Beyond Counterterrorism:
Data Sharing, Privacy, and Organizational Histories of DHS Fusion Centers

Priscilla M. Regan, Department of Public and International Affairs,George Mason University, Fairfax, VA, USA

Torin Monahan, Department of Communication Studies, The University of North Carolina at Chapel Hill, Chapel Hill, NC, USA

ABSTRACT

Decentralized organizational approaches to security provision introduce new challenges for controlling information-sharing practices, safeguarding civil liberties, and ensuring accountability. Department of Homeland Security "fusion centers," and the multiple organizations and databases that are part of fusion centers, engender an environment in which information is migrating beyond original purposes of counterterrorism. Indeed, based on intensive qualitative research, the authors have found that fusion centers that were originally oriented toward "counterterrorism" have quickly broadened their scope to include all crimes, and those that began as "all crimes" have migrated only marginally to terrorism. This is the result of three quite predictable factors: fusion centers have to be valuable to their states, there is too little activity that is clearly terrorism related, and fusion center personnel have to use their time and skills constructively. Nonetheless, even if local policing needs are met through fusion-center funding and support, many of the activities of fusion-center analysts lend themselves to mission creep and violations of civil liberties.

Keywords: *Data Sharing, Civil Liberties, Fusion Centers, Privacy, Terrorism*

The U.S. Department of Homeland Security (DHS), under both 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. Department of Homeland Security, 2006). As of 2012, there were 77 state and local fusion centers, some of which were created in response to terrorist threats, while others emerged from existing law enforcement efforts (such as drug interdiction, crime control, or regional coordination). Although a number of concerns have been raised about fusion centers, particularly civil liberties violations, ineffectiveness, and cost (Monahan & Palmer, 2009; Permanent Subcommittee on Investigations, 2012), little attention has been given

DOI: 10.4018/jep.2013070101

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

to the ways in which the unique identities of fusion centers contribute to such problems.

This paper explores the question of what factors shape the data-sharing practices of fusion centers, with particular attention to the organizational histories of fusion centers. Specifically, we argue that there is more data sharing with less oversight (i.e., mission creep) when: fusion centers take on responsibility for addressing "all crimes" or "all hazards" instead of addressing terrorist threats alone; state and local agencies seek out "dual purpose" functions that meet perceived local needs; multiple jurisdictions and actors with different policy orientations are involved; policies for data sharing or data management are unclear; oversight or enforcement of existing policies and laws is inadequate; and budgetary constraints under which fusion centers operate are great. Moreover, the technological systems deployed by fusion centers tend to facilitate data-collection, data-mining, and pattern-searching activities that are in tension with existing privacy laws.

The findings discussed here are based on a three-year empirical study of information sharing by—and organizational dynamics of—fusion centers. From 2010-2012, data for this project were drawn from government documents, reports of think tank and interest groups, and interviews with fusion center representatives and civil society groups. For the interview portion of our research, we spoke with data analysts and high-level personnel, most often the directors or co-directors, of 36 fusion centers, 33 of which are official DHS fusion centers. Of these 36 centers, 27 are state level centers, all of which are official DHS fusion centers, and 9 are sub-state (regional within a state). Fifty-six interviews have been conducted in total. Most of these interviews were conducted over the phone and lasted for about an hour, although six interviews were conducted with personnel at fusion-center sites. Confidentiality of interviewees and identities of fusion centers have been ensured through human subjects agreements.

Background on Fusion Centers

DHS fusion centers coordinate data sharing among state and local police, intelligence agencies, and private companies. These public-private partnerships became a central component of the U.S. homeland security framework in the wake of 9/11, and they have continued in importance under President Obama's administration (Monahan, 2011). 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 (Kean et al., 2004). As DHS Secretary Janet Napolitano (2009) stated at a conference of fusion center officials:

I believe that Fusion Centers will be the centerpiece of state, local, federal intelligence-sharing for the future and that the Department of Homeland Security will be working and aiming its programs to underlie Fusion Centers…And by the way, let's not forget the private sector when we're looking at those partnerships.

Based on DHS data, the U.S. Government Accountability Office estimated that states have used approximately $426 million in DHS grant funding from FY 2004 to 2009 and that about 60% of fusion center funding is from federal grants, 30% from state funds, and 10% from local funds (Government Accountability Office, 2010, pp., 14-16). More recent figures outlined in a Senate report put the total spending on fusion centers at up to $1.4 billion since 2003 (Permanent Subcommittee on Investigations, 2012). The difficulty in identifying precisely how much has been spent on these entities is reflective of the varied and complex nature of these sites and their federal, state, and local funding sources, which suggests an accountability problem that is reproduced in attempts to oversee the activities of fusion centers more generally.

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Given the data-sharing mission of fusion centers, one might expect that they would have taken off rapidly after 9/11, but this was not the case. Instead, after the passage of the USA Patriot Act in 2001, a controversial proposal was put forward for the creation of a federal-level "Total Information Awareness" program that would keep tabs on everyone in the U.S. (Regan, 2004). After significant public backlash, TIA was scuttled in 2003. Fusion centers then emerged to conduct some of the activities proposed by TIA, but in an ad-hoc and decentralized manner, therefore relatively insulated from public awareness or critique. After the release of the 9/11 Commission report in 2004, fusion centers became an explicit response to the failures in intelligence sharing outlined in that report, whereupon DHS invested more heavily in funding their operations and working toward a fusion-center presence in every state. Since President Obama took office in 2009, 19 more fusion centers have come online, illustrating the ongoing commitment of DHS to this organizational and technological approach to counterterrorism and crime control (Monahan, 2011; Permanent Subcommittee on Investigations, 2012).

Fusion centers have origins in a number of law enforcement and intelligence paradigms. They can be thought of as part of a crime- and terrorism-prevention approach known as "intelligence-led policing," which involves a triage-like system where specific criminal activities or suspected criminals or terrorists are targeted explicitly for monitoring and intervention under the assumption that focusing on high-risk activities or people will reduce crime or terrorism across the board (Bureau of Justice Assistance, 2005; Ratcliffe, 2003). As a U.S. Department of Justice report puts it: "Good policing is good terrorism prevention" (Bureau of Justice Assistance, 2005). Fusion centers also have roots in "community policing," which emphasizes partnerships and collaboration among local entities and a proactive problem-centered approach (Bureau of Justice Assistance, 1994), even if such an approach has been criticized for artificially constructing a governable subject that can be made responsible for structural problems in communities (Chesluk, 2004; Herbert, 2005; Ruben & Maskovsky, 2008). Most recently, fusion centers have been viewed as a key component of the "information sharing environment" (ISE) established after 9/11 and authorized by the Intelligence Reform and Terrorism Prevention Act of 2004 (Citron & Pasquale, 2011). The ISE is supposed to incorporate five primary areas: homeland security, law enforcement, defense, foreign affairs, and intelligence. GAO has recently reported that most of its focus to date has been on homeland security and law enforcement (Government Accountability Office, 2011).

From their inception, fusion centers have generated concern among privacy and civil liberties advocates and scholars for a range of reasons including their lack of transparency, the commingling of law enforcement and intelligence information and purposes, their involvement of the private sector in what has traditionally been government activities, the conflation of innocent or everyday behavior with terrorist or criminal behavior, and the wideapread sharing of personally identifiable information (Electronic Privacy Information Center, 2007; Geiger, 2009; German & Stanley, 2008; Monahan, 2011; Newkirk, 2010; O'Harrow Jr., 2008; Rollins, 2008).[1] Some of the known cases where civil liberties have been encroached upon include the monitoring of blog postings by and preemptive arrest of Green Party member Kenneth Krayeske in Connecticut, the infiltration and monitoring of an activist group in Maryland, the infiltration of a military agent into a non-violent, anti-war protest group in the state of Washington, the targeting of students at historically black colleges in Virginia, and the spying on of protestors involved in Occupy Wall Street events (Monahan, 2011; Partnership for Civil Justice Fund, 2012). Rather than review all these issues and the evidence that various groups and scholars have collected and analyzed, our goal in this paper is to provide some empirical information about the information sharing activities of fusion centers, to identify the conditions under which unfettered

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

information sharing is likely to occur, and to analyze the implications of the data sharing activities we have identified.

Expectations for Information Sharing

The multiple partners and databases that are housed in fusion centers provide a ripe environment for information sharing to migrate beyond what was originally intended. To use the language of "fair information practices," fusion centers are likely to facilitate broader sharing of information that was collected for one purpose, such as counterterrorism, and its use for a secondary, unrelated purpose. This type of mission creep is facilitated by fusion centers taking on responsibility for addressing "all crimes" or "all hazards" instead of addressing terrorist threats alone. While government reports have stressed the absence of fiscal accountability and ineffectiveness at disrupting terrorism (Permanent Subcommittee on Investigations, 2012), our focus here is on the conditions that contribute to such mission creep and the potential negative ramifications for citizens.

Mission creep is enabled by unclear policies for data sharing or data management, inadequate oversight or enforcement of existing policies and laws, and budgetary constraints that compel fusion centers to justify their existence through intelligence or investigative activities. The physical location of fusion centers is also important in that information sharing occurs more readily with local law enforcement when fusion centers are co-located with these entities and less readily when fusion centers operate as stand-alone facilities. Finally, information sharing among organizations occurs more easily when personnel from those organizations are physically present as "embedded analysts" in the fusion center (Monahan & Regan, 2012).

Origins/Evolution of Fusion Centers

Most personnel we interviewed defined their fusion centers as "all crimes, all hazards." This is consistent with earlier studies conducted by the Congressional Research Service (Masse, O'Neil, & Rollins, 2007) and the Government Accountability Office (2010). Terrorism, if mentioned at all, is discussed in the context of local threats or possible connections to local criminal activities. The interviews reveal three primary explanations for the "all crimes" focus.

The *first* is that both the funding and also the political reality dictate that fusion centers have to be valuable primarily to the state and secondarily to the federal government. This dual dependence is perhaps most clearly stated by an official at a state-level center: "These are not federal centers…the fact is everyone started from a different place, and everyone has different levels of funding and capacity and I think the challenge for fusion centers is to accomplish this mission with the federal government, but at the same time providing relevance and value to their state." This is echoed in the comments of an official at another state-level fusion center, which began as a crime intelligence division: "ours ended up being an all crimes center initially, because that was the basis that we already had here as far as, you know, assisting local jurisdictions with information on criminal cases." Another fusion center official was quite candid in stating the reality that he saw: "most chiefs or sheriffs are not concerned about a terrorist attack. They don't really care. I mean, they've just, they got their own stuff to worry about, and I don't blame 'em."

The *second* explanation for the all crimes focus is that terrorism is inherently too restricted and narrow as a focus for such centers. An official at a state-level fusion center, whose statute defines its mission as "terrorism related" not "all crimes" describes the situation as follows: "you tell me what crimes are the precursors for sure of terrorism, and then I'll focus on those. So my argument has always been that we have to look at all crimes." He went on to say that he did not think fusion centers should be involved in bank robberies, unless it was serial bank robberies, or in homicides but should focus on "financial crimes, narcotics, things that would either support or fund terrorism."

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Another official at a state-level fusion center stated, initially "its only priority was counter or anti-terrorism. It grew into what was necessary and is only logical, into an all-crimes fusion center…you don't want to promise the public or other government agencies something and not be able to fulfill the promise…you would have the chance of setting up a system that's gonna fail because they're not gonna connect some of those euphemistic dots that start out as some other crime and really are terror financing…So it's just the logical thing to do."

The *third* explanation involves the need for fusion center personnel to be professionally active and involved. An official at a state-level fusion center argued that the center would be too limited if it focused solely on terrorism and would lose contacts with other organizations as well as analytical and investigative skill sets: "We don't deal with that [terrorism and terrorism alone] because if the only time I talked to the TLO [Terrorism Liaison Officer] is when he has something, well in four years I'll hear from him. So we take an all crimes approach so that those lines of communication are constantly being tested…[and] enforced."

Location/Identity

Most fusion centers in our study emerged from a law enforcement context, are directed by someone with law enforcement background, are co-located with local law enforcement entities, and focus on local law enforcement activities. This appears to contribute to some ambiguity about the fusion centers' role within their states and with the federal government. All the fusion centers we contacted had both a DHS and an FBI official at the site, in virtually all cases on a full-time basis and in some cases with as many as four officials from the FBI. Fusion centers also reported having on-site personnel from other federal agencies, including Transportation Security Agency (TSA), Alcohol, Tobacco and Firearms (ATF), Drug Enforcement Agency (DEA), Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP). But the great majority of staff at the fusion centers were from local law enforcement, with other staff from a range of state agencies such as public health, corrections, parole and probation, fire, emergency management, environmental protection, highway, and gaming and fishing.

Several of our interviewees quoted the refrain that "if you've seen one fusion center, you've seen one," often remarking that DHS does not like this statement. However, this seems to be precisely the case. Who is involved in a fusion center is, not surprisingly, very much reflective of the geographic, economic and demographic characteristics of a state. The size of fusion centers also varied quite widely with one having as few as 4 staff, most having around 30 staff, and a few with 80 staff. Almost all fusion centers had some governance structure, an advisory board or committee, but most of these are composed of law enforcement officials whose staff are actively associated with the fusion center. There is little public accountability – on their advisory boards, one fusion center had a citizen representative and two had ACLU representatives, and some had arms-length oversight by the governor's office. But the advisory boards rarely meet, and the majority of fusion centers operate squarely within the culture and confines of the law enforcement community.

The variation in the actual activities of fusion centers, their location, and staffing is somewhat fueled and further complicated by what many of our informants perceive as a lack of real guidance by DHS. Although DHS gives grant guidance and has identified baseline activities for fusion centers (U.S. Department of Homeland Security, 2008), the reality appears to be that the actual day-to-day functioning of fusion centers is largely centered on reacting to what is going on in their state and communities. An official at a sub-state fusion center noted that although the center received millions of dollars a year from DHS and had a "fantastic" person from DHS, there was "no guidance to him on what his mission and roles and responsibilities [should be], and luckily…between him and I and the FBI, we were able to…cobble that

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

out and make it functional and make it really productive." An official at a state-level fusion center believed that DHS was "kingdom building" and that "the great majority of the people who are being hired [for reviewing privacy policies], wouldn't know a terrorist from a tadpole." Another sub-state-level fusion center official noted that "DHS has grown into quite the monster machine."

All the fusion centers participating in our study received funding from both the federal government, always from DHS and in some cases from the High Intensity Drug Trafficking Areas (HIDTA) or the FBI's Joint Terrorism Task Force (JTTF) programs, and from their state and local governments. In most cases technology and special projects were funded by federal grants and staff salaries were funded by the states and localities. The funding constraints and issues interviewees raised were reminiscent of what state officials find in other intergovernmental policy areas such as education, environment, and healthcare programs. Almost all fusion center officials talked about the need for "sustainment funding" for fusion centers – this became almost a mantra among the fusion center officials, something that DHS had clearly heard many times. Most fusion centers seem to rely primarily on state funding which they see as vulnerable to state fiscal woes. But they do not believe that they can count on DHS grant funding and, in some cases, have to dance around DHS requirements in order to secure the DHS funding that is available. For example, some DHS funding does not go to states but to local entities so in some cases fusion centers subcontract with local entities and run the funding through the local organization. One state level fusion center official described this as follows: "we have to go find a local jurisdiction that is willing to be the subgrantee for that money, and then they enter into a memorandum of understanding with us to allow us to have access to that funding to hire personnel and support the fusion center."

Data Sharing

All fusion center mission statements emphasize the role of the center in facilitating information sharing within the state, among states, with the federal government, and with components of the private sector (generally related to critical infrastructure protection). In some cases mission statements refer to the centers as "information hubs" with access to a range of databases. Most of these databases existed prior to the creation of the fusion center. We were particularly interested in three aspects of the data sharing that are occurring within and among fusion centers: 1) what databases are being accessed and by whom, and what other data sharing activities are occurring; 2) through what mechanisms and channels is data sharing taking place; and, 3) what laws and policies govern data sharing and dissemination.

Data Sharing Activities

Fusion center officials refer to a range of databases that they access on a more or less regular basis with varied results – these include federal databases, state and local databases, and private sector databases. Most of these databases existed prior to the creation of fusion centers but the centers create value in bringing the databases "under one roof" and providing, as one state level official said, a "one stop shop" for those needing information. One state-level fusion center official (whose center began with a focus on terrorism and evolved to all crimes) describes this as follows: "we're remotely connected in now, where we can get a whole host of information by just logging in and pulling it out ourselves, and analyzing it, and going from there." However, an official at an all crimes, all hazards center expressed some frustration with the sheer number of databases available: "the biggest challenge that we face when it comes to information sharing is overcoming those multiple paths that we have to use or have available to us."

With respect to federal databases, many officials mention the FBI's Law Enforcement

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Online (LEO) portal[2] as being helpful and easy to use; LEO is a long-standing system, which began in 1995 and provides access to a range of databases such as the National Center for Missing and Exploited Children (Federal Bureau of Investigation, 2012a). They also refer to the Department of Justice's Regional Information Sharing Systems (RISS) program.[3] Officials frequently mention the FBI's e-Guardian system, a terrorism-focused database into which fusion centers can input terrorism-related leads and extract relevant information through the LEO portal, as being generally helpful and easy to use but limited in its focus on terrorism. The e-Guardian system was developed in 2003 by the FBI's Threat Monitoring Unit. It is a "secret" level system that, as part of its jurisdiction, collects suspicious activity reports (SARs) made to the FBI and reviews them to determine those that warrant additional investigative follow-up (Federal Bureau of Investigation, 2012b). One state level official noted that his fusion center staff "work very closely and are trusted by the Bureau, which is not, it's not what I would've predicted seven years ago, to be honest with you. I wasn't sure where this was gonna go. But the cooperation has only gotten better—and the trust."

Also mentioned frequently is 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 cyberinfrastructure but expanded, after 9/11, to include critical infrastructure more generally. As of October 2012, InfraGard had 51,953 members, including the FBI (InfraGard, 2012). InfraGard is integrally involved in supporting information sharing, not just on counterrorism and cyber crime, but also 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 state official at an all crimes/all hazards/all threats center asserted, "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 ensure credibility." However, a few fusion center staff see InfraGard as more of a public relations or outreach tool with limited practical utility: "it's FBI's kind of backhanded attempt to do critical infrastructure. That's not their business, and you know, it's kind of the FBI trying to be all things to all people... it's as much of a propaganda tool as it is anything else."

Although most fusion center officials give relatively high marks to the FBI systems, they are less enamored with the usefulness of the DHS systems. An official at a sub-state fusion center focused on terrorism and all crimes noted that with respect to HSDN, the classified version of the Homeland Security Network, "Honestly we never use it because there's nothing in it." Another state level official at an all crimes center noted that DHS puts out a level of duplication of information that is "ridiculous" and that occurs "long after we have gotten it from other sources."

States themselves have a range of databases that tend to vary quite a bit by state. What appears to be occurring more regularly with the creation of fusion centers is that states are giving other states more access to these databases, such as prescription drug tracking programs. In other cases, state systems in specific areas, such as suspicious activity reports or highway patrol systems, are now linked to federal databases through one state portal, often managed by the fusion center; these state databases are then available to other states through the federal portals.

Fusion center analysts also draw upon a range of more or less established private sector database sources, such as LexisNexis's Accurint and LocatePlus, especially for searches of public record information. Most fusion center personnel tend to see private sector databases as having the same problems that they have traditionally had. As one state-level official

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

at a fusion center that began as terrorism and became all crimes noted, "We do have some subscription center databases, obviously that we pay for with grant money. But…you'll find that that information that is in some of these databases has to be verified."

In addition to database access and sharing, fusion center officials often mention Suspicious Activity Reports (SARs) as a way of sharing information. Law enforcement has been using some form of SARs for decades, collected through a variety of mechanisms including hotlines, 911 calls, neighborhood watches, schools and community centers, etc. The value and reliability of such reporting have often been questioned, especially as their use expands in a way that will likely result in an overload of information of dubious quality that requires a huge investment of time to investigate (American Civil Liberties Union, 2010; Nojeim, 2009; Randol, 2009). However, as a practical mechanism for collecting information and raising public awareness SARs have persisted as a tool of community oriented policing (Steiner, 2010). Since its creation, DHS has included SARs in its counter-terrorism activities, with a few different information sharing systems and the newest public outreach being Secretary Napolitano's, "If You See Something, Say Something Campaign."[4]

Our research finds that SARs reporting is labor intensive. An official at one state level fusion center, which began as counter-terrorism and became all crimes, stated "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, 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 an all crimes state level 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."

Mechanisms/Channels for Data Sharing

Our interviews indicate that in their day-to-day activities fusion centers rely less on technology enabled collaboration and rely more on email, phone calls, and personal networking at conferences. This statement of a sub-state fusion center official is typical: "our main source of communication is through email right now." Officials realize the limitations of technology and elaborate databases. An official at a state-level fusion center lamented that the different federal agencies, DHS and FBI in particular, "have their secure networks of communication which requires registering, getting authorization, logging on, and they're, we're still kind of stuck in this looping of information where there's too many portals that we have to go to, to get information." Another state official commented: "I think we are in a position like many where, more often than not we get our breaking news from CNN and MSNBC before we get it through our federal law enforcement partners."

Several fusion center officials noted that they used Microsoft Fusion Core, which was designed and marketed by, Microsoft especially for use by fusion centers. As Microsoft describes it:

Microsoft Fusion Framework is an integrated, holistic technology architecture for fusion centers, which can help you to enhance information-sharing and security by automating collection, intake, workflow management, collaborative analysis, data visualization, dissemination, auditing, and capture of business-performance metrics. (Microsoft, 2012)

Notwithstanding the rapid standard usage of Microsoft Fusion Core and other third-party databases and platforms, most fusion center officials we interviewed voiced palpable frustration with information technology vendors. One sub-state official commented: "We get bombarded by the vendor community." Another referred to the vendors as "vultures," noting that they "follow the grant money." A

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

similar sentiment was expressed by a sub-state official who said: "9/11 created this whole new industry of what I call grant whores." Still another pointed out that the vendors "have a huge lobby on Capitol Hill that proposes FCC regulation changes that result in them being able to sell more of their product or a newer version of the product." Almost all mentioned that they actively avoid phone calls from vendors. Fusion center officials from three different states specifically recommended that DHS or DOJ vet the vendor products and provide guidance as to what systems and products were reliable, cost-effective, and appropriate for fusion centers.

While the private sector may provide some of the platforms for information acquisition and analysis, fusion centers have also opened up some channels for sharing between the public and private sectors. For instance, as mentioned above, the InfraGard program encourages private owners of critical infrastructure (e.g., utility companies, shipping companies, universities, or hotels) to report suspicious activities or perceived threats, and these companies are provided updates, in turn, of non-classified information that may be relevant to them. Likewise, some fusion centers allow industry representatives to work alongside other analysts at fusion centers, thereby granting them direct access to information that they would not have otherwise. For instance, the Seattle fusion center hosts an analyst from the company Boeing, and executives from Boeing have argued that they should have access to both unclassified *and* classified information (German & Stanley, 2007). As difficult as the regulation of information sharing appears to be for law enforcement and intelligence agencies, it is certainly made more challenging—and perhaps more open to privacy and civil liberties violations—when private companies are integrated into the process. This is particularly the case because the sharing of personal information by private companies is not subject to the same legal guidelines that apply to law enforcement agencies.

Policies Governing Data Sharing

Information sharing occurs in a somewhat traditional context of law enforcement, set by Title 28 Part 23 of the Code of Federal Regulations (28 CFR Part 23), the federal regulations for the collection, retention and disclosure by state and local law enforcement systems that receive federal funds.[5] 28 CFR Part 23 requires, in part, that before information be collected there be "reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity (quoted in German & Stanley, 2008, 2). Fusion center officials appear to be relying on 28 CFR Part 23 when questions are raised about the appropriateness of their information gathering practices. For example, one official at a state fusion center observed that "it's what's going to save us; if, if we get looked at by the ACLU, or whoever wants to come in; we're 28 CFR compliant. We make sure of that…we have our reliance for protection against suits and things of that nature."

A few fusion centers pointed out that 28 CFR Part 23 required management of information and that information systems "that allow us to properly store information and to comply with 28 CFR at the same time" were worth buying with grant money. Other fusion center officials, though, were more vague pointing out that this regulation covers "criminal intelligence" and that it becomes operative when "intelligence files" are created. For example, one state official remarked that "within our center we comply with 28 CFR which basically, unless there's a nexus to terrorism or criminal activity…we can't get involved in it. So anything that we do has a criminal nexus." This would appear to leave other categories of information in need of other protection.

It is here that a host of DHS privacy requirements come into play – requirements that several fusion center officials have found difficult to navigate. Most fusion centers have adopted privacy policies, but in some cases found DHS approval overly bureaucratic and

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

would have preferred more DHS guidance or direction. For example, one official commented "they all could have the same privacy policy, right, and instead of having seventy-two of 'em, 'cause sometimes they'll be submitted into the Department of Homeland Security and it'll take six to seven months or more to get it back." This was echoed by another official: "Why don't the Feds just put one [privacy] policy out and say this is what everybody will follow? We have spent hours writing and researching the policy. We went through four reviews with the Feds because, you know, we submitted it, they kicked it back. We submitted it, we had a different analyst reviewing it, so they found different things, kicked it back." Interestingly, DHS and DOJ have jointly issued fairly detailed guidelines for the development of fusion center privacy policies, including a policy development template (U.S. Department of Homeland Security and Department of Justice, 2010) – and many fusion center privacy policies appear to follow the boilerplate organization and language that DHS provided.[6]

The clear impression from our data is that fusion centers are aware of the need to use personally identifiable information appropriately – but their primary context is one of local experiences with criminal intelligence information. The law enforcement culture, with is emphasis on protecting confidentiality of information and sources so that investigative information would be ruled admissible in court, provides the framework for thinking about personal information. The DHS framework of privacy notices and fair information practices (FIPs) is one that seems bureaucratic and somewhat alien to them. Privacy scholars have also questioned the relevance of a FIPs approach, which is premised on individual records, in more complex and fluid information environments; additionally, the FIPs framework may not be appropriate for the networked information sharing environment within which fusion centers operate (Citron & Pasquale, 2011).

CONCLUSION

The creation of DHS fusion centers, and the multiple organizations and databases that are part of fusion centers, have engendered an environment in which information is migrating beyond the intended focus on counterterrorism. Indeed, fusion centers that were originally oriented toward "counterterrorism" have quickly broadened their scope to include all crimes, and those that began as "all crimes" have migrated only marginally to terrorism, and arguably as a result of the grant opportunities that DHS made available. As we discuss above, this is the result of three quite predictable factors: fusion centers have to be valuable to their states, there is too little activity that is clearly terrorism related, and fusion center personnel have to use their time and skills constructively.

In part because most fusion centers are "all crimes" we did not find much variation in mission creep among the fusion centers we examined. The variation we did find seems to be largely explained by the geographic, economic and demographic characteristics of the state. If the state had large components of a particular critical infrastructure (for example, a nuclear power plant or busy international port), then it was likely to be collecting and sharing information with those components of the private sector. If a state contained military bases or large scientific research enterprises, that would affect its information sharing. Similarly if a state had a large immigrant population, it would be attuned to the activities of that group. These variations also map onto the different origins of fusion centers, such that those growing out of High Intensity Drug Trafficking Areas programs still emphasize drug interdiction and the investigation of gang activity, whereas those emerging from and co-located with Joint Terrorism Task Force programs appear to contribute more regularly to suspicious activity report databases and run training operations for law enforcement and other public-sector agencies.

Generally, although fusion center officials do see themselves as "connecting the dots" as identified in the 9/11 Commission Report, our

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

interviews reveal that they do not appear to see themselves as doing something fundamentally different from what they had been doing under the aegis of "community policing" or "intelligence-led policing." Fusion center personnel are talking across more organizations, both within the state/local area and across neighboring states as well as with the federal government, but the information they are talking about largely involves ongoing criminal investigations and to some extent communications about suspicious activity reports. We queried all the fusion center officials about "success stories" and virtually all who chose to respond relayed a local law enforcement incident – a child abduction, a local suspect fleeing by car to another state, a law enforcement impersonator operating in two locations within a state, etc. Contrary to some of the claims quoted earlier that fusion centers tend to focus on crimes that are precursors to terrorism, these "success stories" illustrate that daily practices at fusion centers are much closer to basic policing.

Some fusion center representatives perceive the focus on all crimes and the support for local law enforcement as part of the maturing process for fusion centers. As one informant noted: "how we mature fusion centers is maturing the local and state law enforcement's understanding of intelligence, criminal intelligence and homeland security as well. They understand it from a very operational perspective. 'What can you do for me to help me catch the next criminal?'" However, the fact that fusion centers are, for the most part, co-located within police or sheriff units and populated with law enforcement personnel makes it unclear if the influence is going to work in the direction of inclusion of homeland security and terrorism, or if fusion centers will primarily provide more coordinated general law enforcement. The fact that many fusion center officials find fault with DHS funding, responsiveness, and direction suggests that the centers are more likely to move towards more general law enforcement, especially in the context of threats of budget cuts at the federal level.

Although this may well be a laudable national goal, it is not what the 9/11 Commission recommendations or the formation of the Department of Homeland Security intended. This question about which way fusion centers will evolve is reflected in something of a disconnect between the rhetoric about fusion centers at the federal level (DHS and National Fusion Center organization) and what fusion center officials say in interviews. The federal level emphasizes the value to national or homeland security, whereas state and local officials emphasize the value to the state. If the current funding arrangements for fusion centers and the mix of personnel currently working in fusion centers continue, it appears likely that fusion centers will continue to evolve in the direction of being dual purpose, with some national security/intelligence activities but supporting more domestic/law enforcement goals. If this is the case, then there is likely to be continued confusion among fusion center officials about the primary accountability and legal frameworks they should follow. Under such circumstances, even if local policing needs are met through fusion-center funding and support, one should expect cases of mission creep and privacy violations to continue unabated.

ACKNOWLEDGMENT

This research is funded by the National Science Foundation, SES 0957283, SES 0957037, and SES 1339199. Krista Craven and JoAnn Brooks provided research assistance.

REFERENCES

American Civil Liberties Union. (2010, June 29). *More about suspicious activity reporting.* Retrieved October 30, 2012, from http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting

Bureau of Justice Assistance. (1994). *Understanding community policing: A framework for action*. Washington, DC: U.S. Department of Justice.

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Bureau of Justice Assistance. (2005). *Intelligence-led policing: The new intelligence architecture*. Washington, DC: U.S. Department of Justice.

Chesluk, B. (2004). Visible signs of a city out of control: Community policing in New York City. *Cultural Anthropology*, *19*(2), 250–275. doi:10.1525/can.2004.19.2.250

Citron, D. K., & Pasquale, F. (2011). Network accountability for the domestic intelligence apparatus. *The Hastings Law Journal*, *62*, 1441–1494.

Electronic Privacy Information Center. (2007, June). *National network of fusion centers raises specter of COINTELPRO*. Retrieved October 30, 2012, from http://epic.org/privacy/surveillance/spotlight/0607/

Federal Bureau of Investigation. (2012a). Law enforcement online. Retrieved October 30, 2012, from http://www.fbi.gov/about-us/cjis/leo

Federal Bureau of Investigation. (2012b). *Privacy impact assessment for the eguardian threat tracking system*. Retrieved October 30, 2012, from http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat

Geiger, H. (2009, December 15). Fusion centers get new privacy orders via DHS grants. Retrieved June 2, 2010, from http://www.cdt.org/blogs/harley-geiger/fusion-centers-get-new-privacy-orders-dhs-grants

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). ACLU fusion center update. Retrieved from http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf

Government Accountability Office. (2010, September 29). *Information sharing: Federal agencies are helping fusion centers build and sustain capabilities and protect privacy, but could better measure results (GAO-10-972)*. Retrieved October 30, 2012, from http://www.gao.gov/products/GAO-10-972

Government Accountability Office. (2011, July 21). *Information sharing environment: Better road map needed to guide implementation and investments (GAO-11-455)*. Retrieved October 30, 2012, from http://www.gao.gov/new.items/d11455.pdf

Herbert, S. (2005). The trapdoor of community. *Annals of the Association of American Geographers. Association of American Geographers*, *95*(4), 850–865. doi:10.1111/j.1467-8306.2005.00490.x

InfraGard. (2012). *InfraGard -- Public private partnership*. Retrieved October 30, 2012, from http://www.infragard.net/about.php?mn=1&sm=1-0

Kean, T. H., Hamilton, L. H., Ben-Veniste, R., Kerrey, B., Fielding, F. F., Lehman, J. F., & Thompson, J. R. (2004). *The 9/11 commission report: Final report of the national commission on terrorist attacks upon the United States*. Washington, DC: U.S. Government Printing Office.

Masse, T., O'Neil, S., & Rollins, J. (2007, July 6). *Fusion centers: Issues and options for congress*. Congressional Research Service. Retrieved October 30, 2012, from http://epic.org/privacy/fusion/crs_fusionrpt.pdf

Microsoft. (2012). *Microsoft fusion core solution*. Retrieved October 30, 2012, from http://www.microsoft.com/industry/government/solutions/Fusion_Core_Solution/default.aspx

Monahan, T. (2011). The future of security? Surveillance operations at homeland security fusion centers. *Social Justice (San Francisco, Calif.)*, *37*(2-3), 84–98.

Monahan, T., & Palmer, N. A. (2009). The emerging politics of DHS fusion centers. *Security Dialogue*, *40*(6), 617–636. doi:10.1177/0967010609350314

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. doi:10.1353/jls.2012.0033

Napolitano, J. (2009). *Remarks by homeland security secretary Janet Napolitano to the national fusion center conference in Kansas City, Mo. on March 11, 2009*. Kansas City, MO: Department of Homeland Security.

Newkirk, A. B. (2010). The rise of the fusion-intelligence complex: A critique of political surveillance after 9/11. *Surveillance & Society*, *8*(1), 43–60.

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 October 2013, from https://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. *Washington Post*. Retrieved August 20, 2008, from http://www.washingtonpost.com/wp-dyn/content/article/2008/04/01/AR2008040103049.html

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Partnership for Civil Justice Fund. (2012, December 22). FBI documents reveal secret nationwide occupy monitoring. *Partnership for Civil Justice Fund*. January 4, 2013, from http://www.justiceonline.org/commentary/fbi-files-ows.html

Permanent Subcommittee on Investigations. (2012, October 3). Federal support for and involvement in state and local fusion centers. *U.S. Senate*. Retrieved October 30, 2012, from http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04

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 October 30, 2012, from http://www.ijis.org/docs/NSI Report_R40901.pdf

Ratcliffe, J. H. (2003). Intelligence-led policing. *Trends and Issues in Crime and Criminal Justice*, *248*, 1–6.

Regan, P. M. (2004). Old issues, new context: Privacy, information collection and homeland security. *Government Information Quarterly*, *21*(4), 481–497. doi:10.1016/j.giq.2004.08.003

Rollins, J. (2008). *Fusion centers: Issues and options for congress*. Washington, DC: Congressional Research Service.

Ruben, M., & Maskovsky, J. (2008). The homeland archipelago: Neoliberal urban governance after September 11. *Critique of Anthropology*, *28*(2), 199–217. doi:10.1177/0308275X08090549

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 October 30, 2012, from http://www.hsaj.org/?article=6.3.5

U.S. Department of Homeland Security. (2006, July 7). DHS strengthens Intel sharing at state and local fusion centers. Retrieved December 19, 2012, from https://http://www.hsdl.org/?view&did=476394

U.S. Department of Homeland Security. (2008). *DHS' role in state and local fusion centers is evolving*. Washington, DC: U.S. Department of Homeland Security.

U.S. Department of Homeland Security and Department of Justice. (2010, April). Fusion process technical assistance programs and services. *Fusion Center Privacy Policy Development: Privacy, Civil Rights and Civil Liberties Policy Template*. Retrieved October 30, 2012, from http://it.ojp.gov/docdownloader.aspx?ddid=1269

ENDNOTES

1 For a compendium of material about fusion centers and privacy, see: http://epic.org/privacy/fusion/

2 The FBI's LEO homepage describes LEO as follows: "LEO is a secure, Internet-based communications portal for law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. LEO catalyzes and strengthens collaboration and information-sharing by providing access to sensitive but unclassified information and various state-of-the-art communications services and tools. It is available to vetted users anywhere in the world around the clock and is offered free of charge to members." See: http://www.fbi.gov/about-us/cjis/leo

3 For more information see: http://www.riss.net/Default/Overview

4 For more information see: http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm

5 28 CFR Part 23 has become the de facto national standard for sharing criminal intelligence information. This has happened over the last several years for a variety of reasons. The primary reason is that the regulation has been in place since 1980, with only minor revision and clarification to address emerging technology, providing clear and succinct guidance to hundreds of intelligence systems. Also, a recent impetus is that the *National Criminal Intelligence Sharing Plan* (NCISP) recommends the use of the regulation in order to ensure that the collection/submission, access or storage, and dissemination of criminal intelligence information by law enforcement agencies conforms to the privacy and constitutional rights of individuals, groups, and organizations. The NCISP recommends that this occur regardless of whether or not an intelligence system is Crime Control Act-funded and therefore subject to the regulation. The adoption of 28 CFR Part 23 as a guideline allows agencies to demonstrate a good-faith effort toward protecting individuals' rights, thereby protecting agencies from potential civil liability. For more information see: http://www.iir.com/Justice_Training/28cfr/FAQ.aspx?AspxAutoDetectCookieSupport=1#q1

6 For links to privacy policies of individual fusion centers see: http://www.nfcausa.org/default.aspx/MenuItemID/121/MenuGroup/Map.htm

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Priscilla M. Regan is Professor and Chair of the Department of Public and International Affairs at George Mason University. Her primary research interests have focused on both 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 over forty articles or book chapters, as well as Legislating Privacy: Technology, Social Values, and Public Policy *(University of North Carolina Press, 1995). As a recognized researcher in this area, Dr. Regan has testified before Congress and participated in meetings held by the Department of Commerce, Federal Trade Commission, Social Security Administration, and Census Bureau. She was a member of the National Academy of Sciences, Computer Science and Telecommunications Board, Committee on Authentication Technologies and their Privacy Implications.*

Torin Monahan is 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 the ways in which surveillance and security programs tend to reproduce social inequalities. His most recent books include SuperVision: An Introduction to the Surveillance Society *(with John Gilliom, University of Chicago Press, 2013) and* Surveillance in the Time of Insecurity *(Rutgers University Press, 2010), which won the 2011 Surveillance Studies Book Prize from the International Surveillance Studies Network. Monahan is an elected council member of the Sociology of Science and Technology division of the International Sociological Association and is an associate editor of the leading academic journal on surveillance,* Surveillance & Society.

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.