Zones of Opacity: Data Fusion in Post-9/11 Security Organizations*

Torin Monahan and
Priscilla M. Regan

A new paradigm of information sharing is transforming state surveillance practices in the United States and beyond. Just as network logics are altering other organizations, so too are police and intelligence agencies seeking effective ways to share information to combat crime and terrorism. While this shift is clearly part of larger, ongoing technological and cultural processes, one major catalyst was a widespread recognition that US intelligence agencies failed to act in concert to prevent the attacks of September 11, 2001.[1] On the national level, this motivated the creation of the massive Department of Homeland Security (DHS) in 2002, which incorporated 22 government agencies and employs over 230,000 people.[2] On state and local levels, DHS has sought to create a robust network of "fusion centres" to disseminate and analyse data on suspicious individuals or activities, assist with investigations, and identify potential threats.[3] Because fusion centres face the difficult task of harmonizing national security imperatives with local police needs, they are especially revealing of problems with the emerging state-surveillance apparatus.

In this article, we draw upon empirical research on fusion centres to theorize contemporary state surveillance. We conducted 55 semi-structured interviews from 2010 to 2012, predominantly with fusion-centre directors and analysts, but also with select representatives of private industry, activist organizations, and civil-society groups. In some instances we interviewed

* This material is based upon work supported by the National Science Foundation under grant numbers SES 0957283 and 0957037. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. JoAnn Brooks and Krista Craven provided research assistance.

1 Thomas H. Kean et al., *The 9/11 Commission Report: Final Report of The National commission on Terrorist Attacks upon the United States* (Washington, DC: US Government Printing Office, 2004).

2 See, e.g., Torin Monahan, *Surveillance in the Time of Insecurity* (New Brunswick, NJ: Rutgers University Press, 2010); US Department of Homeland Security, "About the Directorate for Management," (Washington, DC: Directorate for Management, 2011), http://www.dhs.gov/xabout/structure/editorial_0096.shtm.

3 Torin Monahan, "The Murky World of 'Fusion Centres'," *Criminal Justice Matters* 75, 1 (2009), 20–21; John Rollins, "Fusion Centers: Issues and Options for Congress," (Washington, DC: Congressional Research Service, 2008), http://www.fas.org/sgp/crs/intel/RL34070.pdf.

Canadian Journal of Law and Society / Revue Canadienne Droit et Société, 2012, Volume 27, no. 3, pp. 301–317.

multiple representatives from a single site, but in total, 36 separate fusion centres are represented in our interview sample. In addition, we conducted site visits at four fusion centres and two government/industry conferences and engaged in document analysis of fusion-centre products and government reports.

Instead of viewing fusion centres as central repositories for stockpiling and sharing personal data, we introduce the concept of "centres of concatenation" to describe how disparate data are drawn together as needed, invested with meaning, communicated to others, and then discarded such that no records exist of such surveillance activities. This can be contrasted with what theorist Bruno Latour has termed "centres of calculation"—where scientific laboratories work with mobile, static, and combinable data points to accrete knowledge and achieve control at a distance.[4] Fusion centres may be sites where information comes together, but they do not occupy a central, controlling position on the network; instead, they function as nodes on a decentralized network, usually responding to rather than directing the investigations of others. Also, in Latour's formulation, laboratories contend with a glut of information by forming useful abstractions and black-boxing agreed upon knowledge so that actors are not overwhelmed with detail. While fusion centres may operate in this capacity when they write and circulate intelligence documents, which do rely upon generalizations (e.g., about what groups or activities are threatening), their more usual role is that of finding and enumerating specific details. Thus, *centres of concatenation* can be characterized by the transience of the knowledge they produce, their responsiveness to the instrumental needs of others, and their affinity for detail over abstraction.

Overview of Fusion-Centre Activities

As of 2012, there were 77 official, DHS-sponsored fusion centres, which is a number that does not include the many unofficial public- and private-sector intelligence analysis organizations that perform similar functions. Most fusion centres are located in state or local police departments, but some are sited in other government buildings, on military bases, or are entirely free standing. Clearly, being co-located with law enforcement affords information sharing with police and continuity among intelligence organizations, such as the Federal Bureau of Investigation's Joint Terrorism Task Force (JTTF) or the federal High Intensity Drug Trafficking Areas (HIDTA) programs. In a number of cases, we found that JTTF or HIDTA programs simply mutated to incorporate fusion-centre roles and responsibilities so that even though the programs might have different names, they comprise the same individuals performing the same functions in the same locations.

---

[4] Bruno Latour, *Science in Action: How to Follow Scientists and Engineers through Society* (Cambridge: Harvard University Press, 1987).

All fusion centres are different. As informants put it: "If you've seen one fusion centre, you've seen one fusion centre."[5] Some employ a handful of analysts who work on a few computer stations and struggle to keep up with information requests. Others employ close to 100 staff members who monitor futuristic video walls, access secure rooms, and actively assist with ongoing investigations. Funding also varies radically from one fusion centre to the next. Many receive $1 million per year from DHS grants, for which they must apply and submit to routine audits. Others boast that they received $44 million in initial start-up funds and could count on $11 million per year in DHS grants. Most sites also depend heavily on state and local financial support, whether for office space, infrastructure investments, or personnel.

One thing that most fusion centres have in common is that they are oriented toward "all crimes," even if the original impetus for their creation was counterterrorism. By adopting an all-crimes approach, personnel at fusion centres make their activities directly relevant to the policing needs of their cities or regions, be they investigating methamphetamine production, illegal immigration, or sex trafficking. In addition, this approach assists fusion centres in securing additional funding from their states. As one informant explained:

> You know, terrorism is not the number one thing that we're looking at in [our state]. People are really worried about meth labs. They're worried about child exploitation. Those are kind of big; those are kind of the big crime issues, public visibility crime issues that we've got [here]. And so the fusion center was really focused on those things. And I think because of that, they could go to the legislature and say, "We have this fusion center. We have this DHS funding. Kick in some ongoing [state] funding for it, because we're looking at these things that are important to your constituents."

Fusion-centre directors rationalize applying counterterrorism resources to local needs by saying that they concentrate on crimes that are "precursors" to terrorism: "You know, we are focused on financial crimes, narcotics, things that would either support or fund terrorism; or could be precursor indicators of planning, you know, surveillance [of critical infrastructures], things like that."

Practically speaking, fusion centres make themselves relevant at the local level by sharing information, assisting with investigations, and generating intelligence "products" that aim to identify threats or risks. The sharing of information may be relatively innocuous, such as passing along FBI bulletins. Assisting with investigations can include anything from looking up a suspect in databases to assisting with setting up wiretaps. Generating products can include "threat assessments" for events (like the Superbowl or a political rally), "vulnerability assessments" of critical infrastructure (like bridges,

[5] All interviews were conducted in confidentiality, and the names of interviewees are withheld in accordance with our universities' ethics review board protocols.

monuments, power plants, or universities), or "suspicious activity reports" for anything from someone spray-painting a wall, to someone taking photographs of a building, to someone contributing to a political blog.

Intelligence products are fraught in that they require analysts to make judgments about others largely in advance of any evidence of wrongdoing. Under the rubric of "intelligence-led policing," these documents may seek to anticipate who will engage in a criminal act. They may try to explain to local law enforcement why something happening elsewhere could be relevant and important to them (such as bombs being sent through UPS carriers in another country). And they may attempt to identify patterns in local crimes that could be of interest to law enforcement personnel in other jurisdictions. Creating an intelligence product is an interpretive act: the analysts are not just communicating facts, but saying what the facts mean; not just identifying known threats, but imagining what the next threats might be.

Thus, these analysis documents seem to invite racial and religious profiling and civil liberties violations because they reflect the biases of those compiling them.[6] As one technology vendor succinctly put it: "they [fusion centres] desperately want to go look for young Muslim men. I mean, that's the reality." The many unprompted examples offered by fusion-centre staff in interviews affirm this prejudice. Fusion centres assist with investigations at Mosques, attempt to identify and keep track of Yeminis, file suspicious activity reports on people "talking on the phone in a foreign language," and track people who they think might be sending money to "freakin' somewhere in the Middle East." While the focus of this article is on the development of information-sharing practices, it is important to bear in mind that the same interpretive mechanisms that allow fusion centres to tailor their work to local needs also seem to invite profiling and other abuses.[7]

Fighting a Network with a Network

Technological interconnection and fluid movement are viewed as threatening to law enforcement when mobilized by criminals or terrorists, but cultivating these attributes is perceived as the appropriate response to such threats. Whereas the initial rationale for fusion centres was to "connect the dots" to prevent future terrorist attacks, the discourse has since morphed to one of combating invisible networks of criminals with networks of police and data.[8] One fusion-centre director explained:

> The best way to counter a criminal network is with a [police] network . . . Threats are getting more significant. The only way to counter that is to be smart about it and share information. You

---

6 See generally Torin Monahan, "The Future of Security? Surveillance Operations at Homeland Security Fusion Centers," *Social Justice* 37, 2–3 (2011).

7 See, e.g., Keith Guzik, "Discrimination by Design: Predictive Data Mining as Security Practice in the United States' 'War on Terrorism'," *Surveillance & Society* 7, 1 (2009); also see Monahan, "The Future of Security?"

8 Mimi Hall, "State-Run Sites Not Effective vs. Terror; Report Blasts Costly Intelligence Centers," *USA Today* (July 24, 2007): 1A.

> know, it's gone beyond the traditional "need to know, right to know" to—as you know the FBI has made it clear—to a mindset of "need to share." It's recognized that you've gotta share information in order to accomplish the goal.

This logic of networked information sharing—across jurisdictions and organizations—drives the practices of fusion-centre personnel and gives rise to structures that support those practices.

It may seem counterintuitive, but the primary way that networked information sharing occurs at fusion centres is through the embodied presence of individuals from different agencies at one physical location. Put simply, at most fusion-centre sites, "embedded analysts" sit together in a room, access the respective databases of their agencies, and share verbally (and textually) with one another. Some of the possible agencies represented by these personnel are the FBI, DHS, Secret Service, National Guard, Coast Guard, Marine Corps, Customs and Border Protection, Immigration and Customs Enforcement, Drug Enforcement Agency, state-level Departments of Corrections, Highway Patrol, and many others, including private-sector analysts and security representatives from private companies. According to a ranking officer at a fusion centre,

> The true benefit is to have those agents from the different agencies sitting next to each other with all of their datasets, all their legacy and their parent agency data, piped right to their desk. You'd have a DEA Intel analyst sitting next to an ICE Intel analyst sitting next to a DHS border analyst, and they all have their agency data right at their fingertips. That's the true value of fusion.

Because each analyst possesses the requisite security clearance for his or her agency's databases and can access those databases remotely, this facilitates rapid information exchange. There is no need to call the FBI, for instance, when an FBI analyst is sitting right next to you and can pull up any information you require. (As a caveat, though, we should note that in one interview a fusion-centre director expressed frustration at not receiving the "full story" from analysts working in his centre, most likely because the director lacked the appropriate clearance to hear certain classified information.) An additional benefit of the model of "embedded analysts" is that oftentimes the respective agencies will pay a portion, if not the entirety, of those analysts' salaries, which increases the viability of the centres, although it can also introduce ambiguity about chains of command.

"One-Stop Shop" for Data

The amount of data that fusion centres can access is truly impressive. A sampling of possibilities include welfare and unemployment checks, firearm licenses, car-rental information, credit reports, department of motor vehicles records and photos, employment histories, addresses and phone numbers, pawn-shop information on customers, postal department inquiries, public health data, police investigation data, identity-theft reports, suspicious activity

reports, and probation, parole, and booking information from police departments and correctional facilities. In addition to the slew of local and state databases, some of the top federal-agency databases used are the FBI's InfraGard (for critical infrastructure information), the FBI's eGuardian (for suspicious activity reports), the FBI's National Crime Information Center, the FBI's Interstate Identification Index (for criminal histories), DHS's Homeland Security Information Network (for unclassified information), and DHS's Homeland Security Data Network (for classified information).

Analysts also avail themselves of databases and technology platforms provided by the private sector for accessing and sharing law-enforcement data, such as SRA International's "Gangnet" application for recording, monitoring, or sharing data on gang activity; i2's "Coplink" for finding patterns in data—ostensibly to locate potential terrorists or criminal suspects; or Microsoft's "Fusion Core," which is quickly becoming the standard, primary system for information management at fusion centres. Finally, analysts routinely take advantage of a range of private-sector, "for-a-fee" databases compiled by data aggregators and containing personal information about individuals. Some of the most often referenced companies or databases of this type were Entersect, LexisNexis' Accurint, LocatePlus, and Targus. In sum, by means of ubiquitous data collection and the convergence of public and private database systems,[9] analysts can acquire fine-grained, three-dimensional information on individuals with amazing ease.

Data access, fusion, and dissemination define the everyday practices of analysts. As one director told us, "We'll leverage all the databases. We buy a lot of commercially available data and then we have, I believe 53 other databases that we utilize, and we did over 16,000 requests of that type [domestic terrorism] last year alone with 28,000 products disseminated so that's a pretty large amount." (In this instance, "products" refers to responses to information requests, not threat or risk assessments.) Most requests for data come from police working on investigations or from other fusion centres, although sometimes the private sector will request information concerning critical infrastructure protection. Interestingly, informants indicated that the majority of requests are made the "old-fashioned way"—either through email or by phone. This occurs in spite of the many high-tech networking platforms designed for sharing data, primarily due to a lack of standardization or problems with interoperability among systems.

Fusion centres have become key portals for *any* law-enforcement or counterterrorism information requests, in large part because of the unprecedented access that they have to data:

> So, we're fortunate enough that we have access to many, many databases here that, I don't want to say a lot of 'em, they existed prior to the fusion centre being born, but we just have, most fusion centres actually bring all those databases under one roof, if you will. We're

[9] See generally David Murakami Wood and C. William R. Webster, "The Normality of Living in Surveillance Societies," *Innovating Government* 20, 3 (2011).

> kind of like a "one stop shop" if somebody needs information. We're able to access those databases. So we get requests. I think we had well over two thousand requests last year for information.

As law-enforcement personnel learn about them and as their functionality improves, fusion centres bring about heightened expectations for rapid and easy information sharing. The "one-stop shop" analogy begins to become a factual observation rather than aspiration:

> The network, it's grown a lot, and I guess, I hate to use [the term] "one-stop shopping," [but] I mean it's one place to go 24/7 where you can get an answer whether it's terrorism or whether it's a hit-and-run accident and you're trying to find a partial registration plate and everything in between.

Thus, with the systems in place, police do not have to limit their requests to terrorism-related activities; instead they have access to almost any data they desire for any investigation. Data-gathering by fusion centres may also include the use of unmanned aerial drones,[10] as well as traffic and public-safety closed-circuit television (CCTV) cameras.[11] The ease of accessing data for any purpose clearly illustrates the function-creep potential of fusion centres.

Patterns, Prejudices, and Criminal Predicates

Fusion-centre analysts refer to their database queries as being "like Google," except for police. This understanding implies a similarity between analysts' queries and everyday searches for information on the Internet. But such heightened search capabilities can introduce challenges when certain criteria must be met *before* searches can commence. Explicitly, Title 28 Part 23 of the Code of Federal Regulations (CFR) prohibits the collection or storage of criminal intelligence information without "reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."[12]

Software applications designed to search for unknown "patterns" in data, like some of those mentioned previously, clearly rub against the grain of this legal restriction, encouraging searches for wrongdoing absent any prior evidence.[13] For instance, the press material for i2's popular Coplink system,

---

[10] Public Intelligence, "Drone Aircraft Are Patrolling U.S. Cities," *Public Intelligence,* April 26, 2010, http://publicintelligence.net/drone-aircraft-are-patrolling-u-s-cities/; also see Tyler Wall and Torin Monahan, "Surveillance and Violence from Afar: The Politics of Drones and Liminal Security-Scapes," *Theoretical Criminology* 15, 3 (2011).

[11] See Laura Crimaldi, "Boston Police Unveil New 'Real Time' Tech Center," *BostonHerald.com* (March 2, 2010) http://news.bostonherald.com/news/regional/view/20100302boston_police_boast_early_success_with_new_real_time_technology_center/ (last accessed March 20, 2010); see also Blake Harris, "Chicago Fusion Center Gives Police New Criminal Investigation Tools," *Digital Communities* (April 21, 2008), http://www.govtech.com/dc/261463.

[12] Mike German and Jay Stanley, "ACLU Fusion Center Update" (July 2008), 2, http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.

[13] See Rosamunde van Brakel and Paul de Hert, "Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies," *Journal of Police Studies* 20, 3 (2011).

which is used by many fusion centres, states: "COPLINK®'s ability to instantly detect non-obvious relationships, associations and patterns to generate actionable investigative leads will reduce the time it takes to identify and apprehend criminal or terrorism suspects."[14] Searching for relationships, associations, and patterns before identifying a suspect, as this quote advises, is tantamount to conducting an illegal "fishing expedition." The ways in which fusion centres understand and navigate these tensions—between technical capabilities and legal requirements—determines whether civil liberties and privacy protections are preserved or attenuated, both now and into the future.

One discursive move made by our interviewees at fusion centres was to try to draw a clear line between legal and illegal queries and to assert that they always establish a solid link to crime or terrorism before accessing any information:

> As long as we're constantly keeping our eye on the ball here, and understanding that there has to be a criminal predicate or a nexus to terrorism before we start collecting the different information on our citizens, or those that are not necessarily citizens but living within our boundaries, what we do is legitimate.

Other informants affirm this position by saying that when they receive information requests, they always ask for a "case number" to make certain that someone is not just acting on a hunch.

But the supposed standard of establishing a connection to terrorism seems quite vague and perhaps too easy to accomplish. One director succinctly explained that a "nexus to terrorism" could be any "behaviors and incidents that could spell terrorist activities," such as taking photographs of buildings. Indeed, a law-enforcement-sensitive "Terrorism Indicators Reference Card," put together by the New York State fusion centre, makes it seem simple to establish reasonable suspicion based on someone displaying any of an incredibly inclusive list of indicators, 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."[15]

There is also the reality that people at fusion centres may perceive legal requirements as being overly burdensome and unnecessarily bureaucratic. A ranking officer at one site explained deviations from regulations as unremarkable:

> Interviewer: Have there been any incidents where someone was seen to transgress what they should've been doing with the fusion centre?
> Interviewee: Probably, like anywhere, you have people that will, you

[14] i2 Group, "COPLINK&® Deployed to Boost Crime Solving and Anti-Terrorism Initiatives at the Chicago Police Department's Crime Center" (October 3, 2007), http://www.i2group.com/news-article.asp?id=75.

[15] 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/.

> know, try and save a step and, you know, skirt around a policy that might require them to make a notification that they're gonna be sending out information.

He continued to say that in such circumstances, which have occurred at his site, it is simply up to supervisors to be aware of these shortcuts and gently correct the person involved. At the same time, though, the FBI has been active in radically changing the legal-threshold requirements for fusion-centre analysts and others. According to the *New York Times,*

> Under current rules, agents must open such an inquiry before they can search for information about a person in a commercial or law enforcement database. Under the new rules, agents will be allowed to search such databases without making a record about their decision. Mr. German [at the ACLU] said the change would make it harder to detect and deter inappropriate use of databases for personal purposes. But Ms. Caproni [the FBI general counsel] said it was too cumbersome to require agents to open formal inquiries before running quick checks. She also said agents could not put information uncovered from such searches into F.B.I. files unless they later opened an assessment.[16]

In other words, running searches can be done without demonstrating a need, but saving information will require authorization. Thus, it seems that the norms people have for Internet searches (i.e., Googling anything on a whim) will be officially permitted for police work with sensitive databases, such that "running quick checks" on people without establishing reasonable suspicion or a "nexus to terrorism" will become commonplace and will be entirely undocumented unless an investigative case is opened.

It's in the Cloud

The developing norms and practices of fusion centres introduce difficulties for ensuring the protection of civil liberties. If fusion centres are not keeping track of their "quick" searches and are not storing search data on site, then there may be no records for oversight bodies, the media, civil society groups, or others to inspect. Indeed, an important part of the story told by fusion-centre personnel is that they simply channel information from one party to another:

> I know people always have like this kind of conspiracy theory of what they don't know, but the reality is this is *just* information—that threats come in, which is reasonable suspicion, probable cause; the information is looked at from a number of different perspectives, and you know, classified and unclassified systems; and then moved over to the Joint Terrorism Task Forces, which then disrupt terrorism. We're a channel.

---

[16] Charlie Savage, "F.B.I. Agents Get Leeway to Push Privacy Bounds," *New York Times* (June 12, 2011), http://www.nytimes.com/2011/06/13/us/13fbi.html?_r=1&nl=todaysheadlines&emc=tha2.

In this construction, analysts act as neutral intermediaries; organizationally speaking, they are the Google system for investigations. Of course, Google's algorithms tailor results to what they predict individual users will want to see based on past searches and Internet browsing,[17] so this analogy could be extended to say that fusion-centre analysts might also be acting upon unspoken assumptions of what their intended law-enforcement audiences desire to see.

The narrative of not collecting or storing information, while certainly not entirely true,[18] is deployed to insulate fusion centres from external scrutiny. One director even suggested that they had the ACLU's full support because no information was being held on site:

> Interviewee: When we first opened up . . . we did bring in ACLU, and we gave 'em a complete brief of everything we were doing and how we were doing it, and all that.
> Interviewer: How did that go?
> Interviewee: In fact, they were ecstatic. They wanted to know what we were doing, and how we were doing it, and we showed 'em and we told 'em. And they said, "Well, what information are you storing?" And we told them, "We can't store anything unless there's a criminal predicate."

Other evidence suggests that groups like the ACLU may not be all that supportive of this situation. For example, the ACLU chapter of New Mexico felt stonewalled when it filed open-records requests of that state's fusion centre and was told that there was no information to share because there was technically no "material product" generated from accessing or mining data located elsewhere.[19] In an era of networking and cloud computing, where it is commonplace for data to be held by other parties in remote locations, existing legal mechanisms for oversight and accountability may be woefully out of date.[20] This is especially true, it seems, for oversight dependent upon locally stored materials or data.

At the same time, though, fusion centres may be taking advantage of technological changes to claim partial immunity from existing legal constraints, such as the Code of Federal Regulations restrictions described above. The following passage from a fusion-centre director is quoted at length because it captures some of the nuance of this position, wherein fusion centres request patience and leeway for infractions while they work out the bugs and the law catches up:

> We're at a place where you've got fusion centres that are really working hard to professionalize [their activities], and to do it in a structure that

---

17 Eli Pariser, "How the Net Traps Us All In Our Own Little Bubbles," *The Guardian,* June 12, 2011, http://www.guardian.co.uk/technology/2011/jun/12/google-personalisation-internet-data-filtering?cat=technology&type=article.

18 See Danielle Keats Citron and Frank Pasquale, "Network Accountability for the Domestic Intelligence Apparatus," *Hastings Law Journal* 62 (2011).

19 Hilary Hylton, "Fusion Centers: Giving Cops Too Much Information?" *Time.com,* March 9, 2009, http://www.time.com/time/nation/article/0,8599,1883101,00.html.

20 Citron and Pasquale, "Network Accountability for the Domestic Intelligence Apparatus."

> honors the civil rights, the civil liberties, that law enforcement has been expected to honor for years. The difference is, is now you're in an age of a more advanced technology and a lot more information than we've ever had before at our fingertips, and that has to be sorted out and decisions have to be made by leadership and by, at times, Congress, or by state legislators as to what is considered acceptable for the United States. So there isn't a lot of precedent . . .
>
> And fusion centres need the flexibility and room, they need the structure and they need the guidance, and they need guidelines, and rules to go by, but they also need the Congress and the American public to be patient and give us time to mature. There's lots of reasons to believe that that's happening every month, that we're maturing and improving our capabilities and our processes, and we're getting better at knowing the difference between a behavior or an action that may have a relationship to terrorism, and something that's constitutionally protected . . .
>
> So this is a learning curve for everybody. It's a learning curve not only for the fusion centres, but for the leadership that is responsible for a fusion centre, a learning curve for the federal government and how to interface with us, and how to support us in a meaningful way, because it's different than what you would support, they support themselves or support another federal organization. And for laws to be structured to take into account all the new data accesses and all the technology that was not around even five years ago in many respects.

What this articulation sidesteps is the fact that there is not much ambiguity with existing legal guidelines that require "reasonable suspicion" in order for law enforcement to engage in intelligence operations.[21] Rather, there seems to be uncertainty about how to establish effective oversight of network interactions *among* agencies and organizations (i.e., "fusion") when previous oversight mechanisms concentrated mostly on action *within* single agencies.[22] It is also telling that this informant draws a distinction between "a behavior or an action that may have a relationship to terrorism, and something that's constitutionally protected." The intended meaning of this passage is that individual privacy and freedom of speech and assembly should not be impinged upon, but the implied meaning is that people can have their constitutional rights stripped from them if they appear to be connected in any way to (the possibility of) a terrorist plot. It is disturbing to think that constitutional rights can be withdrawn from any citizen, but especially if all that is required is the appearance of possessing the capacity for terrorism. There is ample evidence that this concern is justified. Some of the known instances of overreach of this sort include the infiltration of a peace and anti-death-penalty activist group in Maryland, the preemptive arrest of law student and Green Party member Kenneth Krayeske in Connecticut, the infiltration (by a military agent) of a non-violent, anti-war

---

[21] See German and Stanley, "ACLU Fusion Center Update"; also see Monahan, "The Future of Security?"

[22] See Citron and Pasquale, "Network Accountability."

protest group in the state of Washington, and the widespread spying on Muslim communities by the New York Police Department's "Demographics Unit."[23]

Our interviews show that while fusion-centre staff do run full, detailed searches on individuals, they seek to craft an appearance of not being overzealous. Thus, they prefer using one master portal (or as few portals as possible) to access data so that they can minimize any semblance of impropriety:

> I'd be concerned with looking at whether or not multiple dives into some large amounts of databases would create, if not the actual, the perception of some kind of a civil liberties issue. I don't think it would, if you're just diving into the same system [instead of multiple ones].

Technological systems of networked information exchange can provide additional layers of defence for fusion centres, too, particularly when privacy protections are delegated to software. Many sites have implemented software applications, like i2's "Analyst's Notebook," which automates many of the Code of Federal Regulations privacy guidelines concerning what information to store and for how long:

> This [system] will also serve as our intake point for intelligence, and where we establish intelligence files, and it is, and it has within it a essential accounting and clock for 28CFR [Title 28 of the Code of Federal Regulations] that allows you, once you create the intelligence file, you can trigger the mechanism that identifies the elements that have to be in place before it could be considered an intelligence file . . . And it also essentially triggers the clock that starts tracking the timeframe for that intelligence file so that you will be notified when it comes time for review and due for consideration of purging, according to the regulation, the federal regulation. So . . . it's gonna take almost all of the manual nature of what we're doing right now out of the equation.

More than being an efficient tool, these applications are viewed as software shields to protect fusion centres from lawsuits. One director confided that he constantly feels "one mouse-click away or one news release away from a lawsuit," so anything that could minimize that possibility is highly desirable. There is an irony here, of course, in that the same company's (i2's) software that searches for "patterns" and "associations" prior to identifying suspects is perceived as automating civil-liberties protections so that analysts do not need to worry about them.

---

[23] See, e.g., Associated Press, "NYPD Official: Muslim Spying by Secret Demographics Unit Generated No Leads, Terrorism Cases," *The Washington Post* (August 21, 2012), http://www.washingtonpost.com/national/on-faith/nypd-official-muslim-spying-in-neighborhoods-led-to-no-leads-terror-cases-in-over-6-years/2012/08/21/e14d96f6-eb5b-11e1-866f-60a00f604425_story.html (last accessed August 22, 2012); Monahan, "The Future of Security?"; see also Anthony B. Newkirk, "The Rise of the Fusion-Intelligence Complex: A Critique of Political Surveillance after 9/11," *Surveillance & Society* 8, 1 (2010); The Nation, "Can Anyone Rein in the NYPD's Spies?" *The Nation,* March 7, 2012, http://www.thenation.com/article/166673/can-anyone-rein-nypds-spies.

Blocking Oversight

Apart from ambiguities introduced by technological advances, like the version of cloud computing and networked queries mobilized by fusion centres, conditions for meaningful oversight are being obstructed on other fronts. One of our standard questions for each of the people we interviewed at 36 fusion centres was about oversight of their activities. Almost without fail, informants related that they had "executive" or "advisory" boards with whom they conferred, or that they simply followed the "chain of command," meaning that personnel reported—and were subject—to their superior officers.

Existing oversight boards are constituted in large part by law enforcement. In only two instances did we hear that advisory boards had representatives from a civil-society group, and those boards apparently met only once a year, at which time they were given a descriptive report summarizing the activities for the year. Moreover, it seems that the primary goals of these oversight boards are to discuss future needs or plans and offer advice about how to spend grant funds:

> We have a statewide-like oversight committee for the centre that helps us with, or looks at like technology, and grants, as far as how we're utilizing our money and things like that. And it's comprised of key representatives throughout the state from law enforcement agencies and things like that. That is our oversight committee.

The only other routine oversight comes in the form of audits of DHS grants, whose primary focus seems to be on verifying that the "percent effort" of analysts and other staff is accurate; this means that auditors make certain that the people being funded by DHS are working on fusion-centre-related projects for the appropriate percentage of their time. Evidently, there are no institutionalized mechanisms for external, public oversight of data collection and sharing.[24]

Given the well-documented culture of police protecting each other from outside scrutiny,[25] it should not be surprising that law-enforcement–staffed advisory boards would be poor substitutes for public oversight. Many of the critical stories that have come to light about fusion centres were sparked by documents obtained through leaks, open-records requests, or lawsuits from civil-society groups.[26] The activist libertarian group Operation Defuse has also been instrumental in filing open-records requests, hosting public debates, and conducting site visits to fusion centres.[27] Although they sometimes, but not often, begrudgingly comply, fusion centres have certainly

---

[24] See, e.g., Priscilla M. Regan and Torin Monahan, Beyond Counterterrorism: Data Sharing, Privacy, and Organizational Histories of DHS Fusion Centers, International Journal of E-Politics (forthcoming); Rollins, "Fusion Centers."

[25] See generally Gabriel J. Chin and Scott C. Wells, "The Blue Wall of Silence as Evidence of Bias and Motive to Lie: A New Approach to Police Perjury," *University of Pittsburgh Law Review* 59 (1997).

[26] See, e.g., German and Stanley, "ACLU Fusion Center Update"; Monahan, "The Future of Security?"; Newkirk, The Rise of the Fusion-Intelligence Complex."

[27] Monahan, "The Future of Security?"

not embraced these requests for disclosure of their activities. Nor do fusion centres seem to hold much respect for activists making information requests, as revealed by the following quote from a fusion-centre representative about Operation Defuse:

> It was a guy out of Texas, and he went around and talked to all the fusion centres, and wanted to actually come into the fusion centres. And we did meet with him, and now I can't think of his name, young kid with a young girl . . . Anyway, they came here and basically wasted about freaking three hours of my time asking me [questions].

Meanwhile, apart from evasion tactics like claiming there are no materials to release or no records of quick searches, one disturbing response is for states to pass legislation *exempting* fusion centres from open-records requests, which Virginia did in 2008.[28]

The mainstream media could investigate fusion centres with more regularity and depth and report to the public, but with some exceptions,[29] they seldom do. When there are controversies, success stories, or DHS briefings, the media may communicate those facts before quickly moving on.[30] Part of the reason for this could be the decline in support for investigative journalism and downsizing of media outlets, which is an explanation volunteered by one interviewee to a question about the fusion centre's connections with the media:

> As little as possible, and for very good reason. So much of what we do is for official use only. And now, when we allocate funds, we notify the media that we have allocated taxpayer dollars, and what for, and why, because that's absolutely in the domain of the public. But interestingly, in [our state], unless somebody sniffs something that could be a scandal, the media doesn't pay any attention to us . . . They don't have the people anymore to cover [reporting needs]. And when they do ask us questions, they're clueless about what we do . . . I prefer it this way.

Another complementary explanation, however, could be that the work of analysts is largely abstract and that there is nothing that mediagenic about running searches on databases, even if the results of those searches can have major implications for civil liberties or security.

As part of the general guidelines of the federal government's Information Sharing Environment (ISE), in 2010 DHS implemented a civil-liberties certification process for fusion centres and tied new funding to the approval and implementation of a site-specific privacy policy at each fusion centre.[31] There

---

28 See generally German and Stanley, "ACLU Fusion Center Update."

29 See, e.g., Robert O'Harrow, Jr., "Centers Tap Into Personal Databases; State Groups Were Formed After 9/11," *The Washington Post* (April 2, 2008), A01; Robert O'Harrow, Jr. and Ellen Nakashima, "National Dragnet Is a Click Away; Authorities to Gain Fast and Expansive Access to Records," *The Washington Post* (March 6, 2008), A01.

30 See generally Torin Monahan and Neal A. Palmer, "The Emerging Politics of DHS Fusion Centers," *Security Dialogue* 40, 6 (2009).

31 Harley Geiger, "Fusion Centers Get New Privacy Orders via DHS Grants" (December 15, 2009), http://www.cdt.org/blogs/harley-geiger/fusion-centers-get-new-privacy-orders-dhs-grants.

is room to doubt the effectiveness of such certifications, however, as a Center for Democracy and Technology story observes:

> In many places, the ISE Guidelines require only that participant agencies have a policy in place, with scant specifics on how that policy should be carried out . . . The generalized nature of the ISE Guidelines makes it difficult to assess compliance among participant agencies in the absence of blatant violations, and there are no clear penalties for noncompliance . . . The ISE Guidelines urge participant agencies to consult the Privacy and Civil Liberties Oversight Board for ongoing guidance in protecting civil liberties in participants' use of the ISE—but the Board currently has no members and has been inactive for nearly two years.[32]

Taken at face value, these new requirements could indicate a desire to protect the rights of individuals and prevent overreaches of the kind that have led to racial, religious, and political profiling by these organizations.[33] If abuses were minimized, this would also reduce controversies and demands for reform. Of course, the civil-liberties and privacy-policy requirements, along with civil liberties training for fusion-centre staff, could simultaneously serve as a type of inoculation against demands for more significant oversight. It is telling that the leadership at some of the fusion centres we visited had not even heard of this certification process, including a ranking officer at one of the largest fusion centres in the country who claimed, "No, we haven't had any policy changes or anything. And usually when something is [changed], we hear about it pretty quick."

Many of the sites had nothing but disdain for the drafting and approval process for privacy policies, in part because every site had to create one from scratch in order to comply with different state laws and the unique missions of each fusion centre. When asked if there was one thing that he would like to change, one informant candidly said:

> Oh, shit, yeah. Every fusion centre has to have an approved privacy [policy] . . . Why don't the Feds just put one 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, [and] kicked it back . . . Just give us the privacy policy and tell us to follow it.

Another director opined that the problem was that DHS was having external contractors review the privacy policies and that these contractors "wouldn't know a terrorist from a tadpole." The site's chief of staff continued to explain:

> We're on like the third, fourth generation of this thing, and we're not being refused or rejected by DHS employees. It's some bonehead contractors they got working for 'em, who I think got their collective law degrees from Phoenix online or something . . . It's the Institute for

---

[32] Ibid.

[33] See, e.g., Citron and Pasquale, "Network Accountability"; Monahan, "The Future of Security?"

> Intergovernmental Research (IIR), that's the primary DHS contractor . . . IIR, I spit on all of 'em.

Because aggravation with privacy policies was a consistent theme in our data, and few people knew the details of them, this does call into question the likely effectiveness or purpose of such policies. Instead, informants boiled down their plans to simple statements, such as, "We're going to work nice; we're going to share information; we're going to respect privacy." As well intentioned as fusion-centre staff may be, without serious oversight, this assertion is equivalent to saying, "trust us."

Conclusion

Fusion centres are complex organizational entities. They forge connections between local and federal levels, routine law-enforcement and counterterrorism, and public and private sectors. We propose that these entities can be understood as "centres of concatenation" in that they draw out temporary patterns of meaning from disparate data, through a process of combination and contextualization, and then move on to other activities, sometimes leaving no trace of the fusion that they actualized. Rather than being all-knowing organizations, after they meet their objectives of delivering multidimensional information packages to others, fusion centres are typically severed from the communicative chain, unaware of the effects that their actions might have brought about. In the words of one analyst, "We may never know about a success . . . It's not that we don't have the [appropriate security] clearances; it's just that we don't have the need to know."

Fusion centres, as centres of concatenation, may be more problematic because they do not attract attention. By being distributed throughout the country and varied in their activities, they do not provide an easy foil for public awareness or concern. The organizational structure and technological systems used by fusion centres also pose obstacles to effective oversight. With the presence of embedded analysts with access to their respective agencies' databases, safeguards against inappropriate data sharing may become ambiguous and infractions difficult to document. This is especially the case when analysts do not have to keep track of their searches and when sites can elude open-records requests. In these ways, fusion centres perform an erasure, or a selective non-generation, of data about their own practices, thereby creating zones of opacity that shield them from accountability.

Thus, fusion centres illustrate trends in the asymmetry of visibility after 9/11. Whereas individuals may be much more transparent to law-enforcement agencies, the same organizations are becoming more opaque and less responsive to meaningful oversight. This is concerning particularly because fusion centres are rapidly becoming primary portals for law-enforcement investigations and the model for information sharing by security agencies more broadly. Just as existing legal guidelines should be followed strictly, as law-enforcement agencies embrace network logics, new systems of accountability should be developed to deter overreaches and abuse.

Abstract

In this paper, we draw upon empirical research on fusion centres to theorize contemporary state surveillance. Instead of viewing fusion centres as central repositories for stockpiling and sharing personal data, we introduce the concept of "centres of concatenation" to describe how disparate data are drawn together as needed, invested with meaning, communicated to others, and then discarded such that no records exist of such surveillance activities. In these ways, fusion centres perform an erasure, or a selective non-generation, of data about their own practices, thereby creating zones of opacity that shield them from accountability. This is concerning particularly because fusion centres are rapidly becoming primary portals for law-enforcement investigations and the model for information sharing by security agencies more broadly.

Keywords: data sharing, fusion centres, civil liberties, privacy, surveillance

Résumé

Dans cet article, nous nous penchons sur des recherches empiriques sur les centres d'intégration afin de théoriser la surveillance contemporaine de l'État. Au lieu de considérer les centres d'intégration comme des dépôts centraux pour le stockage et le partage de données personnelles, nous proposons le concept de « centres de concaténation » afin de décrire comment des données disparates sont reliées selon le besoin, chargées de signification, communiquées aux autres, puis ensuite disposées de manière à ce qu'il n'existe aucune documentation sur de telles activités de surveillance. Ainsi, les centres d'intégration assurent que leurs propres pratiques ne sont pas documentées, ce qui crée des zones d'opacité qui les permettent de se soustraire de toutes responsabilités. Cette situation est préoccupante d'autant plus que les centres d'intégration deviennent rapidement les sites primaires des enquêtes menées par les organismes d'application de la loi ainsi que le modèle pour le partage des données des agences de sécurité en général.

Mots clés: partage de données, centres d'intégration, libertés civiles, vie privée, surveillance

Torin Monahan
The University of North Carolina at Chapel Hill
Department of Communication Studies
CB# 3285, 115 Bingham Hall
Chapel Hill, NC 27599-3285 USA
torin.monahan@unc.edu

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