ELECTRONIC FRONTIER FOUNDATION

Re: Notice-PCLOB-2014-04 Docket No. 2014-0001

Comments of the Electronic Frontier Foundation on Suspicious Activity Reports and the Privacy and Civil Liberties Oversight Board's Mid-and Long-Term agenda

Dear Members of the Privacy and Civil Liberties Oversight Board,

The Privacy and Civil Liberties Oversight Board (PCLOB) has indicated that its mid and long-term agenda will include an evaluation of "the functional standards used by state and local law enforcement agencies to report suspicious activity to fusion centers and the Intelligence Community."

EFF is pleased to see the PCLOB taking up the issue of suspicious activity reports, and urges the PCLOB to conduct a thorough examination not only of the standards that govern SAR and the way in which these standards have been applied, but also what safeguards are or should be in place for assuring every agency that participates in SAR is accountable for privacy and civil liberties violations. The latter requires a thorough examination of the flow of data in fusion centers, what laws and regulations apply to each agency participating in fusion centers, and what remedies for violations of privacy and civil liberties (if any) are and should be available. Finally, the PCLOB should use this chance to make more information about fusion centers public, since lack of transparency continues to be a problem.

Suspicious activity reporting (SAR) is defined in the functional standards for Information Sharing Environment as "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."[1] The National Suspicious Activity Reporting Initiative (NSI), conceived in 2008 and rolled out to fusion centers as early as 2010, was meant to standardize the information coming from fusion centers.

Unfortunately, these standards are deeply flawed. They include 16 different criteria that are supposed to be applied to a SAR to determine whether it indicates "pre-operational planning." These standards include the following criteria:

- Photography: "Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person."

- Recruiting: "Building of operations teams and contacts, personnel data, banking data or travel data."

- Observation/surveillance: "Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc."

- Acquisition of Expertise: "Attempts to obtain or conduct training in security concepts; military

1 "Information Sharing Environment, Functional Standards, Suspicious Activity Reporting, Version 1.5", *available at* http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf

weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person."

These criteria are ripe for abuse of discretion. The behaviors listed can take place during completely innocent activity. Furthermore, the standard "arouse suspicion in a reasonable person" is vague, as is "unusual interest." The definition for what constitutes an appropriate SAR does not comport with the constitutionally mandated reasonable suspicion standard for brief police contacts.[2] While a SAR may be less invasive than a stop-and-frisk, it may also have greater ultimate consequences since it can end up in a database, with no knowledge of the individuals involved and no way to purge the data. How this data is used also remains unclear.

Although the SAR guidance contains a footnote that many of the activities used to determine whether "pre-operational planning" is taking place "are generally First Amendment-protected," and notes that race and religion should not be factored in, there is no guidance on how to address privacy and constitutional violations if they may occur.

In fact, SAR standards have been used in a way that has resulted in racial and religious profiling, regardless of the minimal disclaimers in the functional standards that they should not be.[3]

A review of SARs collected through Public Records Act requests in Los Angeles showed that 78% of SARs were filed on non-whites.[4] An audit by the Los Angeles Police Department's Inspector General puts that number at 74%, still a shockingly high number.[5]

Similarly, SARs obtained by the ACLU of Northern California show that most of the reports demonstrate bias, and are based on conjecture rather than articulable suspicion of criminal activity. Some of the particularly concerning SARs include titles like "Suspicious ME [Middle Eastern] Males Buy Several Large Pallets of Water" and "Suspicious photography of Folsom Dam by Chinese Nationals." The latter SAR resulted in police contact: "Sac[ramento] County Sheriff's Deputy contacted 3 adult Asian males who were taking photos of Folsom Dam. They were evasive when the deputy asked them for identification and said their passports were in their vehicle." Both of these SARs were entered into FBI's eGuardian database.[6]

The bidirectional flow of data in fusion centers, as well as interagency cooperation and jurisdictional

---

2 The Supreme Court in *Terry v. Ohio*, 392 U.S. 1 (1968) explained that a limited police stop and search based on less than probable cause is permissible under the Fourth Amendment only when an officer has "specific and articulable facts" that criminal activity is occurring. That must be based on "some minimal level of objective justification" rather than an "unparticularized suspicion or 'hunch.'" *United States v. Sokolow*, 490 U.S. 1, 7 (1989) (quotations and citations omitted). Much of the behavior that constitutes a potential SAR invites precisely the sort of reporting based on "hunches" that the Fourth Amendment forbids.

3 *Supra* note 1 at 7, 29.

4 StopLAPD Spying, "A People's Audit of the Los Angeles Police Department's Special Order 1," April 2, 2013, *available at* http://stoplapdspying.org/wp-content/uploads/2013/04/PEOPLES-AUDIT-UPDATED-APRIL-2-2013-A.pdf.

5 Inspector General, Los Angeles Police Commission, "Suspicious Activity Report Audit," March 12, 2013, *available at* http://www.lapdpolicecom.lacity.org/031913/BPC_13-0097.pdf.

6 ACLU of Northern California, "Selected Suspicious Activity Reports from the Central California Intelligence Center and Joint Regional Intelligence Center," *available at* https://www.aclunc.org/sites/default/files/asset_upload_file470_12586.pdf.

blurriness, makes accountability and a clear understanding of the applicability of laws and regulations difficult. As scholars Priscilla M. Regan and Torin Monahan pointed out in a recent comprehensive empirical study of fusion centers across the country:

> [F]usion centers operate across a variety of jurisdictional boundaries, which often exist in different regulatory and legal environments. It is generally challenging to design and manage accountability in such multijurisdictional and multipurpose settings. A lack of clarity about the organizational position, and hence the accountability, of fusion centers is not surprising when one considers the fact that, as Rollins pointed out in a Congressional Research Service (CRS) report, "fusion centers are not federal entities and, therefore, have no federal statutory basis."[7]

In the midst of this ambiguous and opaque environment, fusion centers have access to a staggering amount of data including the FBI's eGuardian database and a variety of other federal databases.[8] They may even potentially have access to unminimized NSA data.[9] And as data gathered under the problematic SAR standards is entered into these databases, the lines of responsibility for unconstitutional invasions of privacy and civil liberties become ever more unclear.

For example, even compliance with the minimal standards for intelligence gathering found in 28 C.F.R. § 23.20 appears to be voluntary, since the regulation applies only to a very small number of "criminal intelligence systems" funded by a 1968 law.[10] The applicability of state and local standards such as state constitutions or municipal ordinances, is also unclear.[11] Since some facilities work directly with Joint Terrorism Task forces in their area, any local prohibitions on data sharing/intelligence gathering may be jeopardized as well.

There is also evidence of fusion centers being used to disseminate reports that aid repressive police activity and chill freedom of association. A series of public records act requests in Massachusetts shows: "Officers monitor demonstrations, track the beliefs and internal dynamics of activist groups, and document this information with misleading criminal labels in searchable and possibly widely-shared electronic reports."[12] The documents included intelligence reports addressing issues such

---

7 Priscilla Regan and Torin Monahan, "Fusion Center Accountability and Intergovernmental Information Sharing," 2014, *available at* http://torinmonahan.com/papers/FC-Regan_Monahan_Publius.pdf (*citing* Rollins, *infra* note 8).

8 John Rollins, "Fusion Centers: Issues and Options for Congress," CONGRESSIONAL RESEARCH SERVICE, January 18, 2008, *available at* https://www.fas.org/sgp/crs/intel/RL34070.pdf.

9 Laura Poitras & Charlie Savage, "How a Court Secretly Evolved, Extending U.S. Spies' Reach," THE NEW YORK TIMES, March 11, 2014, http://www.nytimes.com/2014/03/12/us/how-a-courts-secret-evolution-extended-spies-reach.html?_r=1.

10 "28 CFR Part 23 applies to any state or local law enforcement agency that operates a criminal intelligence system supported by funding from the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Consequently, 28 CFR Part 23 applies to a very small number of criminal intelligence systems…The vast majority of agencies complying with 28 CFR Part 23 have voluntarily adopted the regulation." Institute for Intergovernmental Research "Frequently Asked Questions," 2014, Criminal Intelligence Systems Operating Policies (28 CFR Part 23), (visited Aug. 27, 2014), https://www.iir.com/28CFR_Program/28CFR_FAQ.

11 For example, the California constitution has a right to privacy in Article 1, section 1. Various cities in California have regulations regarding intelligence gathering, such as San Francisco Police Department's Department General Order 8.10, "Guidelines for First Amendment Activities," *available at* www.sf-police.org/modules/ShowDocument.aspx?documentid=24722.

12 ACLU of Massachusetts and National Lawyers Build, Massachusetts Chapter, "Policing Dissent: Police Surveillance of Lawful Political Activity in Boston," October 2012, *available at* http://www.aclum.org/sites/all/files/policing_dissent_101812.pdf.

internal group discussions and protest planning, and showed evidence of police contact.

All of these issues lead to what the October 2012 U.S. Senate Permanent Subcommittee on Investigations called "'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."[13]

Without even the justification of serving their primary purpose of aiding national security, fusion centers and SAR are superfluous. PCLOB should do a holistic, thorough examination of SAR and the fusion center architecture that they feed into.

Respectfully Submitted,

Nadia Kayyali
Activist
nadia@eff.org
415.436.9333 ext 104

13 "Federal Support for and Involvement in State and Local Fusion Centers," UNITED STATES SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, October 3, 2012, *available at* http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04.