exchange (R-DEX) and National Data Exchange (N-DEX), both of which provide access to criminal justice data. Moreover, the Department of Justice funds six interstate Regional Information Sharing Systems (RISS) that pre-date 9/11 and are strictly limited to criminal intelligence that has met the reasonable suspicion threshold.

197 Recall that the FBI has encouraged fusion center participation by advertising that the eGuardian system would maintain “inconclusive” files for up to five years, during which time they would be viewable by other law enforcement agencies. *Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing: Hearing Before the Subcomm. On Terrorism & Homeland Sec. of the S. Comm. On the Judiciary*, 111th Cong. 11 (2009) (statement of Caroline Fredrickson, Dir., Am. Civil Liberties Union Wash. Legis. Office) [hereinafter *Statement of Caroline Fredrickson*], available at http://www.fas.org/irp/congress/2009_hr/042109fredrickson.pdf; *Privacy Impact*

- Assessment for the eGuardian Threat Tracking System*, FED. BUREAU OF INVESTIGATION [hereinafter *eGuardian Privacy Impact Assessment*], <http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat> (last visited Mar. 10, 2013) (“...[I]f a nexus to terrorism can neither be substantiated nor discounted, the Referred report is determined to be inconclusive, marked as such, and then referred to Guardian for further assessment by the JTTF. Again, at this point, the Referred report will be viewable to other law enforcement agencies with eGuardian accounts. The report will continue to remain in the eGuardian system for tracking and further analytic review. The information in these reports – where a nexus to terrorism is inconclusive or a nexus to terrorism has been substantiated – will be maintained for five years.”).
- 198 FED. BUREAU OF INVESTIGATION, U.S. DEP’T OF JUSTICE, EGUARDIAN BRIEF: IACP 2009 4 (2009), *available at* <http://www.aclu.org/files/assets/aclueg000072.pdf>; *eGuardian Privacy Impact Assessment*, *supra* note 197 (“If a clear determination is made of “a nexus to terrorism,” the information will be passed along to the eGuardian SDR for further dissemination and then on to Guardian for analysis. If no determination can be made regarding “a nexus to terrorism,” but neither can the nexus be discounted, the information will be added to the eGuardian SDR for pattern and trend analysis.”); *see also* PROGRAM MANAGER, INFO. SHARING ENV’T, NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE: CONCEPT OF OPERATIONS 14 (2008), *available at* http://nsi.ncirc.gov/documents/NSI_CONOPS_Version_1_FINAL_2008-12-11_r4.pdf.
- 199 GAO-13-233, *supra* note 3, at 8.
- 200 *Id.* at 53.
- 201 *Id.* at 18; U.S. DEP’T OF HOMELAND SECURITY, 2011 NATIONAL NETWORK OF FUSION CENTERS: FINAL REPORT 20-21 (2012), *available at* <http://www.dhs.gov/sites/default/files/publications/2011-national-network-fusion-centers-final-report.pdf>.
- 202 FED. BUREAU OF INVESTIGATION, U.S. DEP’T OF JUSTICE, EGUARDIAN I (2008), *available at* <http://www.aclu.org/files/assets/aclueg000014.pdf>; FED. BUREAU OF INVESTIGATION, U.S. DEP’T OF JUSTICE, EGUARDIAN QUICK STUDY INSTRUCTIONAL 3 (n.d.), *available at* <http://www.aclu.org/files/assets/aclueg000040.pdf>.
- 203 GAO-13-233, *supra* note 3, at 53.
- 204 *Id.*
- 205 GAO-13-233, *supra* note 3, at 19-20.
- 206 *Id.* at 7 n. “a”.
- 207 *eGuardian Privacy Impact Assessment*, *supra* note 197, at 6.
- 208 GAO-13-233, *supra* note 3, at 7 n. “a”.
- 209 *Id.* at 15.
- 210 *Id.* at 16.
- 211 *Id.* at 2.
- 212 *Id.* at 17.
- 213 Dr. Bridget Nolan, a sociologist at the University of Pennsylvania and a former intelligence analyst at the National Counterterrorism Center (NCTC), interviewed 20 of her NCTC colleagues about their work and found that it is “best described as chaotic and overwhelming,” due in large part to the “perils of too much information.” BRIDGET ROSE NOLAN, INFORMATION SHARING AND COLLABORATION IN THE UNITED STATES INTELLIGENCE COMMUNITY: AN ETHNOGRAPHIC STUDY OF THE NATIONAL COUNTERTERRORISM CENTER 22-23 (2013) (unpublished Ph.D. dissertation, University of Pennsylvania), *available at* http://media.philly.com/documents/Nolan_Dissertation.PDF. According to one analyst, “people will send everything to everybody” for fear of missing something, “but when everybody does that, it creates its own noise. And people drown in it. And as a consequence of too much information sharing, key pieces of information ... may be ignored.” *Id.* “More information is not necessarily better,” the analysts concludes. “Better information is better.” *Id.* at 29. Consequently, Nolan recognizes that “many analysts balk when reporters or politicians use the phrase ‘connecting the dots’ ... [as if it were] as simple as completing the activities on a child’s paper placemat. ... “The page is black with dots.”” *Id.* at 33.
- 214 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 27.
- 215 *Id.* at 36-38, 57-59.

216 SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE
 ACTIVITIES AND THE RIGHTS OF AMERICANS: BOOK II, S. REP. NO. 94-755, at 259 (1976), *available at* [http://www.
 intelligence.senate.gov/pdfs94th/94755_II.pdf](http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf).

217 *Id.* at 260 (internal footnotes omitted).

218 ISE-SAR Functional Standard, *supra* note 184, at 2.

219 *Id.* at 29 n. 11.

220 GLOBAL JUSTICE INFO. SHARING INITIATIVE, U.S. DEP'T OF JUSTICE, TIPS AND LEADS ISSUE PAPER 3 (2007)
 [hereinafter TIPS AND LEADS ISSUE PAPER] (on file with the Brennan Center).

221 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 36.

222 *See, e.g., More About Suspicious Activity Reporting*, AM. CIVIL LIBERTIES UNION (Jan. 18, 2013), [http://www.aclu.
 org/spy-files/more-about-suspicious-activity-reporting](http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting).

223 ISE-SAR Functional Standard, *supra* note 184, at 29 n.11.

224 *Id.*

225 *Id.* at 33.

226 *Terry v. Ohio*, 392 U.S. 1, 27 (1968) (describing reasonable suspicion as something more than an “inchoate and
 unparticularized suspicion or ‘hunch,’” and based on “specific reasonable inferences” drawn from the facts and an
 officer’s experience).

227 *See Characteristics of Terrorist’s Surveillance*, L.A. POLICE DEP’T, [http://www.lapdonline.org/home/content_basic_
 view/27436](http://www.lapdonline.org/home/content_basic_view/27436) (last visited Mar. 11, 2013); N. CAL. REGIONAL INTELLIGENCE CTR., ANTI-TERRORISM (2012) (on file
 with the Brennan Center).

228 ISE-SAR Functional Standard, *supra* note 184, at 29 n.11.

229 The 2009 revised Functional Standard *allows* fusion centers to omit “privacy fields” containing personally
 identifiable information from an ISE-SAR when the report lacks a nexus to terrorism-related crime. *Id.* at 12. But
 the Functional Standard does not *require* fusion centers to omit personal information. *Id.* (“Each ISE participant
 can exclude additional data elements from the Summary ISE-SAR Information format in accordance with its own
 legal and policy requirements.”).

230 *Id.*

231 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 36-38. To their credit, DHS privacy officials
 eventually cancelled federal intelligence reports that sought to use this information, noting that the activities
 were constitutionally protected and that there was nothing illegal, nefarious, or objectionable about them. *Id.*
 According to the Senate investigation, had federal employees disseminated such reports themselves, they would have
 violated provisions of the Privacy Act of 1974. *Id.* at 35. The Privacy Act prohibits federal officials from collecting
 or maintaining information about people in United States for the purpose of monitoring their exercise of First
 Amendment freedoms. 5 U.S.C. § 522a (e)(7) (2013). Fusion centers are almost always owned and operated by state
 and local authorities, exempting them from the Act. 5 U.S.C. § 552a(e)(7); 2012 SENATE HSGAC FUSION CENTER
 REPORT, *supra* note 8, at 35.

232 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 38.

233 *See, e.g., Declaration of Deputy Commissioner David Cohen*, *supra* note 41, at ¶ 52; Philip Mudd, Former Deputy
 Director, Fed. Bureau of Investigation, Nat’l Sec. Branch, Remarks on Panel 3 at Brennan Center for Justice
 Symposium: Intelligence Collection and Law Enforcement: New Roles, New Challenges (March 18, 2011) (transcript
 on file with the Brennan Center). (“[The Intelligence Reform and Terrorism Prevention Act of 2004 dictated] that the
 [FBI] must have a preventive counter terrorism posture. That means stop things before they happen. That means by
 definition, you cannot always tether investigations to proof of criminal activity. It’s not a choice by the Department of
 Justice, by the executive branch, and by people like me.”); *see also* Office of the Inspector General, U.S. Dep’t of Justice,
 Audit Report 04-10, The Federal Bureau of Investigation’s Efforts to Improve the Sharing of Intelligence and Other
 Information 18 (2003), *available at* <http://www.justice.gov/oig/reports/FBI/a0410/final.pdf> (noting that after 9/11,
 the FBI “lacked the ability to ‘connect the dots’ or create a mosaic of information.”).

234 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 27.

235 See *supra* notes 206-210.

236 A 2011 DHS survey found that 66.2 percent of fusion centers use eGuardian, while 38.2 percent use an ISE Shared Space. *Id.* And the Government Accountability Office found that as of November 2012, all fusion centers have adopted eGuardian while only 73 percent use ISE Shared Spaces. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 3, at 18.

237 *Id.* at 33-38.

238 *Id.* at 33-34 (between January 2010 and October 2012, there were 24,599 ISE-SARs added to the ISE, approximately 1,200 of which resulted in an FBI investigation).

239 *Id.* at 35.

240 28 C.F.R. § 23.20(a).

241 *Id.* at § 23.20(b).

242 TIPS AND LEADS ISSUE PAPER, *supra* note 220, at 1.

243 Tautologically, the DOJ distinguishes the two categories by defining “criminal intelligence” as information that meets the reasonable suspicion requirement whereas “tips and leads” or SARs do not. *Id.* This is consistent with the ISE-SAR Functional Standard, which states that fusion centers may share “fact information” without a criminal predicate “in accordance with 28 CFR Part 23.” ISE-SAR FUNCTIONAL STANDARD, *supra* note 184, at 33.

244 TIPS AND LEADS ISSUE PAPER, *supra* note 220, at 2. Because revisions to the Functional Standard in 2009 did not include reasonable suspicion requirement, fusion centers are still relying on DOJ’s guidance in this paper.

245 *Id.* at 2-3. The concept of a “temporary” or “working” file is not new. As early as the 1970s, a private organization called the Law Enforcement Intelligence Unit (LEIU) developed guidance “interpreting” 28 CFR 23 and creating a model policy for law enforcement agencies known as the *LEIU File Guidelines*. One of the most prominent differences between 28 CFR 23 and the *Guidelines* is the way in which the *Guidelines* treat information lacking a criminal predicate. They propose the concept of a “temporary file” in which to store such information for a period of time before being moved to a “permanent file” – if a criminal predicate is established – or being purged from the system. LAW ENFORCEMENT INTELLIGENCE UNIT, CRIMINAL INTELLIGENCE GUIDELINES § IV(B) (2002), available at http://www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf. To be clear, 28 CFR 23 does not even hint at the notion of a “temporary file.” David Carter, however, argues that the *Guidelines* are designed to fill a perceived “operational gap” in the law. CARTER, LAW ENFORCEMENT INTELLIGENCE, *supra* note 36, at 149. According to Carter: “Often, intelligence personnel will receive a tip from the public or perhaps a Suspicious Activity Report (SAR) which suggests a crime but has insufficient information to establish a criminal predicate. ... Since the 28 C.F.R. Part 23 guidelines do not address this circumstance, a practical interpretation of the regulation ... was created in the *LEIU File Guidelines*.” *Id.* at 153-54.

246 *Statement of Caroline Fredrickson, supra* note 197, at 11; see also *eGuardian Privacy Impact Assessment, supra* note 197 (“In keeping with the retention period currently in effect for state criminal intelligence systems under 28 C.F.R. Part 23, suspicious activity reports in this third category (reports for which a determination cannot be made whether or not a nexus to terrorism exists) will be retained for a period of five years and will be used for analytical purposes and/or to demonstrate trends.”).

247 See 28 C.F.R. § 23.20(a). The FBI’s statement appears to ignore this rule and misstate the purpose of 28 C.F.R. § 23.20(h), which authorizes the retention of information that satisfies the reasonable suspicion requirement for up to five years.

248 TIPS AND LEADS ISSUE PAPER, *supra* note 220, at 1.

249 See, e.g., U.S. DEP’T OF HOMELAND SEC., HOMELAND SECURITY GRANT PROGRAM: GUIDANCE AND APPLICATION KIT 4 (2009), available at http://www.fema.gov/pdf/government/grant/2010/fy10_hsgp_kit.pdf (requiring privacy policies “at least as comprehensive as the ISE Privacy Guidelines”); see also INFO. SHARING ENV’T, GUIDELINES TO ENSURE THAT THE PRIVACY AND OTHER LEGAL RIGHTS OF AMERICANS ARE PROTECTED IN THE DEVELOPMENT AND USE OF THE INFORMATION SHARING ENVIRONMENT 5-6 (n.d.), available at <http://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf>; INITIAL PRIVACY AND CIVIL LIBERTIES ANALYSIS, *supra* note 180, at 17.

250 TIPS AND LEADS ISSUE PAPER, *supra* note 220, at 1.

251 CAL. STATE TERRORISM THREAT ASSESSMENT SYS., INFORMATION PRIVACY POLICY 1 (n.d.) [hereinafter CAL. STTAS PRIVACY POLICY], available at <http://www.nfcausa.org/files/DDF/CaliforniaSTTASPrivacyPolicy3.pdf>; see also

- MAJOR CRIMES DIV., L.A. POLICE DEP'T, DIVISIONAL ORDER NO. 15: PRIVACY GUIDELINES FOR INFORMATION SHARING ENVIRONMENT, SUSPICIOUS ACTIVITY REPORT (ISE-SAR) EVALUATION ENVIRONMENT INITIATIVE 1 (2009) (emphasis added), available at http://documents.law.yale.edu/sites/default/files/LAPD_Div_Order15_Aug09-ocr.pdf (“Application of 28 CFR Part 23: All ISE-SAR information posted to LAPD’s shared space under the Initiative shall meet *applicable* provisions of 28 CFR Part 23. This is to include applying the operating policies set forth in 28 CFR § 23.20 to all individual and organizational criminal subjects ...”).
- 252 CAL. STTAS PRIVACY POLICY, *supra* note 251, at 4; MAJOR CRIMES DIV., L.A. POLICE DEP'T, DIVISIONAL ORDER NO. 16: PRIVACY GUIDELINES FOR EVALUATION ENVIRONMENT INITIATIVE 3 (2009) (on file with the Brennan Center) (“Retention and Destruction: ... Information submitted and determined to qualify as an ISE-SAR, but which does not reach the reasonable suspicion standard of 28 CFR Part 23, will be retained as a temporary file for up to one-year to permit the information to be validated or refuted and its credibility and value to be assessed. ... Temporary files that are evaluated during their retention period and determined to meet applicable 28 CFR Part 23 and ISE-SAR criteria, shall be submitted to the shared space. When ISE-SAR information has no further value or meets the applicable criteria for purge, it will be removed from the shared space or the temporary file closed, as appropriate.”).
- 253 According to the Houston privacy policy, “[a]ll information and intelligence will be obtained lawfully and products produced will be handled in accordance with 28 CFR Part 23, and applicable State of Texas laws.” HOUS. REG’L INTELLIGENCE SERV. CTR. (HRISC), HOUSTON REGIONAL INTELLIGENCE SERVICE CENTER (FUSION CENTER) PRIVACY POLICY: PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES POLICY 4 (2009), available at <http://www.nfcausa.org/files/DDF/Privacy%20Policy%20HRISC%20September%2009%20SSNP%20.pdf>.
- 254 *Id.* at 6 (“All SAR data, Inquiries, including tips and leads that are in the SAR database will be kept in that database for a period of one year, unless there is reasonable suspicion of criminal activity, in which [case] they can be retained for up to five years.”).
- 255 *eGuardian Privacy Impact Assessment*, *supra* note 197.
- 256 U.S. GEN. ACCOUNTING OFFICE, OFFICE OF THE COMPTROLLER GENERAL, GGD-81-36, THE MULTI-STATE REGIONAL INTELLIGENCE PROJECTS – WHO WILL OVERSEE THESE FEDERALLY FUNDED NETWORKS? 9 (1980), available at <http://www.gao.gov/assets/140/132128.pdf>.
- 257 *Id.* at 11. As initially conceived, the LEAA guidelines did not specify the level of suspicion necessary to collect and maintain intelligence information. But in response to privacy concerns raised during a notice and comment period, the Justice Department revised the guidelines to explicitly require reasonable suspicion of criminal activity. Criminal Intelligence Systems Operating Policies, 43 Fed. Reg. 28,572 (June 30, 1978). The LEAA touted the result as “some pretty tough, tight guidelines on insuring [sic] that grants for intelligence activities were not used in violation of privacy and political rights of individuals.” *Law Enforcement Assistance Reform: Hearing on S. 241 Before the S. Committee on the Judiciary*, 96th Cong. 78 (1979) (statement of Henry S. Dogin, Acting Administrator of the LEAA) (According to the LEAA Administrator, the guidelines “are an indication of how much we are concerned with the privacy and security of these intelligence systems.”).
- 258 In 1979, Congress passed the Justice System Improvement Act, which restructured the Department of Justice and replaced the LEAA with the Office of Justice Assistance, Research, and Statistics (OJARS). Pub. L. No. 96-157 § 801, 93 Stat. 1167, 1201 (1979). An amendment to the Act introduced by Rep. William Edwards of California required OJARS to prescribe a set of guidelines that would govern all federally funded criminal intelligence systems. And members of Congress already knew exactly what to expect out of OJARS – the LEAA guidelines. Responding to a question on the House floor about what standard the guidelines would employ, Rep. Edwards invoked the LEAA policy: “Mr. Chairman, does the gentleman say there must be criminal activity involved or potential suspected criminal activity? There is a big difference. The guidelines that are in existence at the moment are instructions from LEAA to say that criminal intelligence information shall be maintained only if it is reasonably suspected that the individual is involved in criminal activity.” 125 CONG. REC. 27,699 (Oct. 10, 1979) (statement of Rep. William Donlon Edwards). Indeed, the standard promulgated by OJARS in 1980 and codified in 28 CFR 23 is identical to the 1978 LEAA guidelines: “Criminal intelligence information concerning an individual shall be collected and maintained only if it is reasonably suspected that the individual is involved in criminal activity and that the information is relevant to that criminal activity.” *Compare* Criminal Intelligence Systems Operating Policies, 43 FED. REG. 28,572 § 1(A) (June 30, 1978) with 28 C.F.R. § 23.20(a).
- 259 OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T OF JUSTICE, 1993 REVISION AND COMMENTARY: FINAL REVISION TO THE

- OFFICE OF JUSTICE PROGRAMS, CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICY 11 (1993), available at http://www.it.ojp.gov/documents/28cfr_part_23.pdf.
- 260 AM. CIVIL LIBERTIES UNION, UNLEASHED AND UNACCOUNTABLE: THE FBI'S UNCHECKED ABUSE OF AUTHORITY 23-27 (2013), available at <https://www.aclu.org/sites/default/files/assets/unleashed-and-unaccountable-fbi-report.pdf>.
- 261 Cynthia A. Brown, *Divided Loyalties: Ethical Challenges for America's Law Enforcement in Post 9/11 America*, 43 CASE W. RES. J. INT'L L. 651, 667 (2011).
- 262 See Kim Murphy, *L.A. Sheriff Watchdog Merrick Bobb Hired as Seattle Police Monitor*, L.A. TIMES, Oct. 30, 2012, available at <http://www.latimes.com/news/nation/nationnow/la-na-nn-merrick-bobb-seattle-police-20121030,0,6073936.story>.
- 263 POLICE ASSESSMENT RES. CTR., REVIEW OF NATIONAL POLICE OVERSIGHT MODELS FOR THE EUGENE POLICE COMMISSION 2 (2005), available at http://www.parc.info/client_files/Eugene/Review%20of%20National%20Police%20Oversight%20Models%20%28Feb.%202005%29.pdf; see also MERRICK BOBB, POLICE ASSESSMENT RES. CTR INTERNAL AND EXTERNAL POLICE OVERSIGHT IN THE UNITED STATES 9-19 (2005), available at http://www.parc.info/client_files/Altus/10-19%20altus%20conf%20paper.pdf.
- 264 POLICE ASSESSMENT RES. CTR., *supra* note 263, at 11.
- 265 CITY OF HOUSTON, EXECUTIVE ORDER NO. 1-5 REVISED § 6.1 (2011) (Independent Police Oversight Board), available at <http://www.houstontx.gov/execorders/1-5.pdf>.
- 266 The Inspector General for the City of Houston serves as an “ombudsmen” to assist citizens in filing complaints. CITY OF HOUSTON, EXECUTIVE ORDER NO. 1-39 REVISED § 5.1.5 (2011) (Establishment of Office of Inspector General for Investigation of Employee Misconduct), available at <http://www.houstontx.gov/legal/1-39.pdf>. The IG may also conduct its own investigation if it agrees with the Independent Police Oversight Board that additional investigation is necessary and the Chief of Police has refused to do so. CITY OF HOUSTON, EXECUTIVE ORDER NO. 1-5, *supra* note 265, at § 7.1.6; City of Houston, *Press Conference: Police Oversight Initiatives*, YOUTUBE.COM (Feb. 23, 2011), <http://www.youtube.com/watch?v=Sk9wuAY5G7k>. The Houston Independent Police Oversight Board also has authority to make policy recommendations on a limited range of issues: hiring new police officers, training on the proper treatment of citizens, and community concerns. CITY OF HOUSTON, EXECUTIVE ORDER NO. 1-5, *supra* note 265, at § 5.2.
- 267 Cindy George, *Some Doubt City's Efforts to Rebuild Trust in HPD*, HOUSTON CHRON. (Feb. 18, 2011), <http://www.chron.com/news/houston-texas/article/Some-doubt-city-s-efforts-to-rebuild-trust-in-HPD-1690326.php>; see also *Who's Policing the Police?*, MYFOX HOUSTON (Feb. 11, 2011), <http://www.myfoxxhouston.com/story/18179645/whos-policing-the-police>; James Pinkerton, *Punishments for HPD Officers Often Unravel*, HOUSTON CHRON. (Feb. 20, 2011), <http://www.chron.com/news/houston-texas/article/Punishments-for-HPD-officers-often-unravel-1687733.php>.
- 268 See generally *What We Do*, OFFICE OF OMBUDSMAN OF L.A. CNTY., <http://ombudsman.lacounty.info/what-we-do.aspx> (last visited Mar. 18, 2013). The Ombudsman “only reviews completed service reviews or investigations which have been appealed to the Ombudsman by dissatisfied complainants. The Ombudsman does not have investigative authority and is not empowered to initiate or conduct an administrative investigation, nor will he involve himself in criminal investigations of misconduct.” *Transparency, Openness, Public Trust, and the Los Angeles County Sheriff's Department*, L.A. CNTY. SHERIFF'S DEP'T, <http://1.usa.gov/XIE24H> (last visited Mar. 18, 2013).
- 269 The St. Paul Police-Civilian Internal Affairs Review Commission is a seven-member commission that includes two St. Paul police officers; all members are appointed by the mayor with approval by the city council. POLICE-CIVILIAN INTERNAL AFFAIRS REVIEW COMM'N, CITY OF SAINT PAUL, ANNUAL REPORT: 2009 6 (2010), available at <http://www.stpaul.gov/DocumentCenter/Home/View/13234>. The police department's internal affairs unit investigates all civilian complaints. *Id.* The Review Commission has subpoena power and can review completed investigations, but the final word on disposition and discipline belongs to the police chief. *Id.* at 12, 14.
- 270 The Portland Citizen Review Committee is a six-member body appointed by the City Council and includes at least two community members as well as the director of the Independent Police Review Division, which is part of the Office of the City Auditor. OFFICE OF THE CITY AUDITOR, CITY OF PORTLAND, PSF-5.06, CITIZEN REVIEW COMMITTEE (CRC) – INDEPENDENT POLICE REVIEW DIVISION (IPR) – PROCESS FOR APPOINTMENT AND REAPPOINTMENT TO THE CRC ¶ 2 (2007), available at <http://www.portlandonline.com/auditor/index.cfm?&a=9035&c=27455>. The Review Committee does not process civilian complaints; it hears appeals and is limited to agreeing or disagreeing

- with the police department's investigation. OFFICE OF THE CITY AUDITOR, CITY OF PORTLAND, PSF-5.03, CITIZEN REVIEW COMMITTEE (CRC) – INDEPENDENT POLICE REVIEW DIVISION (IPR) – APPEALS PROCEDURES (2012), available at <http://www.portlandonline.com/auditor/index.cfm?&a=9030&c=27455>. The Review Committee does not have subpoena power.
- 271 The Seattle Office of Professional Accountability Auditor is an independent civilian contractor appointed by the mayor and confirmed by the city council. SEATTLE, WASH., CODE § 3.28.850 (2002), available at <http://clerk.seattle.gov/~scripts/nph-brs.exe?d=CODE&s1=3.28.850.snum.&Sect5=CODE&Sect6=HITOFF&l=20&p=1&u=/-public/code1.htm&r=1&f=G>. Although the name of the office has been the source of some confusion, the Auditor functions like an appellate review board, responsible for “auditing” all investigations conducted by the Office of Professional Accountability. *Id.* at § 3.28.855; OFFICE OF PROF’L ACCOUNTABILITY REVIEW Bd., CITY OF SEATTLE, POLICY REPORT: REVISED NAMES, ROLES, AND POWERS OF THE OFFICE OF PROCESSIONAL ACCOUNTABILITY REVIEW BOARD 5-6 (2012) [hereinafter REVIEW BOARD POLICY REPORT], available at http://clerk.seattle.gov/~CFS/CF_312426.pdf. The Auditor does not have subpoena power, but he or she can request additional investigation. *Id.* The Auditor prepares biannual reports on these investigations and can make policy recommendations but is not allowed to make any disciplinary recommendations. *Id.*; see, e.g., ANNE LEVINSON, OFFICE OF PROF’L ACCOUNTABILITY, SEMI-ANNUAL REPORT OF THE CIVILIAN AUDITOR (2012), available at http://www.seattle.gov/police/OPA/Docs/Auditor/Auditor_Report_Dec_11_May_12.pdf; see also REVIEW BOARD POLICY REPORT, *supra*, at 8-9.
- 272 N.Y. CIVIL LIBERTIES UNION FOUND., CIVILIAN REVIEW OF POLICING: A CASE STUDY REPORT 3 (1993), available at, <http://www.nyclu.org/files/publications/NYCLU.CivilianReviewPolicing.CaseStudyRep.1993.pdf>.
- 273 SAMUEL WALKER, THE NEW WORLD OF POLICE ACCOUNTABILITY 20 (2005); see generally PATRICK O’HARA, WHY LAW ENFORCEMENT ORGANIZATIONS FAIL: MAPPING THE FAULT LINES IN POLICING (2005). And as Matthew Waxman notes, “the counter-terrorism agenda may influence or disrupt systems and patterns of political accountability of local police agencies.” See Waxman, *supra* note 27, at 378.
- 274 POLICE ASSESSMENT RES. CTR., *supra* note 263, at 13.
- 275 BOBB, *supra* note 263, at 9-10.
- 276 *Id.* at 9.
- 277 *Id.*
- 278 See Howard Cohen, *Miami-Dade Commissioner Predicts ‘More People Will Lose Their Jobs’*, MIAMI HERALD, Sept. 10, 2009; Charles Rabin & Jennifer Lebovich, *Miami-Dade Mayor Proposes Sweeping Pay Cuts*, MIAMI HERALD, July 16, 2009, at D1.
- 279 *Id.* at 11.
- 280 *Id.*
- 281 SEATTLE HUMAN RIGHTS COMM’N, CITY OF SEATTLE, REPORT ON POLICE ACCOUNTABILITY AND RECOMMENDATIONS 5 (2012), available at http://www.seattle.gov/humanrights/Documents/SHRC_PoliceAcctRpt010812.pdf.
- 282 For example, the current iteration of New York’s Civilian Complaint Review Board (CCRB) was established in 1993 because of prevalent concerns about police abuse and brutality. See Dennis Hevesi, *14 on Council Propose Removing Review Board from Police Dept.*, N.Y. TIMES, Jan. 23, 1992, available at <http://www.nytimes.com/1992/01/23/nyregion/14-on-council-propose-removing-review-board-from-police-dept.html>. The CCRB gained subpoena power, although it has never exercised this authority to obtain information from the NYPD. Previous iterations of the CCRB, which more closely resemble review and appellate models, date back to 1953. *History of the CCRB*, N.Y.C. CIVILIAN COMPLAINT REVIEW Bd., <http://www.nyc.gov/html/ccrb/html/history.html> (last visited Dec. 19, 2012). Similarly, Portland’s Independent Police Review Division replaced the Police Internal Investigations Auditing Committee in 2001 after years of persistent criticism that the Committee, established in 1982 without subpoena power, had not been successful in monitoring, reviewing, or reporting on the police internal investigation system. See Portland, Or., Ordinance 175652 (May 24, 2001), available at <http://www.portlandonline.com/auditor/index.cfm?c=27072&a=8101>. In Philadelphia, the Police Advisory Commission gained support in 1994 only after civil judgments and settlements against the city in police-misconduct or abuse cases exceeded \$10 million a year. Jan Ransom & Phillip Lucas, *Police Advisory Commission Must Cut Through Backlog of Complaints*, PHILLY.COM (Mar. 12, 2012), http://articles.philly.com/2012-03-12/news/31152747_1_pac-backlog-complaints/2.

283 BOBB, *supra* note 263, at 12.

284 See N.Y.C. CIVILIAN COMPLAINT REVIEW BD., 2011 ANNUAL REPORT 18 (2012), available at <http://www.nyc.gov/html/ccrb/pdf/ccrbann2011.pdf> (finding that the NYPD declined to discipline officers in 16 percent of substantiate cases in 2011; 18 percent in 2010; 27 percent in 2009; 32 percent in 2008; and 35 percent in 2007). Even where the NYPD has sought discipline – *i.e.*, in cases where the CCRB finds there is credible evidence that an officer engaged in misconduct, the department most frequently awards the mildest form of discipline. *Id.* at 19 (finding that officers received “instructions” in 71 percent of the cases in 2011 and 74 percent in 2010).

285 N.Y. CITY CHARTER § 440(c)(3).

286 *Id.* at § 440(d)(1).

287 The board reserves its subpoena power for obtaining evidence from third parties, such as medical records from a hospital or surveillance video from a business. See *The Investigative Process*, N.Y.C. CIVILIAN COMPLAINT REVIEW BD., <http://www.nyc.gov/html/ccrb/html/how.html> (last visited Mar. 13, 2013).

288 See ROBERT A. PERRY, N.Y. CIVIL LIBERTIES UNION, MISSION FAILURE: CIVILIAN REVIEW OF POLICING IN NEW YORK CITY 1994-2006 44 (2007), available at http://www.nyclu.org/files/publications/nyclu_pub_mission_failure.pdf; Michael Wilson, *Top Officers Are Said to Ignore Complaint Board’s Inquiry*, N.Y. TIMES, Sept. 15, 2005, available at <http://www.nytimes.com/2005/09/15/nyregion/15protest.html>.

289 David Noriega, *When I Tried Policing the NYPD*, SALON (Aug. 29, 2012, 2:11 PM), http://www.salon.com/2012/08/29/policing_the_police/.

290 When examining “policy” issues, the CCRB has relied on publicly available literature or its own docket of complaints rather than reviewing the NYPD’s records. For example, when the CCRB examined the issue of police “stop and frisk” tactics, its report explicitly noted that it did not “describe the Police Department’s stop-and-frisk practices,” but rather offered “an interesting and useful picture of those individuals who filed complaints with the CCRB after being stopped by the police, the officers involved, the nature of those encounters, and the results of the complaints.” CIVILIAN COMPLAINT REVIEW BD., STREET STOP ENCOUNTER REPORT: AN ANALYSIS OF CCRB COMPLAINTS RESULTING FROM THE NEW YORK POLICE DEPARTMENT’S “STOP & FRISK” PRACTICES 1 (2001), available at <http://www.nyc.gov/html/ccrb/pdf/stop.pdf>. For a list of CCRB recommendations since 1998, see *CCRB Reports*, N.Y.C. CIVILIAN COMPLAINT REVIEW BD., <http://www.nyc.gov/html/ccrb/html/reports.html> (last visited Mar. 13, 2013).

291 PERRY, *supra* note 288, at 7; see also David Noriega, *The Thin Blue Lie*, THE NEW INQUIRY (Aug. 29, 2012), <http://thenewinquiry.com/essays/the-thin-blue-lie/>.

292 These are: the Chicago Police Department (Independent Police Review Authority); the Detroit Police Department (Board of Police Commissioners); the Los Angeles Police Department (Police Commission); the Los Angeles Sheriff’s Department (Office of Independent Review); the Metropolitan Police Department of Washington, DC (Office of Police Complaints); the Miami Police Department (Civilian Investigative Panel); the Minneapolis Police Department (Civilian Police Review Authority); the New York City Police Department (Civilian Complaint Review Board); the Philadelphia Police Department (Police Advisory Commission); the Portland Police Bureau (Independent Police Review Division); the San Francisco Police Department (Office of Citizen Complaints); and the Seattle Police Department (Office of Professional Accountability).

293 *Private Eyes: Phila. Police Department Needs More Outside Scrutiny*, PHILLY.COM (Aug. 31, 2012) http://articles.philly.com/2012-08-31/news/33522151_1_police-oversight-police-department-police-officers. As of March 2012, the Police Advisory Commission had a backlog of 129 cases as old as 2008. And since its creation in 1994, it has issued just 21 recommendations to the police department in response to citizen complaints. *Id.*

294 See SFPD DGO 8.10, *supra* note 128.

295 BOBB, *supra* note 263, at 6.

296 *Id.* at 14.

297 *Id.*

298 PATEL, *supra* note 42, at 7.

299 *Id.*

300 INDEP. COMM’N ON THE L.A. POLICE DEP’T, REPORT OF THE INDEPENDENT COMMISSION ON THE LOS ANGELES POLICE DEPARTMENT 171-74, 178 (1991), available at http://www.parc.info/client_files/Special%20Reports/1%20

- [-%20Christopher%20Commission.pdf](#), at. In Los Angeles, the Inspector General both performs an investigative function (for example, the department's Use of Force Unit reports to the Inspector General, who is involved in the investigation and adjudication of all officer-involved shootings, head strikes, in-custody deaths, and injuries involving hospitalization), and conducts broader reviews and investigations. See *Mission Statement*, OFFICE OF THE INSPECTOR GEN., L.A. POLICE DEP'T, <http://www.oiglapd.lacity.org/isgig1.htm> (last visited Mar. 13, 2013); *The Function and Role of the Board of Police Commissioners*, L.A. POLICE DEP'T, http://www.lapdonline.org/police-commission/content_basic_view/900 (last visited Mar. 13, 2013). The office issues multiple public reports each month auditing the department's policies and performance on a wide range of issues, from use of force incidents to traffic collisions and ethics violations. See *generally Reports*, OFFICE OF THE INSPECTOR GEN., L.A. POLICE DEP'T, <http://www.oiglapd.lacity.org/isgrp1.htm> (last visited Mar. 13, 2013). Unlike the LASD's Special Counsel or Seattle's Review Board, the Inspector General has the authority to conduct independent investigations into "sensitive and/or high profile matters," either at the request of the Board of Police Commissioners or the city's Public Safety Bureau. See *Mission Statement*, *supra*.
- 301 JAMES G. KOLTS ET AL., L.A. CNTY. SHERIFF'S DEP'T, A REPORT I (1992), available at http://www.parc.info/client_files/Special%20Reports/3%20-%20Kolts%20Report%20-%20LASD.pdf. The LASD Special Counsel is a good example of the evaluative and performance-based model. The Special Counsel is a lawyer retained by the Los Angeles County Board of Supervisors. Armed with "unfettered access" to all relevant persons, documents and records, the Special Counsel creates public reports that address excessive force and integrity issues on an agency – rather than individual case – level. BOBB, *supra* note 263, at 13. The aim is to "foster a constructive, problem-solving dialog" that aims to "eliminate excessive or unnecessary lethal or non-lethal force" and reduce legal liability for the Sheriff's Department. *Id.*
- 302 The Board of Supervisors initially selected James Kolts for the purpose of conducting an inquiry and making recommendations for reform. The Kolts Commission, like the Christopher Commission, found that the LASD had "too many officers who have resorted to unnecessary and excessive force," had "not done an adequate job of disciplining them," and had "not dealt adequately with those that supervise them." KOLTS ET AL., *supra* note 301, at 4. Kolts issued a host of recommendations for reform, including calls for "responsible review" of citizen complaints and greater accountability throughout the chain of command. *Id.* The Board of Supervisors responded by making the role of special counsel a permanent arm of the Board. Merrick Bobb, a nationally renowned expert in police oversight and member of the Kolts Commission, became the first such Special Counsel in 1993 and continues to serve in that capacity. MERRICK J. BOBB ET AL., L.A. CNTY. SHERIFF'S DEP'T, 1ST SEMIANNUAL REPORT I (1993), available at http://parc.info/client_files/LASD/1st%20Semiannual%20Report.pdf.
- 303 Christina Villacorte, *L.A. County screening candidates for sheriff's inspector general job*, L.A. DAILY NEWS (April 10, 2013), http://www.dailynews.com/ci_22999138/l-county-screening-candidates-sheriffs-inspector-general-job.
- 304 Steve Miletich, *ACLU Calls for Police-Policy Reform – Report Urges New Plan For Internal Investigations*, SEATTLE TIMES, June 13, 1999, available at <http://community.seattletimes.nwsouce.com/archive/?date=19990613&slug=2966270>.
- 305 Editorial, *Panel Report Outlines Course For Seattle Police*, SEATTLE TIMES, Aug. 23, 1999, available at <http://community.seattletimes.nwsouce.com/archive/?date=19990823&slug=2978810>; Steve Miletich & Mike Carter, *Report's In: Next Move Is Up to Schell, Stamper – Panel Wants Civilian to Oversee Investigations of Police*, SEATTLE TIMES, Aug. 20, 1999, available at <http://community.seattletimes.nwsouce.com/archive/?date=19990820&slug=2978330>; Alan Snel & Kimberly A.C. Wilson, *Citizen Oversight of Police Called For – Report Finds Huge Flaws In Internal Investigations*, SEATTLE-POST INTELLIGENCER, Aug. 20, 1999, at A1. By 2000, the City Council had created the Office of Professional Accountability (based on investigative and quality assurance models), the Office of Professional Accountability Auditor (serving a review and appellate function), and the Office of Professional Accountability Review Board (following evaluative and performance-based models). See Seattle, Wash., Ordinance 119,805 (Dec. 21, 1999) (establishing OPA Director); Seattle, Wash., Ordinance 119,816 (Dec. 21, 1999) (creating OPA); Seattle, Wash., Ordinance 119,893 (Mar. 23, 2000) (setting forth duties of OPARB Internal Investigations Auditor); Seattle, Wash., Ordinance 120,728 (Feb. 22, 2002) (further modifying the OPARB).
- 306 WALKER, *supra* note 273, at 136.
- 307 *Id.*
- 308 SEATTLE HUMAN RIGHTS COMMISSION, *supra* note 281, at 6.
- 309 *Id.* The Seattle Human Rights Commission recently called for legislation authorizing the Review Board to independently investigate claims of police misconduct and function as an "appellate review panel of SPD

- disciplinary cases involving allegations of police misconduct, force-related incidents, and biased policing.” SEATTLE HUMAN RIGHTS COMMISSION, *supra* note 281, at 8; *see also* OFFICE OF PROFESSIONAL ACCOUNTABILITY REVIEW Bd., TRANSPARENCY, ACCOUNTABILITY, EFFECTIVENESS AND INDEPENDENCE: RECOMMENDATIONS REGARDING CIVILIAN OVERSIGHT OF THE SEATTLE POLICE DEPARTMENT 4 (2012), *available at* http://www.seattle.gov/council/OPARB/reports/2012oparb_recommendations.pdf. The recommendation follows a 2011 Justice Department investigation that found “a pattern or practice of constitutional violations regarding the use of force that result from structural problems, as well as serious concerns about biased policing.” CIVIL RIGHTS DIV., DEP’T OF JUSTICE, & U.S. ATTORNEY’S OFFICE FOR THE W. DIST. OF WASH., INVESTIGATION OF THE SEATTLE POLICE DEPARTMENT 2 (2011), *available at* http://www.justice.gov/crt/about/spl/documents/spd_findletter_12-16-11.pdf. In addition to problems with training and supervision, the DOJ report faulted the Office of Professional Accountability for outsourcing investigations to precinct supervisors. *Id.* at 5. “Indeed, none of the uses of force our review finds to be excessive were referred to OPA for its review.” *Id.* Nonetheless, the DOJ found that “the structure of OPA is sound, and the investigations OPA itself conducts generally are thorough.” *Id.* A subsequent federal lawsuit and consent decree, approved in July 2012, reiterated the Justice Department’s assessment of OPA but also implemented strict reporting requirements for use of force incidents and created a Community Police Commission to serve as an advisory board. *See* Settlement Agreement & Stipulated [Proposed] Order of Resolution at ¶¶ 3-12, 91-118, 164, *United States v. City of Seattle*, No. 12-CV-1282 (W.D. Wash. Jul. 27, 2012), *available at* http://www.justice.gov/crt/about/spl/documents/spd_consentdecree_7-27-12.pdf (entered with modifications by Stipulation and Order for Modification and For Entry of Preliminary Approval of the Parties’ Settlement Agreement and Stipulated Order of Resolution, *United States v. City of Seattle*, No. 12-CV-1282 (W.D. Wash. Sept. 21, 2012), *available at* http://www.justice.gov/crt/about/spl/documents/spd_orderapprovingsettlement_9-21-12.pdf).
- 310 PROCEDURES AND TACTICS PUBLICATION, *supra* note 128, at 11, 15-16 (implementing SEATTLE, WASH., ORDINANCE No. 108333). The most recent audit revealed no violations of the law. *See* Letter from John Diaz, Chief, Seattle Police Dep’t, to Mayor Michael Patrick McGinn (May 19, 2011) [hereinafter May 2011 Audit Letter], *available at* http://clerk.seattle.gov/-CFS/CF_311606.pdf.
- 311 PROCEDURES AND TACTICS PUBLICATION, *supra* note 128, at 16.
- 312 *Id.* at 16-17.
- 313 OFFICE OF THE INSPECTOR GEN., L.A. POLICE COMM’N, ANTI-TERRORISM INTELLIGENCE SECTION AUDIT, FISCAL YEAR 2009-2010 (2012) [hereinafter “LA OIG Report 2009-2010”], *available at* http://www.oiglapd.lacity.org/Reports/ATIS_FY09-10_1-19-12.pdf; OFFICE OF THE INSPECTOR GEN., L.A. POLICE COMM’N, ANTI-TERRORISM INTELLIGENCE SECTION AUDIT, FISCAL YEAR 2008-2009 (2009), *available at* http://www.oiglapd.lacity.org/Reports/A-T_IntellSecfy08-09_4-9-09.pdf; OFFICE OF THE INSPECTOR GEN., L.A. POLICE COMM’N, ANTI-TERRORISM INTELLIGENCE SECTION AUDIT, FISCAL YEAR 2006-2007 (2007), *available at* http://www.oiglapd.lacity.org/Reports/ATIS_phase1_3-6-07.pdf.
- 314 LA OIG Report 2009-2010, *supra* note 313, at 5-7. These audits did not address the LAPD’s controversial use of suspicious activity reporting or its relationship with regional and statewide fusion centers. However, a Special Order issued by Chief Charlie Beck in August 2012 now directs the Inspector General to conduct an annual audit of LAPD’s SAR program. *See* L.A. POLICE DEP’T, SPECIAL ORDER No. __: REPORTING SUSPICIOUS ACTIVITY POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM – REVISED; AND SUSPICIOUS ACTIVITY REPORT NOTEBOOK DIVIDER, FORM 18.30.03 – REVISED 1 (Aug. 16, 2012) [hereinafter BECK SPECIAL ORDER], *available at* http://www.lapdpolicecom.lacity.org/082812/BPC_12-0358.pdf.
- 315 *See generally* LAPD SAR AUDIT, *supra* note 137.
- 316 *Id.* at 5-7; *see also* STOP LAPD SPYING COALITION, TO OBSERVE AND TO SUSPECT: A PEOPLE’S AUDIT OF THE LOS ANGELES POLICE DEPARTMENT’S SPECIAL ORDER 1 at 1-2 (2013), *available at* <http://stoplapdspying.org/wp-content/uploads/2013/03/PEOPLES-AUDIT-FINAL.pdf>.
- 317 In addition to San Francisco, Los Angeles, Washington, D.C., and Seattle, the Chicago Police Department has conducted intelligence audits pursuant to a 1982 consent decree. It required the Chicago Police Commission to hire an independent auditor every five years. *See* Alliance to End Repression, 561 F. Supp. at 569. But since the decree was dissolved in 2009, the department has not established independent audit procedures for investigation of First Amendment conduct.
- 318 *See* YOLANDA BRANCH, OFFICE OF THE D.C. AUDITOR, AUDIT OF THE METROPOLITAN POLICE DEPARTMENT’S

- INVESTIGATIONS AND PRELIMINARY INQUIRIES INVOLVING FIRST AMENDMENT ACTIVITIES (2012), *available at* <http://dcauditor.org/sites/default/files/DCA232012.pdf>. Despite its title, this audit contains no data on the use of preliminary inquiries. This is particularly troubling for three reasons. First, the number of reported “investigations” based on reasonable suspicion between 2005 and 2011 was extremely low (27), suggesting that the police may be relying instead on “preliminary inquiries” as the preferred mechanism for information gathering. *Id.* at 13. Second, the audit found that officers had not received any training on conducting preliminary inquiries. *Id.* at 18. And third, the audit recognized that the department has no standard operating procedures for preliminary inquiries. *Id.* at 19.
- 319 PROCEDURES AND TACTICS PUBLICATION, *supra* note 128, at 15-16.
- 320 *See, e.g.*, DAVID BOERNER, POLICE INTELLIGENCE AUDITOR, REPORT OF POLICE INTELLIGENCE AUDIT PURSUANT TO SEATTLE MUNICIPAL CODE 14.12 (Feb. 22, 2011), *available at* http://clerk.seattle.gov/-CFS/CF_311543.pdf; DAVID BOERNER, POLICE INTELLIGENCE AUDITOR, REPORT OF POLICE INTELLIGENCE AUDIT PURSUANT TO SEATTLE MUNICIPAL CODE 14.12 (Aug. 22, 2011), *available at* http://clerk.seattle.gov/-CFS/CF_311750.pdf; DAVID BOERNER, POLICE INTELLIGENCE AUDITOR, REPORT OF POLICE INTELLIGENCE AUDIT PURSUANT TO SEATTLE MUNICIPAL CODE 14.12 (Jan. 10, 2012), *available at* http://clerk.seattle.gov/-public/meetingrecords/2012/pscr20120404_2a.pdf; DAVID BOERNER, POLICE INTELLIGENCE AUDITOR, REPORT OF POLICE INTELLIGENCE AUDIT PURSUANT TO SEATTLE MUNICIPAL C ODE 14.12 (Dec. 13, 2012), *available at* http://clerk.ci.seattle.wa.us/-CFS/CF_312732.pdf.
- 321 Alliance to End Repression, 561 F.Supp. at 569.
- 322 *See* FAIZA PATEL & ANDREW SULLIVAN, BRENNAN CTR. FOR JUSTICE, A PROPOSAL FOR AN NYPD INSPECTOR GENERAL 3-4 (2012), *available at* <http://www.brennancenter.org/publication/proposal-nypd-inspector-general>.
- 323 ISE ANNUAL REPORT, *supra* note 17, at 90.
- 324 **New York:** Oversight of the New York State Intelligence Center (NYSIC) rests with the NYSCI director, a captain in the New York State Police. N.Y. STATE INTELLIGENCE CTR., INFORMATION AND INTELLIGENCE PRIVACY POLICY 4 (2010), *available at* <http://www.nfcausa.org/files/DDF/NYSIC%2bPRIVACY%2bPOLICY-FINAL%2bDRAFT-10182010.pdf>. The privacy policy states that “NYSIC will conduct periodic audit and inspection of the information contained in its ISE-SAR shared space.” *Id.* at 38. The audits may be conducted by either an independent auditor or NYSIC staff. *Id.* As of March 2013, NYSIC officials had not conducted any such audit, but told the Brennan Center that they planned to do so in the future. NYSIC officials also said they hope to partner with another fusion center and conduct reciprocal audits.
- Chicago:** The regional Crime Prevention and Information Center (CPIC) in Chicago is led by a commander in the Chicago Police Department. The CPIC commander appoints a privacy officer “to assist in enforcing the provisions of [the privacy policy] and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy.” CHI. POLICE DEP’T’S CRIME PREVENTION INFO. CTR., ISE-SAR EVALUATION ENVIRONMENT INITIATIVE PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTION POLICY 2 (n.d.), *available at* <http://www.aclu-il.org/wp-content/uploads/2012/08/ACLU-letter-to-CPD-of-12-11-re-CPIC.pdf>. The privacy policy states that “CPIC will conduct periodic audit and inspection of the information contained in its ISE-SAR shared space.” However, the audits may be conducted by independent auditor or CPIC staff. *Id.* at 9. The Brennan Center is unaware of any independent audits conducted by CPIC. The Illinois State Police operate the Statewide Terrorism & Intelligence Center (STIC). The state police are responsible for “monitoring the use of all STIC data sources to guard against inappropriate or unauthorized use”; “investigat[ing] misuse of STIC data and conduct[ing] or coordinat[ing] audits concerning the proper use and security of STIC data by users.” *See* STATEWIDE TERRORISM & INTELLIGENCE CENTER, ILL. STATE POLICE, PRIVACY POLICY 22 (2010), *available at* <http://www.aclu-il.org/wp-content/uploads/2012/08/STIC-Privacy-Policy-4-10-searchable.pdf>. STIC’s privacy officer is a lieutenant with the Illinois State Police and there is no provision for independent audits. *Id.* at 20 n.21.
- Los Angeles, LA County, and San Francisco:** The California state fusion center and all regional components, including those in Los Angeles and San Francisco, all operate under a single privacy policy. CAL. STATE TERRORISM THREAT ASSESSMENT CTR., INFORMATION PRIVACY POLICY 1 (n.d.), *available at* <http://www.nfcausa.org/files/DDF/CaliforniaSTTASPrivacyPolicy1.pdf>. Each fusion center designates a “privacy official” who is responsible for “handling reported errors and violations and, in accordance with specific direction and authorization” and serves as “the focal point for ensuring that the center adheres to this policy and the provisions of the Information Sharing

Environment Privacy Guidelines.” *Id.* at 17. The privacy policy states that “STTAS Components will periodically conduct audits and inspections of the information contained in its information systems.” *Id.* at 15. However, the audits may be conducted by either “a designated representative of the agency or by a designated independent party.” *Id.* The Brennan Center is unaware of any independent audit examining the records of any fusion center in California. However, the Northern California Regional Intelligence Center told the Brennan Center that it plans to partner with another STTAS component to conduct reciprocal audits. Such reciprocal audits are a step toward independent oversight, but still miss the mark.

Philadelphia: The Delaware Valley Intelligence Center (DVIC) is a regional fusion center serving the Philadelphia area. The DVIC director appoints a privacy officer who is responsible for receiving reports and coordinating complaint resolution regarding alleged errors or violations with a privacy policy committee. DEL. VALLEY INTELLIGENCE CTR., *supra* note 128, at 4. The privacy policy requires annual audits of the information and intelligence retained by DVIC, but such audits may be conducted by either an independent party or a representative of DVIC. *Id.* at 16. The Brennan Center is unaware of any independent audit conducted by DVIC. Some reports have incorrectly indicated that the DVIC is still under construction and does not yet exist. *See, e.g.*, David Henry, *Is Philly’s Anti-Terrorism Center a Waste of Your Money*, WPVI-TV (Nov. 19, 2012), http://abclocal.go.com/wpvi/story?section=news/special_reports&cid=8891872. In reality, the center currently exists as a small office staffed 12 hours a day by one federal agent and 12 to 20 officers from the Philadelphia Police Department’s Homeland Security Unit. Jonathan Tamari, *Federal Report Cites Unfinished Philadelphia Counterterrorism Center as Flawed*, PHILA. INQUIRER, Oct. 5, 2012, available at http://articles.philly.com/2012-10-05/news/34261225_1_regional-intelligence-center-federal-money-fusion-centers. DVIC is in the process of renovating a new 40,000-square-foot facility, which has been under construction since 2006 and has cost \$2.3 million in federal funds. *Id.* The state level fusion center, known as the “Pennsylvania Criminal Intelligence Center” (PaCIC), has a designated privacy officer who is also the Analytical Intelligence Section Commander. PA. CRIMINAL INTELLIGENCE CTR., PA. STATE POLICE, PRIVACY POLICY 14 (n.d.), available at http://www.nfcausa.org/files/DDF/PennsylvaniaPaCICApprovedPrivacyPolicy02-11_3.pdf. The privacy officer also leads a Privacy Policy Committee, which is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system, among other things. *Id.* The privacy policy requires periodic audits to assess compliance with the policy and applicable law, conducted by fusion center staff under the direction of the privacy officer. *Id.* at 15. It also requires periodic audits of the “information contained in the justice information system” to be conducted by a designated independent party or a representative of the Pennsylvania State Police. *Id.* at 16. It is unclear whether such audits have ever been conducted.

Houston: The Houston Police Department operates the Houston Regional Intelligence Service Center HOUS. REG’L INTELLIGENCE SERV. CTR., PRIVACY POLICY: PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES POLICY 3 (2009), available at <http://www.nfcausa.org/files/DDF/Privacy%20Policy%20HRISC%20September%2009%20SSNP%20.pdf>; see also HOUS. POLICE DEPT., FY2012 CORE SERVICES ASSESSMENT 20-22 (2011) available at <http://www.houstontx.gov/council/11/csad/hpd-csa.pdf>. A police sergeant is responsible for overseeing compliance with the center’s privacy policy and responding to public complaints concerning privacy civil rights, and civil liberties violations. HOUS. REG’L INTELLIGENCE SERV. CTR., *supra*, at 5. And the Houston Police Department is responsible for conducting compliance audits according to departmental procedure. *Id.* at 10. The Texas Department of Public Safety operates the state’s primary fusion center, the Texas Fusion Center. The state privacy policy requires annual audits of fusion center records, but that responsibility falls to a privacy officer appointed by the general counsel for the Department of Public Safety. TX. FUSION CTR., PRIVACY, CIVIL RIGHT, AND CIVIL LIBERTIES POLICY 2, 15 (2010), available at <http://www.dps.texas.gov/docs/TxFCPrivacyPolicy113010.pdf>. The privacy officer is an attorney from the Department of Public Safety. *Id.* at 2. A 2011 state law created a “Fusion Center Policy Council” within the Texas Department of Public Safety, designed to assist the state in monitoring the activities of all fusion centers in Texas. TEX. GOV’T CODE ANN. § 421.083 (West 2013). The Council, however, is composed entirely of representatives from the fusion centers. *Id.*

Washington, D.C.: The Washington Regional Threat & Analysis Center (WRTAC) is the regional fusion center for Washington, D.C.. An executive board of directors is responsible for appointing a privacy officer whose duties include receiving reports and coordinating complaint resolution regarding alleged errors or violations of the center’s privacy policy. WASH. REGIONAL THREAT AND ANALYSIS CTR., *supra* note 128, at 2. The privacy policy requires annual audits of the information and intelligence maintained by WRTAC, and commendably, it specifies that the audit “will be conducted by a designated independent panel.” *Id.* at 19.

Miami & Miami-Dade: The director of the Southeast Florida Fusion Center (SEFFC), part of the Miami-Dade Police Department, appoints a privacy officer to assist in enforcing the privacy policy and receive reports regarding

alleged errors and violations. SE. FLA. FUSION CTR. *supra* note 128. An intelligence analyst supervisor or police sergeant at SEFFC is responsible for conducting periodic audits of the information contained in the center's ISE-SAR shared space. *Id.* at 10. With respect to the state-run Florida Fusion Center, the general counsel for the Florida state police serves as the privacy officer. FLA. FUSION CTR., *supra* note 128, at 15. Responsibility for periodic audits, however, falls to an inspector general. *Id.* at 6. The inspector general is "organizationally aligned" with the police, but must transmit all final reports to an independent auditor general. *See Office of Inspector General*, FLA. DEP'T OF LAW ENFORCEMENT, www.fdle.state.fl.us/oig/ (last visited Mar. 14, 2013); FLA. STAT. ANN. § 20.055(5)(f) (2011). The Florida Fusion Center also has a "Constitutional Protections and Privacy Advisory Board," although it is unclear whether it is active or who its members are. In theory, it "collaborates with community privacy advocacy groups" and is "comprised of three members not actively associated or employed by the [Florida Fusion Center]." FLA. FUSION CTR., *supra* note 128, at 5. It is empowered to periodically review fusion center policies for protecting civil rights and civil liberties and to make recommendations to the fusion center's Executive Advisory Board. *Id.* In addition, the Board "may be consulted" in "any independent inquiry into complaints" alleging a violation of the privacy policy and offer "recommended corrective action." *Id.* at 6.

Detroit & Dearborn: The Detroit and Southeast Michigan Information and Intelligence Center (DSEMIIC) is a component of the Detroit Police Department. In addition to the City of Detroit, it includes representatives from surrounding Macomb, Monroe, Oakland, St. Clair, Washtenaw and Wayne Counties. OAKLAND CNTY. BD. OF COMM'RS, MINUTES 116 (Feb. 16, 2012), available at https://www.oakgov.com/boc/Documents/minutes/12_min/12_02_16.pdf; *see generally* *The State of Northern Border Preparedness: A Review of Federal, State, and Local Coordination: Hearing Before the H. Comm. on Homeland Sec., Subcomm. On Emergency Preparedness, Response, & Comm'ns* (statement of Captain W. Thomas Sands, Deputy State Director, Emergency Management and Homeland Security, Michigan State Policy, Emergency Management and Homeland Security Division), available at <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Sands.pdf>. DSEMIIC is a node for the state's primary fusion center, the Michigan Intelligence Operations Center (MIOC). The MIOC privacy policy applies to all nodes, including DSEMIIC. MICH. INTELLIGENCE OPERATIONS CTR., MIOC PRIVACY POLICY 1 (2011), available at https://www.michigan.gov/documents/msp/MIOCprivacypolicy_355596_7.pdf. The fusion centers are "guided by an agency-designated privacy committee that liaises with community privacy advocacy groups to ensure that privacy and civil rights are protected. ..." *Id.* at 2-3. The fusion center director appoints a privacy officer who leads the privacy committee and handles reports regarding alleged errors and violations of the provision of the privacy policy. *Id.* at 3; *see also* DETROIT & SE. MICH. INFO. CTR., DRAFT PRIVACY POLICY 5 (n.d.), available at <http://www.nfcausa.org/files/DDF/DetroitPrivacyPolicy.pdf> (establishing an advisory board led by an appointed privacy officer). The MIOC privacy policy states that "an independent entity designated by the Director of the [Michigan State Police]" will conduct an annual audit of the information contained in MIOC's criminal intelligence system. MICH. INTELLIGENCE OPERATIONS CTR., *supra*, at 12; DETROIT & SE. MICH. INFO. CTR., *supra*, at 15 (requiring an "independent panel" to conduct annual audits). In practice, however, it is unclear if either fusion center has actually conducted such an audit.

Seattle: The Washington State Fusion Center (WSFC) has an executive board that is responsible for "ensuring that audit and oversight mechanisms are in place to ensure compliance" with the fusion center privacy policy. WASH. STATE FUSION CTR., PRIVACY POLICY 2 (2009), available at <http://www.nfcausa.org/files/DDF/WSFCPrivacyPolicy.pdf>. The executive board is comprised of fusion center participants, including: the Washington State Patrol Chief, the FBI Seattle Field Division Special Agent-In-Charge, the Seattle Police Department Chief, the King County Sheriff, the U.S. Attorney for the Western Washington District, the U.S. Attorney for the Eastern Washington District, the Washington State Homeland Security Advisor, and two representatives from the Washington Association of Sheriffs and Police Chiefs. DHS-DOJ FUSION PROCESS TECHNICAL ASSISTANCE PROGRAM & SERVS., WASHINGTON STATE FUSION CENTER AND THE PACIFIC NORTHWEST REGION: BUILDING A CRITICAL INFRASTRUCTURE / KEY RESOURCE INFORMATION SHARING CAPABILITY 1 (2009), available at <http://www.regionalresilience.org/Portals/0/reports%20and%20AARs/DHS-DOJ%20Fusion%20Center%20Background.pdf>. The executive board must "ensure that an annual audit is conducted to review compliance with WSFC information systems requirements and the WSFC Privacy Policy," although there is no public record of such audits being conducted. *See* WASH. STATE FUSION CTR., *supra*, at 6.

Portland: The Oregon Terrorism Information Threat Assessment Network is a state-level fusion center. Its designated privacy officer is an attorney for the fusion center who is appointed by the Chief Counsel of the Oregon Department of Justice Criminal Division. OR. TERRORISM INFO. THREAT ASSESSMENT NETWORK, PRIVACY POLICY 2 (2011), available at http://www.nfcausa.org/files/DDF/OR%20TITAN%20Fusion%20Center%20Privacy%20Policy_FINAL_17FEB2011.pdf. He or she "receives reports regarding alleged errors and violations of the provisions

of the policy, receives and coordinates complaint resolution under the Center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented . . ." *Id.* The privacy policy requires audits, but not independent audits. *Id.* at 18 ("The Oregon TITAN Fusion Center will adopt and follow procedures and practices to ensure and evaluate the compliance of its users and the system itself with the provisions of this Privacy Policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer or Center Director the Center."). An internal "Executive Advisory Committee" is also required to "conduct or coordinate audits and inspections of the information contained in information systems located at the Center's headquarters." *Id.* at 19. The Brennan Center was unable to locate any record of such audits.

Minneapolis & St. Paul: The Minnesota Joint Analysis Center (MNJAC) is a state-level fusion center. It has a privacy officer that is a member of the MNJAC staff as well as a Privacy Policy Committee tasked with ensuring the protection of privacy and civil rights. MINN. JOINT ANALYSIS CTR., PRIVACY POLICY 6-7 (2011), *available at* <https://dps.mn.gov/divisions/bca/bca-divisions/investigations/Documents/MNJAC%20Privacy%20Policy%20approved%20122011%20final.pdf>. An "Oversight Group," composed of representatives from each agency participating in the fusion center, is responsible for overseeing MNJAC operations and "conducting or coordinating annual and random internal or external audits, including audits by the legislative auditor, and for investigating misuse of MNJAC's information systems." *Id.* at 23. MNJAC has taken the commendable step of contracting an independent auditor to review its operations and publish audit reports online. *See, e.g.*, JOHN J. WILSON, INST. FOR INTERGOVERNMENTAL RESEARCH, DATA COMPLIANCE AUDIT REPORT FOR THE MINNESOTA JOINT ANALYSIS CENTER 1 (2010), *available at* <https://dps.mn.gov/divisions/bca/Documents/MNJAC%20Data%20Compliance%20Audit%20Report.pdf>.

- 325 U.S. GEN. ACCOUNTING OFFICE, *supra* note 256, at 10.
- 326 *See generally* DHS/DOJ FUSION PROCESS TECHNICAL ASSISTANCE PROGRAM AND SERVICES, FUSION CENTER PRIVACY POLICY DEVELOPMENT: PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES POLICY TEMPLATE 9 (2010), *available at* www.it.ojp.gov/docdownloader.aspx?ddid=1269.
- 327 *Id.* at 9, 28-29.
- 328 Internal fusion center audits are more susceptible to manipulation by individuals, especially if the audit is not independent or the results are likely to reflect negatively on a fusion center's reputation. *See* DATA PRIVACY AND INTEGRITY ADVISORY COMM., U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY RECOMMENDATIONS FOR A FEDERATED INFORMATION-SHARING SYSTEM 10 (2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/dpiacwhitepaperdhsinformationsharingpolicyconsiderations2011_draft.pdf. By contrast, a centralized, external audit process is less susceptible to manipulation, better positioned to recognize aberrations or abuses, and more effective at standardizing the interpretation of laws and policies that apply to all components. *Id.* at 11.
- 329 The following fusion centers have audit requirements: the New York State Intelligence Center; the Chicago Crime Prevention and Information Center; the Los Angeles Joint Regional Intelligence Center; the Northern California Regional Intelligence Center, the California State Terrorism Threat Assessment Center; the Washington Regional Threat & Analysis Center, the Delaware Valley Intelligence Center, the Pennsylvania Criminal Intelligence Center, the Houston Regional Intelligence Service Center; the Texas Fusion Center; the Southeast Florida Fusion Center; the Florida Fusion Center; the Detroit and Southeast Michigan Information and Intelligence Center; the Michigan Intelligence Operations Center; the Washington State Fusion Center; the Oregon Terrorism Information Threat Assessment Network; and the Minnesota Joint Analysis Center.
- 330 *Cf.* RECOMMENDATIONS FOR FUSION CENTERS, *supra* note 14, at 16 (recommending that "an independent auditor should review fusion center audit logs at least once every two years and issue a report describing data-security practices and any abuses or unauthorized access.").
- 331 *See, e.g.*, WILSON, *supra* note 324.
- 332 FLA. FUSION CTR., *supra* note 128, at 4-5.
- 333 The Northern California Regional Intelligence Center plans to partner with another fusion center in California in order to audit each other's files. While such reciprocal audits are certainly a step in the right direction, they do not replace the need for an outside, independent auditor. It is also difficult to see how this model could be replicated when fusion centers operate under different state laws.

- 334 ISE ANNUAL REPORT, *supra* note 17, at 12. According to DHS, such audits reduce the risk of inappropriate information sharing. DATA PRIVACY AND INTEGRITY ADVISORY COMM., *supra* note 328, at 11.
- 335 2012 SENATE HSGAC FUSION CENTER REPORT, *supra* note 8, at 36.
- 336 28 C.F.R. § 23.20(c) (“In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.”).
- 337 The Intelligence Reform and Protection Act of 2004, as amended, mandates that the ISE must incorporate “strong mechanisms to enhance accountability and *facilitate* oversight, including audits.” Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458 § 1016(b)(2)(I), 118 Stat. 3638 (emphasis added). And privacy guidelines issued in 2006 require agencies participating in the ISE to implement mechanisms to *enable* an adequate audit. MAJOR CRIMES DIV., *supra* note 251, at 4-5. But no federal agency has an obligation to actually *conduct* such an audit and one has never been conducted. There is also no obligation to ensure that the participating agencies have conducted their own audits. A 2012 DHS memorandum simply “presume[s]” that audits are a part of current practice before going on to weigh the pros and cons of audits performed by component agencies as opposed to a centralized function. Memorandum from Richard Purcell, Chair, U.S. Dep’t of Homeland Sec. Privacy and Integrity Advisory Comm., to Janet Napolitano, Sec., U.S. Dep’t of Homeland Sec., & Mary Ellen Callahan, Chief Privacy Officer, U.S. Dep’t of Homeland Sec. 11-12 (Jan. 31, 2012), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_report_2011_01.pdf.
- 338 OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, THE DEPARTMENT OF JUSTICE’S TERRORISM TASK FORCES iv (2005), *available at* <http://www.justice.gov/oig/reports/plus/e0507/final.pdf>.
- 339 FED. BUREAU OF INVESTIGATION, U.S. DEP’T OF JUSTICE, JOINT TERRORISM TASK FORCE: STANDARD MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION AND HOUSTON POLICE DEPARTMENT (2007) [hereinafter HOUSTON JTTF MOU] (on file with Brennan Center).
- 340 The City of Detroit responded to a Brennan Center freedom of information request by stating that it “does not possess such a record,” but only because it did not retain a copy: “Based on information provided by a DPD personnel [sic], although the DPD was required to sign the MOU, the Department did not retain a copy of the agreement.” Letter from Ellen Ha, Senior Assistant Corp. Counsel, Governmental Affairs Section, Detroit Police Dep’t, to Michael Price, Counsel, Liberty & Nat’l Sec. Program, Brennan Ctr. for Justice (Apr. 26, 2012) (on file with the Brennan Center).
- 341 Most police departments detail just a handful of officers to their local JTTF. In New York, however, the size of this contingent increased dramatically after 9/11, jumping from 17 to 130 officers. *Kelly May 18, 2004 Testimony, supra* note 54, at 4; *see also* Raymond Kelly, Comm’r, N.Y.C. Police Dep’t, Address at the Council on Foreign Relations Meeting: The Post-9/11 NYPD: Where Are We Now? (Apr. 22, 2009), *available at* www.cfr.org/homeland-security/post-911-nypd-we-now/p19198. By some accounts, this was Commissioner Kelly’s attempt to “pack” the JTTF with loyal officers who would feed information to the revamped Intelligence Division and give the NYPD greater control over Task Force operations. Comiskey, *supra* note 14, at 18; Craig Horowitz, *The NYPD’s War on Terror*, N.Y. MAG., Feb. 3, 2003, *available at* http://nymag.com/nymetro/news/features/n_8286/index1.html (“One of Kelly’s earliest moves was to pump up the number of detectives from 17 to 125, a huge commitment that the FBI matched. Kelly’s intensity and his willingness to push the envelope were demonstrated early on when he tried to muscle control of the JTTF away from the FBI.”). But it is not clear that Kelly’s plan had the intended effect. Recent reports indicate a rift between the JTTF and the Intelligence Division, with NYPD JTTF officers “in total sync” with the FBI while Intelligence Division officials are “running their own pass patterns.” E-mail to Fred Burton, V.P. of Intelligence, Stratfor Global Intelligence (Nov. 30, 2011), *available at* <http://wikileaks.org/gifiles/docs/915038-re-alpha-note-feedback-fbi-nypd-tensions-highlighted-in.html>.
- 342 *See generally* FED. BUREAU OF INVESTIGATION, U.S. DEP’T OF JUSTICE, JOINT TERRORISM TASK FORCE MEMORANDUM OF UNDERSTANDING (MOU), *available at* http://www.it.ojp.gov/fusioncenterguidelines/joint_terrorism_task_force_mou.pdf (generic JTTF MOU).
- 343 OR. REV. STAT. § 181.575 (2011) (Information Not to be Collected or Maintained). By contrast, the Attorney General Guidelines governing FBI investigations do not require a criminal predicate in order to collect information about activities protected by the First Amendment. EMILY BERMAN, *supra* note 7, at 22.

344 See, e.g., FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, JOINT TERRORISM TASK FORCE: MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION (PORTLAND) AND THE PORTLAND POLICE DEPARTMENT (2000) , available at <http://www.portlandonline.com/shared/cfm/image.cfm?id=329922> (“[I]n situations where the statutory or common law of Oregon is more restrictive than comparable Federal law, the investigative methods employed by state and local law enforcement agencies shall conform to the requirements of such Oregon statutes or common law.”); FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, JOINT TERRORISM TASK FORCE: MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION (PORTLAND) AND THE PORTLAND POLICE DEPARTMENT (2002) (same), available at <http://www.portlandonline.com/shared/cfm/image.cfm?id=329912>.

345 See AM. CIVIL LIBERTIES UNION OF OR., ACLU BACKGROUNDER: JOINING THE FBI JOINT TERRORISM TASK FORCE IS STILL A BAD IDEA 2 (2011) [hereinafter ACLU BACKGROUNDER], available at http://aclu-or.org/sites/default/files/JTTF_Backgrounder_Feb_2011_0.pdf; *City of Portland Withdraws From JTTF!*, AM. CIVIL LIBERTIES UNION OF OR. (Apr. 28, 2005), <http://aclu-or.org/content/city-portland-withdraws-jttf-2005>.

346 ACLU BACKGROUNDER, *supra* note 345, at 3.

347 *City of Portland Withdraws From JTTF!*, *supra* note 345.

348 Portland, Or., Resolution Substitute 36315 (April 26, 2005), available at <http://www.portlandonline.com/shared/cfm/image.cfm?id=329904>.

349 Portland, Or., City Council Resolution 36,859 (2011), <http://www.portlandonline.com/auditor/index.cfm?a=349687&c=54882>. The resolution enjoyed the support of all five members of the Portland City Council, including Mayor Adams, as well as the ACLU of Oregon. Press Release, Am. Civil Liberties Union of Or., Portland City Council Passes JTTF Substitute Resolution; ACLU Supports with Reservations (Apr. 28, 2011), available at <http://aclu-or.org/content/portland-city-council-passes-jttf-substitute-resolution-aclu-supports-reservations>.

350 Portland, Or., *supra* note 349.

351 *Id.*

352 *Id.*

353 *Id.* A copy of the Resolution is included with the Standard Operating Procedure used by the Criminal Intelligence Unit of the PPB when working with the JTTF. PORTLAND POLICE BUREAU, *supra* note 80, at 4-7.

354 CITY AND CNTY. OF S.F. HUMAN RIGHTS COMM'N, COMMUNITY CONCERNS OF SURVEILLANCE, RACIAL AND RELIGIOUS PROFILING OF ARAB, MIDDLE EASTER, MUSLIM, AND SOUTH ASIAN COMMUNITIES AND POTENTIAL REACTIVATION OF SFPD INTELLIGENCE GATHERING 16 (2011), available at <http://www.safesf.org/wp-content/uploads/2012/02/SF-Human-Rights-Commission-Report-Community-Concerns-of-Surveillance-Racial-and-Religious-Profilng-of-Arab-Middle-Eastern-Muslim-and-South-Asian-Communities-and-Potential-Reactivation-of-SFPD-Intelligence-Gathering1.pdf>.

355 *Id.*; SFPD DGO 8.10, *supra* note 128 at 1, 3.

356 S.F., Cal., Ordinance 120046 § 1(g) (Jan. 9, 2012) (proposed), available at <http://www.safesf.org/wp-content/uploads/2012/02/Proposed-Safe-SF-Civil-Rights-Ordinance.pdf>.

357 S.F., CAL., ADMIN. CODE § 2A.74 (2012), available at [http://www.amlegal.com/nxt/gateway.dll/California/administrative/chapter2aexecutivebranch?f=templates\\$fn=default.htm\\$3.0\\$vid=amlegal:sanfrancisco_ca\\$anc=JD_2A.74](http://www.amlegal.com/nxt/gateway.dll/California/administrative/chapter2aexecutivebranch?f=templates$fn=default.htm$3.0$vid=amlegal:sanfrancisco_ca$anc=JD_2A.74). The Board of Supervisors initially approved a much stronger version of the ordinance. See S.F., Cal., *supra* note 356. But Mayor Ed Lee vetoed the legislation. Steven T. Jones, *Lee Veto Protects the SFPD's Ability to Spy on You*, S.F. BAY GUARDIAN (Apr. 11, 2012), <http://www.sfbg.com/politics/2012/04/11/lee-veto-protects-sfpds-ability-spy-you>.

358 S.F., CAL., *supra* note 357; Steven T. Jones, *Mayor Lee Signs Watered-Down Limits on SFPD Spying*, S.F. BAY GUARDIAN (May 9, 2012, 4:56 PM), <http://www.sfbg.com/politics/2012/05/09/mayor-lee-signs-watered-down-limits-sfpd-spying>. SFPD Chief Greg Suhr presented the first public report in January 2013, but it was roundly criticized for its lack of detail. Steven T. Jones, *Activists Slam Hollow Report of SFPD-FBI Spying*, S.F. BAY GUARDIAN (Jan. 31, 2013, 4:33 PM), <http://www.sfbg.com/politics/2013/01/31/activists-slam-hollow-report-sfpd-fbi-spying>. Suhr then issued an apology for the sparse report and pledged to work with activists to develop a more detailed report. Steven T. Jones, *Suhr Apologizes for Sparse Spying Report, Pledges More Info*, S.F. BAY GUARDIAN (Feb. 1, 2013, 5:54 PM), <http://www.sfbg.com/politics/2013/02/01/suhr-apologizes-sparse-spying-report-pledges-more-info>.

- 359 In addition to Portland and San Francisco, Miami-Dade may be the only other jurisdiction in the Brennan Center survey with a policy requiring officers assigned to the local JTTF to comply with local rules. However, the Brennan Center was unable to verify this information. In response to an open records request, the Miami-Dade Police Department stated that FBI requirements prevented it from releasing a copy of its memorandum with the JTTF. At the same time, the department issued a written response stating that “MDPD Task Force Officers must not, in the course of their assignments, violate any of the policies set forth by the MDPD’s Departmental Manual.” Letter from Glen Stoltzenberg, Major, Miami-Dade Police Dep’t, to R. Kyle Alagood, Brennan Ctr. for Justice (May 24, 2012) (on file with the Brennan Center).
- 360 In Houston, a memorandum in effect since 2007 cites the FBI guidelines as a “controlling document” with only a caveat that any conflict with state or local law “will be jointly resolved.” HOUSTON JTTF MOU, *supra* note 339. This leaves Houston officers assigned to the JTTF with little practical guidance. By comparison, a previous memo from 1993 clearly stated that “personnel of the HPD shall be required to utilize only those investigative techniques consistent with their given standards and procedures.” HOUS. COUNTERTERRORISM TASK FORCE, MEMORANDUM OF UNDERSTANDING 1 (1993) (on file with the Brennan Center). It also mandated that “[t]o the extent that HPD standards and procedures impose any greater restrictions upon the use for their informants and cooperating witnesses, such personnel shall be bound by those restrictions.” *Id.* at 4-5. Police in Chicago, Philadelphia, Washington, D.C., and Minneapolis all operate under language identical to the 2007 San Francisco MOU. The St. Paul Police Department adheres to an MOU that is even less specific, although the department was in the process of negotiating a new agreement as of March 2012. The existing MOU states any “[p]roblems or difficulties which may arise” will be “mutually addressed...at the lowest possible administrative level.” MINNEAPOLIS JOINT TERRORISM TASK FORCE, MEMORANDUM OF UNDERSTANDING 1-2 (n.d.) (on file with the Brennan Center). And the Los Angeles Police Department permits officers assigned to a multi-agency task force to engage in the investigative methods authorized for the agency heading that task force, “as long as those methods do not violate current laws.” Intradepartmental Correspondence from Charlie Beck, Chief, L.A. Police Dep’t, to the Honorable Board of Police Comm’rs, Amendment to Major Crimes Division Standards and Procedures 15 (Mar. 17, 2010) (on file with the Brennan Center). Without additional guidance, there remains a risk that local officers will be unsure of which set of current laws they must follow.

STAY CONNECTED TO THE BRENNAN CENTER

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

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

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

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

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

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

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

What the Government Does with Americans' Data
Rachel Levinson-Waldman

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

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

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

Reforming Funding to Reduce Mass Incarceration
Inimai Chettiar, Lauren-Brooke Eisen, and Nicole Fortier

Early Voting: What Works
Diana Kasdan

Federal Judicial Vacancies: The Trial Courts
Alicia Bannon

The Case for Voter Registration Modernization
Brennan Center for Justice

How to Fix Long Lines
Lawrence Norden

For more information, please visit www.brennancenter.org.

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

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

[Share / Email](#)

Fusion Center Locations and Contact Information

[State and major urban area fusion centers \(/state-and-major-urban-area-fusion-centers\)](#) (fusion centers) are owned and operated by state and local entities, and are designated by the governor of their state.

In accordance with the [Federal Resource Allocation Criteria \(RAC\) policy](#) (http://www.ise.gov/sites/default/files/RAC_final.pdf) (PDF, 144 KB, 4 pages), which defines objective criteria and a coordinated approach for prioritizing federal resource allocation to fusion centers, the federal government recognizes these designations and has a shared responsibility with state and local governments to support the national network of fusion centers.

There are two types of fusion centers:

- **Primary Fusion Centers:** A primary fusion center typically provides information sharing and analysis for an entire state. These centers are the highest priority for the allocation of available federal

resources, including the deployment of personnel and connectivity with federal data systems.

- **Recognized Fusion Centers:** A recognized fusion center typically provides information sharing and analysis for a major urban area. As the Federal Government respects the authority of state governments to designate fusion centers, any designated fusion center not designated as a primary fusion center is referred to as a recognized fusion center.

[Collapse All Sections \(#\)](#)

Alabama (#)

- [Alabama Fusion Center](http://fusion.alabama.gov/) (<http://fusion.alabama.gov/>) (Primary) – 334-517-2660

Alaska (#)

- Alaska Information and Analysis Center (Primary) – 907-269-8900 / 855-692-5425

Arizona (#)

- [Arizona Counter Terrorism Information Center](http://www.azactic.gov/) (<http://www.azactic.gov/>) (Primary) – 602-644-5805 / 877-272-8329

Arkansas (#)

- Arkansas State Fusion Center (Primary) – 501-618-8001/866-787-2332

California (#)

- California State Threat Assessment Center
(/redirect?url=http%3A%2F%2Fwww.calstas.org%2F)
(Primary) – 916-636-2900
- Central California Intelligence Center; Sacramento, CA
(/redirect?url=http%3A%2F%2Fwww.sacrtac.org%2F)
(Recognized) – 916-808-8383 / 888-884-8383
- Los Angeles Joint Regional Intelligence Center; Los Angeles, CA
(/redirect?url=http%3A%2F%2Fwww.jric.org%2F).(Recognized) – 562-345-1100
- Northern California Regional Intelligence Center; San Francisco, CA
(/redirect?url=http%3A%2F%2Fwww.ncric.org%2F).(Recognized) – 866-367-8847
- Orange County Intelligence Assessment Center; Orange County, CA
(/redirect?url=http%3A%2F%2Fwww.ociac.org%2F).(Recognized) – 714-289-3949
- San Diego Law Enforcement Coordination Center
(/redirect?url=https%3A%2F%2Fsd-lecc.org%2F); San Diego, CA (Recognized) – 858-495-7200

Colorado (#)

- Colorado Information Analysis Center
(/redirect?url=http%3A%2F%2Fcoloradoiaa.com%2F)

[url=http%3A%2F%2Fdhsem.state.co.us%2Fhome](http://www.fdhsem.state.co.us) (Primary)
– 877-509-2422

Connecticut (#)

- [Connecticut Intelligence Center](#)
(<http://www.ct.gov/demhs>) (Primary) – 860-706-5500

Delaware (#)

- [Delaware Information and Analysis Center](#)
(</redirect?url=http%3A%2F%2Fwww.dediac.org%2F>)
(Primary) – 302-739-5996

District of Columbia (#)

- [Washington Regional Threat Analysis Center](#)
(Primary) – 202-481-3075

Florida (#)

- [Florida Fusion Center](#) (</redirect?url=http%3A%2F%2Fwww.fdle.state.fl.us%2F>) (Primary) – 850-410-7060
- [Central Florida Intelligence Exchange; Orlando, FL](#)
(</redirect?url=http%3A%2F%2Fwww.ocso.com%2Fcfix%2F>)
(Recognized) – 407-858-3950
- [Southeast Florida Fusion Center; Miami, FL](#)
(<http://www.miamidade.gov/police/contacts-homeland.asp>)

(Recognized) – 305-470-3880

Georgia (#)

- Georgia Information Sharing and Analysis Center
(<http://investigative.gbi.georgia.gov/georgia-information-sharing-analysis-center>) (Primary) – 404-486-6420

Guam (#)

- Mariana Regional Fusion Center (Primary) – 671-478-0281

Hawaii (#)

- Hawaii Fusion Center (Primary) – 808-356-4467

Idaho (#)

- Idaho Criminal Intelligence Center
(<http://www.isp.idaho.gov/icic/>) (Primary) – 208-846-7676

Illinois (#)

- Illinois Statewide Terrorism and Intelligence Center (Primary) – 877-455-7842
- Chicago Crime Prevention and Information Center; Chicago, IL (Recognized) – 312-745-5669

Indiana (#)

- Indiana Intelligence Fusion Center
(<http://www.in.gov/iifc>) (Primary) – 800-400-4432

Iowa (#)

- Iowa Division of Intelligence and Fusion Center
([/redirect?url=http%3A%2F%2Fwww.dps.state.ia.us%2Fintell%2Ffusion.shtml](#))
(Primary) – 800-308-5983

Kansas (#)

- Kansas Intelligence Fusion Center (Primary) –
785-274-1805

Kentucky (#)

- Kentucky Intelligence Fusion Center
(<http://www.homelandsecurity.ky.gov/>) (Primary) – 502-564-
2081

Louisiana (#)

- Louisiana State Analytical & Fusion Exchange
([/redirect?url=http%3A%2F%2Fwww.la-safe.org%2F](#))
(Primary) – 225-925-4192 / 800-434-8007

Maine (#)

- Maine Information and Analysis Center
(<http://www.maine.gov/miac/>) (Primary) – 207-624-7280 / 877-786-3636

Maryland (#)

- Maryland Coordination and Analysis Center
(<http://www.mcac.maryland.gov/>) (Primary) – 800-492-8477

Massachusetts (#)

- Massachusetts Commonwealth Fusion Center
(<http://www.mass.gov/eopss/home-sec-emerg-resp/fusion-center/>) (Primary) – 978-451-3700 / 888-872-5458
- Boston Regional Intelligence Center; Boston, MA
(</redirect?url=http%3A%2F%2Fbpdnews.com%2Fbia>)
(Recognized) – 617-343-4328

Michigan (#)

- Michigan Intelligence Operations Center
(<http://www.michigan.gov/mioc/>) (Primary) – 517-241-8000 / 877-616-4677
- Detroit and Southeast Michigan Information and Intelligence Center; Detroit, MI (Recognized) – 313-967-4600

Minnesota (#)

- Minnesota Fusion Center ([/redirect?url=http%3A%2F%2Fwww.icefishx.org%2F](#)) (Primary) – 651-793-3730 / 800-422-0798

Mississippi (#)

- Mississippi Analysis and Information Center (<http://www.homelandsecurity.ms.gov/Pages/MSAIC.aspx>) (Primary) – 601-933-7200 / 888-4SAFE-MS

Missouri (#)

- Missouri Information Analysis Center ([/redirect?url=http%3A%2F%2Fwww.miacx.org%2F](#)) (Primary) – 866-362-6422
- Kansas City Regional Terrorism Early Warning Interagency Analysis Center; Kansas City, MO ([/redirect?url=http%3A%2F%2Fwww.kctew.org%2F](#)) (Recognized) – 816-413-3588 / 816-474-TIPS
- St. Louis Fusion Center; St. Louis, MO ([/redirect?url=http%3A%2F%2Fwww.sltew.org%2F](#)) (Recognized) – 314-615-4839

Montana (#)

- Montana Analysis & Technical Information Center

[\(https://dojmt.gov/enforcement/investigations-bureau/\)](https://dojmt.gov/enforcement/investigations-bureau/)

(Primary) – 406-444-1330

Nebraska (#)

- Nebraska Information Analysis Center

[\(/https://statepatrol.nebraska.gov/vnews/display.v/SEC/Divisions%7C](https://statepatrol.nebraska.gov/vnews/display.v/SEC/Divisions%7C)

(Primary) – 402-479-4049

Nevada (#)

- Southern Nevada Counter-Terrorism Center

[\(/redirect?url=http%3A%2F%2Fwww.snctc.org%2F\)_]((/redirect?url=http%3A%2F%2Fwww.snctc.org%2F)_) (Primary)

– 702-828-2200

- Nevada Threat Analysis Center; Carson City

[\(/redirect?url=http%3A%2F%2Fwww.ntacnv.org%2F\)_]((/redirect?url=http%3A%2F%2Fwww.ntacnv.org%2F)_), NV

(Recognized) – 775-687-0450

New Hampshire (#)

- New Hampshire Information and Analysis Center

[\(/http://www.nh.gov/safety/information-analysis-center\)](http://www.nh.gov/safety/information-analysis-center)

(Primary) – 603-223-3859

New Jersey (#)

- New Jersey Regional Operations Intelligence Center (Primary) – 609-963-690

New Mexico (#)

- New Mexico All Source Intelligence Center
([/redirect?url=http%3A%2F%2Fwww.nmdhsem.org%2F](http://redirect?url=http%3A%2F%2Fwww.nmdhsem.org%2F))
(Primary) – 505-476-9600

New York (#)

- New York State Intelligence Center (Primary) –
866-723-3697

North Carolina (#)

- North Carolina Information Sharing and Analysis Center (<https://www2.ncdps.gov/Index2.cfm?a=000003,002965,003125>) (Primary) – 919-716-1111 / 888-624-7222

North Dakota (#)

- North Dakota State and Local Intelligence Center
(<http://www.nd.gov/des/homeland/fusion-center/>) (Primary) –
701-328-8172 / 866-885-8295

Ohio (#)

- Ohio Strategic Analysis and Information Center
(<http://www.homelandsecurity.ohio.gov/index.stm>) (Primary) –

614-799-3555 / 877-647-4683

- Greater Cincinnati Fusion Center; Cincinnati, OH

([/redirect?url=http%3A%2F%2Fwww.gcfc.org%2F](#))

(Recognized) – 513-263-8000

- Northeast Ohio Regional Fusion Center;

Cleveland, OH ([/redirect?](#)

[url=http%3A%2F%2Fwww.neorfc.us%2F](#)) (Recognized) –

216-515-8477 / 877-515-8477

Oklahoma (#)

- Oklahoma Information Fusion Center

(<https://www.ok.gov/okfusion/>) (Primary) – 405-842-8547

Oregon (#)

- Oregon Terrorism Information Threat Assessment

Network ([/redirect?url=https%3A%2F%2Fortitan.org%2F](#))

(Primary) – 503-378-6347 / 877-620-4700

Pennsylvania (#)

- Pennsylvania Criminal Intelligence Center

(<http://www.psp.pa.gov/>) (Primary) – 877-777-6835

- Delaware Valley Intelligence Center; Philadelphia,

PA ([/redirect?url=https%3A%2F%2Fwww.dvicphila.org%2F](#))

(Recognized) – 267-322-4131

- Southwestern PA Region 13 Fusion Center

([/redirect?url=http%3A%2F%2Fwww.pa-](#)

region13.org%2Ffusioncenter.asp); Pittsburgh, PA
(Recognized) – 412-473-2550

Puerto Rico (#)

- National Security State Information Center
(Primary) – 787-399-0833

Rhode Island (#)

- Rhode Island State Fusion Center
(<http://www.fusioncenter.ri.gov/>) (Primary) – 401-444-1117

South Carolina (#)

- South Carolina Information and Intelligence Center
([/redirect?url=http%3A%2F%2Fwww.sciic.org%2F](http://redirect?url=http%3A%2F%2Fwww.sciic.org%2F)) (Primary)
– 803-896-7133 / 866-472-8477

South Dakota (#)

- South Dakota Fusion Center
(https://dps.sd.gov/homeland_security/fusion_center.aspx)
(Primary) – 605-367-5940

Tennessee (#)

- Tennessee Fusion Center

(<https://www.tn.gov/tbi/topic/tennessee-fusion-center>)

(Primary) – 877-250-2333

Texas (#)

- Texas Joint Crime Information Center ([/redirect?url=https%3A%2F%2Fwww.txdps.state.tx.us%2FIntelligenceCounter](#))
(Primary) – 512-424-7981 / 866-786-5972
- Austin Regional Intelligence Center; Austin, TX
([/redirect?url=https%3A%2F%2Farictexas.org%2F](#))
(Recognized) – 512-974-2742
- Dallas Fusion Center; Dallas, TX ([/redirect?url=http%3A%2F%2Fwww.dallaspolice.net%2Fabouts%2FfusionCer](#))
(Recognized) – 214-671-3482
- El Paso Multi-Agency Tactical Response Information eXchange (MATRIX); El Paso, TX (Recognized) – 915-680-6500
- Houston Regional Intelligence Service Center; Houston, TX (Recognized) – 713-884-4710
- North Central Texas Fusion Center; McKinney, TX
(http://www.collincountytx.gov/homeland_security/fusion_center/Pag)
(Recognized) – 972-548-5537
- Southwest Texas Fusion Center
(<http://www.sanantonio.gov/SouthwestTexasFusionCenter.aspx>)
; San Antonio, TX (Recognized) – 210-207-7680

U.S. Virgin Islands (#)

- U.S. Virgin Islands Fusion Center (Primary) – 340-776-3013

Utah (#)

- Utah Statewide Information and Analysis Center
(<http://siac.utah.gov/>) (Primary) – 801-256-2360

Vermont (#)

- Vermont Intelligence Center
(<http://vsp.vermont.gov/criminal/vic/>) (Primary) – 802-872-6110

Virginia (#)

- Virginia Fusion Center ([/redirect?url=http%3A%2F%2Fwww.vsp.state.va.us%2FFusionCenter%2F](#))
(Primary) – 804-674-2196
- Northern Virginia Regional Intelligence Center;
Fairfax, VA (Recognized) – 703-212-4590

Washington (#)

- Washington State Fusion Center
(<http://www.wsfc.wa.gov/>) (Primary) – 877-843-9522

West Virginia (#)

- West Virginia Intelligence Fusion Center
(<http://www.fusioncenter.wv.gov/>) (Primary) – 304-558-

4831 / 866-989-2824

Wisconsin (#)

- Wisconsin Statewide Information Center
(<http://milwaukee.gov/wiwatch/wsic>) (Primary) – 608-242-5393
- Southeastern Wisconsin Threat Analysis Center; Milwaukee, WI (/redirect?url=[http%3A%2F%2Fwww.wiwatch.org%2F](http://www.wiwatch.org)) (Recognized) – 414-935-7741

Last Published Date: June 10, 2016

Was this page helpful?

Yes No

Submit

NYPD's Muslim surveillance violated regulations as recently as 2015: report

NYPD inspector general finds investigators consistently failed to get proper authorization for surveillance, and that 95% of reviewed cases targeted Muslims

Mazin Sidahmed

Wednesday 24 August 2016 08.47 EDT

The New York City police department has violated several regulations in its surveillance of predominantly Muslim communities as recently as 2015, a report released on Thursday found.

The 67-page report was completed by the NYPD's inspector general, and examined the police department's intelligence unit.

ADVERTISING

The report found that, when examining political groups, investigators consistently failed to get

proper authorization or timely extensions for investigations or the use of informants and undercover cops.

“This investigation demonstrates a failure by NYPD to follow rules governing the timing and authorizations of surveillance of political activity,” said Mark G Peters, commissioner of the department of investigations (DOI), a city-wide watchdog. NYPD’s inspector general office is a part of the DOI and was only created two years ago following a law passed in the city council.

NYPD’s guidelines for investigating are dictated by the Handschu agreement, established 32 years ago following a class-action lawsuit filed by several political organizations that accused the NYPD of unconstitutional surveillance.

“The Guidelines were designed to establish certain baseline controls on NYPD’s considerable investigative power,” the report explained.

The office of the inspector general examined investigations that were closed between 2011 and 2015, some of which started as early as 2004.

The number of reports the inspector general examined was redacted but in a footnote on the first page, the authors note that more than 95% of the individuals under investigation were Muslim and/or engaged in activity associated with Islam.

“I am deeply disturbed to learn that 95% of the sample investigative statements reviewed by the IG were Muslims or entities associated with Islam,” said Linda Sarsour, executive director of the Arab American Association of New York. “Is this a confirmation of a Muslim surveillance program?”

The findings troubled many activists in New York’s Muslim community due to the NYPD’s tumultuous history with Muslim American New Yorkers. In 2011, the department was revealed to have unconstitutionally infiltrated Muslim student groups, mosques, religious bookstores, hookah bars and other predominantly Muslim areas to spy on people.

The demographics unit, which was responsible for the program, was dismantled in 2014.

The original surveillance program sparked a series of lawsuits, one of which concluded earlier this year. In the settlement of the case of Raza v The City of New York - which is still subject to court approval - the NYPD agreed to several reforms including: requiring facts before an investigation is launched, limiting the use of informants and undercovers, and prohibiting investigations in which race, religion or ethnicity is a substantial motivating factor.

Naz Ahmad, a staff attorney for Creating Law Enforcement Accountability & Responsibility (Clear) Project, which represented the plaintiffs in the case, welcomed the inspector general’s findings.

“We welcome the inspector general’s report confirming what our clients have long known: that

the NYPD's surveillance of American Muslims operated without oversight and often in violation of the rules," Ahmad said.

The use of informants and undercover police, known as human sources, came under scrutiny in the report. Of the requests for human sources reviewed, none contained any details about the anticipated role of that source. It also criticized the use of "boilerplate" language when providing reasons for extending the use of informants.

Preliminary inquiries, which allow the police to gather information even when no law has been broken, were allowed to continue indefinitely, and 100% of the extensions reviewed by the office of the inspector general contained no reason for the extension.

The report found the NYPD's intelligence unit would also routinely continue investigations even after legal authority had expired, which amounted to months of time over the course of investigations.

The NYPD did not have any qualms with the findings of the report.

"I am very pleased the inspector general's audit has independently confirmed this to be true, and I thank the IG's office for its work on this audit and report," said outgoing police commissioner William J Bratton.

Fahd Ahmed, the executive director of Desis Rising Up & Moving (Drum), said the report confirms their suspicions and evidence. Drum conducted a survey of the Muslim community between 2011 and 2015 and found that surveillance by the NYPD was ongoing.

"They might as well rename it the Muslim Investigations Department," Ahmed said.

More news

Topics

NYPD New York Islam Surveillance US policing

Save for later Article saved

Reuse this content