SUSPICIOUS TO WHOM? REFORMING THE SUSPICIOUS ACTIVITY REPORTING PROGRAM TO BETTER PROTECT PRIVACY AND PREVENT DISCRIMINATION

NICOLAS DUQUE FRANCO[∞]

[∞] Nicolas is a graduate of the University of Chicago and New York University (NYU) School of Law. He recently completed a fellowship with the Center for Appellate Litigation, where he advocated on behalf of indigent clients appealing criminal convictions. He will be clerking in the Southern District of California during the 2019 to 2020 term. He is grateful to the thoughtful editors of the Review of Law and Social Change and extends special thanks to Professor Stephen J. Schulhofer at NYU School of Law for his invaluable guidance.

ABBREVIATIONS

ACLU American Civil Liberties Union
ATS American Terrorism Study
CIA Central Intelligence Agency
DHS Department of Homeland Security
DOJ Department of Justice
FBI Federal Bureau of Investigation
FIPP Fair Information Practice Principles
FOIA Freedom of Information Act
FS Functional Standard
ISE Information Sharing Environment
IRTPA Intelligence Reform and Terrorism Prevention Act of 2004
JTTF Joint Terrorism Task Force
LAPD Los Angeles Police Department
MTA Metropolitan Transportation Authority
NNFC National Network of Fusion Centers
NPSP The National Public Safety Partnership
NPYD New York Police Department
NPR National Public Radio
NSA National Security Agency
NSIDR Nationwide SAR Initiative Data Repository
PII Personally Identifiable Information
P/CRCL Privacy, Civil Rights and Civil Liberties
PM-ISE Program Manager of the Information Sharing Environment
SAR Suspicious Activity Report
SSLT State, Local, Tribal, and Territorial
START Study of Terrorism and Response to Terrorism
TSCFBI's Terrorism Screening Center

INTRODUCTION

> "The threat from terrorism is real, but we will overcome it….Our success won't depend on tough talk, or abandoning our values, or giving into fear. That's what groups like ISIL are hoping for. Instead, we will prevail by being strong and smart, resilient and relentless, and by drawing upon every aspect of American power."[1]

When President Barack Obama spoke these words in 2015, the United States' primary conduit for sharing anti-terrorism information within the law enforcement and intelligence community—the National Network of Fusion Centers ("NNFC")—was already nearly ten years old.[2] The NNFC had been created to connect law enforcement agencies nationwide and to help them share information that would allow them to combat terrorism in the post-9/11 world. By 2015, the collection and dissemination of reports intended to document terror-related incidents and observations, also known as Suspicious Activity Reports ("SARs"), had become critical to this nationwide strategy.

Some say the NNFC has proven itself capable of linking agencies as intended. For example, by 2015, the NNFC already helped connect police agencies nationwide to thwart a domestic terrorist in Minnesota,[3] identify a bombing suspect in Colorado,[4] and convict an individual that was believed to have been planning a "Virginia Tech style" attack in Illinois.[5] Yet, despite these successes, the NNFC remains largely invisible to the American public. Where the NNFC has received attention, it has often been for scandals related to alleged violations of civil liberties, some of which have even resulted in litigation over the collection

---

1. President Barack Obama, Address on National Security at Oval Office of the White House (Dec. 6, 2015), https://www.reuters.com/article/us-california-shooting-obama-address-tex/full-text-of-obama-speech-on-national-security-threat-of-terrorism-idUSKBN0TQ09A20151207 [https://perma.cc/9ZVE-P699].

2. The Network is made up of 78 fusion centers which are dispersed across U.S. states, territories, and major urban areas. Fusion centers are offices dedicated to receiving, analyzing, assessing, and sharing threat-related information across the national law enforcement ecosystem. In 2016, the NNFC operated a budget of $322.15M and was funded by "[f]ederal (both through grants and direct contributions), SLTT and private sector sources." *See* DEP'T. OF HOMELAND SEC., 2016 NATIONAL NETWORK OF FUSION CENTERS: FINAL REPORT 5, 11 (2017) [hereinafter NNFC 2016 REPORT], https://www.dhs.gov/sites/default/files/publications/2016_National_Network_of_Fusion_Centers_Final_Report.pdf [https://perma.cc/Y62A-L2X3].

3. *2013 Fusion Center Success Stories*, DEP'T. OF HOMELAND SEC., https://www.dhs.gov/2013-fusion-center-success-stories [https://perma.cc/HX7J-WR5V] (last visited Jan. 20, 2019).

4. *2011 Fusion Center Success Stories*, DEP'T. OF HOMELAND SEC., https:// www.dhs.gov/2011-fusion-center-success-stories [https://perma.cc/G76A-PV22] (last visited Jan. 20, 2019).

5. *2007-2009 Fusion Center Success Stories*, DEP'T. OF HOMELAND SEC., https://www.dhs.gov/2007-2009-fusion-center-success-stories [https:// perma.cc/4G33-MWCZ] (last visited Jan. 20, 2019).

of information on innocent Americans.[6] In 2012, the U.S. Senate Permanent Subcommittee on Investigations described the program as a "pool[] of ineptitude."[7] Today, the same fundamental problems that have plagued the NNFC and the SAR Program remain, including the white noise caused by an overabundance of reports, the ambiguity of its rules for enforcement, its over-surveillance of racial and religious minorities, and the potential for privacy harms against any report's target.

For as long as the SAR program has existed, it has been criticized by lawyers, academics, and social scientists. Some critiques stem from civil liberties groups external to the government, while other critiques arise from within the law enforcement community itself. This Article takes up those critiques and builds on them to suggest workable solutions that will benefit both law enforcement and the American public. Importantly, this Article does not address whether the SAR Program should exist in the first place. Rather, after examining SAR's origins and touching lightly on the important functions it serves, this Article focuses instead on how the SAR Program can be improved to better protect people's privacy and prevent discrimination.

The Article proceeds in four parts. Part I explains how the SAR Program arose in the wake of the September 11, 2001 attacks as a solution to a critical flaw in American law enforcement—an inability to share information effectively. Part II describes how the SAR Program functions. This Section analyzes the Functional Standard—the policy framework which undergirds the SAR Program—and reviews how SARs are collected, analyzed, and disseminated. Part III examines the SAR Program's major criticisms. The Section questions whether the SAR Program meaningfully prevents terrorism, whether its analysts can cope effectively with the "white noise" created by overbroad collection, and whether its reports are, in fact, reliable. This Section also touches on the discriminatory impact of the current SAR Program, including its effects on racial and religious minorities as well as how it can deter free expression. Lastly, Part IV provides various avenues for reform. This Section first examines potential constitutional challenges to the current system. Then, the Section examines various policy recommendations the NNFC could implement, including changing the standards for publishing reports, adopting a heightened review for reports with sensitive information, and implementing a process for notifying targets and providing them with the opportunity to challenge reports pertaining to them. It is my hope that this analysis will help provide insight into how this secretive, but

6. *Gill v. DOJ – Challenge to Government's Suspicious Activity Reporting Program*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/cases/gill-v-doj-challenge-governments-suspicious-activity-reporting-program [https://perma.cc/JWW4-QD94] (last visited Jan. 20, 2019).

7. *See* Robert O'Harrow Jr., *DHS 'Fusion Centers' Portrayed as Pools of Ineptitude and Civil Liberties Intrusions*, WASH. POST (Oct. 2, 2012), https://www.washingtonpost.com/investigations/dhs-fusion-centers-portrayed-as-pools-of-ineptitude-and-civil-liberties-intrusions/2012/10/02/10014440-0cb1-11e2-bd1a-b868e65d57eb_story.html?utm_term=.5ed7e9199892 [https:// perma.cc/D9GK-5M99].

incredibly important, program functions today and how its stakeholders can rectify its shortfalls.

I.
THE SAR PROGRAM: A RESPONSE TO 9/11 & THE NEED FOR INFORMATION SHARING

After 9/11, the law enforcement community did "a lot of soul searching."[8] Slowly, a consensus coalesced that a lack of information sharing among law enforcement agencies was the single most important problem in pre-9/11 policing. The 9/11 Commission found that the Department of Justice's ("DOJ") rules and practices on sharing intelligence information, as well as relevant actions before the Foreign Intelligence Surveillance Court ("FISC"), created a culture that suppressed information sharing.[9] In addition, criminal prosecutors and law enforcement agents broadly "misunderstood and misapplied" the 1995 procedures issued by then-Attorney General Janet Reno on the proper methods for sharing intelligence information.[10] The law enforcement community interpreted the 1995 regulation as creating a "wall" between DOJ and the Federal Bureau of Investigation ("FBI"), with the Office of Intelligence Policy and Review serving as the gatekeeper.[11] Over time, and due in part to pressure from leadership across these agencies and even FISC itself, a similar "wall" arose between intelligence and criminal justice agents within the FBI. Agents came to believe that the FBI could

8. Jefferson B. Sessions, U.S. Att'y Gen., Remarks at National Fusion Center Association Meeting (Nov. 9, 2017), https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-national-fusion-center-association [https://perma.cc/MNU8-949F].

9. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 78–80 (2004), http://govinfo.library.unt.edu/911/report/911Report.pdf [https://perma.cc/D5US-BKBW].

10. *Id.* at 79; *see also* DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL (OIG), A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS 33 (2004), https://oig.justice.gov/special/s0606/final.pdf **[**https://perma.cc/V8QR-ZLJD**]**

> [A prior] OIG report found that the 1995 Procedures were largely misunderstood and often misapplied, resulting in undue reluctance by intelligence agents to provide information to criminal investigators and prosecutors. The report stated that 'the tumult that accompanied [the] creation [of the 1995 Procedures] drastically altered the relationship between [the FBI] and prosecutors.' The report found that because of [Office of Intelligence Policy and Review] OIPR's criticism of the FBI during the [Aldrich] Ames investigation, FBI agents had become 'gun shy' about conversations with Criminal Division attorneys, and the FBI's General Counsel's Office had recommended that FBI agents take a 'cautious approach' by initially conferring with OIPR attorneys rather than Criminal Division attorneys. The report also noted that as a result of the FBI's concerns about OIPR's criticisms, the FBI had been 'needlessly chilled' from sharing intelligence information with the Criminal Division. The report stated that the 1995 Procedures were vaguely written and provided ineffective guidance for the FBI. The report recommended that the Criminal Division, OIPR, and the FBI resolve conflicting understandings about the 1995 Procedures, and the FBI issue guidance to disabuse FBI personnel of 'unwarranted concerns about contact with prosecutors.
> *Id.*

11. THE 9/11 COMMISSION REPORT, *supra* note 9, at 79.

not share "*any* intelligence with criminal investigators, even if no FISA procedures had been used" to obtain it.[12]

The 9/11 Report carefully documents specific breakdowns in the information sharing process that hampered a timely response to the Twin Towers attack, including several related to one of the hijackers, Khalid al-Mindhar, who helped crash American Airlines Flight 77 into the Pentagon.[13] In January of 2001, the Central Intelligence Agency's ("CIA") Bin Ladin Unit was able to identify Mindhar when a source confirmed his identity from surveillance footage of him speaking with a senior security official who served Bin Laden.[14] The CIA, however, failed to transmit that identification to the FBI and did not urge the FBI to look into him.[15] Later, in another FBI-CIA meeting in June of 2001, an FBI agent failed to share National Security Agency ("NSA") reports linking Mindhar to a suspected terrorist facility in the Middle East because her counterparts were engaged in a criminal investigation (i.e., for fear that doing so would break the "wall").[16] At the same time, another CIA officer failed to disclose information that Mindhar had a US visa and might soon be traveling to New York, in part, because he was "not authorized to answer FBI questioning regarding CIA information."[17]

Ultimately, a search for Mindhar was initiated, but it was too little, too late. The 9/11 Commission found that widespread "confus[ion] about the rules governing the sharing and use of information gathering in intelligence channels" contributed to the agencies' failure to locate and interview Mindhar.[18] Though there is some disagreement among the intelligence community as to whether law enforcement could have intervened in time had Mindhar been found, the Commission asserted that stopping him and detaining him for "immigration violations or as [a] material witness[]" to other attacks in which he may have participated "could have derailed" the 9/11 attacks.[19]

Reflecting on this and other lapses in effective information sharing, the 9/11 Commission called on President Bush to "lead the government-wide effort to bring the major national security institutions into the information revolution."[20]

---

12. *Id.*
13. *See id.* at 2–3, 8–10.
14. *Id.* at 267–68.
15. *Id.*
16. *Id.* at 268–69.
17. *Id.*
18. *Id.* at 267.
19. *Id.* at 272.
20. It bears noting, however, that other issues like diffuse responsibility, a lack of centralized accountability, limited processes for joint action, etc., were also problems. In fact, the 9/11 Commission saw all these issues, including information sharing, as only "symptoms" of the greater disease of a system unprepared to deal with the complexities of terrorism. Hence, when making a tradeoff calculation as to the value of information sharing versus privacy or civil liberties concern, it is important to contextualize information programs as just one of several important structural flaws in our counter-terrorism operations. *See id.* at 400.

Specifically, the Commission noted that national security institutions lacked cohesive "rules for acquiring, accessing, sharing, and using the vast stores of public and private data that may be available."[21] The Commission also urged that funding be shared between the states and the Office of Management and Budget, and that location-specific processes, whether in "Pakistan or Texas," be subject "to the same quality standards."[22]

In 2007, the SAR Program, known officially as the Nationwide SAR Initiative ("NSI"), was established as a partnership between federal government agencies and their state, local, tribal, and territorial ("SLTT") partners in reaction to the 9/11 Commission's findings and similar subsequent documents. The SAR Program derived its legal authority, in part, from the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA"), which also established government oversight for the Program through the Director of National Intelligence as well as a technological platform through which the Program could transmit sensitive information, the Information Sharing Environment.[23] The SAR Program corresponded to a Federal Government strategy outlined in a contemporaneous report entitled, *The National Strategy for Information Sharing*.[24] Today, three federal agencies—the Department of Homeland Security ("DHS"), the FBI, and the Bureau of Justice Assistance ("BJA")—run the NSI together.[25] Under their leadership, the NSI "assist[s] agencies with adopting compatible processes, policies, and standards that foster broader sharing of SARs, while ensuring that privacy, civil rights, and civil liberties are protected."[26]

These organizations rely in large part on the NNFC to operationalize the SAR Program. As discussed in the DOJ's first "Fusion Center Guidelines," the fusion centers emerged as a byproduct of the broader law enforcement "paradigm shift" to a more "preventive approach" that would permit the government to better share information and "coordinate effective responses in the event of a terrorist attack."[27] The government hoped that these centers would apply an ana-

21. *Id.* at 419.

22. *Id.* at 417.

23. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638; *see also* U.S. SENATE COMM. ON GOVERNMENTAL AFFAIRS, SUMMARY OF IRTPA (2004), https://fas.org/irp/congress/2004_rpt/s2845-summ.pdf [https://perma.cc/UZ27-D43B] (summarizing the Act in a report issued eleven days before the Act's passage); Exec. Order No. 13388, 70 Fed. Reg. 62023 (Oct. 7, 2005), https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-13388 [https://perma.cc/T9EA-8FTQ] (President Bush's executive order expanding on the IRTPA).

24. WHITE HOUSE, NATIONAL STRATEGY FOR INFORMATION SHARING (2007), https://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf [https:// perma.cc/ 75YX-JRE7].

25. *About the NSI*, NATIONWIDE SAR INITIATIVE, https://nsi.ncirc.gov/about_nsi.aspx [https://perma.cc/ZPM7-4MXD] (last visited Jan. 20, 2019).

26. *Id.*

27. *See* DEP'T OF HOMELAND SEC., ET AL, FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW WORLD 11, 14 (2005), https://www.ialeia.org/docs/Fusion_Center_Guidelines_for_Law_Enforcement.pdf

lytical method, referred to as "data fusion," which could "dramatically improve information and intelligence sharing."[28] As defined by the CIA, data fusion involves the "ordering of finite information in an externally imposed order [such as a] chronology [or] in dimensional space" under the reasoning that "if enough data are put together and considered as a whole, patterns and possibly answers will emerge."[29] Today's success in applying this methodology stems, in part, from the fusion centers' ability to bring in representatives from SLTT partner organizations, as well as the federal government, into each center.[30]

Some law enforcement leaders and top elected officials claim that the fusion centers' impact on information sharing is integral to national defense. Former Attorney General Sessions recounted numerous fusion center successes at a recent convening of the National Fusion Center Association in 2017, noting that when the government has "the right information in a usable form, swiftly accessible—bad criminals are at greater risk, and our officers are safer."[31] Similarly, when speaking to the National Counterterrorism Center in 2015, President Obama endorsed a see-something-say-something approach and emphasized how "fusion cells" played an integral role in "prevent[ing] attacks at home" by "receiving tips and pushing information out to local law enforcement."[32] Even in the face of a scathing Senate report on fusion center failures in 2012, then-Chairman of the U.S. Senate Committee on Homeland Security & Governmental Affairs, Senator Joe Lieberman reiterated that "fusion centers have played a significant role in many recent terrorism cases and have helped generate hundreds of tips and leads that have led to current FBI investigations."[33] In light of these statements, and to the degree that there is consensus around the prudence of information sharing, it is difficult to contest the need for a network that can collect, analyze, and disseminate intelligence to law enforcement organizations around the country.

[https://perma.cc/K92Z-TJXX].

28. *Id.* at 11–12.

29. James M. Simon Jr., *Intelligence Analysis as Practiced by the CIA*, 26 INT'L J. OF INTELLIGENCE & COUNTERINTELLIGENCE 641, 643 (2013), https://www.tandfonline.com /doi/pdf/10. 1080/08850607.2013.807186 [https://perma.cc/ADA5-JKWD].

30. Robert W. Taylor & Amanda L. Russell, *Failure of Police Fusion Centers & the Concept of National Intelligence Sharing Plan*, 13 POLICE PRAC. & RES.: AN INT'L J. 185, 186–87 (2012), https://www.tandfonline.com/doi/pdf/10.1080/15614263.2011.581448?needAccess=true [https://perma.cc/J6WD-WYNM].

31. Jefferson B. Sessions, U.S. Att'y Gen., Remarks at National Fusion Center Association Meeting (Nov. 9, 2017), https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-national-fusion-center-association [https://perma.cc/MNU8-949F].

32. President Barack Obama, Statement at the National Counterterrorism Center (Dec. 17, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/12/17/statement-president-after-briefing-national-counterterrorism-center [https://perma.cc/MXL4-ND2T].

33. Tal Kopan, *Lawmakers Split Over Fusion Center Report*, POLITICO (Oct. 3, 2012), https://www.politico.com/blogs/under-the-radar/2012/10/lawmakers-split-over-fusion-center-report-137411 [https://perma.cc/6CAP-2G7N].

II.
THE POLICIES AND PROCEDURES OF THE SAR PROGRAM

A. The SAR Functional Standards

The SAR Program operates pursuant to the "Functional Standard," a governance document issued by the Program Manager of the Information Sharing Environment ("PM-ISE"). The PM-ISE is a group located within the Office of the Director of National Intelligence, whose leadership in turn reports directly to the President of the United States.[34] In 2008, the PM-ISE issued its first Information Sharing Environment ("ISE") Functional Standard ("FS") for Suspicious Activity Reports (Version 1.0). The report established a uniform definition for Suspicious Activity Reports: "[o]fficial documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention."[35] The report also called on myriad government organizations—"all departments or agencies that possess or use terrorism or homeland security information, [or] operate systems that support or interface with the ISE"—to adopt that standard.[36]

Since 2008, the PM-ISE has twice updated SAR guidance, most recently in 2015 by issuing FS Version 1.5.5.[37] While PM-ISE has developed a more complex technical architecture and guidance on collection criteria, the original FS remains largely unchanged in structure and scope despite these updates.[38] Notably, however, the 2015 FS contains a different definition than the original guidance of what constitutes an SAR: an "[o]fficial documentation of observed behavior *reasonably indicative* of pre-operational planning associated with

34. *See generally Who We Are – ISE*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, https://www.dni.gov/index.php/check-the-status-of-a-request/201-about/organization/information-sharing-environment/378-who-we-are-ise [https://perma.cc/D4V5-22MF] (last visited Jan. 20, 2019).

35. INFO. SHARING ENV'T (ISE), FUNCTIONAL STANDARD (FS) SUSPICIOUS ACTIVITY REPORTING (SAR) VERSION 1.0, at 1–2 (2008) [hereinafter FS 1.0], https://www.dni.gov/files/ISE/documents/DocumentLibrary/SAR/ISE-FS-200_SAR_Functional_Standard.pdf [https://perma.cc/KDG2-3HHZ].

36. *Id.*

37. INFO. SHARING ENV'T (ISE), FUNCTIONAL STANDARD (FS) SUSPICIOUS ACTIVITY REPORTING (SAR) VERSION 1.5.5 (2015) [hereinafter FS 1.5.5], https:// nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf [https://perma.cc/XT9V-LC3K]. Importantly, the Functional Standard does not include a functioning definition of "terrorism" or "terrorism-related events." This leaves fusion center analysts vulnerable to both over-including innocuous conduct and under-including harmful conduct they may deem not related to terrorism as they understand the term. In the last year, a concern has grown that such blind spots on terrorism might include, for example, white, far-right domestic terrorist organizations like Identity Evropa, the Proud Boys, and the Rise Above Movement. *See, e.g.*, Janet Reitman, *U.S. Law Enforcement Failed to See the Threat of White Nationalism. Now They Don't Know How to Stop It*, N.Y. TIMES, Nov. 3, 2018, (Magazine) https://www.nytimes.com/2018/11/03/magazine/FBI-charlottesville-white-nationalism-far-right.html [https://perma.cc/9U8L-M6Z8].

38. Compare FS 1.5.5, *supra* note 37, at 19–32, 41–51 with FS 1.0, *supra* note 35 at 12–21, 27–32.

terrorism or other criminal activity."[39] The 2015 guidance goes on to note that the determination of what is "reasonably indicative" is discretionary and based on the "circumstances in which that observation is made…[as understood by] the mind of the reasonable observer" and the "training and experience of a reasonable law enforcement officer."[40] The 2015 standard, however, does not define who qualifies as a "reasonable observer" or a "reasonable law enforcement officer," thereby leaving open the door to potentially harmful, but permissible, discretionary conduct.

The PM-ISE and collaborating agencies recognized the importance of standardizing local implementation of the Functional Standard early in the process. In 2008, the Department of Justice published a report summarizing key action steps that local law enforcement could adopt to align themselves to the SAR Program after conducting site visits to the Los Angeles, Chicago, Boston and Miami-Dade Police Departments.[41] Through this report, the DOJ encouraged a broad "all-crimes approach to gathering, processing, reporting, analyzing, and sharing of suspicious activity."[42] It also recommended training officers appropriately, integrating local processes for collection and reporting, and standardizing the reports and collection codes used within the SAR Program to facilitate collaboration across agencies.[43] Early leadership of the SAR Program hoped that "national guidelines [would] allow for the timely sharing of SAR information" while still respecting the discretion retained by local jurisdictions to account for any "unique circumstances and relationships within [their] community."[44]

B. The Procedure for SAR Collection, Analysis, and Dissemination

The law enforcement community operationalizes the Functional Standard in a five-stage process: (1) planning, (2) gathering and processing, (3) analysis and production, (4) dissemination, and (5) reevaluation.[45]

Planning. At the first stage, SAR planning, the ISE disseminates information products about terrorist plans, intentions, and capabilities, which become

39. FS 1.5.5, *supra* note 37, at 4 (emphasis added).

40. *Id.*

41. *See generally* DEP'T OF JUSTICE, FINDINGS AND RECOMMENDATIONS OF THE SUSPICIOUS ACTIVITY REPORT (SAR) SUPPORT AND IMPLEMENTATION PROJECT (2008), https:// nsi.ncirc.gov /documents/SAR_Report_January_2009.pdf [https://perma.cc/K5XC-8WJS].

42. *Id.* at 1.

43. *Id.* at 11–21.

44. *Id.* at 1, 6.

45. *See* FS 1.5.5, *supra* note 37, at 11. For additional insight into SAR processes and operations, *see* PM-ISE, NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE CONCEPT OF OPERATIONS 16–23 (2008) [hereinafter NSI CONOPS], https:// nsi.ncirc.gov/documents/NSI_CONOPS_Version_1_FINAL_2008-12-11_r4.pdf [https://perma.cc/H45U-9DAA]; Daniel Poniatowski, *A Constructive Problem: Redemption of Unlawful Arrests via Fusion Centers*, 2014 WIS. L. REV. 831, 838 (2014), http://wisconsinlawreview.org/wp-content/uploads/2014/11/Poniatowski-Final-2-Online.pdf [https://perma.cc/RAG7-R4M4] (describing the SAR Process briefly).

available to ISE participants (i.e., to law enforcement agencies).[46] This helps guide ISE intelligence in the field and, in turn, communicates specific intelligence needs or findings to the participants.

Gathering and Processing. At the second stage, "gathering and processing," the intake of potential intelligence and its subsequent analysis begins. First, an "initial observer" reports suspicious activity to a law enforcement agency.[47] The "initial observer" varies and could include a "private citizen" (e.g., person at a train station on the way to work who sees a person carrying a suspicious bag), a "representative of a private-sector partner" (e.g., contractor working on public project at a national park), or even a "government official" (e.g., staff at a Department of Motor Vehicles office).[48] A suspicious activity report could be communicated as a tip to local, state, or federal law enforcement through various channels including, for example, a 911 dispatch call, a field interview with an officer, or an online hotline for "E-Tips."[49] Alternatively, the "initial observer" might be a member of law enforcement.[50] In this case, the officer would directly observe someone engaged in "suspicious" behavior and report this conduct.

Regardless of who reports the initial observation, the local, state, or federal agency receiving the tip then "filter[s] out those [tips] that can be determined not to have a potential nexus to terrorism."[51] Importantly, the Functional Standard permits broad discretion by the reviewing agency, in the first instance, as to how to conduct any follow-up on the reported conduct.[52] As the SAR Concept of Operations explains, "[c]ontext is an important factor" in the agency's suspicion determination and the "initial investigation or fact gathering" falls within the purview of the local, state, or federal agency receiving the tip.[53] Hence, that organization's respective standards will govern whether there is immediate fol-

46. *See* NSI CONOPS, *supra* note 45, at 17.

47. *See* FS 1.5.5, *supra* note 37, at 13.

48. The FS 1.5.5 list of potential observers reflects the breadth of potential sources for this program: "a private citizen, a representative of a private-sector partner, a government official, or a law enforcement or homeland security officer." *Id.*

49. James E. Steiner, *More is Better: The Analytic Case for a Robust Suspicious Activity Reports Program*, 6 HOMELAND SEC. AFF. (2010) [hereinafter *More is Better*], https://www.hsaj.org/articles/80 [https://perma.cc/HZ2F-AC84] (providing a graphic of the "Notional SAR Process").

50. *See* FS 1.5.5, *supra* note 37, at 13.

51. *Id.*

52. *Id.* at 53.

An official of a Federal, State, local, tribal, or territorial agency with jurisdiction responds to the reported observation. This official gathers additional facts through personal observations, interviews, and other investigative activities. At the discretion of the official, further observation or engaging the subject in conversation may be required. Additional information acquired from such limited investigative activity may then be used to determine whether to dismiss the activity as innocent or escalate to the next step of the process.

Id.

53. *See* NSI CONOPS, *supra* note 45, at 19.

low-up on the tip. In some cases, officers may seek out the targets and investigate them. In other situations, the tip may be documented as an SAR without a subsequent inquiry. The degree of information captured in the SAR about the tip's target will thus vary accordingly.

Once any investigation associated with the initial tip finishes, the state, local, or federal agency determines whether to document it officially as an SAR and then transmit it to a regional fusion center for further processing and investigation. This determination depends on whether the local, state, or federal law enforcement agency finds that the report is reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.[54] Also, depending on the nature of the SAR, the agency at issue might also directly transmit that SAR to a Joint Terrorism Task Force ("JTTF")[55] responsible for investigating the specific conduct at issue.[56]

Analysis and Production. Next, at the third stage of the SAR process, "analysis and production," fusion centers play a major role. Fusion centers are regional government offices which function as the backbone of the SAR network. They are the "primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal and SLTT partners."[57] Though originally envisioned as primarily counter-intelligence centers, most fusion centers today have adopted an "all threats and all hazards" approach to the intelligence they analyze. In other words, though originally intended for terrorism-focused data collection, fusion centers today gather information pertaining to "immigration, radicalization, demographic changes, hurricanes, biological and chemical threats, as well as common criminal activity."[58]

---

54. *See* FS 1.5.5, *supra* note 37, at 52 n.22; *see also* NSI CONOPS, *supra* note 45, at 18–20.

55. A JTTF differs from a fusion center in several ways. *See Fusion Centers and Joint Terrorism Task Forces*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces [https://perma.cc/2XL4-LX4E] (last updated July 29, 2016). First, while fusion centers focus on information sharing and "enhancing the national threat picture," JTTFs focus more narrowly on counterterrorism. *Id.* Second, while the fusion centers are largely operated by state and local law enforcement, JTTFs are managed by the FBI and include other law enforcement as partners. *Id.* Lastly, while fusion centers "[r]eceive, analyze, gather, produce, and disseminate a broad array of threat-related information," JTTFs conduct investigations and create intelligence assessments. *Id.*

56. *See* NSI CONOPS, *supra* note 45, at 20.

> Depending on the nature of the activity, the information could cross the threshold of "suspicious" and move immediately into law enforcement operations channels for follow[ ]on action against the identified terrorist activity. In those cases where the local agency can determine that an activity has a direct connection to a possible terrorist-related crime, it will provide the information directly to the responsible JTFF for use as the basis for an assessment or investigation of a terrorism-related crime as appropriate.

Id.

57. *National Network of Fusion Centers Fact Sheet,* DEP'T OF HOMELAND SEC. (June 21, 2017), https://www.dhs.gov/national-network-fusion-centers-fact-sheet [https://perma.cc/62W7-SU53].

58. *See* Lindsey Garber, *Have We Learned a Lesson? The Boston Marathon Bombings and*

At a fusion center, a trained analyst or an investigator reviews the SAR in context and assesses whether the reported behavior aligns with the "pre-operational behaviors associated with terrorism" defined by Functional Standard.[59] These behaviors include seven categories of conduct that could reasonably be presumed as criminal (e.g., cyberattacks, threats, theft) and nine categories that are not necessarily criminal (e.g., photography, eliciting information about an event or location, observing a building beyond mere curiosity or in a professional role).[60] The Functional Standard requires that an analyst's assessment of the SAR consider all known information about the report which, as noted at Stage Two, may include a preliminary investigation by local law enforcement.[61] If the analyst determines that the reported conduct does not fit into one or more of these 16 conduct categories, or does not have a nexus to terrorism based on his or her professional judgment, then the analyst will not make the report accessible to their SLTT partners.[62]

Dissemination. On the other hand, if an analyst determines the report is reasonably indicative of pre-operational planning associated with terrorism, the fourth stage – "dissemination" – begins. The analyst repackages and formats the intelligence as an Information Sharing Environment – Suspicious Activity Report ("ISE-SAR"). This nomenclature is important because it applies ISE guidance on privacy protections to the information[63] and signals to any future reader that the report's target "can be presumed…to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism)."[64] The analyst then uploads the SAR to the Nationwide SAR Initiative Data Repository ("NSIDR"),[65] thereby rendering it available to all SLTT part-

Information Sharing, 67 ADMIN. L. REV. 221, 247 (2015); *see also* Samuel J. Rascoff, *The Law of Homegrown (Counter)Terrorism*, 88 TEX. L. REV. 1715, 1743–44 (2010). The primary difference here is whether the center focuses primarily on tracking acts of terrorism or whether, instead, the center focuses on other types of targets. The latest report from the National Network of Fusion Centers suggests that, of the 77 centers reporting, there is some variability in their primary focus areas: Counterterrorism only (2), All-Crimes only (5), All-Hazards only (1), some combination of two focuses (19), and a focus on all three areas (50). *See* DEP'T OF HOMELAND SECURITY, 2017 NATIONAL NETWORK OF FUSION CENTERS: FINAL REPORT 2 (2018), [hereinafter NNFC 2017 REPORT], https: //www.dhs.gov/sites/default/files/publications/2017_National_Network_of_Fusion_Centers_Final%20Report.pdf [https://perma.cc/TF84-92F4].

59. *See* FS 1.5.5, *supra* note 37, at 14.

60. *Id.* at 42–51 (noting, defining, and providing examples of each category of conduct).

61. *Id.* at 53.

62. *Id.* at 14. Importantly, it is not clear what happens with SARs that are not uploaded to the ISE. The protocols for storing, deleting, or further analyzing such information vary by jurisdiction. MICHAEL PRICE, BRENNAN CTR FOR JUST., NATIONAL SECURITY AND LOCAL POLICE 21 (2013), https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf [https://perma.cc/DY4N-TT69].

63. For a catalogue of all types of information that would appear on an ISE-SAR, refer to Section IV of Functional Standard 1.5.5. *See* FS 1.5.5, *supra* note 37, at 17–34.

64. *Id.* at 15.

65. *See generally* NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE, NATIONWIDE SUSPICIOUS ACTIVITY REPORTING: PROCESS IMPLEMENTATION CHECKLIST 16 (2017),

ners.[66] The government thus brands anyone appearing in an ISE-SAR as a plausible terrorist and shares their identity as such internationally.

Reevaluation. This provides a powerful tool for law enforcement to draw from when conducting investigations, attempting to "connect the dots" on potential targets, and creating more detailed intelligence reports for other partner organizations.[67] This tool, however, has some gaps in its reliability as the fifth stage—"reevaluation"—lacks clear processes and definitions. The guidance on ISE-SARs does not detail, for example, an appropriate feedback process to inform source organizations, and notify ISE participants, of incorrectly coded reports or reports which remain on file for individuals later shown to have no plausible connection to terrorism. Despite acknowledging this issue in the 2008 Concept of Operations and the 2015 Functional Standard 1.5.5, the PM-ISE has not yet issued a policy to address it across all fusion centers.[68]

---

https://nsi.ncirc.gov/documents/sar_implementation_checklist.pdf

[The NSI SDR] is a decentralized distributed data model used to make standardized terrorism-related information available through Common Terrorism Information Sharing Standards applications and services. Developing a SAR process and involvement in the NSI SDR will enable fusion center users to access federal, state, local, tribal, territorial, and regional SAR data. The NSI SDR provides an easy solution for fusion centers to share terrorism-related suspicious activity information, while still maintaining local control of SAR data collected from local agencies. Law enforcement agencies are able to share information with other agencies via the NSI SDR. Each agency has control of the information it makes available for sharing. The NSI SDR is made available for search by authorized user agencies via a secure network.

Id.

66. While the technical aspects of the systems used to collect, store, and disseminate SARs are beyond the scope of this paper, it is notable that fusion centers regularly work across multiple data sharing tools and systems. For example, DHS has designed a tool specially for SAR collection that is situated within their broader network, the Homeland Security Information Network (HSIN). *See* HOMELAND SEC. INFO. NETWORK, DEP'T OF HOMELAND SEC., 2017 ANNUAL REPORT: DELIVERING MISSION SUCCESS (2018), https://www.dhs.gov/sites/default/files/publications/HSIN-2017-Annual-Report.pdf [https://perma.cc/S3CL-GJ3R]. This tool is called HSIN – Critical Infrastructure (HSIN-CI). *See Suspicious Activity Reporting Tool*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/suspicious-activity-reporting-tool [https://perma.cc/QU62-WEC4] (last updated Feb. 1, 2018). In addition, fusion centers share SARs through "shared space[s]," a part of the digital Information Sharing Environment. *See* NATIONWIDE SAR INITIATIVE, ANNUAL REPORT 2011 6–7 (2012), https://nsi. ncirc.gov/documents/NSI_Annual_Report_2011.pdf [https://perma.cc/2XFA-AJ6A]. Fusion centers also interact with the FBI's unclassified system for sharing SARs named "eGuardian." *Id.* Shared space technology and eGuardian have an "automatic transfer capability" which ensures that the FBI receives all ISE-SARs generated by the fusion centers. *Id.* For more information on eGuardian, see 32 C.F.R. § 635.21 ("eGuardian is the Federal Bureau of Investigation's (FBI) sensitive-but-unclassified web-based platform for reporting, and in some instances, sharing, suspicious activity and threat related information with other federal, state, tribal, and territorial law enforcement and force protection entities.") and *eGuardian*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/resources/law-enforcement/eguardian (last visited Jan. 20, 2019). Other organizations within the federal government, such as the Department of Defense, also use eGuardian for SAR purposes. *See* Department of Defense, Instruction No. 2000.26 (Sept. 23, 2014), https://www.hsdl.org/?abstract&did=758648 [https://perma.cc/X9FN-CAK2].

67. *See* FS 1.5.5, *supra* note 37, at 14–15.

68. *See id.* at 15; NSI CONOPS, *supra* note 45.

III.
CRITICISMS OF THE NATIONWIDE SAR INITIATIVE

Members of both law enforcement agencies and civil liberties groups raise serious criticisms of the Nationwide SAR Initiative. Even Congress has weighed in, noting nearly one dozen distinct problems arising out of the Suspicious Activity Reporting Program.[69] The following issues represent some of the most salient, recurring concerns impacting the SAR Program's broad components.

A. Problems with the Efficacy and Reliability of the SAR Program

The following subsections address distinct criticisms of the SAR Program: (i) that SARs do not contribute sufficiently to stopping terrorism, (ii) that the current collection process overwhelms the analysts with white noise, and (iii) that there are reasons to doubt the accuracy or reliability of individual reports. Each subsection weighs the relative merits of these claims, identifying arguments for and against each criticism for the reader to consider.

i. SARs have Not Contributed Meaningfully to Stopping Terrorism

The SAR Program seeks to enable information sharing "vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities with a potential nexus to terrorism."[70] However, individual inquiries into the Program's efficacy suggest that it falls short of that goal. For example, when questioned by a Congressional Subcommittee as to the Program's efficacy, "DHS [] struggled to identify a clear example in which a fusion center provided intelligence which helped disrupt a terrorist plot" from 2007 to 2012.[71] Similarly, on a more local level, a Los Angeles Police Department ("LAPD") Commander confirmed in 2009 that their local SAR Program had "not foiled any terrorist plots."[72] Following up on the program six years later in 2015, the Los Angeles Times confirmed there had been no progress. "There are no known examples of an SAR leading authorities to uncover a real terror threat" around the United States.[73]

Since these findings, some local and state governments have anecdotally tracked success stories.[74] However, no systemic review of the national SAR

69. *See generally* U.S. SENATE PERMANENT SUBCOMM. ON INVESTIGATIONS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 45 (2012) [hereinafter 2012 SENATE REPORT], https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf [https://perma.cc/9LGL-URBB].

70. *See* FS 1.5.5, *supra* note 37 at 9.

71. 2012 SENATE REPORT, *supra* note 69, at 83.

72. Eric Schmitt, *Surveillance Efforts Draws Civil Liberties Concern*, N.Y. TIMES (Apr. 28, 2009), http://www.nytimes.com/2009/04/29/us/29surveil.html?pagewanted=all [https://perma.cc/VS3K-PG3G].

73. *See* Joel Rubin & Richard Winton, *The Journey of LAPD's Anti-Terror Suspicious Activity Reports*, L.A. TIMES (Jan. 31, 2015), http://www.latimes.com/local/california/la-me-suspicious-20150131-story.html [https://perma.cc/PN9Y-GFG3].

74. For example, New Jersey released seven examples of cases where SARs had played an

Program has corroborated a broader pattern of success. None of the agencies at issue—DHS, the FBI, or the BJA—have released a comprehensive, public study of whether the SAR Program achieves that goal and contributes meaningfully to stopping domestic terrorism.

In response to these criticisms, SAR Program advocates assert that the SAR Program has in fact seen successes. One 2015 report from the University of Maryland's National Consortium for the Study of Terrorism and Response to Terrorism ("START"), for example, analyzed prior, known terrorist plots for signs of SARs-related behavior.[75] The START report suggests that, even if no comprehensive study catalogues acts of terrorism stopped by the SAR Program, the "pre-incident activities occurring prior to acts of terrorism crimes do often align with existing SAR indicators."[76] In other words, the SAR Program has the potential to be a valuable tool as long as those associated behaviors can be tracked.

To reach this conclusion, the START report analyzed two public source projects, including the American Terrorism Study ("ATS").[77] Focusing on ATS, the authors identified 2,032 precursor behaviors (i.e., specific acts or conduct) from court documents and media reports in about 303 ATS cases which aligned with the sixteen SAR conduct categories.[78] The START report found that seven of the sixteen SAR categories accounted for more than 99% of the observed 2,032 precursor behaviors in these 303 cases: Materials Acquisition (497), Weapons Acquisition (380), Threat (374), Misrepresentation (334), Acquiring Expertise (196), Surveillance (160), and Recruiting (70).[79] The authors concluded that five of those categories (these same seven with the exceptions of "Misrepresentation" and "Recruiting") were "significantly related to incident failure."[80] Hence, terrorists who engaged in one of these five types of activities more often than not

important role in identifying potential terrorists prior to a potential, significant event or had aided law enforcement in identifying and capturing the perpetrators. As some of these examples clearly happened prior to the Senate Report and subsequent new stories, these examples highlight a key problem in assessing the effectiveness of this and other national security programs: limited transparency. *See* STATE OF N.J, OFFICE OF HOMELAND SEC. AND PREPAREDNESS, NEW JERSEY SUSPICIOUS ACTIVITY REPORTING: SUCCESS STORIES (2017), https://static1.squarespace.com/static/54d79f88e4b0db3478a04405/t/59bbeded9f8dce35ac0c172c/1505488367426/NJSAR+Success+Stories+%285.22.17%29.pdf [https://perma.cc/WT69-G3XT].

75. JEFF GRUENEWALD, WILLIAM S. PARKIN, BRENT L. SMITH, STEVEN M. CHERMAK, JOSHUA D. FREILICH, PAXTON ROBERTS & BRENT KLEIN, NAT'L CONSORTIUM FOR THE STUDY OF TERRORISM & RESPONSES TO TERRORISM (START), VALIDATION OF THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING (SAR) INITIATIVE: IDENTIFYING SUSPICIOUS ACTIVITIES FROM THE EXTREMIST CRIME DATABASE AND THE AMERICAN TERRORISM STUDY (2015), https://www.start.umd.edu/pubs/START_ValidationofNationwideSARInitiative_Feb2015.pdf [https://perma.cc/JAT7-9LFL].

76. *Id.* at 14.

77. *Id.* at 1–3.

78. *Id.* at 12.

79. *Id.* (providing the number of times that a behavior was observed in the data set).

80. *Id.*

failed in their mission or were stopped by police.[81] This suggests that the greatest value for national security is derived from tracking behaviors associated with the "Surveillance," "Acquiring Expertise," "Threat," "Weapons Acquisition," and "Materials Acquisition" categories.

Dr. James E. Steiner, Director of the University of Albany's Homeland Security Program, also rejects the criticism that SARs have not meaningfully contributed to stopping terrorist threats in his 2010 article.[82] Specifically, Steiner contends that the Nationwide SAR Initiative should collect and analyze *more* data to "increase the probability of identifying pre-operational terrorist activity."[83] Steiner argues that the intelligence community needs to "harness[] the power of statistics and analysis" to solve the signal problem.[84] Applying the law of large numbers, Steiner asserts that by aggregating more SARs, analysts will be able to determine a "normal pattern of SAR[s]" by geography against which abnormalities in the SARs could be identified to predict terrorist threats.[85] Such abnormalities would presumably include spikes or precipitous drops in SAR frequency or, perhaps, a change in some other identifiable metric for SARs. Importantly, however, Steiner acknowledges that beyond the sheer number of SARs required for these changes to be detectable, the SAR database would have to be uniform and consistent. Given that "over 18,000 local, state, and federal law enforcement organizations" collect information potentially resulting in a SAR, this raises a serious challenge to implementing Dr. Steiner's recommendations.[86]

Putting aside these criticisms, however, the reality remains that, even if SARs could contribute meaningfully to stopping terrorism,[87] the United States government has not systematically evaluated their success. In 2013, the Government Accountability Office ("GAO") assessed the SAR Program and critiqued the Program's inability to "track what difference the ISE-SARs have made, for example, in terms of their role in deterring terrorist activities or the number of arrests or convictions achieved."[88] As long as the SAR Program fails

81. *Id.* at 12 n.8 (noting importantly that the high failure rates for terrorists engaging in these five behaviors were driven both by law enforcement conduct and reasons not involving "law enforcement interdiction" such as device failures).

82. *See More is Better, supra* note 49 at 1.

83. *Id.* at 1.

84. *Id.* at 6–7.

85. *Id.* at 7.

86. *Id.*

87. This, however, does not mean that SARs have no function. As described in a GAO report in 2013, for example, a SAR reported by two Marines initiated an investigation that led to a successful arrest for assault. Though traditional police interdiction may have led to this same result given the defendant's conduct (i.e., defendant tried to run the marines off the road), the SAR nonetheless preceded the defendant's arrest, and shows how SARs can contribute to public safety. *See* 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 35 (2013) [hereinafter GAO ADDITIONAL ACTIONS], https://www.gao.gov/assets/660/652995.pdf [https://perma.cc/XF9H-DSK5].

88. *Id.* at 33.

to track "results-oriented outcomes" of existing ISE-SARs, it will be difficult for the government to demonstrate the concrete impact of SARs on terrorism.[89]

ii. SARs Have Blunted the Analytical Power of the NNFC with White Noise

The Homeland Security Policy Institute ("HSPI") highlights a second, related concern. In addition to some ambiguity as to the SAR Program's ability to identify potential terrorists, the Program may also inadvertently target innocent Americans. The SAR Program's permissive collection process "has flooded fusion centers, law enforcement, and other security entities with white noise."[90] This volume of innocuous or meaningless reports can limit fusion centers to mere "passive collection and dissemination."[91] Consequently, white noise reduces analysts' ability to distinguish innocent conduct from conduct having a nexus to terrorism or crime, and thus increases the likelihood that innocent people will be included in the Nationwide SAR Initiative Data Repository. The HSPI has called for greater investment in fusion centers analysts to correct this imbalance in resources. Specifically, the HSPI has suggested that center analysts need increased guidance, training, and connectedness to the broader intelligence community to avoid "the stove-piping of perspectives and information."[92]

The interrelated problems of staff training and connectedness, however, have received mixed treatment since 2012. On the one hand, internal reforms suggest the National Network of Fusion Centers is working hard to address these issues. For example, the NNFC recently suggested that the composition of its analyst workforce may help achieve "deep integration with local law enforcement operations and a focus on analytical production."[93] The NNFC's latest year-end report shows increased co-location with law enforcement, more co-authored reports, and greater support from SLTT representatives.[94] On the other hand, fusion centers today "lack a meaningful measure" for their analysts' proficiency level and fusion center directors continue to turnover at a "high rate."[95] In addition, the 2017 report both reveals a 40% ($3 million) decrease in the budget for training and exercises from 2016, and cautiously indicates that this shortfall

89. *Id.* at 36.

90. FRANK J. CILLUFFO, JOSEPH R. CLARK, MICHAEL P. DOWNING & KEITH D. SQUIRES, GEORGE WASH. U., HOMELAND SEC. POL'Y INST., COUNTERTERRORISM INTELLIGENCE: FUSION CENTER PERSPECTIVES 31 (2012), http://www.justiceacademy.org/iShare/Library-DHS/Fusion/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf [https://perma.cc/87QB-WX3G].

91. *Id.*; *see also* Rascoff, *supra* note 58, at 1744–45 (critiquing fusion centers' broad approach to information collection and dissemination as erroneously "presuppos[ing] the existence of intelligence that has already been acquired and properly analyzed").

92. CILLUFFO, CLARK, DOWNING & SQUIRES, *supra* note 90.

93. *See* NNFC 2016 REPORT, *supra* note 2, at 9.

94. *See* NNFC 2017 REPORT, *supra* note 58 at 10, 12. The percentage of Fusion Centers co-locating with (1) the FBI and (2) state, county, and city law enforcement agencies has increased by 8% and 5% respectively. *Id.*

95. *Id.* at 13.

fails to account for "free training offered to fusion center personnel via DHS and other government entities."[96] This latter caveat thus leaves open the possibility that "fusion centers are finding other means to complete necessary training."[97] These training, retention, and co-location issues all represent opportunities for improvement that bear on the Program's efficacy.

In addition, based on the NNFC's own reporting, it is not clear whether the Network's increased volume of analytical products has substantially helped law enforcement, or whether the greater volume of products may be exacerbating the white noise problem. The NNFC's performance statistics suggest a continued improvement in the production capabilities of fusion centers nationally. For example, the number of distributable analytic products—distributable reports that are based on a fusion center's analysis of raw data and other reporting—that have been co-authored by one or more fusion centers increased by about 33% from 137 in 2015 to 182 in 2017.[98] Similarly, the number of situational awareness products—shorter, quick-response analyses or information disseminated to other agencies—developed and disseminated by fusion centers have more than doubled from 99,820 in 2015 to 202,007 in 2017.[99] The data shows comparable increases for NNFC participation in Special Event Assessment Rating (SEAR) level events (35% increase in number of events receiving NNFC support from 2016).[100]

Statistics measuring the value or impact of the fusion centers' services over a two-year period, however, provide mixed results. For example, the number of

96. *Id.* at 16.

97. *Id.*

98. *Id.* at 24–25. "Distributable analytic products" are defined as a

> [R]eport or document that contains assessments, forecasts, associations, links, and/or other outputs from the analytic process that is disseminated via HSIN-Intel for use in the improvement of preparedness postures, risk mitigation, crime prevention, target hardening, or apprehension of offenders, among other activities. Analytic products may be created or developed jointly with federal, state, and local partners.

Id. at A-1.

99. *Id.* at 25. "Situational Awareness Products" describe "an event or incident of interest to customers (e.g., Be-On-the-Lookout reports, notes, event reports, daily bulletins, Situational Reports, raw reporting)" of the various fusion centers throughout the law enforcement community. *Id.* at A-1.

100. *Id.* at 21.

> In capturing pre-planned events, fusion centers identified direct role support they provided to both SEAR events—Levels 1-5—and National Special Security Events (NSSE). SEAR events are preplanned special events below the level of NSSE that have been submitted via the annual National Special Event Data Call. SEAR Level 1 events involve federal support, while SEAR Level 5 typically only require state and/or local resources. The majority of these events are state and local events that may require support augmentation from the federal government. Meanwhile, NSSEs are events of national significance deemed by the Secretary of Homeland Security to be a potential target of terrorism or other criminal activity. NSSE events include presidential inaugurations, major international summits held in the U.S., major sporting events, and presidential nominating conventions.

Id.

SARs vetted and disseminated by fusion centers that initiated or enhanced an FBI investigation increased by about 15%.[101] At the same time, however, the number of SARs vetted and submitted by fusion centers that involve an individual on the Watchlist has decreased by about 80%.[102] Also, the percentage of requests for information from the FBI's Terrorism Screening Center (TSC) for which fusion centers provided information for a case file dropped from 75% in 2015 to 49% in 2017.[103] These competing statistics are accompanied by a softer metric for value: the relative satisfaction of NNFC key customers. The satisfaction with NNFC products and services, the sense of the relevancy of NNFC products and services, and the reviews of NNFC products and services' timeliness have all fallen modestly from 2016 among key customers—though they remain an improvement from the 2015 numbers.[104]

Collectively, these data points demonstrate that fusion centers have increased their output in various ways but leave some ambiguity as to whether the quality and impact of NNFC contributions have similarly improved. The 2017 report raises an additional concern that this ambiguity in value is paralleled by an apparent drop in the per capita production of each analyst. Compared to 2015, the 2017 NNFC vetted about 10% fewer tips and leads and responded to about 4% fewer requests for information while employing 12% more analysts.[105] Lastly, the unexplained volatility across the fusion center network belies any certainty that the general improvements made in 2017 regarding the statistics above will continue in the coming years.[106] In order to resolve the white noise problem, the NNFC will need to improve the impact and value generated by its services as it continues to increase production. It will also need to better measure its own performance.

---

101. *Id.* at 25 (increasing from 225 in 2015 to 258 in 2017).

102. *Id.* at 25 (decreasing from 148 in 2015 to 28 in 2017). The "Watchlist" is a "database that contains sensitive national security and law enforcement information concerning the identities of those who are known or reasonably suspected of being involved in terrorist activities." *Id.* at A-2.

103. *Id.* at 25.

104. *Id.*

105. In 2017, the NNFC dedicated a total of 1,179 staff to the "analysis" function. *Id.* at 11. Whereas in 2015 the NNFC dedicated only 947 staff to analysis. DEP'T OF HOMELAND SEC., 2015 NATIONAL NETWORK OF FUSION CENTERS: FINAL REPORT 6 tbl.2 (2016), https://www.hsdl.org/?view&did=796365 [https://perma.cc/PC95-JTF3]. In 2015, the Network reported 74,379 tips and leads vetted and 443,881 RFIs responded. *See* NNFC 2017 Report, *supra* note 58 at 25. In 2017, the Network reported 66,758 tips and leads vetted and 426,394 RFIs responded. *Id.*

106. A review of the performance table available in the 2017 report shows unexplained drops in some of the statistics during the 2016 year. *Id.* at 25 (e.g. SARs contributing to investigations, SAR involving Watchlist targets, RFIs, case support and/or tactical products). In light of this variability, more reporting is necessary before observers can distill a clear pattern as to the NNFC's performance.

iii. Unclear Definition for SARs Undermines Reliability of Reports

A third problem in how SARs function is the lack of clarity as to what constitutes a suspicious activity meriting law enforcement's attention. This problem arises, in part, from the innate subjectivity of the standard. As described by professors Regan, Monahan, and Craven, determining what is "suspicious" enough to merit submitting an SAR "is in and of itself a…subjective decision and very much influenced by the perspective of the individual making that judgment, including his or her upbringing and experiences, as well as the context in which the activity takes place."[107] In other words, what one person considers suspicious will differ from what another considers suspicious. Because there are no bright line rules excluding or requiring the reporting of specific conduct beyond the Functional Standard, this inherent subjectivity undermines the credibility of all ISE-SARs.

Inconsistent guidance from local police departments on what constitutes a suspicious activity, both with respect to locally-run collection and also the SARs submitted to the National Network of Fusion Centers, amplifies the problem created by the FS's ambiguity.[108] For example, the Houston Police Department broadly requires officers to report on suspicious activity involving (1) photography and other surveillance of buildings, (2) the possession of posters or other publications, (3) all protests or demonstrations associated with terrorism, and (4) any other person or event which an officer determines is suspicious.[109] The Chicago Police Department has a similarly broad policy. The Department allows officers to conduct an investigation—even when the investigated conduct implicates First Amendment rights—for any "'reasonable law enforcement purpose' including 'public safety issues, whether they amount to criminal conduct or not.'"[110] On the other hand, several cities' police departments (including Detroit and Philadelphia) prohibit officers from collecting and disseminating reports on

107. Priscilla M. Regan, Torin Monahan & Krista Craven, *Constructing the Suspicious: Data Production, Circulation, and Interpretation by DHS Fusion Centers*, 47 ADMIN. & SOC'Y 740, 747–48 (2013) [hereinafter *Constructing the Suspicious*].

108. *See* PRICE, *supra* note 62, at 14.

109. *See id.* at 54 n.128 (quoting HOUSTON POLICE DEP'T, GENERAL ORDER 800-07: CRITERIA FOR SUBMITTING INCIDENT REPORTS 2–4 (2007)), https://www.brennancenter.org/sites/default/files/analysis/FN%20185%20%28Houston%20Police%20Dep%27t%2C%20General%20Order%20800-07—Criteria%20for%20Submitting%20Incident%20Reports%29.pdf [https://perma.cc/VP93-BSLZ] (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.").

110. *See id.* at 53 n.128 (citing CHICAGO POLICE DEP'T, GENERAL ORDER G02-02-01, INVESTIGATIONS DIRECTED AT FIRST AMENDMENT-RELATED INFORMATION A(2)(b) (2012), http://directives.chicagopolice.org/directives/data/a7a57be2-12936eaa-d1812-9373-a45df889893a9f52.html [https://perma.cc/MBL5-GVQ6]).

First Amendment protected activity without establishing reasonable suspicion first.[111] Many other cities fall between these two approaches. Consequently, the conduct included in the SARs of each jurisdiction vary in scope and focus by jurisdiction.[112]

Lastly, given the differing personal biases or capabilities among specific officers and agencies, there is a risk that some analysts and officers will overreport while others might become more "risk adverse [sic]."[113] For example, the 2012 Senate Subcommittee investigation on the SAR Program found that four reporting officials from different fusion centers "generated 108 of the 188" raw intelligence reports that were canceled over a 13-month period by senior DHS officials for reporting, in part, on constitutionally protected activity.[114] While most government programs will inevitably have some "bad apples," this problem seems to be particularly acute in environments, such as the SAR Program, which lack clear, actionable regulations on what information to collect and report.

B. Civil Liberties and Privacy Problems with the SAR Program

In addition to issues regarding the SAR Program's efficacy and reliability, there is also a risk that SARs may inflict privacy and reputational harms on its targets, and that such harms may disproportionally affect minority Americans. Several critics have also expressed concern that SARs may limit expressive conduct, political speech, and religious activity.

i. Functional Standard's Plain Language Provides Some Privacy Protections

Importantly, these criticisms must be situated within the context of the plain language of the SAR Program guidance which, despite the guidance's implementation, aims in some respects to minimize intrusions of privacy. First, the Functional Standard 1.5.5 relies on a "behavior-focused approach."[115] In other words, the Functional Standard requires analysts to assess the described *conduct*—as opposed to a person's characteristics—in determining whether there are grounds for filing an ISE-SAR. Hence, the standard, on its face, prohibits analysts or trained investigators from considering "race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity" as factors in their analysis of what constitutes conduct "reasonably indicative of pre-operational planning associated with terrorism" or other criminal activity.[116]

Functional Standard 1.5.5 also includes language intended to limit the sharing of personally identifiable information (PII). The FS defines PII broadly to

111. PRICE, *supra* note 62, at 53–56 n.128.
112. *Id.* at 14, 53–56 n.128.
113. *See Constructing the Suspicious*, *supra* note 107, at 748.
114. *See* 2012 SENATE REPORT, *supra* note 69, at 45–46.
115. *See* FS 1.5.5, *supra* note 37, at 10.
116. *Id.* at 10–11.

include "[i]nformation that may be used to identify an individual," and in practice limits such information to a specific list of protected data fields.[117] This limitation incorporates the legal framework established by the Privacy Act of 1974 and other government regulations intended to protect information privacy.[118] The FS recommends, but does not require, anonymizing ISE-SAR reports by excluding any data elements which contain personal identifying information as one means of reducing the risk to information privacy.[119]

Finally, Functional Standard 1.5.5 explicitly calls for the government actors in this process to protect privacy, civil rights, and civil liberties. For example, the PM-ISE is tasked with developing "implementation guidance, training, and governance structure, as appropriate, to address privacy, civil rights, and civil liberties-related policy, architecture, and legal issues."[120] Analysts, moreover, are required to act "in accordance with agency policies and procedures, including privacy policies, and records management schedules and should implement auditing and accountability measures."[121] In addition, all actors are bound by the Functional Standard's broader commitment to the protection of privacy as indicated by its incorporation of two internal assessments of the program's privacy implications into the most recent version of the standard.[122] Importantly, however, the sanctions applied for violations of these privacy standards may be inconsistent across different fusion centers, as each is encouraged to develop its own sanctions policies, and limited information exists on the frequency or impact of analyst sanctions.[123]

---

117. *See id.* at 3–4 (defining "personally identifiable information" and "privacy fields"); *see also id.* at 19–33 (noting which data elements constitute "privacy fields" within an ISE-SAR).

118. *See generally* Privacy Act, 5 USC §552a (1974). Importantly, however, not all actors in the SAR Program are subject to the same privacy requirements under federal law. While the Privacy Act prohibits federal officials from maintaining "record[s] describing how any individual exercises rights guaranteed by the First Amendment," 5 U.S.C § 522a(e)(7) (2013), most fusion centers are operated by state and local authorities and thus not subject to the Act. *See* PRICE, *supra* note 62, at 61 n.231.

119. *See* FS 1.5.5*, supra* note 37, at 17.

120. *Id.* at 5.

121. *Id.* at 15.

122. *See id.* at 1 (referencing the "Initial Privacy and Civil Liberties Analysis for the Information Sharing Environment, Version 1.0, September 2008" and the "Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations, Nationwide Suspicious Activity Reporting Initiative (July 2010)").

123. *See* DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE 25 (2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf [https://perma.cc/6Q9S-74TS]; *see also, e.g.*, NE. OHIO REG'L FUSION CTR., PRIVACY POLICY 12, http://www.neorfc.us/pdf_neorfc/en-US/NEORFC%20Privacy%20Policy%203-11.pdf [https://perma.cc/YF7L-6P9B] (last visited Jan. 20, 2019) (illustrating one fusion center's sanctions policy).

ii. The Legal Standard for Suspicion in the FS Undermines Personal Privacy

The protections outlined above are undermined, however, by the suspicion threshold applicable in the SAR process. As described in Part II.B, a Suspicious Activity Report, whether originally reported by a private party, government official, or law enforcement officer, will be assessed in two stages: first by local law enforcement as they submit SARs to the fusion centers, and again by fusion centers as they upload ISE-SARs to the Nationwide SAR Initiative Data Repository. In the second instance, fusion center analysts are asking (1) whether the conduct aligns with the Functional Standard's 16 conduct categories and (2) whether the conduct in the report may be "reasonably indicative" of "pre-operational planning associated with terrorism or other criminal activity."[124]

This framework exists outside the legal standard which normally governs police interaction with private citizens—the Fourth Amendment. The text of the Fourth Amendment guarantees people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[125] A search conducted "without a warrant…is per se unreasonable" and the warrant requirement is "subject only to a few specifically established and well-delineated exceptions."[126] To obtain a warrant, the government must establish probable cause before a neutral magistrate and narrowly delineate the scope of the authorized search.[127] This protection ensures that the government does not intrude upon society's "reasonable expectation of privacy."[128] It also guarantees that the government does not intrude upon a person's property.[129]

However, for this standard to apply, there must be a forcible stop or search in the first place.[130] As a general matter, a police officer's questioning does not

---

124. *See* FS 1.5.5, *supra* note 37, at 4.

125. U.S. CONST. amend. IV.

126. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973). *But see* Clifford S. Fishman, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable* Cause, 65 RUTGERS L. REV. 995, 1001 n.21 (2013), https://scholarship.law.edu/cgi/viewcontent.cgi?article=1137&context=scholar [https://perma.cc/CX8Z-HYVZ] (cataloguing exceptions).

127. Kentucky v. King, 563 U.S. 452, 459 (2011).

128. Katz v. United States, 389 U.S. 347, 360 (1967).

129. Florida v. Jardines, 569 U.S. 1, 5 (2013) (quoting United States v. Jones, 565 U.S. 400, 406 n.3 (2012)) ("'When the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a "search" within the original meaning of the Fourth Amendment has undoubtedly occurred'").

130. *See* United States v. Mendenhall, 446 U.S. 544, 554 (1980) (defining seizures as government conduct pursuant to which, "in view of all the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave"); *see also Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring) (defining a search on privacy grounds as a government conduct transgressing a person's expectation of privacy which "society is prepared to recognize as reasonable"); *Jones*, 565 U.S. at 407 (2012) (citing *Katz*, 389 U.S. at 286) (defining searches on a property-based rationale as any "physical intrusion of a constitutionally protected area in order to obtain information").

amount to either a forcible stop or a search.[131] A wide variety of similar police conduct also falls below the threshold for a seizure.[132] Consequently, much, if not all, of the government's conduct prior to filing a SAR or ISE-SAR—that is, when an officer questions someone in a public place, observes and takes notes on suspicious conduct, speaks to the acquaintance of the target, overhears a person's public statements, or reviews someone's public social media activity—is unlikely to be prohibited by the Fourth Amendment.

Acknowledging that traditional Fourth Amendment requirements of probable cause and a warrant would impose too great a burden on officers collecting SARs, civil liberties organizations have advocated for adopting reasonable suspicion as the legal standard in SAR collection and dissemination.[133] Yet this standard would probably also be unavailing in the SAR context. In *Terry v. Ohio*, the Court recognized that, under the "appropriate circumstances and in an appropriate manner," the combination of governmental interests in crime prevention and officer safety might render a search permissible pursuant to a lower threshold of suspicion than probable case – namely, reasonable suspicion.[134] For

131. *See* United States v. Drayton, 536 U.S. 194, 200–01 (2002) (citations omitted)

Law enforcement officers do not violate the Fourth Amendment's prohibition of unreasonable seizures merely by approaching individuals on the street or in other public places and putting questions to them if they are willing to listen. Even when law enforcement officers have no basis for suspecting a particular individual, they may pose questions, ask for identification, and request consent to search luggage—provided they do not induce cooperation by coercive means. If a reasonable person would feel free to terminate the encounter, then he or she has not been seized.

Id.; see also Florida v. Bostick, 501 U.S. 429, 434 (1991); United States v. Martin, 598 F. App'x 156, 158 (4th Cir. 2015); United States v. Childs, 277 F.3d 947, 954 (7th Cir. 2002).

132. *See, e.g.*, Haberle v. Troxell, 885 F.3d 170, 176 (3d Cir. 2018) (finding officer's "knock and talk" at a private residence was not a seizure); United States v. De Castro, 905 F.3d 676, 682 (3d Cir. 2018) (finding that police officer's request to defendant to remove his hands from his pocket was not a seizure); United States v. Barry, 394 F.3d 1070, 1076–77 (8th Cir. 2005) (finding defendant was not seized when the officer approached defendant's parked vehicle in vacant parking lot, after parking the patrol car about 15 feet away, and knocked on the window of the defendant's vehicle several times). *But see* United States v. Hernandez, 847 F.3d 1257, 1265 (10th Cir. 2017) (finding officers' request to defendant that he stop walking, after closely following him in a police cruiser and questioning him while he continued to walk, was a "seizure" within meaning of Fourth Amendment). Even more threatening or serious conduct has, at times, fallen below the level of a seizure. *See, e.g.*, Burg v. Gosselin, 591 F.3d 95, 98 (2d Cir. 2010) (finding "issuance of a pre-arraignment, non-felony summons requiring a later court appearance" was not a seizure); Ferrante v. Peters, 135 F. App'x 846, 848 (6th Cir. 2005) (finding no seizure where "officers shot at and hit the [defendants] car, but did not successfully restrain [their] movement"); Brown v. Battle Creek Police Dep't, 844 F.3d 556, 567 (6th Cir. 2016) (finding that officers' shooting and killing of defendant's two pit bulls was reasonable and thus not a seizure).

133. *See, e.g.*, AM. CIVIL LIBERTIES UNION, *More About Suspicious Activity Reporting*, https://www.aclu.org/other/more-about-suspicious-activity-reporting (last visited Jan. 20, 2019) [https://perma.cc/5W3P-5LZY].

134. *See* Terry v. Ohio, 392 U.S. 1, 22–23 (1968)

We are now concerned with more than the governmental interest in investigating crime; in addition, there is the more immediate interest of the police officer in taking steps to assure himself that the person with whom he is dealing is not armed with a weapon that could unexpectedly and fatally be used against him.

an officer to conduct a *Terry* Stop based on reasonable suspicion, the Court has explained that they must have a "reasonable basis to think that the person to be detained 'is committing or has committed a criminal offense.'"[135] Importantly, this suspicion threshold requires more than a mere, "inarticulate hunch[]."[136] The officer must provide specific and articulable facts which establish an objective suspicion underlying the search.[137] However, for the same reasons discussed above, much of the conduct required during the SAR process will also not be protected by the reasonable suspicion standard.[138]

Recently, the Ninth Circuit entertained an appeal questioning whether a regulatory standard akin to "reasonable suspicion" might replace the Functional Standard's "reasonably indicative" standard.[139] In *Gill v. Department of Justice*, the ACLU sued the DOJ and PM-ISE, arguing that the adoption of the Functional Standard was arbitrary and capricious because it conflicted with 28 C.F.R. Part 23.[140] This regulation "prohibit[s] the collection of 'criminal intelligence'" – which according to the plaintiffs would include ISE-SARs – "unless supported by 'reasonable suspicion.'"[141] Importantly, the applicability of this standard does not hang on whether an officer's conduct amounted to a search or seizure and is instead triggered by sharing and retaining information across law enforcement agencies. The government responded that SAR information is not criminal in nature, but rather "information about suspicious behavior that has a potential nexus to terrorism."[142] Consequently, since Part 23 only governs "criminal" intelli-

---

Id.; Michigan v. Summers, 452 U.S. 692, 707 (1981) (emphasizing the importance of officer safety as a second, necessary basis for reasonable suspicion).

135. United States v. Bailey, 743 F.3d 322, 332 (2d Cir. 2014) (quoting Arizona v. Johnson, 555 U.S. 323 (2009)).

136. *Terry*, 392 U.S. at 22.

137. Ashcroft v. al-Kidd, 563 U.S. 731, 749 n.3 (2011) (quoting Reasonable Suspicion, Black's Law Dictionary (9th ed.2009)) (defining "reasonable suspicion" to mean "[a] particularized and objective basis, supported by specific and articulable facts, for suspecting a person of criminal activity"); Maryland v. Buie, 494 U.S. 325, 327 (1990) (permitting a protective sweep of a home having established reasonable suspicion via "specific and articulable facts").

138. *See, e.g.*, United States v. Smith, 633 F.3d 889, 892 (9th Cir. 2011) (finding that officer's use of sirens to call defendant's attention and stop him in the street was not a Fourth Amendment seizure requiring reasonable suspicion); United States v. Smith, 649 F.2d 305, 308 (5th Cir. 1981) (finding that officers' request to see a passenger's tickets and their subsequent conversation with him at the airport was not a Fourth Amendment violation because they neither searched or seized him, and thus it did not matter that officers could not establish reasonable suspicion or probable cause).

139. *See* 28 C.F.R. § 23.20(a) (2017) ("A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.").

140. *See* Brief for Appellant at 20–23, Gill v. Dep't of Justice, No. 17-16107 2017 WL 5166659 (9th Cir. Nov. 3, 2017).

141. Gill v. Dep't of Justice, 246 F. Supp. 3d 1264, 1266 (N.D. Cal. 2017).

142. Brief for Appellee at 18, *Gill*, No. 17-16107 (9th Cir. Feb. 16, 2018); *see also* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1750 (2014), https://georgetownlawjournal.org/articles/74/panvasive-

gence, the government argued that the law is inapplicable to the SAR process and not in conflict with the Functional Standard. The District Court held for the government, finding that "the Functional Standard was developed to address data collection and dissemination issues not already within the scope of Part 23" and thus was neither at conflict with Part 23 nor arbitrary and capricious.[143] The Ninth Circuit affirmed, holding that the regulation was not arbitrary and capricious for failing to adhere to Part 23 because the program purposefully gathers information that does "not rise to the level of criminal intelligence."[144]

Given the inapplicability of the Fourth Amendment to SAR intelligence collection, and the Ninth Circuit's decision in *Gill*, it seems likely that the PM-ISE will continue to operate on the "reasonably indicative" standard. In doing so, the PM-ISE condones police surveillance and disseminates ISE-SARs without regard for the legal standards rising out of the Fourth Amendment. Designed to help law enforcement "connect the dots" through a "mosaic" containing all known information relevant to a potential terrorist, the "reasonably indicative" standard facilitates a collection system that requires officers to report, document, and disseminate SARs on a mere *hunch*.[145] The lack of a meaningful privacy standard creates a new privacy harm through the distribution of the names and personal information of SAR targets in association with terrorism—a harm doubly amplified by the reports' longevity and broad, 18,000-agency audience.

iii. Today's Enforcement Violates Civil Liberties

In addition, the Functional Standard's suspicion threshold facilitates potential privacy and civil liberties violations. ISE-SARs disclosed by the government through Freedom of Information Act (FOIA) requests raise concerns that the SAR Program has, in some instances, targeted and stifled expressive conduct (e.g., photography and video recording). Such ISE-SARs also suggest that the fusion centers' reporting and investigation may, in some jurisdictions, disproportionately impact people of color and immigrants. Such a practice would contradict the Functional Standard's rules on race, religion, and other suspect categories.

Threat to Photography. Since 2008, advocacy groups like the ACLU have raised concerns about the SAR Program's scrutiny of expressive activity such as

surveillance-political-process [https://perma.cc/75TV-498B]

DOJ contends that SARs are 'tips and leads' data that are not criminal intelligence. Thus, for instance, the fact that someone is seen scanning an area with binoculars or snapping a picture of a ferry with a cellphone might be entered into the SAR database, and over time additional information about the 'suspicious' individual—employment history, financial data, phone numbers, and so on—might be added to the file.

Id.

143. *Gill*, 246 F. Supp. at 1271 (finding that "defendants are entitled to summary judgment that adoption of the Functional Standard did not violate the APA as arbitrary and capricious.").

144. Gill v. United States Dep't of Justice, 913 F.3d 1179, 1188 (9th Cir. 2019).

145. *See* GAO ADDITIONAL ACTIONS, supra note 87**,** at 32.

photography.[146] "[P]hotography" is included as one of the 16 behavioral categories establishing a nexus to terrorism in Functional Standard 1.5.5.[147] The Functional Standard's definition of this category— "[t]aking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person"—gives law enforcement broad discretion over what to report and investigate as it relates to photography.[148] There is limited guidance on what should be interpreted as "unusual or surreptitious," or which "persons, facilities, buildings, or infrastructure" should be discernable as inappropriate targets for an SAR.[149] Even the examples provided in the Functional Standard, which are presumably intended to guide law enforcement and analysts in applying the standard, permit overbroad discretion. These examples include "taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc."[150]

In at least one regional fusion center, the California Central Intelligence Center, the reports permitted by the Functional Standard's broad policy have brought into question the efficacy and fairness of that Center's implementation of SAR processes.[151] Several publications sharply criticized the kinds of conduct deemed suspicious enough to have a nexus to terrorism in 1,800 SARs released by the Center in 2012: a "[f]emale Subject taking photos of Folsom Post Office," "a male nonchalantly taking numerous pictures inside a purple line train" in Los Angeles, and a person "taking photographs of a bridge crossing the American River Bike Trail."[152] Such reports, which were kept on record and disseminated to other law enforcement, raise the concern that anyone photographing officers,

146. *See generally* MIKE GERMAN & JAY STANLEY, AM. CIVIL LIBERTIES UNION, FUSION CENTER UPDATE (July 2008) [hereinafter ACLU FUSION CENTER UPDATE], https://www.aclu.org/files/pdfs/privacy/fusion_update_20080729.pdf [https://perma.cc/E39E-3WU9].

147. FS 1.5.5, *supra* note 37, at 48.

148. *Id.*; *see also* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L. J. 1441, 1451–52 (2001), https://digitalcommons.law.umaryland.edu/fac_pubs/991/ [https://perma.cc/4DJB-NPV9] ("Fusion centers encourage the public to report suspicious activity, including people who photograph, videotape, sketch, or ask detailed questions about airports, bridges, hospitals, the Internet, and cable.").

149. FS 1.5.5, *supra* note 37, at 48.

150. *Id.*

151. *See* ACLU OF N. CAL., SELECTED SUSPICIOUS ACTIVITY REPORTS FROM THE CENTRAL CALIFORNIA INTELLIGENCE CENTER AND JOINT REGIONAL INTELLIGENCE CENTER (Aug. 6, 2012), https://www.aclunc.org/sites/default/files/asset_upload_file470_12586.pdf [https:// perma.cc/A6QY-AVRV].

152. JOSHUA REEVES, CITIZEN SPIES: THE LONG RISE OF AMERICA'S SURVEILLANCE SOCIETY 155–156 (2017); Michael Zhang, *The US Govt Has Records of 'Suspicious' Photographers Legally Taking Pictures*, PETAPIXEL (Sept. 20, 2013), https://petapixel.com/2013/09/20/us-govt-records-suspicious-photographers-legally-taking-pictures/ [https://perma.cc/66MN-488P]; *see also* Paul Elias, *New Files from the ACLU Show Ordinary Americans Targeted in Counterterrorism Spying*, BUSINESS INSIDER (Sept. 19, 2013, 3:49 PM), http://www.businessinsider.com/aclu-files-domestic-spying-2013-9 [https://perma.cc/Q6QD-BYSM].

people, or places in public may become the target of attention from law enforcement.[153] The limited transparency of the Center's reasoning and processing of such SARs reinforces this concern. Notably, National Public Radio (NPR), when reporting on SAR, was unable to obtain a comment from the Department of Justice about the program or its implications.[154]

These concerns are grounded in numerous incidents that illustrate law enforcement's generally negative treatment of photography.[155] In 2008, for example, local police in Bay City, Texas stopped, questioned, and ran background checks on an Al-Jazeera television crew filming more than a mile away from a nuclear power plant.[156] Despite confirming their identities and finding "no criminal history or other problems," a spokesperson for the Matagorda County Sheriff Department stated that the department "would continue to monitor this situation" without specifying why.[157] In 2009, officers from New York's Metropolitan Transportation Authority (MTA) stopped Mr. Robert Taylor from taking photographs in the subway—an activity protected by MTA Rule 1050.9(c)—and then charged him with taking photographs illegally, impeding traffic, and causing unreasonable noise.[158] After the photograph charge was dismissed, the police department's chief spokesperson stated only that the "officers misinterpreted the rules concerning photography" and that the "summons was issued in error," noting that the police intended to go forward on the other charges.[159] In 2013, Philadelphia Police arrested a Temple University student, Richard Fields, and confiscated his phone for recording a group of officers as they broke up a house party.[160] On appeal before the Third Circuit, the officers at issue were found to have violated Mr. Richard's "commensurate right to record—photograph, film, or audio record—police officers conducting official police ac-

153. *See, e.g.*, Gericke v. Begin, 753 F.3d 1, 2–3 (1st Cir. 2014) (finding that filming a traffic stop was a valid exercise of First Amendment rights despite New Hampshire's wiretapping statute); Am. Civil Liberties Union of Ill. v. Alvarez, 679 F.3d 583, 589 (7th Cir. 2012) (finding that eavesdropping statutes create a credible threat of prosecution for the ACLU and its employees).

154. Martin Kaste, *ACLU Posts Fed-Collected 'Suspicious' Activity Reports Online*, NPR (Sept. 19, 2013), https://www.npr.org/2013/09/19/223721407/aclu-posts-suspicious-activity-reports-online [https://perma.cc/2V6X-2MSU].

155. *See* Morgan Leigh Manning, *Less than Picture Perfect: The Legal Relationship Between Photographers' Rights and Law Enforcement*, 78 TENN. L. REV. 105, 108–12 (2010) (cataloguing seven incidents between law enforcement and photographers).

156. GERMAN & STANLEY, *supra* note 146, at 6; Heather Menzies, *Deputies Question Al Jazeera Film Crew*, BAY CITY TRIBUNE (June 3, 2008), http://freerepublic.com/focus/f-news/2028223/posts [https://perma.cc/S2DW-7SRG].

157. Menzies, *supra* note 156.

158. *See* Jim Dwyer, *No Photo Ban in Subways, Yet an Arrest*, N.Y. TIMES (Feb. 7, 2009), http://www.nytimes.com/2009/02/18/nyregion/18about.html [https://perma.cc/4NVF-NVVZ].

159. *Id.*

160. *See* Holly Otterbein, *Lawsuit Claims Philly Police Officers Harassed Photographers*, NEWSWORKS.ORG (July 27, 2014), https://www.nbcphiladelphia.com/news/local/ACLU-Claims-Philly-Cops-Harass-Photographers-268728291.html [https://perma.cc/5TC4-UKH4].

tivity in public areas."[161] Similarly, as demonstrated by the released video footage in another case, protester Jessica Benn was pushed up against the side of a bus and had her phone taken by an officer after recording his conduct during an anti-police rally in downtown Denver in 2015.[162]

These examples raise the concern that, while the SAR Program does not encourage the immediate seizure of mobile phones or physical arrest, the Program has, nonetheless, created two civil liberties problems related to photography. First, given the tense relationship between photography and law enforcement, and the permissive definition of photography for SAR purposes, the Functional Standard's designation of photography as a behavior indicative of "terrorism or other criminal activity" seems likely to encourage officers to interfere with lawful photography and video recording, thereby leading to additional privacy and civil liberties violations.[163] In other words, the SAR framework creates an additional reason—one tied to terrorism and national security—for local law enforcement to scrutinize public photography and video recording. Second, SARs also present an added risk for people who are engaging in public photography or video recording. In addition to being criminally charged, losing their mobile phones, or having their data deleted, such individuals may also find themselves (and their personal information) published to the Nationwide SAR Initiative Data Repository as targets of an ISE-SAR. Any such target might, in turn, be "tracked…cross-country," have officers visit their home, have officers "question[] a neighbor" about them, be threatened with placement on a "watch list," or otherwise become the subject of increased police scrutiny by any officer engaging with them who happens to be aware of the ISE-SAR.[164]

Suppression of Political Speech. As reflected in various FOIA requests, scholarly papers, and news articles, there is also a rising concern that the SAR Program could lead to the suppression of political speech.

For example, email communications released from several fusion centers pursuant to a FOIA request by the Center for Media and Democracy show that the centers collaborated with the FBI and the DOJ during 2011 and 2012 to monitor the "constitutionally protected activities of Occupy protestors in various cit-

161. Fields v. City of Philadelphia, 862 F.3d 353, 360 (3d Cir. 2017).

162. Kevin J. Beatty, *Lawsuit Against Denver Police Camera Seizure Raises Questions About DPS Video Policy*, WESTWORD (Mar. 31, 2016), https://www.westword.com/news/lawsuit-against-denver-police-camera-seizure-raises-questions-about-dps-video-policy-7753327 [https://perma.cc/6NAF-7BJM]; Kit O'Connell, *The First Amendment Hasn't Stopped Police from Harassing Copwatchers*, TRUTHOUT.ORG (Apr. 23, 2016), http://www.truth-out.org/news/item/35731-the-first-amendment-hasn-t-stopped-police-from-harassing-copwatchers [https://perma.cc/MVA4-WW53]; Andy Thayer, *Demonstrator Who Recorded Arrest Sues for Unlawful Seizure of Cell Phone*, LOEVY & LOEVY (Mar. 28, 2016), http://www.loevy.com/blog/demonstrator_arrest_cell_phone/ [https://perma.cc/J6GM-2GMF].

163. *See* FS1.5.5, *supra* note 37, at 4.

164. Gill v. Dep't of Justice, No. 14-CV-03120-RS (KAW), 2015 WL 9258075, at *2-3 (N.D. Cal. Dec. 18, 2015) (describing plaintiffs' interactions with law enforcement after becoming the targets of an ISE-SAR).

ies throughout the nation."[165] Interviews with the centers' directors and staff by Professors Craven, Monahan, and Regan showed a "disconnect" as to this conduct.[166] While the centers claimed "to distinguish constitutionally protected protest activity from potential threats to public safety," their interviews and emails revealed that fusion centers regularly disseminated information on individuals "not involved in any form of criminal activity."[167] In just one instance, for example, 31 fusion centers and law enforcement agencies responded to a request from the Arizona Counter Terrorism Information Center with intelligence on Occupy Wall Street protests, significant events, and arrests.[168] These fusion centers collaborated across various jurisdictions, most notably Arizona and Massachusetts, despite internal regulations and memoranda clarifying that such conduct risked violating the targets' privacy and civil liberties.[169]

The fusion centers also seem to have been sharing their intelligence reports, likely based on information obtained from SARs, with private entities.[170] These fusion centers warned private entities of upcoming protests and provided them with personal information about the protesters gained from undercover sources and online surveillance.[171] The disclosure of similar documents to the Partnership for Civil Justice Fund further corroborates the fusion centers' broad tracking of Occupy Wall Street activists, including the fusion centers' efforts towards assembling lists of protesters and other Occupy events, tallying attendees at such events, tracking the appearances of prominent Occupy supporters, and disseminating this information to the NNFC's law enforcement partners.[172]

---

165. Krista Craven, Torin Monahan & Priscilla Regan, *Compromised Trust: DHS Fusion Centers' Policing of the Occupy Wall Street Movement*, 20(3) SOC. RES. ONLINE 7 (2015) [hereinafter *Compromised Trust*]; *see also* BEAU HODAI, CTR. FOR MEDIA AND DEMOCRACY, DISSENT OR TERROR: HOW THE NATION'S COUNTER TERRORISM APPARATUS, IN PARTNERSHIP WITH CORPORATE AMERICA, TURNED ON OCCUPY WALL STREET (May 2013), https://www.prwatch.org/files/Dissent%20or%20Terror%20FINAL.pdf [https://perma.cc/7EZB-P3X3].

166. *See Compromised Trust*, *supra* note 165, at 7–8.

167. *Id.*

168. *Id.* at 8.

169. *Id.*

170. *Id.* at 9–10. In the summer of 2018, a bill entitled, Enhancing Suspicious Activity Reporting Act (H.R. 5094), passed the House which might increase government "collusion" with the private sector and increase "warrantless monitoring." See David Hensley, *New Bill Incorporates Private Sector Into Terrorism Monitoring and Reporting,* ELECTRONIC FRONTIER FOUNDATION – AUSTIN (July 8, 2018, 5:56 PM), https://effaustin.org/2018/07/new-bill-incorporates-private-sector-into-terrorism-monitoring-and-reporting/ [https://perma.cc/2MSW-BF28].

171. *Compromised Trust*, *supra* note 165, at 9–10 (describing generally DHS's efforts to "monitor planned protests of private companies and organizations, such as the CITI Bank, the Salt River Project…and the American Legislative Exchange Council [ALEC]" and providing, as an example, a detailed analysis of the Arizona Fusion Center's efforts to undermine an Occupy Wallstreet protest of ALEC from November 28, 2011 to December 2, 2011).

172. Colin Moynihan, *Officials Cast Wide Net in Monitoring Occupy Protests*, N.Y. TIMES (May 22, 2014), https://www.nytimes.com/2014/05/23/us/officials-cast-wide-net-in-monitoring-occupy-protests.html [https://perma.cc/3VAQ-3HTS] (discussing the role of fusion centers in tracking Occupy Wall Street based on their FOIA disclosure of 4,000 pages of unclassified emails and reports from 2011 and 2012); Naomi Wolf, *Revealed: How the FBI Coordinated the Crack-*

More recently, it has come to light that the government tracked another prominent activist group: Black Lives Matter. In 2015, a FOIA request to DHS revealed documents "detailing live updates and Google Maps images of Black Lives Matter protestors' movements during an April 29th protest in Washington," and it seems such tracking was managed, at least in part, through the National Network of Fusion Centers.[173] Similarly, in 2017, a FOIA request sent by the Center for Constitutional Rights to DHS revealed a series of emails and reports tracking the actions of what they referred to as "black supremacist extremists attempting to violently co-opt the upcoming" national Democratic and Republican party conventions.[174] In short, the participation of the fusion centers in organized counterterrorism surveillance against Black Lives Matter[175] and other organizations[176] demonstrates the potential for fusion centers to burden the political speech of people exercising their constitutionally protected rights "to assemble, and to petition the Government for a redress of grievances."[177]

Impermissible Bias Against Race and Religion. Some critics have also expressed concern that what is "driving the suspicion [in some SAR reports] is not the photography, but bias against the person taking the picture."[178] While the Functional Standard technically does not allow for the use of constitutionally

down on Occupy, THE GUARDIAN (Dec. 29, 2012), https://www.theguardian.com/commentisfree/2012/dec/29/fbi-coordinated-crackdown-occupy [https://perma.cc/3L8V-AZYM] (discussing how fusion centers supported FBI investigations of Occupy Wall Street as documented in a 2012 FOIA disclosure of FBI documents to the Partnership for Civil Justice Fund).

173. George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, THE INTERCEPT (July 24, 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/ [https://perma.cc/Z28L-9JGG].

174. Sweta Vohra, *Documents Show US monitoring of Black Lives Matter*, ALJAZEERA (Nov. 28, 2017), https://www.aljazeera.com/news/2017/11/documents-show-monitoring-black-lives-matter-171128110538134.html [https://perma.cc/W93M-8C2E].

175. Adam Johnson, *5 Examples of Our Government Treating BlackLivesMatter Movement Like a Terrorist Group*, ALTERNET (Apr. 27, 2015), https://www.alternet.org/news-amp-politics/5-examples-our-government-treating-blacklivesmatter-movement-terrorist-group [https://perma.cc/SZ5H-STVP] (discussing five examples of police surveillance of Black Lives Matter activity, with at least two such instances directly involving the participation of regional fusion centers).

176. Curtis Waltman, *Homeland Security Reports Show Overwhelming Focus on Violence from the Left, While Downplaying Threat from White Supremacists*, MUCKROCK (Jan. 8, 2018), https://www.muckrock.com/news/archives/2018/jan/08/fusion-centers-antifa/ [https://perma.cc/E39E-3WU9] (discussing the involvement of fusion centers in monitoring Antifa across various jurisdictions, including Kentucky, California, and Nevada).

177. U.S. CONST. amend. I; *See* Matthew A. Wasserman, *First Amendment Limitations on Police Surveillance: The Case of the Muslim Surveillance Program*, 90 N.Y.U. L. REV. 1786, 1791–98 (2015) (describing how the NYPD Muslim surveillance program and other domestic intelligence programs burden Muslim's First Amendment rights); Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,*" 58 B.U. L. REV. 685, 694–705 (1978) (analyzing the chilling effect of governmental action on First Amendment conduct generally).

178. Steve Gorman, *ACLU Faults 'Suspicious Activity' Reporting by Law Enforcement* Reuters (Sept. 19, 2014 10:10 P.M.), https://www.reuters.com/article/us-usa-security-profiling/aclu-faults-suspicious-activity-reporting-by-law-enforcement-idUSBRE98J01N20130920 [https://perma.cc/LTJ2-UWMG] (quoting the ACLU's Michael German).

protected categories in an analyst's or trained investigator's determination of suspicion, some reports entering the system suggest a reliance on these biases. This problem seems to occur throughout the SAR lifecycle, including the "gathering and processing," "analysis and production," and "dissemination" stages described in Part II.B.

By way of example, a series of incidents and reports reveal how anti-Muslim bias may influence the conduct of various actors across the SAR lifecycle. Beginning first at the planning stage, some centers have expressly advised targeting individuals for being Muslim. In 2009, a fusion center in Texas circulated a bulletin calling upon "law enforcement officers to report activities such as Muslim 'hip hop fashion boutiques, hip hop bands, use of online social networks, video sharing networks, chat forums and blogs'" because, in the view of the center, Muslim lobbying groups provided "an environment for terrorist organizations to flourish."[179] At the collection phase, similar anti-Muslim biases have surfaced. In 2012, reacting to the frequency with which individuals were described as "Muslim" in a batch of released SARs, Asian Americans Advancing Justice claimed that "Islamophobia and prejudice [were] powerful forces in the federal government's counter-terrorism programs."[180] In addition, once such reports are submitted to a fusion center for vetting and dissemination, analysts do not appear to consistently reject the improper use of religion in determining what constitutes valid suspicion. Some reports, for example, have relied on the presence of actual or perceived connections to Islam, including the documenting and sharing of (1) "information about reading suggestions by a Muslim community group," (2) "information about a U.S. citizen lecturing at a mosque," and (3) "a report on a Muslim organization hosting a daylong seminar on marriage."[181] Importantly, Muslim communities, perceiving that they are unfairly targeted for law enforcement harassment, are unlikely to view law enforcement as legitimate or to cooperate in legitimate law enforcement activities.[182]

The system has similarly demonstrated a bias against people of color. For example, an analysis of Suspicious Activity Reports stemming from the Mall of

179. THE CONST. PROJECT, RECOMMENDATIONS FOR FUSION CENTERS: PRESERVING PRIVACY & CIVIL LIBERTIES WHILE PROTECTING AGAINST CRIME & TERRORISM 10 (2012), https://constitutionproject.org/pdf/fusioncenterreport.pdf [https://perma.cc/FN6E-9HGK] (quoting NORTH CENT. TEX. FUSION SYSTEM, *Prevention Awareness Bulletin* (Feb. 19, 2009), https://www.privacylives.com/wp-content/uploads/2009/03/texasfusion_021909.pdf [https://perma.cc/ZT8R-4C8R]).

180. Yaman Salahi, *Islamophobia a Major Force in Suspicious Activity Reporting Program*, ASIAN AMERICANS ADVANCING JUSTICE (Sept. 19, 2013), https://www.advancingjusticealc.org/news_and_media/islamophobia-a-major-force-in-suspicious-activity-reporting-program/ [https://perma.cc/TLV5-ULU2].

181. *See* PRICE, *supra* note 62, at 26.

182. Tom R. Tyler, Stephen J. Schulhofer & Aziz Huq, *Legitimacy and Deterrence Effects in Counter-Terrorism Policing: A Study of Muslim Americans*, 44 LAW & SOC'Y REV. 365, 368–69 (2010) (suggesting, based on interviews with Muslim Americans in New York City between March and June 2009, that the perception of procedural justice in policing has a "robust correlation" with a population's likeliness to cooperate and report).

America security office in Minneapolis, Minnesota showed that nearly two thirds of their reports involved non-whites.[183] The Mall's security director stated that, in his opinion, his office was the "[number one] source of actionable intelligence" for the Minnesota Fusion Center.[184] In Los Angeles, similar issues have been found. A local activist group named "Stop LAPD Spying" found that "78% of SARs [filed between March 2008 and April 2012] were filed on non-whites."[185] Later, in January of 2015, the Los Angeles Inspector General made a comparable finding with respect to data from the 2013-2014 fiscal year: 67% of all SARS sent to a nearby fusion center, the Joint Regional Intelligence Center, targeted non-whites.[186]

Keeping these incidents and concerns in mind, it is also helpful to consider how the National Network of Fusion Centers has acted in reaction to civil liberties criticisms. In 2015, for example, the NNFC noted three positive improvements. First, the number of fusion centers with a formal Privacy, Civil Rights and Civil Liberties (P/CRCL) outreach plan increased from 23.6% in 2011 to 79.2% in 2015.[187] Second, by 2015, every fusion center had a P/CRCL Officer and the average tenure of these officers was over three years.[188] Third, fusion centers reported reviewing 100% of all analytic products for P/CRCL issues prior to dissemination, up from just 57% in 2013.[189] While these measures are insufficient to prevent civil liberties abuses under the Functional Standard—indeed, the 2015 report itself notes that work on this issue remains to be done—such advances seem to reflect a serious commitment to curb civil liberties violations.

183. Daniel Zwerdling, G.W. Schulz, Andrew Becker & Margot Williams, *Mall of America Visitors Unknowingly End up in Counterterrorism Reports* MPRNEWS (Sept. 7, 2011), https://www.mprnews.org/story/2011/09/02/sept11-moa-security-npr [https://perma.cc/4YC7-2CNM]; *Under Suspicion at the Mall of America* NPR (Sept. 7, 2011), http://www.npr.org/2011/09/07/140234451/under-suspicion-at-the-mall-of-america [https://perma.cc/S7AU-9LRC].

184. Zwerdling, Schulz, Becker & Williams, *supra* note 183.

185. STOP LAPD SPYING, A PEOPLE'S AUDIT OF THE LOS ANGELES POLICE DEPARTMENT'S SPECIAL ORDER 1 11 (2013), https://stoplapdspying.org/wp-content/uploads/2013/04/PEOPLES-AUDIT-UPDATED-APRIL-2-2013-A.pdf [https://perma.cc/VF4R-ZVK9] (noting information derived following a data request under the California Public Records Act made with the help of the National Lawyers Guild).

186. L.A. POLICE COMMISSION, OFFICE OF THE INSPECTOR GENERAL, REVIEW OF SUSPICIOUS ACTIVITY REPORTS, FISCAL YEAR 2013/2014, at 3 (2015), https://docs.wix static.com/ugd/b2dd23_197536b31f834289bc1cf0c94b32a40e.pdf [https://perma.cc/KL6Y-47MY] (finding 69 of 103 persons involved in a SAR with a known race were non-white); *see also* L.A. POLICE DEP'T, OFFICE OF THE INSPECTOR GENERAL, SUSPICIOUS ACTIVITY REPORTING SYSTEM AUDIT 4 (Mar. 12, 2013), https://docs.wixstatic.com/ugd/b2dd23_a000774e4074ac5da6af41f276f3d4b4.pdf [https://perma.cc/F68Z-EM2J] (finding 25 of 32 involved persons involved in a SAR with a known race were non-white).

187. DEP'T OF HOMELAND SEC., 2015 NATIONAL NETWORK OF FUSION CENTERS: FINAL REPORT 18 (2016), https://www.hsdl.org/?view&did=796365 [https://perma.cc/VY6F-5ACX].

188. *Id.* at 6, 22.

189. *Id.* at 14.

A sociological study of "trust" within fusion centers from 2015 provides a more nuanced view of how fusion centers perceive their interaction with civil liberties, and whether these improvements represent actual progress.[190] Undoubtedly, issues of civil liberties are on the minds of analysts and leadership at fusion centers around the country. These leaders have attempted to build more trusting relationships with other law enforcement, the private sector, and the public through the Department of Justice's Building Communities of Trust program.[191] Their engagement spans a broad variety of activities and suggests a genuine investment in building relationships, "supporting 'terrorism liaison officers' in police departments, operating tips hotlines and programs, engaging in outreach to the private sector for reporting threats to critical infrastructure, offering counterterrorism training sessions, and generally communicating that they are a 'one-stop shop' for data for all police investigations."[192] Moreover, interviews with center directors and analysts reflect an express commitment to defending civil liberties. As one director stated when questioned on civil liberties: "We're in compliance, complete compliance as far as our privacy policy and concern for civil rights [and] civil liberties. We have nothing to hide here."[193] In another interview, an analyst put it more emphatically, "I think it's something that's taken very seriously. I think that they've done a significant amount of training on [privacy and civil liberties], that I think everybody's very sensitive to [that idea]…if [collected information] doesn't have an intelligence need, it gets destroyed."[194]

However, the paper also notes that the reality often falls short of this rhetoric and such claims may be based on inherently biased assumptions. More specifically, the authors observed that while "the public was frequently noted as a key stakeholder with whom trust building is imperative, only a few fusion center officials recounted explicit efforts to build relationships with local communities."[195] Also, when they did so, it was not with the objective of protecting the privacy of those community members or their civil liberties. For example, one director expressed a belief that building respectful relationships with local Yemeni and Somalian communities was important because, in his opinion, such communities were bound to be connected to terrorist cells abroad.[196] While the notion of building community relationships is a sound policing practice, the underlying assumption of a higher, inherent incidence of terrorism in such commu-

190. *See Compromised Trust*, *supra* note 165, at 2 ("Overall . . . the competing interests of the multiple stakeholders served by fusion centers often hinder the efforts and good intentions of fusion center personnel in building trust with their largest stakeholder, the public.").

191. *Id.*

192. *Id.*

193. *Id.* at 5.

194. *Id.*

195. *Id.* at 6.

196. *Id.* at 6–7.

nities "is highly problematic and may, in fact, impede the development of trust between the fusion center and community members."[197]

IV.
PATH TO IMPROVING SARS

A. Litigation

While the SAR Program serves an important national security function, it suffers from the myriad problems described in Part III. Litigation may provide one avenue for reform. Given the difficulty, however, of establishing intentional First Amendment and Fourteenth Amendment violations, and the facially neutral policies currently in place, it may be very difficult for plaintiffs to challenge the SAR Program in court. A preliminary analysis of these litigation strategies suggests internal reforms may be more effective and timelier in resolving the issues described in Part III.

i. The Free Exercise Clause of the First Amendment

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[198]

The Free Exercise Clause provides the most appropriate First Amendment challenge to suspicious activity reporting on religious discrimination grounds.[199] Plaintiffs could choose to bring a facial claim against the Functional Standard. Assuming for the purposes of this article that the FS is a final rule with legal enforcement powers, plaintiffs would nonetheless have some difficulty bringing a facial challenge given the language of the Standard. The Free Exercise Clause protects against laws that "impose[] special disabilities on the basis of ... religious status."[200] As a result, the Court typically strikes down laws or policies which directly restrict a benefit from a religious group that is otherwise enjoyed by society at large.[201] Where a law is neutral on its face, the Court more general-

197. *Id.* at 7.

198. U.S. CONST. amend. I.

199. *See generally* GOVERNMENT DISCRIMINATION: EQUAL PROTECTION LAW AND LITIGATION § 9:4 (2017)

Typically, government action interfering with religious practices had been reviewed under the free exercise clause of the First Amendment and historically accorded strict scrutiny requiring a compelling state interest for any coercion as to or interference with religion, for example, in associational activities, compliance with neutral state laws, conscientious objection to militarism, dress or appearance, missionary activities, organizational membership, preferential hiring by religious entities, Sabbath and other worship rituals, and other areas where the action carries such an effect. *Id.*

200. Church of Lukumi Babalu Aye, Inc. v. Hialeah, 508 U.S. 520, 533 (1993) (internal quotation marks omitted).

201. *See, e.g.*, McDaniel v. Paty, 435 U.S. 618, 628 (1978) (striking down a Tennessee stat-

ly rejects Free Exercise claims.[202] Here, the Functional Standard not only does *not* target a religious subgroup on its face, but it explicitly states that targets cannot be found suspicious on the basis of their religion.[203] Thus, a facial claim seems improbable.

Where a facial claim is unavailable, however, litigants could argue that the Functional Standard's enforcement creates an undue burden on their practice of religion. A recent case before the Supreme Court, *Lukumi*, is instructive on this point.[204] In *Lukumi*, the Court found that the city of Hialeah had passed an ordinance not for the proffered public safety rationale, but to prohibit sacrificial rituals integral to the plaintiffs' religion and distasteful to city residents.[205] The evidence in the case established the city's discriminatory purpose. Thus, like the defendant city in *Lukumi*, a Muslim plaintiff, for example, could choose to argue that the PM-ISE and DOJ had a discriminatory purpose in passing the Functional Standard, which, in turn, has led to their community's "unequal treatment."[206] The plaintiff would want to show that the discrimination stemming from the FS burdened, embarrassed, and harmed innocent Muslims in myriad ways (e.g., direct contact with plaintiffs through search, seizures, and/or questioning prompted by ISE-SARs; law enforcement's contact with other members of the plaintiffs' community causing a reputational injury; the sharing of reports and intelligence information about plaintiffs with other law enforcement and private parties).

In the recently settled case *Raza v. City of New York*, we can find an analogue for this claim that is helpful in understanding a theory under the Free Exercise clause.[207] Here, the ACLU claimed that New York operated a surveillance program under the "unconstitutional premise that Muslim beliefs and practices are a basis for law enforcement scrutiny" and asked for relief under the Free Exercise Clause.[208] As alleged in the original complaint, the New York Police De-

ute disqualifying ministers from serving as delegates to the State's constitutional convention).

202. *See, e.g.*, Employment Div., Dept. of Human Resources of Oregon v. Smith, 494 U.S. 872 (1990) (rejecting a Free Exercise claim brought by two members of a Native American church who were denied unemployment benefits because they had violated Oregon's drug laws by ingesting peyote for sacramental purposes); Lyng v. Northwest Indian Cemetery Protective Association, 485 U.S. 439 (1988) (holding that the government's harvesting of timber and road construction did not violate the Free Exercise clause even though such actions would obstruct the religious practices of Native Americans).

203. *See* FS 1.5.5, *supra* note 37, at 10 (prohibiting analysts from considering "race, ethnicity, gender, national origin, *religion*, sexual orientation, or gender identity" in their assessments of SARs) (emphasis added).

204. *Lukumi*, 508 U.S. at 536 ("Again, the burden of the ordinance, in practical terms, falls on Santeria adherents but almost no others").

205. *Id.* at 532–33.

206. *Id.* at 534 (internal quotation marks removed).

207. Hina Shamsi, *Revised Settlement Means Even Stronger Protection from NYPD Surveillance for New York's Muslims,* AM. CIVIL LIBERTIES UNION: SPEAK FREELY BLOG (Mar. 6, 2017), https://www.aclu.org/blog/national-security/privacy-and-surveillance/revised-settlement-means-even-stronger-protection [https://perma.cc/9LMG-4L92].

208. *Raza v. City of New York – Legal Challenge to NYPD Muslim Surveillance Program*, AM. CIVIL LIBERTIES UNION (Aug. 3, 2017), https://www.aclu.org/cases/raza-v-city-new-york-

partment (NYPD) "singled out Muslim religious and community leaders, mosques, organizations, businesses, and individuals for pervasive surveillance that [was] not visited upon the public at large or upon institutions or individuals belonging to any other religious faith."[209] The plaintiffs argued that this policy placed "a substantial burden on Plaintiffs' religious exercise in the practice of their faith" and "unjustifiably subjected Plaintiffs to adverse treatment because of their religion."[210] The City of New York and the NYPD denied all of the plaintiffs' claims.[211] Ultimately, the parties reached an approved settlement in federal court which, though stipulating no admission of guilt on behalf of the defendants, subjected the defendants to a revised consent decree founded upon a companion case, *Handschu*.[212] The consent decree will "prohibit overly broad, open-ended investigations; require that investigations account for their potential impact on religious activity; and limit their use of undercovers and informants."[213]

The comparison to *Raza* helps illustrate the challenges litigants may encounter in bringing a Free Exercise claim. First, presumably unlike *Raza*, the Functional Standard and its supporting reports have documented efforts to address civil liberties violations. Hence, by comparison, litigants would be at a disadvantage when attempting to demonstrate that the government intended to burden practicing Muslims.[214] Second, as was evidenced in the *Raza* litigation, there is an ever-present concern that the compelling interest of national security would outweigh the burden placed on Muslims.[215] Third, the litigation itself may take years. In *Raza*, nearly four years passed between the filing date of the first complaint (June 18, 2013) and the date of the approved settlement (March 20, 2017).[216] Fourth, the volume and detail of alleged facts necessary to establish a

---

legal-challenge-nypd-muslim-surveillance-program [https://perma.cc/8HPF-GC6V].

209. Complaint at 1, Raza v. City of New York, 998 F. Supp. 2d 70 (E.D.N.Y. 2013) (No. 13–CV–3448).

210. *Id.* at 30–31.

211. Answer of Defendants, *Raza* 998 F. Supp. 2d 70 (No. 13–CV–3448), https://www.aclu.org/legal-document/raza-v-city-new-york-defendants-answer [https:// perma.cc/RZ5Q-NXCV].

212. Stipulation of Settlement and Order at 3–5, *Raza*, 998 F. Supp. 2d 70 (No. 13–CV–3448), https://www.aclu.org/legal-document/raza-v-city-new-york-order-approving-stipulation-settlement [https://perma.cc/7DGE-75PT] (binding parties to the revised consent decree set forth in the companion case, *Handschu*, and attached to Judge Chen's order as Exhibit A).

213. *See* Shamsi, *supra* note 207.

214. *See* Ashcroft v. Iqbal, 556 U.S. 662, 677 (2009) (stating claims of "invidious discrimination in contravention of the First and Fifth Amendments . . . the plaintiff must plead and prove that the defendant acted with discriminatory purpose"); *see also infra* Part A.ii ii. The Equal Protection Clause of the Fourteenth Amendment. (discussing of intent).

215. *See* Cutter v. Wilkinson, 544 U.S. 709, 722, (2005) (recognizing that compelling interests can, at times, override religious beliefs even where protected by the Free Exercise Clause); *see also* Thomas v. Review Bd. of Indiana Emp. Sec. Div., 450 U.S. 707, 718 (1981) (noting that the government "may justify an in-road on religious liberty [only] by showing that it is the least restrictive means of achieving some compelling state interest").

216. *Compare* Complaint, *supra* note 209, *with* Updated Joint Stipulation of Settlement, *Ra-*

pattern like the one in *Raza* may require tremendous efforts by investigative journalists and the broad use of Freedom of Information Requests, a time-consuming and resource intensive process.[217] Fifth, as there are many agencies—over 18,000 local, state, federal, and tribal agencies—involved with the SAR Program, and many more jurisdictions affected by the program than in *Raza*, this added complexity would present significant procedural hurdles for any potential litigants. Lastly, class certification may be an issue as the potential litigants affected by the SAR Program may be more diverse than those in *Raza* in terms of their issues and interactions, and thus it may be difficult for them to certify effectively in bringing comprehensive litigation against the program.[218]

ii. The Equal Protection Clause of the Fourteenth Amendment

[N]or shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.[219]

In addition to a Free Exercise claim, potential plaintiffs may consider an Equal Protection Clause claim, as the two are complementary. The literature in this area and publicly available SARs suggest some compelling facts around which to frame an Equal Protection Clause claim. When considering the explicit or clear racial bias of a law or government policy, the Equal Protection Clause requires judges to apply the "most rigid scrutiny."[220] Under this "strict scrutiny" standard, the policy can only survive where it serves a "compelling government interest" and is "narrowly tailored."[221] This challenging standard requires a "searching examination" and ultimately places a high burden on the government to show that its racial classification was "clearly identified and unquestionably legitimate."[222] In contrast, where explicit racial classifications are not at issue, the Court applies a lower constitutional standard: the rational basis test.[223] Here

za, 998 F. Supp. 2d 70 (No. 13–CV–3448).

217. See *Factsheet: The NYPD Muslim Surveillance Program*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program [https://perma.cc/P6SV-DJZP] (last visited Jan. 20, 2019), for details on the preciseness of, and factual support for, the claims against the City of New York's police in *Raza*.

218. *See* FED. R. CIV. P. 23; *see also* Tyson Foods, Inc. v. Bouaphakeo, 136 S. Ct. 1036, 1045–49 (2016) (discussing the use of statistical models to buttress anecdotal proof of sufficiently common questions of law and fact among class members for the purposes of certification); Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 348–61 (2011) (discussing issues pertaining to the commonality requirement of F.R.C.P. 23).

219. U.S. CONST. amend. XIV.

220. *See, e.g.*, Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 227 (1995); Loving v. Virginia, 388 U.S. 1, 11 (1967).

221. Grutter v. Bollinger, 539 U.S. 306, 343 (2003) ("In summary, the Equal Protection Clause does not prohibit the Law School's narrowly tailored use of race in admissions decisions to further a compelling interest in obtaining the educational benefits that flow from a diverse student body.").

222. Fisher v. Univ. of Texas at Austin, 570 U.S. 297, 310 (2013).

223. *See* U. S. Dep't of Agric. v. Moreno, 413 U.S. 528, 533 (1973) ("Under traditional

the Court requires only that the legislation or policy be "rationally related to a legitimate state interest."[224] This standard is substantially easier for the government to satisfy but it must have some specificity.[225]

Because the rational basis test strongly favors the government, a plaintiff is likely to argue that "strict scrutiny" should nonetheless apply in the court's assessment of a facially neutral statute. Importantly, however, while plaintiffs may draw on data to demonstrate a correlation between state action and its consideration of race, such proof alone is insufficient to require that a court apply strict scrutiny and invalidate a statute or policy as unconstitutional. In other words, "disproportionate impact" alone is insufficient.[226] Rather, in such circumstances, a plaintiff must prove that the defendants acted with a "racially discriminatory intent or purpose."[227] Because people who discriminate in this fashion often seek to hide their unscrupulous conduct, it can be "extremely difficult to prove intent to discriminate."[228] Moreover, there is still some question as to the kind of proof that sufficiently substantiates intent.[229] Hence, the intent inquiry is often insurmountable for plaintiffs.

---

equal protection analysis, a legislative classification must be sustained, if the classification itself is rationally related to a legitimate governmental interest."); Williamson v. Lee Optical of Oklahoma Inc., 348 U.S. 483, 491 (1955); *see also* Thomas B. Nachbar, *The Rationality of Rational Basis Review*, 102 VA. L. REV. 1627 (2016) (describing the elements of rational basis review).

224. Lawrence v. Texas, 539 U.S. 558, 579 (2003) (O'Connor, J., concurring); Cleburne v. Cleburne Living Ctr., Inc., 473 U.S. 432, 440 (1985); Moreno, 413 U.S. at 534.

225. *See, e.g.*, Gomillion v. Lightfoot, 364 U.S. 339, 342 (1960) (finding that an Alabama statute failed because the Court could not identify a legitimate interest in the statute's redrawing of the Tuskegee city map to exclude nearly every black resident from the city).

226. Washington v. Davis, 426 U.S. 229, 239 (1976) (noting that the Court's "cases have not embraced the proposition that a law or other official act, without regard to whether it reflects a racially discriminatory purpose, is unconstitutional solely because it has a racially disproportionate impact").

227. Village of Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 265 (1977); *see also* Henry L. Chambers, *Retooling the Requirement under the Fourteenth Amendment*, 13 TEMP. POL. & CIV. RTS. L. REV. 611, 611 (2004) ("[T]he intent requirement the Supreme Court has installed as a trigger for strict scrutiny review of state action under the Equal Protection Clause of the Fourteenth Amendment is not consistent with the Amendment's principles.").

228. Michael Martin, *The Difficulties of Proving Housing Discrimination*, NPR (Feb. 8, 2013 12:00 PM), https://www.npr.org/2013/02/08/171478361/the-difficulties-of-proving-housing-discrimination [https://perma.cc/M63L-3CFT]; *see also* K.G. Jan Pillai, *Shrinking Domain of Invidious Intent*, 9 WM & MARY BILL OF RTS. J. 525, 530 (2001) (observing that "the challengers' burden of proof under the [modern intent] rule is so insurmountable that in most cases they cannot establish invidious intent"); Gayle Binion, *Intent and Equal Protection: A Reconsideration*, 1983 SUP. CT. REV. 397, 403 (1983) ("Because it must be shown that the decisionmakers were motivated by that which they deny, the plaintiffs must prove them to be liars."); Alan Freeman, *Racism, Rights and the Quest for Equality of Opportunity: A Critical Legal Essay*, 23 HARV. C.R.-C.L L. REV. 295, 306–08 n.22–35 (1988) (describing the retreat of "substantive anti-discrimination law" and the growing focus on "intent").

229. *See* Julia Kobick, *Discriminatory Intent Reconsidered: Folk Concepts of Intentionality and Equal Protection Jurisprudence*, 45 HARV. C.R.-C.L L. REV. 517, 529–532 (2010) (discussing how the foreseeability of the harm caused by the discriminatory law or policy impacts the intent inquiry).

In the case of the SAR Program, it is difficult to assess a potential litigant's ability to demonstrate racially discriminatory intent. At first, litigants would want to attempt to show that "decisionmakers placed substantial negative reliance on an illegitimate criterion in reaching their decision"[230] Remarks by officials at the PM-ISE or DOJ that were "contemporaneous with the [Functional Standards] or causally related to the [Functional Standards'] decision making process" would be a strong indicator of such bias.[231] Alternatively, plaintiffs would want to investigate these issues further and identify any publicly available evidence that could preliminarily substantiate the *Arlington Heights* factors for intent.[232] Hence, in addition to contemporaneous statements from the FS drafters, litigants would want to find examples relevant to the SAR Program's disparate impact, historical background, recent events, and changes in SAR procedures or substantive rules that may evince a discriminatory intent.[233] As described in Part II.B.iii, *supra*, this paper documents various reports, academic papers, and Freedom of Information Act requests that could be marshalled for that purpose. Regardless, considering the overwhelmingly high standard required under the *Arlington Heights* factors, this would seem to be a challenging task,[234] and so potential litigants would be wise to consider the quantum of evidence found sufficient in recent cases.[235]

B. Policy

While litigation provides one avenue for reforming the Functional Standard and the SAR Program, significant improvements might also be achieved by working within the existing program to address the shortfalls described in Part III. What follows is a list of salient recommendations derived from the publications and reports of relevant academic, government, and non-profit entities that regularly engage with the SAR Program. As with any large government program, there exists here the possibility that structural issues, such as implicit bias,

230. Price Waterhouse v. Hopkins, 490 U.S. 228, 277 (1989) (O'Connor, J., concurring).

231. Kennedy v. Schoenberg, Fisher & Newman, Ltd., 140 F.3d 716, 723 (7th Cir. 1998) (citations omitted).

232. *See Arlington Heights*, 429 U.S. at 266–68 (1977) (discussing the factors for intent which include, among others, the disproportionate impact of the challenged decision on one race, the historical background of similar decisions by the government, the events leading up to the decision, and the legislative history of the decision).

233. *See* Abbott v. Perez, 138 S. Ct. 2305, 2346–49 (2018) (Sotomayor, J., dissenting) (describing and applying *Arlington Heights* factors in case pertaining to Texas's redistricting plans).

234. *See* David Kairys, *Unexplainable on Grounds Other Than Race*, 45 AM. U. L. REV. 729, 731 (1996) (describing the "near impenetrable brick wall" of establishing an equal protection claim for racial minorities).

235. *See, e.g.*, Avenue 6E Invs., LLC v. City of Yuma, 818 F.3d 493, 509 (9th Cir. 2016) (reversing district court's summary judgment dismissal and finding developer sufficiently alleged Equal Protection claims against City of Yuma after the City denied the developer's rezoning request based on "public hearings filled with what a reasonable jury could interpret to be racially tinged code words," among other potential evidence of racial bias).

may undermine the effectiveness of internal reforms.[236] Nonetheless, given the risks and roadblocks of litigation, these internal reforms may promise faster, more effective solutions to contemporary criticisms of the SAR Program.

i. Heightening the Legal Standard for Suspicion

As described above, the collection of Suspicious Activity Reports, and their subsequent dissemination, purposefully do not follow the traditional Fourth Amendment standards of reasonable suspicion or probable cause.[237] Instead, an officer's notes of innocuous conduct may substantiate the Functional Standard's requisite "nexus," thereby branding a potentially innocent video gamer as a terrorist.[238] As a result, the government is able to collect large amounts of information on the unknowing public, despite the concern that this, like other large data collection programs, might "eclipse longstanding civil rights protections."[239] Consequently, the Functional Standard's low threshold for suspicion admits SARs that, as a result, may perpetuate negative stereotypes, harm people of color, and violate people's privacy and civil liberties.[240] Heightening the legal standard required for submitting and then disseminating reports as ISE-SARs to reasonable suspicion would have the important effects of lessening "white noise" and restoring constitutional protections to the government's scrutiny of its citizens.

ii. Improving Data Management and Integrity

As the volume of data collected and published through the Information Sharing Environment increases, the issues identified in Part III may correspond-

236. For example, research shows that reducing implicit bias requires immersing oneself in regular contact and making positive connections with people from different and diverse groups, which might be especially hard in the context of on-duty law enforcement. *See* Thomas F. Pettigrew & Linda R. Tropp., *A Meta-Analytic Test of Intergroup Contact Theory*, 90 J. PERSONALITY & SOC. PSYCHOL. 751, 766 (2006), http://www.iaccp.org/sites/default/files/pettigrew_tropp_2006_contact_theory_0.pdf [https://perma.cc/C5E8-CMBW]. For further research on implicit bias in law enforcement contexts, see LORIE A. FRIDELL, PRODUCING BIAS-FREE POLICING 7–30 (1st ed., 2017); Katherine B. Spencer, Amanda K. Charbonneau & Jack Glaser, *Implicit Bias and Policing*, 10 SOC. & PERSONALITY PSYCHOL. COMPASS 50 (2016), https://gspp.berkeley.edu/assets/uploads/research/pdf/SpencerCharbonneauGlaser.Compass.2016.pdf [https://perma.cc/JN3F-E8NM].

237. *See supra* Part III.0.

238. Tim Cushing, *Lawsuit Over DHS First Amendment-Violating Suspicious Activity Reports Given Green Light by Judge*, TECHDIRT (Mar. 13, 2015, 2:54 PM), https://www.techdirt.com/articles/20150225/09584130140/lawsuit-over-dhs-first-amendment-violating-suspicious-activity-reports-given-green-light-judge.shtml [https://perma.cc/Q4BB-S52U] ("Unemployed. Doesn't hang out with cops. Plays games and uses the internet. All inherently suspicious because of this tenuous thread: the 9/11 terrorists used flight simulators to train for their attacks.").

239. *See* John Podesta, Penny Pritzker, Ernest J. Moniz, John Holdren & Jeffrey Zients, EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES iii (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf [https://perma.cc/9LLY-TACH].

240. *See supra* Part III.0.

ingly increase. Careful data management, already a critical factor in the ISE's success, will only become more imperative. One potential solution lies in a back-to-basics approach of revising and improving the current data management system pursuant to the time-tested Fair Information Practice Principles (FIPPs).[241] The National Public Safety Partnership (NPSP)[242] recently announced a series of data management recommendations applicable to fusion centers based on the FIPPs.[243] Drawing on the NPSP's recommendations, this subsection addresses three ideas that can help root out bias, diminish the program's threat to privacy, and make SAR-ISEs more reliable.

Greater Scrutiny for SARs with PII. The NPSP recommends that fusion centers "ensure that a valid lawful purpose exists and is documented for all collection of PII."[244] PII could include, for example, a person's race. This recommendation implicitly reinforces a central prohibition within the Functional Standard, which seems to lack consistent enforcement in light of the publicly released SARs: "factors such as race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion."[245] By requiring that any mention of PII be reviewed to ensure that a "valid lawful purpose exists" for its collection, the NPSP seems to implicitly acknowledge that PII may have been collected for inappropriate reasons in the past. This additional review could entail a second opinion from a peer analyst and require an additional superior's approval. Where a "valid lawful purpose" is identified and the information is then retained, the lawful purpose should be documented and written down by the corresponding analyst for posterity and to ensure compliance.

Thinking one step ahead, however, this requirement might not address the underlying issue of bias given the Supreme Court's caselaw on pretextual

241. FIPPs are a 5-point framework for ensuring that any organization's data management practice is fair and provides adequate information privacy protection. The concept was originally proposed as the "Code for Fair Information Practices" by the United States Secretary's Advisory Committee on Automated Personal Data Systems (ACAPDS) in 1973. *See generally* ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, PUB. NO. (OS) 73-94, COMPUTERS, AND THE RIGHTS OF CITIZENS xx (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/8CTK-HYTA].

242. As noted on the PSP website, this body is led by the Attorney General and was created following the Presidential Executive Order on a Task Force on Crime Reduction and Public Safety. *See About*, NAT'L PUB. SAFETY PARTNERSHIP, https://www.nationalpublicsafetypartnership.org/#about [https://perma.cc/ELM5-WPZE] (last visited Jan. 20, 2019); *see also* Exec. Order No. 13,776, 82 Fed. Reg. 10,699 (Feb. 9, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-task-force-crime-reduction-public-safety/ [https://perma.cc/W43C-HAZG].

243. *See* NAT'L PUB. SAFETY PARTNERSHIP (PSP), THE FAIR INFORMATION PRACTICE PRINCIPLES (FIPPS) IN THE INFORMATION SHARING ENVIRONMENT (ISE) [hereinafter NPSP FIPPS RECOMMENDATIONS] https://www.nationalpublicsafetypartnership.org/Documents/The_Fair_Information_Practice_Principles_in_the_Information_Sharing_Environment.pdf (last visited Jan. 20, 2019).

244. *Id.* at 1.

245. *See* FS 1.5.5, *supra* note 37, at 10–11.

searches and other police activity.[246] If officers come to know that their reports will be more heavily scrutinized at the inclusion of PII (and specifically PII which mentions a suspect category), officers will be incentivized not to record PII if avoidable. Accordingly, officers who wish not to be scrutinized may offer a "pretext" for why they are writing the report and selectively leave out PII if possible. Hence, the efficacy of the NPSP's broad recommendation to increase scrutiny on SARs containing some PII may hinge upon whether pretextual conduct would survive the inquiry of a "valid lawful purpose" as understood by the NPSP and the PM-ISE.

Arguably, such conduct would be permissible for the same reasons espoused in *United States v. Whren*. In *Whren*, the Supreme Court made clear that (1) an evaluation of an officer's subjective reasoning should not preclude conduct that is otherwise objectively permissible and (2) that the court should not be engaging in the kind of state-of-mind inquiry under the Fourth Amendment that would be required to assess pretext.[247] Here, that reasoning would counsel analysts to admit pretextual reports because the standards for validating a nexus to terrorism are low, and thus it is not likely difficult to establish that a report is otherwise objectively permissible.

There is some evidence that courts may be moving away from the kind of reasoning espoused in *Whren*.[248] Moreover, the latest research supports the common sense finding that such practices dramatically reduce community trust in the police, which may be persuasive to some officers and law enforcement leadership as reasons to not rely on such practices.[249] Changes to the Court's pretext precedents, however, would dramatically upend Fourth Amendment doctrine, and are thus unlikely to protect innocent, would-be targets of a pretextual ISE-SAR. Nonetheless, while pretext may become an issue following implementation, the NPSP's recommendation as discussed here represents a positive step forward that should be implemented broadly and tracked year over year.

---

246. *See* Whren v. United States, 517 U.S. 806, 811–13 (1996); *see also* Gunar Olsen, *How the Supreme Court Authorized Racial Profiling*, HUFFINGTON POST (Jan. 25, 2016, 2:47 PM), https://www.huffingtonpost.com/gunar-olsen/how-the-supreme-court-aut_b_9061838.html [https://perma.cc/3X26-SFHK]. Importantly, this reference to *Whren* is not intended to suggest that the Fourth Amendment will govern police conduct under the SAR Program. Rather, this reference is merely an acknowledgement that the same thinking espoused in *Whren* may become an issue for assessing pretextual conduct within the SAR Program.

247. *Whren*, 715 U.S. at 812 ("[W]e never held…that an officer's motive invalidates objectively justifiable behavior under the Fourth Amendment"); *id.* at 814 ("[T]he petitioners would have us ask, in effect, whether (based on general police practices) it is plausible to believe that the officer had the proper state of mind.").

248. *See* David Schoen, *Are Courts Viewing Pretextual Searches and "Good-Faith" Exceptions More Skeptically*, AM. BAR ASS'N (Mar. 16, 2016), http://apps.americanbar.org/litigation/committees/civil/articles/031616-are-courts-viewing-pretextual-searches-good-faith-exceptions-more-skeptically.html [https://perma.cc/GG3F-F78M] (last visited Jan. 20, 2019) (describing several Courts of Appeals decisions expressing concern over the limits of *Whren*).

249. CHARLES R. EPP, STEVEN MAYNARD-MOODY, AND DONALD P. HAIDER-MARKEL, PULLED OVER: HOW POLICE STOPS DEFINE RACE AND CITIZENSHIP 142–44 (2014).

Transparency & Statutory Adherence on Data Retention. The NPSP also recommends "designing a data storage system to pull data for review and then, if appropriate, automatically purge data after the specified retention period has been reached."[250] Here, the NPSP is acknowledging another long-term concern of civil liberties advocates over data collected by the SAR Program—the length of retention. An automatic process for purging data after an appropriate amount of time would help address this concern, as long as such a rule is transparent to the public and consistent cross fusion centers.

At the moment, there is some ambiguity as to how long ISE-SARs are retained once shared, and what occurs with SARs which, though submitted to fusion centers, fail the Functional Standard and are not shared.[251] The PM-ISE should identify and communicate a policy on how long SARs are held and under what circumstances. Clarity on this issue would be of immense value because (1) the length of time that a record is held—and what happens to it while held[252]—bears on the degree of privacy harm caused to the individual, (2) the permissible length of time is subject to multiple rules and statutes that mean it may vary by jurisdiction,[253] and (3) the destruction of such records is frequently a primary remedy sought by aggrieved litigants.[254] The PM-ISE should also clarify publicly which records control schedules, under the Federal Records Control Act, gov-

250. *See* NPSP FIPPs RECOMMENDATIONS, *supra* note 243, at 2.

251. *See* AM. CIVIL LIBERTIES UNION OF N. CAL., *Gill v. DOJ (Challenge to Federal Suspicious Activity Reporting)*, https://www.aclunc.org/our-work/legal-docket/gill-v-doj-challenge-federal-suspicious-activity-reporting [https://perma.cc/X82T-XUKV] (last visited Jan. 20, 2019) ("SARs can haunt people for decades, as they remain in federal databases for up to 30 years"); *see also Suspicious Activity Reporting*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/suspicious-activity-reporting/default.html [https://perma.cc/53FH-3VP6] (last visited Jan. 20, 2019) ("In the event that no potential terrorist threat is found, the suspicious activity report can still be retained in local fusion centers or federal agency files in accordance with retention policies and rules.").

252. Gill v. Dep't of Justice, No. 14-CV-03120-RS, 2015 WL 757278, at *4 (N.D. Cal. Feb. 20, 2015)

> The allegations of the complaint, however, show that the gravamen of the alleged injuries lie not in actions of 'front line' authorities standing alone, but in the fact that those authorities, pursuant to the guidance and training provided by defendants, submit SAR reports under criteria and circumstances that are allegedly inconsistent with legal principles and policies embodied in other law. Plaintiffs' cognizable challenge is not to the conduct of law enforcement or private security officers during the alleged encounters per se, although there is at least some implication that plaintiffs believe Defendants' Standards lead front line personnel to overreach even at the point of making initial observations. Plaintiffs are claiming injury from what occurs after the encounters, pursuant to the Standards.

Id.; *see also* FS 1.5.5, *supra* note 37, at 36 (recognizing that purge policies vary from jurisdiction to jurisdiction).

253. *See* DEP'T OF HOMELAND SECURITY, PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES POLICY TEMPLATE (2010), https://it.ojp.gov/documents/d/Fusion%20Center%20Privacy%20Policy%20Development.pdf [https://perma.cc/Z7M5-BF5A] (noting in the policy sample language that retention periods would be impacted by center policy, local and state law, and federal regulation 28 CFR Part 23).

254. *See* Douglas Cox, *"I Want My File": Surveillance Data, Minimization, and Historical Accountability*, 51 U. OF RICH. L. REV. 827, 827 n.1 (2017) (cataloging cases where plaintiffs have sought the destruction of the records or communications at issue).

ern Suspicious Activity Reports, whether uploaded to the ISE or not, as these schedules govern the retention of certain agency records.[255] As has been documented in other information management programs operated by the intelligence and law enforcement communities, efforts to evade federal record keeping laws have not been uncommon and strict adherence to this statute is crucial.[256]

Increased Individual Involvement. The NPSP also recommends, "as appropriate, [c]ollecting information directly from the individual, to the extent possible and practical" and "[p]roviding the individual with the ability to find out whether a project maintains a record relating to him or her, and if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial."[257] This recommendation has the potential to make a valuable impact on the legitimacy and transparency of the SAR process by better involving the public and by validating their rights.

First, as many fusion center personnel are keenly aware, most of the public is either unaware of, or fails to understand, fusion centers and the suspicious activity reporting process.[258] This may be, in part, a by-product of fusion centers' apparent failure to communicate their impact on law enforcement effectively.[259] However, regardless of the reason, the perceived secretiveness of fusion centers naturally has the effect of creating distrust in the public and skepticism that fusion centers are doing a good job. Hence, if officers were able to directly engage the potential subjects of a Suspicious Activity Report (which already happens in some cases) and explain that they are filing a report, this would increase the public's awareness of fusion centers. In addition, this would give officers an opportunity to explain the counterterrorism value of big data collection, the protections for privacy/civil liberties that are currently in place within the SAR Program, and

---

255. *See* 44 U.S.C. § 3101 (2012)

> The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

Id.

256. *See* Cox, *supra* note 254, at 834–38 (discussing several procedures for evading record-keeping regulations including "Do Not File" procedures, nonrecords, and "approved" destruction).

257. *See* NPSP FIPPS RECOMMENDATIONS, *supra* note 243, at 4.

258. *See Compromised Trust*, *supra* note 165, at 4

> Uncertainty abounds for fusion center personnel regarding stakeholders' knowledge of fusion centers and the unique role they play in the intelligence community. Our interviews revealed a nearly ubiquitous concern among fusion center personnel that some stakeholders, particularly the public, do not understand what fusion centers are or do not perceive fusion centers as an effective and necessary element of counterterrorism and crime prevention in the U.S.

Id.

259. *See* Jeremy G. Carter, Carla Lewandowski & Gabrielle A. May, *Disparity Between Fusion Center Web Content and Self-Reported Activity*, 41 CRIM. JUST. REV. 335, 347 (2016), http://journals.sagepub.com/doi/pdf/10.1177/0734016816651925 [https://perma.cc/VJ4C-X4S2] ("Put simply, fusion centers are short selling their contribution to the law enforcement intelligence Landscape.").

the ways in which the public can interact with fusion centers. In addition, encouraging officers to engage with individuals about whom they are writing reports would put pressure on SLTT participants to learn more about the fusion center network and to develop stronger inter-agency relationships—a critical counterterrorism success factor missing from today's fusion centers.[260]

Second, this would greatly improve the sense of agency that individuals have with respect to the Suspicious Activity Reporting program. Public perceptions of modern government tools and practices for data collection have worsened as people have felt that there is no viable redress for such programs and then, in turn, begin to equate such programs with the proverbial "Big Brother."[261] The SAR Program, specifically, has been criticized for failing to give targets more direct access to its procedures.[262] For these reasons, the NPSP recommendation to collect information directly from the target where possible

260. *See* Jeremy G. Carter, David L. Carter, Steve Chermak & Edmund McGarrell, *Law Enforcement Fusion Centers: Cultivating an Information Sharing Environment while Safeguarding Privacy*, 32 J. OF POLICE & CRIM. PSYCHOL. 11, 23 (2017), https://link.springer.com/content/pdf/10.1007%2Fs11896-016-9199-4.pdf [https://perma.cc/4V44-8B9E]

> At the heart of effective threat prevention, mitigation and response is two-way information sharing among all agencies that have a responsibility for the safety, security and sustained functionality of America's communities. To this end, if processes are not developed to ensure full participation of all information sharing partners, the functional capability of the fusion centers will be reduced. Sampled fusion center personnel indicated efforts to develop relationships with different agencies; especially other law enforcement agencies and a more diverse range of public safety, private sector, and public health organizations. To achieve their goals, these partnerships need to be broadened and substantively sustained. While it is achievable, it is a difficult barrier to overcome.

Id.

261. *See Study: Violations of Privacy Rights by Fusion Centers are the Exception, not the Rule,* SCIENCE X (July 22, 2016), https://phys.org/news/2016-07-violations-privacy-rights-fusion-centers.html#jCp [https://perma.cc/W73K-YM8J] ("Some people are concerned that fusion centers are 'Big Brother watching us' and that information is being gathered about people regardless of whether they've done anything wrong").

262. *See* DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR INFORMATION SHARING ENVIRONMENT SUSPICIOUS ACTIVITY REPORTING INITIATIVE 14 (2010), https://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise.pdf [https://perma.cc/EY8K-LTDL] ("Privacy Risk: Individuals who are the subject of ISE-SAR are not made aware of the collection of their information"); DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE 19 (2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf [https://perma.cc/6Q9S-74TS] (recommending that "DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS' use of PII."). Importantly, though there are reasons law enforcement would hesitate to give targets access to reports or engage them before making the report, it is notable that some centers have adopted similar policies to this effect in their police guidelines. *See, e.g.*, COLO. INFO. ANALYSIS CTR, PRIVACY POLICY 12 (2014), https://www.colorado.gov/pacific/dhsem/atom/59996 [https://perma.cc/LL5U-TYUH] ("Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified below, an individual is entitled to know the existence of and to review the information about the individual that has been gathered and retained by the CIAC.").

represents a timely and important policy improvement that may behoove both the public and law enforcement.

In addition to encouraging officers to engage with potential targets and the public, the NPSP also notes the importance of providing targets with information on how to identify and seek redress for being included in a report. This effectively requires two steps: notification that a fusion center or agency has created a report referencing an individual and a venue for challenging the existence and/or dissemination of that report.

In designing a model for notice and challenge for the SAR Program, it is helpful to consider how the government tracks other populations that pose a potential risk to society. Through the National Sex Offender Registry, for example, the Department of Justice keeps a centralized list of individuals recognized as sex offenders based on information provided by each state's registry and the offenders' prior commission of sex-related crimes.[263] As one example among the varying state systems, New York State protects a potential registrant's due process rights by requiring that they receive "notice and [have] an opportunity to be heard" prior to making a determination as to their placement on the registry.[264] With respect to the No-Fly List—a list operated by DHS which designates people as potential terrorists and restricts their ability to travel—notice and the opportunity to challenge are less clear.[265] On the one hand, DHS has established the Traveler Redress Inquiry Program, a service designed to help impacted people "seek resolution regarding difficulties…experienced during travel screening," including "watch list issues."[266] On the other hand, recognizing that this service offers little relief in actuality, many people have filed lawsuits challenging their nomination to the watchlist and criticizing the limited opportunities available to question potential errors in DHS nominations.[267] In a third, more lo-

263. *See National Sex Offender Registry Public Website*, DEP'T OF JUSTICE, https://www.nsopw.gov/en/home/about/ [https://perma.cc/RLU8-4KAB] (last visited Jan.1, 2019).

264. *See* People v. David W., 95 N.Y.2d 130, 133 (2000).

> Does an individual convicted of a sex offense have a constitutional right to notice and an opportunity to be heard before being classified as a sexually violent predator under the Sex Offender Registration Act (SORA)—New York's 'Megan's Law?' In the case before us, we hold that procedural due process requires that this defendant, on probation when SORA went into effect, should have received notice and an opportunity to be heard before his SORA risk level determination was made.

Id.

265. Spencer Ackerman, *How the U.S.'s Terrorism Watchlists Work – and How You Could End Up on One*, THE GUARDIAN (July 24, 2014, 5:41 PM), https://www.theguardian.com/world/2014/jul/24/us-terrorism-watchlist-work-no-fly-list [https://perma.cc/6G6S-WEQD].

266. *DHS Traveler Redress Inquiry Program (DHS TRIP),* DEP'T. OF HOMELAND SEC., https://www.dhs.gov/dhs-trip [https://perma.cc/XR53-MKEG] (last visited Jan. 1, 2019).

267. *See* Tanvir v. Tanzin, 894 F.3d 449, 452 (2d Cir. 2018) (holding that RFRA would permit plaintiffs to recover money damages against law enforcement officers for improperly placing them on the No-Fly list pending further proceedings to assess their potential, qualified immunity); Latif v. Holder, 28 F. Supp. 3d 1134, 1150 (D. Or. 2014) (recognizing that the No-Fly List "constitutes a significant deprivation of their liberty interests").

cal example, the New York Police Department's Gang Database contains information on roughly 18,000 people identified as gang-affiliated which, like the SAR Program, has raised the concern that innocent people are being targeted.[268] This database has been shrouded in secrecy, and the NYPD has provided no mechanism to determine if a person is on the list or to permit them to challenge to their inclusion.[269] Though a local public defender and criminal justice advocacy organization, the Legal Aid Society, has launched a website to help individuals file Freedom of Information Law requests, the New York State analog of FOIA, little change has been achieved as the "police have denied every one of them."[270]

Like these programs, the SAR Program creates a designation with little recourse to challenge it. Moreover, without filing a FOIA request, or having an adverse interaction with law enforcement, a person could appear on an ISE-SAR indefinitely without ever knowing it. To ensure that the people's privacy is protected and the SAR Program does not waste valuable resources tracking innocent people, DHS, the FBI, and the BJA should implement an administrative procedure (1) to notify individual targets of non-classified ISE-SARs that a report has been issued naming them, and (2) to conduct a hearing before an impartial administrative judge where targets can present evidence mitigating their suspicion.

iii. Incorporating More Processes for Tracking and Feedback

Currently, the National Network of Fusion Centers operates with a blind spot on value. While measurements of network performance focus largely on capacity, they fail to measure "bang for the buck."[271] For example, in 2012, the NNFC only tracked five key metrics in the section of the report entitled "Fusion

268. *See* Jeff Coltin, *Why Everyone is Suddenly Talking About the NYPD Gang Database*, CITY & STATE NEW YORK (June 13, 2018), https://www.cityandstateny.com/articles/policy/criminal-justice/why-everyone-suddenly-talking-about-nypd-gang-database.html [https://perma.cc/6G6S-WEQD]; Hazel Sanchez, *Critics, Community Leaders Question Use Of NYPD's Gang Database*, CBS NEW YORK (June 13, 2018, 7:19 PM), https://newyork.cbslocal.com/2018/06/13/nypd-gang-database/ [https://perma.cc/XR53-MKEG].

269. *See* Alice Speri, *New York Gang Database Expanded by 70 Percent Under Mayor Bill De Blasio*, THE INTERCEPT (June 11, 2018, 10:49 AM), https://theintercept.com/2018/06/11/new-york-gang-database-expanded-by-70-percent-under-mayor-bill-de-blasio/ [https://perma.cc/B3MU-U2V6]; Rocco Parascandola and Graham Rayman, *Advocates Suspicious of NYPD's Gang Database Standards*, DAILY NEWS (June 12, 2018, 5:00 PM), https://www.nydailynews.com/new-york/nyc-crime/ny-metro-gang-data-base-nypd-shea-advocates-20180612-story.html [https://perma.cc/84X6-UE55].

270. *See* Alice Speri, *NYPD Gang Database Can Turn Unsuspecting New Yorkers into Instant Felons*, THE INTERCEPT (Dec. 5, 2018, 12:16 PM), https://theintercept.com/2018/12/05/nypd-gang-database/; *see also Are You in a Gang Database*, LEGAL AID SOC'Y, https://legalaidfoil.backspace.com/ [https://perma.cc/HQS3-428D] (last visited Jan. 1, 2018).

271. *See* U.S. HOUSE OF REPRESENTATIVES, COMM. ON HOMELAND SEC., MAJORITY STAFF REPORT ON THE NATIONAL NETWORK OF FUSION CENTERS v (2013) [hereinafter HOUSE MAJORITY REPORT ON NNFC], https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/staff-report-on-fusion-networks-2013.pdf [https://perma.cc/FBR5-D9RN].

Center Performance": (1) percentage of centers which had conducted a privacy review each year in aggregate; (2) number of SARs vetted in 2012 which initiated or enhanced an FBI investigation; (3) percentage of fusion center analytic products that reference fusion center Standing Information Needs; (4) number of fusion center analytic products authored by two or more fusion centers; and (5) number of responses within the Network for fusion center requests for information.[272] As noted by the Majority Staff of the House of Representatives' Committee on Homeland Security, these statistics "are only a partial measure."[273] The metrics do not, for example, capture the correlation between the ratio of SARs submitted to those uploaded as ISE-SARs. The metrics do not measure the impact of the analytical products in terms of how frequently they are used, or for what purposes. The metrics do not state the percentage of reports by year which lead to actual arrests or convictions. The metrics do not provide insight into what percentage of identified and avoided terrorist plots involved the use of an ISE-SAR or, more importantly, which of those would not have been solved *without* an ISE-SAR. By creating better metrics for these outcomes, that can be tracked on an annual basis, the NNFC could better address criticisms that it is not meaningfully combating terrorism.

Metrics could also help increase accountability. For example, it would be helpful for both the public's perception of fusion centers and for the reliability of ISE-SARs if the system could identify individuals or agencies which repeatedly fail to provide information adhering to the Functional Standard. As noted, the 2012 Senate investigation into fusion center performance found that only a handful of officials accounted for a significant portion of the raw intelligence reports that were canceled by senior officials at DHS over a 13-month period for reporting on Constitutionally-protected activity.[274] This kind of analysis facilitates targeted training and sanctions, and thus should be a regularly conducted inquiry. If fusion centers could track such violations and provide that feedback to their partner agencies, the quality of their reports would necessarily improve. Similarly, being able to track officials or agencies that regularly submit reports found not to align with the 16 pre-operational behavioral categories, and then creating a regularly reported metric on this at every fusion center, would allow the NNFC to identify problem agencies, issue new trainings, hire new personnel as needed, and ultimately reduce "white noise."

272. *See* DEP'T OF HOMELAND SEC., 2012 NATIONAL NETWORK OF FUSION CENTERS: FINAL REPORT 47–51 (2013), https://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fusion%20Centers%20Final%20Report_0.pdf [https://perma.cc/MPL8-QCTF].

273. *See* HOUSE MAJORITY REPORT ON NNFC, *supra* note 271, at v.

274. *See* 2012 SENATE REPORT, *supra* note 69, at 45–46.

V.
CONCLUSION

Today's national security landscape requires that law enforcement directly confront the ever-present risk that, without warning and to mass shock, a terrorist attack could happen in any one of America's major cities. The response to that new paradigm has been to aggressively expand surveillance. Along the way, society's demand for privacy has in some ways diminished. However, there remains a clear sense that privacy is a good unto its own, and that programs administered to enhance public safety must accommodate and protect privacy. Moreover, the available data suggests that existing programs, like the SAR Program, may transgress civil liberties and disproportionately harm communities of color and religious minorities.

This paper has analyzed the origins, processes, demand for, and criticisms of the National Network of Fusion Centers and the Suspicious Activity Reporting Program. It has also proposed and evaluated potential litigation challenges and policy solutions for those criticisms. It is the author's hope that this paper encourages other scholars to dig deeper into this surveillance program and that the suggestions contained herein advance the dialogue of advocates, from government and civil society alike, who seek to develop a system that neither "abandon[s] our values [nor] giv[es] into fear."[275]

275. *See* Obama, *supra* note 1.