Article

Administration & Society
2015, Vol. 47(6) 740–762

DOI: 10.1177/0095399713513141
aas.sagepub.com
SAGE

Constructing the Suspicious: Data Production, Circulation, and Interpretation by DHS Fusion Centers

Priscilla M. Regan[1], Torin Monahan[2], and Krista Craven[3]

Abstract

Suspicious activity reports (SARs) are an increasingly important tool in the law-enforcement repertoire, especially for counterterrorism. In spite of significant problems with such reports, they are experiencing a resurgence that can be attributed partly to the institutionalization of Department of Homeland Security (DHS) "fusion centers," which are taking the lead in vetting and interpreting these reports as they enter into law-enforcement and counterterrorism databases. Based on a 3-year study of DHS fusion centers, this article reviews a range of problems with SARs and argues that robust community relationships are necessary to achieve contextually situated reports that eschew overt forms of bias.

Keywords

suspicious activity reports, fusion centers, homeland security

[1]George Mason University, Fairfax, VA, USA
[2]The University of North Carolina at Chapel Hill, USA
[3]Vanderbilt University, Nashville, TN, USA

Corresponding Author:
Priscilla M. Regan, Department of Public and International Affairs, George Mason University, 4400 University Drive, MSN 3F4, Fairfax, VA 22030-4444, USA.
Email: pregan@gmu.edu

Suspicious activity reports (SARs) occupy an interesting, ambiguous position in law-enforcement and counterterrorism practices. While they have the potential to serve as valuable tools for identifying criminal or terrorist activities for preemptive intervention, they can also invite unfounded, prejudicial claims about and investigations of innocent parties. In the construction and circulation of such reports, controls over data may also be relaxed to encourage widespread sharing, which can lead to problems with the validity of claims and privacy protections. Based on a 3-year empirical research project on Department of Homeland Security (DHS) "fusion centers," it has become apparent that SARs are increasingly important in the law-enforcement arena and that fusion centers are emerging as primary sites for vetting and interpreting these reports as they enter into law-enforcement and counterterrorism databases. Indeed, the resurgence in SARs can be attributed partly to the institutionalization of fusion centers and the corresponding search for standardized ways of collecting and sharing information.

Law enforcement has been using some form of SARs for decades, collected through a variety of mechanisms, including information received from tip hotlines, 911 calls, neighborhood watches, schools and community centers, or police in the field. In the United States and the United Kingdom, the value and reliability of such reporting have often been questioned, especially as their use expands in ways that will likely result in an overload of information of dubious quality requiring a large investment of time to investigate (American Civil Liberties Union [ACLU], 2010; Levi & Wall, 2004; Nojeim, 2009; Randol, 2009). Despite these concerns, SARs have persisted as a tool of community-oriented policing, as well as now of intelligence-led policing, and as a practical tool for collecting information and raising public awareness (Steiner, 2010). Since its creation in 2002, DHS has adopted SARs in its counterterrorism activities, with the newest SARs version being Secretary Napolitano's "If You See Something, Say Something" campaign (Reeves, 2012).

Our interviews indicate that SARs reporting is labor intensive and generally does not yield useful information.[1] As an official at one state-level fusion center related,

> A lot of our activity on the counter-terrorism side is responding to suspicious activity reports . . . I would say an overwhelming majority of the reports that we get are, once we do a little bit of checking, we can determine that they [were unfounded], that the person had a reason to be doing what they were doing—and those get closed out and we don't pursue those any further.

An official at another center estimated that the center received "in the realm of four hundred to five hundred SARs a year . . . the SARs are not necessarily all terrorism, but some are."

Despite the widely recognized limitations of SARs, the DHS and the FBI are committed to augmenting the functionality of these reports through a variety of standardized interfaces for submitting, searching, and analyzing them. By looking at the role of SARs in fusion center contexts, this article will investigate some of the problems introduced by them, the current policy landscape pertaining to them, what revisions to that landscape might be necessary, and what intelligence gathering alternatives exist.

Background

The DHS, under the Bush and Obama administrations, has supported the creation of fusion centers, with a mandate to share data across government agencies as well as across the public and private sectors. The stated goal of fusion centers is to "blend relevant law enforcement and intelligence information analysis and coordinate security measures to reduce threats in their communities" (U.S. DHS, 2006, p.1). Fusion centers are seen as a critical component of the response to the problem identified by the 9/11 commission, and within the intelligence community generally, that various agencies did not work in concert to "connect the dots" that are necessary to combat terrorism and that an environment of information sharing should be fostered (National Commission on Terrorist Attacks Upon the United States, 2004). As of 2013, there were 77 officially designated fusion centers at state and regional levels.[2] Some of these were newly created entities funded by DHS in response to terrorism concerns, while others emerged from existing law-enforcement organizations, such as the FBI's Joint Terrorism Task Force (JTTF) or the federal High Intensity Drug Trafficking Areas (HIDTA) programs (Regan & Monahan, 2013).

From their inception, fusion centers have generated concern among privacy and civil liberty advocates and scholars for a range of reasons, including their lack of transparency, the commingling of law enforcement and intelligence information and purposes, the involvement of the private sector in what have traditionally been government activities, the conflation of innocent or everyday behavior with terrorist or criminal behavior, and the widespread sharing of personally identifiable information (Electronic Privacy Information Center, 2007; Geiger, 2009; German & Stanley, 2008; Monahan, 2011; Newkirk, 2010; O'Harrow, 2008; O'Harrow & Nakashima, 2008; Rollins, 2008).[3] A Senate report released in October 2012 confirmed many of these concerns. For example, during the 13-month Senate Subcommittee investigation, DHS reviewers canceled 40 reports filed by personnel at state and local fusion centers for potentially compromising the civil liberties and privacy protections of the individuals implicated in the reports. Likewise,

documents obtained through freedom of information and open access requests reveal that fusion centers were integrally involved in intelligence operations focused on Occupy Wall Street participants, despite the significant threat to civil liberties posed by such operations (Wolf, 2012).

Although counterterrorism was the original impetus for fusion centers, they quickly mutated their missions to include all-crimes, and, in some instances, all-hazards. This has allowed localities to draw upon DHS resources to meet a wider range of law-enforcement needs, oftentimes with only a tenuous connection to counterterrorism (Monahan & Regan, 2012; Regan & Monahan, 2013). SARs, however, have evolved to be a central part of the counterterrorism efforts of fusion centers, especially because of their standardizability and possible relevance for the private sector, which operates the majority of critical infrastructure in the United States.

Fusion centers engage in a variety of outreach programs to private-sector companies to integrate them into their networks. Our data show that there are two stages of training and educational campaigns by fusion centers. The first is oriented toward local law-enforcement organizations, alerting them to the resources offered by fusion centers and training terrorism liaison officers to serve as points of connection among these organizations. But the second stage, which is well underway, involves outreach to private companies, training their security personnel to communicate suspicious activities to fusion centers and undergo background checks to participate in the FBI's InfraGard program for the dissemination of information about possible threats to critical infrastructure. In some instances, fusion centers allow representatives from private companies to be involved in routine activities at fusion center sites (German & Stanley, 2007), which is a finding that is supported by our data as well.[4] Obviously, this can introduce difficulties in restricting the data to which private-sector personnel have access, particularly when fusion centers adopt an "embedded analyst" structure where personnel work in a single room to facilitate the sharing and combining of data from multiple agency databases (Monahan & Regan, 2012).

While the coupling of fusion centers with the private sector does raise concerns about the conflation of industry interests with national security, as well as about protections over the flow of personal information, fusion center personnel are also conceptualizing these arrangements as ways to delegate responsibility to the private sector for robust data collection. As one fusion center intelligence analyst explained,

> In the last year, we started reaching out more towards security with the private sector, for reports coming from them. One of the reasons that we do that is within [our state] . . . outside the metro area, it gets very rural. And it's hard to

> get reporting from those areas, mainly because of understaffing, you know, overworking of law enforcement. They're more focused on, you know, the common crimes that they would come across. So the Suspicious Activity Reports for them sometimes don't get reported up, so we start leaning on the private sector to report up any kind of suspicious activity, [such as] surveillance, things like that around their infrastructure . . . They're trying to protect their assets, so they're more readily going to report that information up to us, than some of the local law enforcement.

Just as fusion centers can direct some federal resources to local needs, so too can they try to outsource reporting functions in a way that is responsive to scale back resources for law enforcement, especially in a period of economic recession.

SARs and Counterterrorism

Fusion centers have incorporated "suspicious activity reports" into their repertoire of data gathering techniques. SARs have roots that were not only predated intelligence-led policing and community policing but were also integrated into both of those practices. The legal status as well as the utility of SARs have always been somewhat murky. They are, basically, just tips in need of further investigation. Post 9/11, there was renewed emphasis on citizen and corporate leads in identifying potential terrorists threats. Jon Michaels (2010) referred to these "newly deputized national security apparatchiks" as "force multipliers" and attributes their rise to four factors: the need for more intelligence gathering, more acceptance of private actors taking responsibility for sensitive national security activities, recognition that it is often easier for private actors to access relevant information, and the public's interest in doing something to help (pp. 1435-1438). The ACLU (2004) noted that the security establishment's concern with the "practical limits on the resources, personnel and organization needed to extend the government's surveillance power to cover hundreds of millions of people" also contributed to the enlistment of "individuals and corporations as auxiliary members of its surveillance networks" (p. 1).

The first iteration of post 9/11 programs was Operation Terrorist Information and Prevention System (TIPS), which the justice department launched to get employees in certain industries, such as transportation, delivery, and energy, to report suspicious activity. Operation TIPS was first scaled back and later defunded due to privacy concerns. It was originally included in the 2002 Homeland Security Act but Representative Dick Armey (R-TX) was instrumental in its removal because of concerns about a law enabling

"Americans to spy on one another" (Hentoff, 2002). However, there were several similar local or sector-specific programs that continued (Michaels, 2010).

In principle, there are two kinds of SARs: those relating to routine criminal behavior and those suggesting some kind of nexus to terrorism. One task of fusion center analysts is to sift through SARs to determine whether some connection to terrorism could exist, and if such a determination is made, then flag the report in the FBI's eGuardian database and notify other fusion centers or relevant organizations. Analysis is an interpretive act that may not be clear-cut. For instance, some of the examples from our study include things such as vandals spray painting a wall outside an industrial site, people taking photographs of bridges, or gang violence. Any of these activities could be related to a potential terrorist act, but upon further investigation, the vast majority of SARs have absolutely no connection to terrorism.

Because of their cautious orientation, though, fusion centers may err on the side of viewing SARs as "early indicators" of terrorist activity. One fusion center director explained, "We are focused on, you know, financial crimes, narcotics, things that would either support or fund terrorism—or could be precursor indicators of planning, you know, [like] surveillance [of critical infrastructure by individuals]." Of course, people taking photographs of sites, for example, could be for tourism, an art project, or something more malevolent, so making this assessment relies to some extent on the subjective judgment of analysts, which creates a space for the insertion of bias, as has been revealed by known cases of fusion centers profiling people by race, religion, or political affiliation (Monahan, 2011). For example, when asked which SARs would be considered serious, one fusion center director noted, "anything that has to do with uh, foreign nationals." In addition, whenever criminal activity is coupled with funds being transferred out of the country, this is also perceived as a possible early indicator of terrorism, as one analyst in our study suggested: "[We look at] mortgage fraud type stuff where the money's going to Pakistan, marijuana stuff where the money's going to freaking somewhere in the Middle East with two guys who are from Saudi Arabia, that type of thing."

Regardless of the validity of assessments about "early indicators" of terrorism, fusion centers have an interest in vetting SARs to legitimize their role in the steady flow of law-enforcement data. This process was articulated by one ranking officer as a way of adding value to SARs:

> One of the things that our duty analyst is also doing is reviewing SARs that have been received, and then evaluating the appropriate dissemination for that SAR, but also bringing value added to that SAR based on our information . . .

> to try to better assess whether it is an explainable or non-criminal or non-threatening event, or whether in fact [it] needs to be looked at a little more carefully. And then, based off of that initial review, they're gonna provide that information to the FBI.

Another way that analysts can try to bolster such reports is by detecting spikes in typical numbers of SARs in an area and then performing additional research to see whether there is a logical reason for such spikes (such as the media running a story on threats); if there is no clear reason for an increase, then the report suggests that the activity may have a higher likelihood of indicating a viable threat. However, one criminal intelligence analyst supervisor we interviewed expressed her concern that focusing on a spike in SARs in a given area rather than the nature of each individual SAR may detract from the goal of identifying legitimate threats:

> People get into the numbers games like wow there's like ten SAR reports in this area. Well, just because there's ten there and there's one over here doesn't mean that the ten are more important than the one over there . . . You can't say oh this area has more SARs. Yeah, it doesn't. It's the vetting and . . . you have to be able to, you know, rate each one of those. So, as long as people understand that SARs are exactly what they are, Suspicious Activity Reporting. It's not threat information until it's investigated or vetted . . . Who has the most SARs doesn't win.

While additional analysis during the vetting process may make for a more robust and accurate report, it also assists fusion centers in making a case for their importance as they compete with other fusion centers for symbolic value. As one analyst related,

> I always tell fusion centers, "Everybody is doing awareness bulletins. Everybody's publishing their statistical analysis of their particular SARs. Everybody's doing the same thing, so give yourself room to maneuver." So that's one of the challenges, I think, in the fusion center business is how do you stay ahead of others, because you have seventy-two centers doing the same thing as you are. It's cutthroat. You'd be surprised.

From this political perspective, if centers can make a strong case for their importance by adding valuable analysis to SARs, then they may receive increased funding in the future or at least ensure their continued existence. And in a funding climate where some fusion centers can count on US$11 million per year in the form of DHS grants, while others are allocated US$1 million, asserting a center's importance is not a trivial goal. Moreover, in the current era of fiscal austerity, some fusion centers are concerned that they will cease to exist if federal funding for fusion centers decreases:

> A hot topic among all fusion centers is wondering, wondering what lays down the road and in the future and whether or not there will be significant layoffs of employees, whether there will be fusion centers that have to shut down and cease to exist . . . and no doubt there will be some that have to shut down.

Fusion centers embrace SARs as a key component of their operational activities as they expand their missions beyond counterterrorism and acquire a central position in the law-enforcement ecology. This emphasis on SARs raised three particularly important issues that we will explore in further depth: the criteria used to label something as "suspicious," the reliability and effectiveness of SARs, and the privacy implications of SARs. Each of these is discussed briefly below before analyzing how the federal Information Sharing Environment (ISE) is handling SARs and whether their current use addresses these issues in a meaningful way.

Defining "Suspicious" Activity

In the area of police investigative work, the lists of behaviors that might be "potentially" suspicious are often inordinately long and populated with rather mundane, routine behaviors. For example, a 2008 Los Angeles Police Department order listed 65 behaviors that could relate to terrorism, including taking pictures, using binoculars, and taking notes—a list that is likely to result in "an ocean of data about innocent individuals that will dominate the investigative resources of the authorities" (German & Stanley, 2008, p. 2). Similarly the New York terrorism card, for instance, lists things such as "Recent travel overseas," "Has student VISA, but not proficient in English," "Refusal of maid service [at a hotel]," owning a "Global Positioning Satellite (GPS) unit," or demonstrating "Unusually calm and detached behavior" (New York State Intelligence Center, 2008).

Every list of "suspicious activities" contains activities that sound quite normal. One can refuse maid service because one is not feeling well, preparing for a meeting and not wanting to be disturbed, or believing that maid service is a wasteful use of environmental resources. Taking pictures is an activity that oftentimes seems downright silly on a list of suspicious activities. Indeed, all of the activities can, and do, occur in everyday circumstances—but in some limited set of circumstances may be associated with criminal or terrorist activity. However, discerning between normal or everyday and suspicious or criminal/terrorist activities seems to be less of a science and more of an art.

The categorization of an activity as "suspicious" is in and of itself a two-stage 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. The context appears to be critically important as "suspicious" is relevant to what is considered "normal." Recognizing "normal" in a particular commercial enterprise (e.g., hotels, hardware stores, Internet cafes) may be easier than recognizing "normal" on a street, in a mall, in a park, or in a railway station where the range of activities that might occur is much broader. The second stage involves deciding to "report" such an activity, which seems to require that one believe that the activity is not only suspicious but also indicative of something problematic, criminal, or terrorism related. The individual thus makes two judgments about which he or she is likely to be relying upon impressionistic criteria.

Reliability and Effectiveness of SARs

Once an agency receives a report of "suspicious activity," the agency then needs to analyze it to determine whether it contains relevant information about terrorists, or potential terrorist activities. This is often referred to as looking for the proverbial "needle in a haystack," and it is widely recognized that there are more "false positives" than reliable hits with SARs—and more SARs than agencies can realistically handle. This seems to hold true for SARs in the financial world and SARs in day-to-day world of police work. Commenting on the counterterrorism SAR regulations in the 2002 amendments to the Bank Secrecy Act, Wolosky and Heifetz (2002-2003) pointed out that most such reports "are stashed away in basements and remain unread by overworked and under-resourced government employees" (p. 2). Similarly, researchers funded by the National Institute of Justice analyzed more than 1.3 million 911 calls to the Washington, D.C., Metropolitan Police Department from 2005 to 2007 and found that 175 calls for 12 locations were identified as potentially related to terrorist activities—an infinitesimal percentage of the total number (Strom, Hollywood, & Pope, 2009, p. 28).

Another problem in gauging the reliability and effectiveness of SARs is that more responsible people may be "risk adverse" because of the ambiguity and uncertainty as to whether something rises to the level of a "suspicious activity." As Michaels notes,

> the responsible would-be participants retreat and the most aggressive participants dominate the landscape—potentially sapping resources as government officials must keep a close watch on them to make sure they do not harass suspects or otherwise frustrate ongoing investigations by dispensing their own forms of justice. (Michaels, 2010, p. 1462)

For example, the Senate report on fusion centers found that just four reporting officials from different fusion centers were responsible for submitting 57% of the raw intelligence reports that were canceled by senior officials at DHS for reporting on Constitutionally protected activity (U.S. Senate Permanent Subcommittee on Investigations, 2012).

Privacy Concerns Regarding SARs

There are four sets of privacy concerns with SARs. The major privacy concern is that these reports are often the result of the reporting person's stereotypes or fears, resulting in racial or ethnic profiling. Data on SARs provide evidence of profiling. For example, NPR News Investigations and the Center for Investigative Reporting analyzed 125 reports from December 2005 to June 2011 that Mall of America security personnel and local police identified as suspicious persons or activities potentially related to terrorism. Of these, 34.6% involved in the reported suspicious activity were White, while 65.4% were not White (23% were reported as Black, 16% as Middle Eastern, 9% as Hispanic, 8% as East Indian; Williams, 2011). Only half of these reports (49.6%) were forwarded to the FBI's JTTF, Minnesota Joint Analysis Center, or Immigration and Customs Enforcement, indicating that half of these were regarded as unfounded once they were investigated further.

A second problem is that in many cases, the reporter of the "suspicious activity" has gleaned the information from access to a private space that government officials would not be able to access without a warrant. This is true not only for delivery or repair people but also for "friends" or neighbors. These private actors do not have to adhere to constitutional privacy principles or privacy statutes, such as Title III, and can give "the government access to more expansive searches than would be permissible were the government to rely on its own personnel" (Michaels, 2010, p. 1465). Moreover, these programs may be more than merely episodic and instead may be ongoing collaborations, the result of "handshake agreements" that "often are inscrutable to Congress and the courts" (Michaels, 2008, p. 904), and thereby avoid accountability requirements.

With respect to sharing information with the private sector, fusion center officials frequently mention the FBI sponsored InfraGard system, which began in the late 1990s and is a "partnership" between the FBI and the private sector. InfraGard was initially focused on cyber infrastructure but expanded after 9/11 to include critical infrastructure more generally. As of March 2013, InfraGard had 55,781 members, including the FBI.[5] InfraGard is integrally involved in supporting information sharing, not just on counterterrorism and cyber crime but also on other major crime programs. One component of

InfraGard is the FBI's Tripwire program designed to identify groups or individuals whose suspicious behavior may be a precursor to an act of terrorism and to alert authorities to such activities. Most fusion center officials find value in InfraGard because, as one fusion center official notes,

> the FBI vets those individuals who are in their program. So it gives us a higher degree of confidence in sharing information with them that's appropriate for the private sector when you know there's been a vetting process in place to, you know, help insure credibility issue[s].

A third concern is whether the information in a SARs can be linked to a particular person and whether that SAR will then constitute a record about that person, or that can be linked to that person, in a persistent database that others can search. Investigating a SAR will inevitably involve the collection of personally identifiable information, such as the name of the person, their address, license plate number, and so on. In those cases where neighbors or service personnel initiate the SAR, the name of the person may be part of the original report. The original report and the investigatory report are likely to contain some personal information—in a way that the person is defined as allegedly engaged in suspicious activity and, perhaps most importantly, without that person's knowledge or opportunity to challenge the classification or interpretation.

A final concern related to SARs is that law-enforcement or homeland security agencies acting upon or investigating "suspicious activity" must protect the Fourth Amendment constitutional protections. This means that policies and procedures under *Terry v Ohio*[6] regarding "stop and frisk" based on reasonable suspicion resulting from "a totality of circumstances" must be followed.

ISE SARs—Do they Correct These Problems?

In launching the latest iteration of SARs, the DHS and Department of Justice (DOJ), working with other federal units, developed a fairly elaborate process for identifying terrorism-related SARs and addressing privacy, civil rights, and civil liberties issues in the emerging "Information Sharing Environment–Suspicious Activity Reporting" (ISE-SAR).[7] Four reports are viewed as particularly important: (a) *Information Sharing Environment–Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis* (September 2008), (b) *Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation Environment* (January 2010), (c) *The Nationwide Suspicious Activity Reporting Initiative*

Status Report (February 2010), and (d) *Privacy, Civil Rights, Civil Liberties Analysis and Recommendations* (July 2010). These reports are all similar in bureaucratic style, providing few details related to discerning what might be legitimate "suspicious activity" and focusing primarily on process. The requirements are somewhat vague; the processes are largely internal to the fusion centers, primarily requiring checklists; there appears to be no requirement for audit trails of information handling and distribution; and there is no ongoing or regular outside reporting or accountability.

SARs can be included in the ISE-SARs shared environment by federal officials or by state officials. One state fusion center official described the state process as follows:

> There is a suspicious activity reporting tool that we just launched on our web portal, and we are in the process of refining it and hopefully identifying some funding to expand it. And when I say expand it, I mean to add an analytical back end to that database [and for sharing] . . . so this reporting tool that we have on our website that's available to the public, is not really the, we designed it to meet the NSI specifications or the specifications of the ISE, but it is not the one that the national SAR initiative actually looks at as being the information moving in the shared space. So, those are reviewed, those field information reports are reviewed by our analysts on a daily basis to determine if there's any activity there that might be indicative of terrorist activity. And then those are reviewed to see if they meet the criteria for moving up to the national SAR database.

On the whole, our interviews during the first phase of data collection (from 2010 to 2011) revealed that fusion center officials were hopeful that the ISE-SARs procedures would help them to process information in a more meaningful way and also to identify the kinds of information that are relevant to counterterrorism efforts. One fusion center official described the overall effort in these words:

> We have been a part of what they call the batter's box for the national SAR initiative . . . we've been capturing SARs at a state level since 2007. About eight months ago, we began contributing the SARs through the FBI's eGuardian system. So we join[ed] the NSI several months ago, and have been going through a number of steps to essentially kick off a strategy on how to move the national SAR initiative more vigorously out into the state, training, oversight from our executive governance board for the fusion center, law, the Chiefs and Sheriffs' Association, exposing them, talking to them about it, but all the while, the SARs that we were merely capturing and sending in a paper form to the FBI offices or electronic form of a file, we're now taking those and we're uploading those into eGuardian. So that means that they end up in a place called, what's

> considered a shared environment, where other fusion centers or other investigators who are looking at SARs can also see [our state's] SARs . . . DOD is now a part of that as well . . . both contributing and getting . . . this is very force protection oriented . . . this SAR program is all about suspicious activity that has, you know, that may have a nexus to terrorism.

Another fusion center official noted that the ISE-SARs system is "the closest thing to a federal program that has a promise of aggregating and analyzing data comprehensively." And a third expressed optimism about the potential of the ISE because "for the first time we'll have a continuity platform between the centers where we can communicate and share information."

Although optimism appeared to be high among fusion center officials at the inception of the ISE-SARs system, interviews conducted with fusion center personnel in 2012 suggest that information sharing across fusion centers continues to be a challenge:

> Ideally, you know, say, for [my county], I'm fusing all the information I get, and I'm looking at it, and I kind of have visibility of it all. Well then, DHS is supposed to take it and kind of do the same thing. But and we should also be able to look at it and see, you know, what's going on in [other fusion centers], that kind of thing. But I don't necessarily think that's occurring to the level of fidelity that one would like.

In addition, the FBI eGuardian and the DHS ISE systems remain largely disconnected from one another, requiring many fusion center personnel to submit SARs to each system separately:

> When we started this it was like okay we want you to put this information in the NSI, the SAR information . . . But we were doing like all [SARs] to the NSI and then FBI came around and [they were] like hey we got E-Guardian, you know, we need to, we want you to put the information in E-Guardian. Well, originally when the NSI came it was like well there's box that you can click and it'll go to the FBI E-Guardian and it will go to SAR, so we're like great, well then we'll just go that way because we're not entering this information twice. Well, apparently that really didn't, that didn't fly, that little box really didn't work even though we thought it did . . . I think it was not just frustration for us, I think it was frustration for a lot of fusion centers. But we took it as, you know, we'll do whatever we have to do to make sure everybody gets what they need. So, then we just physically did two different entries.

Although the above fusion center submits SARs to both systems separately, other fusion centers may privilege one system over the other. For example, one fusion center director stated that his center only uses the FBI system,

while another director shared his concern that he could not amend or remove SARs through eGuardian and thus only regularly submits SARs to the Nationwide SAR Initiative (NSI) unless he knows that it needs to be investigated by the FBI. The disconnect between the FBI and DHS systems was highlighted as a cause of frustration for several individuals we interviewed.

To return to our primary questions for further analysis, does the ISE-SARs environment possess the potential for addressing the three problems that have been traditionally associated with SARs: the criteria to define "suspicious activity," the reliability and effectiveness of SARs, and the privacy implications? Each will be discussed below in the context of what we have learned from our interviews.

Defining Suspicious Activity

The ISE Functional Standard Version 1.5 defines suspicious activity as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."[8] The ISE document points out that the emphasis on behavior would negate consideration of "factors such as race, ethnicity, national origin or religious affiliation" except as descriptors of a specific subject. The ISE document goes on to say that determining whether "suspicious activity constitutes an ISE-SAR is made as part of a two-part process by trained analysts using explicit criteria" that are found in the *Criteria Guidance* and that are seen as "highlighting the importance of context in interpreting such behaviors." However, as one can see from the *Criteria*, there remains a great deal of ambiguity and vagueness in the behaviors described.

One fusion center official emphasized that normal "tips" about things such as teenagers in parking lots are "not being vetted up through the ISE SARs." He noted that "the money going into SARs, and I think this is great, is put into training. It's put into training for police officers to understand what are early indications of terrorist activities."

A compendium of 25 FBI and Bureau of Justice Assistance flyers distributed to a variety of industries collected by Public Intelligence[9] indicates that there has not been much refinement of the criteria used to define "suspicious" activity or behavior. The behaviors that appear on these lists include those that have appeared on such list for many years—altered appearance, burns on hands or body, nervous or secretive behavior, avoidance of security cameras or lobby areas, seeking opportunities to be alone, use of cell-phone cameras, unusual inquiries or comments, mumbling to self, and heavy sweating. A review of the various state-level websites, which would also be feeding information to fusion centers and into the ISE, tends to reveal a similar set of

vague or ambiguous behaviors, although more recently they have included language with the precision and direction suggested in the ISE Functional Standard. For example, the Washington State Fusion Center SARs flyer includes under "Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During Investigation,"

> Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

This Washington state flyer then, as required by the ISE-SAR Revised Functional Standard and using language contained in the ISE Criteria, is providing more information for individuals and law-enforcement personnel and is also noting that the activity might be "criminal" or "non-criminal."

However, it remains true, as noted previously, that defining "suspicious" is an interpretive act, depending not only much on the context but also very much on the interaction between the observer (interpreter) and the observed, and is thus inevitably affected by the perspective that the observer brings to the situation. Training of the observer is critical but would appear to need to extend beyond what is in these flyers to correct for the issues previously identified in defining "suspicious." The various ISE documents emphasize the importance of training and highlight that training is occurring, but it is not obvious what is taking place in those training sessions, who specifically is required to take them, and whether the insights gained in terms of defining "suspicious" are more precise or accurate. For example, the *NSI Privacy, Civil Rights and Civil Liberties Analysis and Recommendations* (July 2010) state,

> Standardized training for front-line officers, investigators, analytic, and supervisory personnel must be provided and required in order to educate personnel on the purpose and use of the multi-layered vetting process required in the Functional Standard; line officers, in particular, should receive specialized training to strengthen their ability to recognize the types of behavior that may be indicative of criminal activity associated with terrorism.

Whether such training is occurring with any degree of success remains to be seen—and is not easily discerned by those outside the fusion centers. Systematic evaluation of the SARs processes seems necessary. However, on the whole, the criteria being listed in SARs indicate that there has been only little improvement in defining activities with more specificity or relevance to terrorism. The net appears to be cast almost as broadly as it was before the ISE-SARs initiative.

Reliability and Effectiveness

If the training and criteria are not successful in more narrowly defining terrorism, then the reliability and effectiveness of SARs as a technique will not improve. One fusion center official reported,

> We receive somewhere in the realm of four hundred to five hundred SARs each year . . . the SARs are not necessarily all terrorism but some are. Some have that nexus to terrorism in them. So one of the things that our duty analyst is also doing is reviewing SARs that have been received, and then evaluating the appropriate dissemination for that SAR, but also bringing value added to that SAR based on our information . . . to try to better assess whether it is an explainable or non-criminal or non-threatening event, or whether in fact there needs to be looked at a little more carefully. And then, based off of that initial review, they're gonna provide that information to the FBI.

Within the ISE environment, there remains the question of whether ISE-SARs will be more effective at identifying relevant suspicious activity because the rationale for the ISE environment is based in part on the belief (assertion) that terrorism activities are being funded "via local or regional criminal organizations whose direct association with terrorism may be tenuous" (ISE-FS-200). This seems to broaden the scope of activities and individuals for whom fusion centers might have an interest and to require that law-enforcement and homeland security professionals work together more closely. However, interviews conducted in 2012 with fusion center officials indicate that many fusion centers have developed their own systems for processing SARs due to the absence of specific guidance from DHS officials. One intelligence analyst highlights the variance in defining and processing SARs across fusion centers, stating that "there are seventy-nine[10] different ways of doing business. There's probably seventy-nine different ways of creating a SAR. There are probably seventy-nine different, different thoughts in terms of, you know, what constitutes a SAR." We found, for example, that fusion centers use a wide array of approaches when vetting SARs, ranging from relying primarily on the expertise of analysts to exercise personal judgment in defining legitimate threats to the utilization of complex rubrics and rating systems.

In terms of evaluating the reliability and effectiveness of the ISE-SARs environment, one fusion center official noted his desire for some feedback regarding the utility of the information he submits to the national SARs database:

We may never know that that piece of suspicious activity reporting got passed up into the national SAR initiative and was picked up by [another

state] and used in something they're doing. So it's hard to close that loop sometimes because those investigations are classified . . . we don't have the need to know . . . it's more beneficial, and we've explained this to the FBI, it's much more beneficial if we get some minimum amount of feedback so that we know at least that we are doing the right thing, or that we're providing the right kinds of information.

Privacy Implications

The ISE-SARs process for protecting privacy and civil liberties rests on three pillars: (a) the development of a privacy policy that satisfies the ISE Privacy Guidelines—it takes an average of 6 months for a fusion center to develop and implement such a privacy policy (July 2010, p.6); (b) technical and policy training of staff at fusion centers; and (c) a "business process"—"a formal and multi-layered vetting process in which each SAR is reviewed by a front-line supervisor and by an experienced investigator or analyst specifically trained in counterterrorism issues before it can be designated as an ISE-SAR" (July 2010, p.7).

A fusion center official described his work regarding SARs processing as follows:

> Regular analysts receive the SAR from numerous areas. They will process it. They will disseminate it according to need. They'll fill out the paperwork and before it is stored, it's submitted to me. And I look for quality, I do basic quality control to make sure the necessary fields are filled out, that I have the basic information needed, and then I look for privacy policy issues, making sure that we we're not violating anybody's First Amendment, we can actually collect this kind of information . . . I make sure that it's been disseminated and stored correctly, and codified correctly. Then I extract certain fields that are important to me . . . you look for basic trends in the SAR report.

During our interviews, many fusion center officials emphasized the importance of protecting privacy and civil liberties during the collection and vetting of SARs. For example, one director explained, "Everything we do, we, we look at privacy, civil rights, and civil liberties issues period. Everything we do. So we highlight it every moment of every day."

The fusion center SARs flyers do appear to alert readers to the First Amendment implications of the activities mentioned as being possibly suspicious with language similar to this found on the Washington State flyer, which is the language in the ISE-SAR Functional Standard 1.5:

> These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).

In addition to flyers, several fusion centers post their privacy policies online. Although interviewees noted that they hoped this would provide important information to the public about the protection of privacy and civil liberties, one director expressed his concern that uploading lengthy policy documents to a fusion center's website may not necessarily make this information easily accessible to members of the public:

> Privacy policies are generally by their nature, are very long and tedious to read through. And they have, and by their very design they have a lot of requirements that our fusion center is required to abide by, and that can get convoluted as you try to explain and provide these documents for people to understand.

Conclusion

Although DHS and DOJ have spent time doing outreach to state officials, law-enforcement organizations, federal agencies, and privacy and civil liberties advocates,[11] and have developed a fairly elaborate process and set of guidelines, it appears that SARs are likely to continue to be plagued by their inherent limitations. Fundamentally, they remain tips, based on the impressions of individuals—ordinary citizens, service personnel, commercial employees, and law enforcement—who make a judgment that something seems "suspicious" and are motivated to report the activity. What the ISE-SARs initiative seems to do is develop guidelines and processes within the fusion centers as a focal point for vetting SARs. The ISE-SARs focus is more on the "information sharing environment (ISE)" and less on the "suspicious activity reporting (SARs)" that feeds that environment.

It remains somewhat remarkable that, given their broadly recognized limitations, SARs have not only persisted as a tool of law enforcement and counterterrorism but also their importance has been elevated in the ISE. The fusion centers, themselves, clearly play the key role in discerning which SARs should be taken seriously and which should not—and the processes and guidelines provide some structure for doing that. But it is still a judgment call based on impressionistic information. This raises a larger concern about the

shifting nature of police work toward predictive, intelligence-led, or preemptive policing, which changes the relationship between the police and communities, shifting it toward suspicion and away from trust; in turn, police practices driven by suspicion will likely infringe on the rights of individuals, while undermining existing legal safeguards (van Brakel & de Hert, 2011).

Because of the importance of making sound and accurate judgments with SARs, it is critical that fusion centers not just focus on internal procedures and sharing with federal and state partners but also cultivate ties to the organizations and individuals in their communities so that they can better evaluate the SARs that do come in (cf. Thacher, 2005). Attention to building trust with community groups, commercial enterprises, and other organizations is vital in giving fusion center officials the context and background for interpreting SARs, and in giving individuals and organizations the skills and information to recognize suspicious activity. There is a long tradition of citizens playing roles in protecting their communities, but this often works most effectively when it is organized in some way, allowing for training and ongoing relationships, rather than when it seeks random tips. Martin Greenberg (2005), who has written an interesting history of the role citizens have played in policing, suggests that in the post 9/11 era "a civilian auxiliary" (p. 229) might be of more assistance than the rather unclear role that has emerged.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This material is based on work supported by the National Science Foundation under Grants SES-0957283, SES-0957037, and SES-1339199.

Notes

1. Between 2010 and 2012, we interviewed 56 representatives from 36 fusion centers, industry partners, and civil society groups, with the bulk of interviews being with high-level personnel at fusion centers. Most of these interviews were conducted over the phone and lasted for about an hour. Confidentiality of interviewees and identities of fusion centers have been ensured through human subjects agreements.
2. A recent Senate report suggests that four fusion centers that are alleged to exist are not fully functional: "One of the ongoing troubling features of Department of Homeland Security's (DHS) fusion center efforts involves nonfunctional fusion

centers whose very existence is a matter of dispute . . . DHS's insistence on listing fusion centers with no physical presence is not only puzzling, but raises questions about its entire assessment process" (U.S. Senate Permanent Subcommittee on Investigations, 2012, pp. 90, 93).

3. For a compendium of material about fusion centers and privacy, see http://epic.org/privacy/fusion/
4. The goal of serving industry partners is part of the explicit orientation of these centers, which is illustrated by public statements from DHS representatives. For instance, in her 2010 testimony before the House Subcommittee on Homeland Security, DHS Under Secretary Caryn Wagner (2010) stated, "I&A [DHS's Office of Intelligence and Analysis] will continue to advocate for sustained funding for the fusion centers as the linchpin of the evolving homeland security enterprise. While I&A's support to state, local and tribal partners is steadily improving, there is still work to be done in how best to *support the private sector*. We intend to explore ways to extend our efforts in this area beyond the established relationships with the critical infrastructure sectors" (italics added).
5. For more information on InfraGard, see http://www.infragard.net
6. 392 U.S. 1 (1968).
7. The co-chairs of the Information Sharing Environment (ISE) Privacy Guidelines Committee are the Chief Privacy and Civil Liberties Officer, Department of Justice; the Civil Liberties Protection Officer, office of the Director of National Intelligence; the Chief Privacy Officer, DHS; and the Officer for Civil Rights and Civil Liberties, DHS.
8. *ISE; Functional Standard (FS) Suspicious Activity Reporting (SAR)*. Version 1.5. (ISE-FS-200). Retrieved from www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise-appendix.pdf
9. See http://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/. The industries include airport service providers, beauty/drug suppliers, construction sites, hotels/motels, shopping malls, Internet cafes, rental cars, and storage facilities.
10. This individual suggested that there are currently 79 fusion centers in operation as opposed to the 77 listed on the DHS website.
11. Appendix C of *Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations* (July 2010, p. 30) lists the following privacy and civil liberties advocates: American-Arab Anti-Discrimination Committee, American Civil Liberties Union of Southern California, American Civil Liberties Union–Washington Legislative Office, Bill or Rights Defense Committee, Center for Democracy and Technology, Electronic Information Privacy Center [*sic*], Freedom and Justice Foundation, Islamic Shura Council of Southern California, Muslim Advocates, Muslim Public Affairs Council, and Rights Working Group.

References

American Civil Liberties Union. (2004, August). *The surveillance-industrial complex: How the American Government is conscripting businesses and individu-*

als in the construction of a surveillance society. Retrieved from www.aclu.org/FilesPDFs/surveillance_report.pdf

American Civil Liberties Union. (2010, June). *More about suspicious activity reporting*. Retrieved from http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting

Department of Justice. (2010, January). *Final report: Information Sharing Environment (ISE)-Suspicious Activity Report (SAR) evaluation environment*. Retrieved from ise.gov/sites/default/files/BJA_Final_Report_ISE_SAR_EE.pdf

Electronic Privacy Information Center. (2007, June). *National network of fusion centers raises specter of COINTELPRO*. Retrieved from http://epic.org/privacy/surveillance/spotlight/0607/

Geiger, H. (2009, April 27). *Thwarting civil liberties—The problem with domestic intelligence*. Center for Democracy and Technology. Retrieved from http://cdt.org/blogs/harley-geiger/thwarting-civil-liberties-problem-domestic-intelligence

German, M., & Stanley, J. (2007, December). *What's wrong with fusion centers?* Retrieved from http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf

German, M., & Stanley, J. (2008, July). *Fusion center update*. Retrieved from www.aclu.org/files/pdfs/privacy/fusion_update_20080729.pdf

Greenberg, M. A. (2005). *Citizens defending America: From colonial times to the age of terrorism*. Pittsburgh, PA: University of Pittsburgh Press.

Hentoff, N. (2002, December 17). The death of operation TIPS: Volunteer spying corps dismissed. *The Village Voice*. Retrieved from http://www.villagevoice.com/2002-12-17/news/the-death-of-operation-tips/

Levi, M. L., & Wall, D. S. (2004). Technologies, security, and privacy in the post-9/11 European Information Society. *Journal of Law and Society*, *31*, 194-220.

Michaels, J. (2008). All the president's spies: Private-public intelligence partnerships in the war on terror. *California Law Review*, *96*, 901-966.

Michaels, J. (2010). Deputizing homeland security. *Texas Law Review*, *88*, 1435-1473.

Monahan, T. (2011). The future of security? Surveillance operations at Homeland Security Fusion Centers. *Social Justice*, *37*(2-3), 84-98.

Monahan, T., & Regan, P. M. (2012). Zones of Opacity: Data Fusion in Post-9/11 Security Organizations. *Canadian Journal of Law and Society*, *27*(3), 301-317.

National Commission on Terrorist Attacks Upon the United States. (2004, July 22). *The 9/11 commission report* (Final Report). Retrieved from http://www.9-11commission.gov/report/911Report.pdf

Newkirk, A. B. (2010). The rise of the fusion-intelligence complex: A critique of political surveillance after 9/11. *Surveillance & Society*, *8*, 43-60.

New York State Intelligence Center, "New York State Law Enforcement Terrorism Indicators Reference Card" (September 3, 2008), http://publicintelligence.net/new-york-state-law-enforcement-terrorism-indicators-reference-card/

Nojeim, G. T. (2009, March 18). *Homeland security intelligence: Its relevance and limitations. Testimony before the house committee on homeland security, subcommittee on intelligence, information sharing, and terrorism risk assessment*.

Retrieved from http://www.cdt.org/testimony/testimony-greg-nojeim-homeland-security-intelligence-its-relevance-and-limitations

O'Harrow, R. Jr. (2008, April 2). Centers tap into personal databases; state groups were formed after 9/11. *The Washington Post*, p. A01.

O'Harrow, R. Jr., & Nakashima, E. (2008, March 6). National dragnet is a click away; Authorities to gain fast and expansive access to records. *The Washington Post*, p. A01.

Randol, M. A. (2009, November 5). *Terrorism information sharing and the nationwide suspicious activity report initiative: Background and issues for congress* (CRS 7-7500). Retrieved from http://www.ijis.org/docs/NSI%20Report_R40901.pdf

Reeves, J. (2012). If you see something, say something: Lateral surveillance and the uses of responsibility. *Surveillance & Society*, *10*, 235-248.

Regan, P. M., & Monahan, T. (2013). Beyond Counterterrorism: Data Sharing, Privacy, and Organizational Histories of DHS Fusion Centers. *International Journal of E-Politics*, *4*(3), 1-14.

Rollins, J. (2008). Fusion Centers: Issues and Options for Congress. Washington, DC: Congressional Research Service.

Steiner, J. E. (2010). More is better: The analytic case for a robust suspicious activity reports program. *Homeland Security Affairs*, *6*(3), 1-12. Retrieved from http://www.hsaj.org/?article=6.3.5

Strom, K., Hollywood, J., & Pope, M. (2009, June). *Using 911 calls to detect terrorism threats* (National Institute of Justice Journal, No. 263, pp. 24-29). Retrieved from http://www.nij.gov/journals/263/911-calls.htm

Thacher, D. (2005). The local role in homeland security. *Law & Society Review*, *39*, 635-676.

U.S. Department of Homeland Security. (2006). DHS Strengthens Intel Sharing at State and Local Fusion Centers. Retrieved from https://www.hsdl.org/?view&did=476394

U.S. Senate Permanent Subcommittee on Investigations. (2012). *Federal support for and involvement in state and local fusion centers*. Retrieved from http://www.hsgac.senate.gov/download/report_federal-support-for-and-involvement-in-state-and-local-fusions-centers

van Brakel, R., & de Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Journal of Police Studies*, *20*, 163-192.

Wagner, C. (2010). *Testimony of Under Secretary Caryn Wagner before the House Subcommittee on Homeland Security on the President's Fiscal Year 2011 Budget Request for the Department's Office of Intelligence and Analysis*. Washington, DC: Department of Homeland Security. Retrieved from http://www.dhs.gov/ynews/testimony/testimony_1267716038879.shtm

Williams, M. (2011, September). Database: Mall of American suspicious activity reports. *NPR*. Retrieved from http://www.npr.org/2011/08/18/139756444/database-mall-of-america-suspicious-activity-reports

Wolf, N. (2012, December 29). Revealed: How the FBI coordinated the crackdown on Occupy. *The Guardian*. Retrieved from http://www.guardian.co.uk/commentisfree/2012/dec/29/fbi-coordinated-crackdown-occupy

Wolosky, L., & Heifetz, S. (2002-2003). Regulating terrorism. *Law and Policy in International Business*, *34*, 1-5.

Author Biographies

Priscilla M. Regan is a chair and professor of public and international affairs at George Mason University. Her primary research interests have focused on the analysis of the social, policy, and legal implications of organizational use of new information and communications technologies and also on the emergence and implementation of electronic government initiatives by federal agencies. She has published more than 40 articles or book chapters, as well as *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995).

Torin Monahan is an associate professor of communication studies at the University of North Carolina at Chapel Hill. His research focuses on institutional transformations with new technologies, with a particular emphasis on surveillance and security programs. His most recent books are *SuperVision: An Introduction to the Surveillance Society* (Chicago University Press, 2013, co-authored with John Gilliom) and *Surveillance in the Time of Insecurity* (Rutgers University Press, 2010).

Krista Craven is a doctoral student in the Community Research and Action program in the Department of Human and Organizational Development at Vanderbilt University. Her research interests are in youth involvement in the immigrant justice movement.