

The Future of Security? Surveillance Operations at Homeland Security Fusion Centers

Torin Monahan*

THE U.S. “WAR ON TERROR” HAS FUELED REMARKABLE DEVELOPMENTS IN STATE surveillance. In the aftermath of the terrorist attacks of September 11, 2001, the country witnessed a rise in domestic spying programs, including warrantless wiretaps of the communications of citizens, investigations into the borrowing habits of library patrons, infiltration of peace-activist groups by government agents, and the establishment of tip hotlines to encourage people to report suspicious others (Monahan, 2010). Rather than interpret these and similar developments as originating with the “war on terror,” scholars in the field of surveillance studies have correctly noted that the events of September 11 provided an impetus for a surge in many preexisting, but perhaps dormant, forms of state surveillance (Wood, Konvitz, and Ball, 2003). Similarly, such domestic surveillance practices neither began nor ended with the George W. Bush administration; instead, state surveillance has grown and mutated in response to changing perceptions of the nature of terrorist threats and the predilections of the Obama administration.

In particular, the Department of Homeland Security (DHS) has renewed its commitment to creating a robust, nationwide network of “fusion centers” to share and analyze data on citizens and others. As of 2010, at least 72 fusion centers existed at the state and regional levels throughout the United States, with many of them listed as “intelligence centers” or “information analysis centers.” Officially, such centers prioritize counterterrorism activities, such as conducting “threat assessments” for events and linking “suspicious activities reports” to other data to create profiles of individuals or groups that might present terrorist risks. In this capacity, fusion centers engage in a form of “intelligence-led policing” that targets individuals who match certain profiles and singles them out for further monitoring or preemptive intervention (Ratcliffe, 2003; Wilson and Weber, 2008).

* TORIN MONAHAN is Associate Professor of Human and Organizational Development and Medicine at Vanderbilt University (e-mail: torin.monahan@vanderbilt.edu). He is a member of the International Surveillance Studies Network. Among his books are *Surveillance in the Time of Insecurity* (Rutgers University Press, 2010), *Schools under Surveillance: Cultures of Control in Public Education* (Rutgers University Press, 2010), *Surveillance and Security: Technological Politics and Power in Everyday Life* (Routledge, 2006), and *Globalization, Technological Change, and Public Education* (Routledge, 2005).

Most fusion centers are located within state and local police departments. Police, FBI, and DHS analysts, whose salaries are usually funded by their respective organizations, typically staff the centers. A common exception is when police representatives are funded in part or completely by DHS grants for the centers. In addition to conducting threat assessments and compiling suspicious-activities reports, fusion center analysts routinely respond to requests for information from state and local police, other fusion centers, or government agencies and organizations such as the FBI, DHS, the Secret Service, or the Department of Defense. When seen as pertinent, fusion centers also share information with private companies, such as those operating public utilities or managing other critical infrastructures (Electronic Privacy Information Center, 2008; Monahan, 2009).

Although the Los Angeles County Terrorism Early Warning Center, established in 1996, is often credited as being the first fusion center (German and Stanley, 2008), most were formed after the release of the September 11 Commission Report in 2004. The early fusion centers built upon and often incorporated the Federal Bureau of Investigation's "Joint Terrorism Task Force" (JTTF) program, thereby hardwiring FBI connections into fusion centers, but allowing for greater information sharing than JTTFs afforded (German and Stanley, 2007). Since their inception, the orientation of many fusion centers has expanded to include "all hazards" and "all threats," such as responding to environmental catastrophes or investigating non-terrorist criminal gangs (Rollins, 2008). One likely reason for this expansion is that the police departments housing fusion centers are trying to translate DHS priorities and apply DHS funds to address local needs (Monahan and Palmer, 2009).

Fusion centers are rapidly becoming a hallmark of the Obama administration's domestic security apparatus. Since 2009, 14 more fusion centers have come on line and the DHS and the Department of Justice have pledged more funding support for fusion centers (Burdeau, 2010; Geiger, 2009). On the surface, the increase in financial and political support for fusion centers should not be that surprising since DHS Secretary Janet Napolitano was a vocal advocate of the well-regarded Arizona-based fusion center, which she helped to create when she was governor of that state (Hylton, 2009). As DHS Secretary, Napolitano (2009) has reaffirmed this support: "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." Attorney General Eric Holder (2010) has also affirmed fusion centers as vital to the ongoing "war on terror": "We are at war. This is the reality in which we live. And our fusion centers are on the frontlines of America's best, and most effective, efforts to fight back."

On a deeper level, fusion centers are probably aligned better with the politics of the Obama administration because its surveillance practices *appear* to be passive, disembodied, and objective. For instance, it has profoundly increased the use of unmanned aerial vehicles (UAVs) internationally and domestically (Wall and

Monahan, 2011; Walters and Weber, 2010). Barring instances of obvious abuse, the fusion and analysis of abstract forms of disparate data do not, in themselves, seem particularly egregious. Indeed, the stated purposes of fusion centers, at least in principle, sound innocuous and rational: “The [fusion] centers’ goals are to blend law enforcement and intelligence information, and coordinate security measures to reduce threats in local communities” (U.S. Department of Homeland Security, 2008). Analysts at fusion centers could be thought of as engaging in types of “soft surveillance” (Marx, 2006) that are minimally invasive, at least for most people, and therefore are not nearly as objectionable to the general public as the more invasive articulations of police or state surveillance, such as physical searches, mandatory DNA collection, or telecommunication wiretaps.

Although fusion centers were formed under the Bush administration, largely in response to criticism from the September 11 Commission over intelligence failures leading up to the September 11 attacks, politically speaking this finding of failure was a sore point for President Bush and the relevant security agencies, such as the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency. Moreover, whereas DHS was established rapidly in 2002, DHS-sponsored fusion centers did not substantially take off until 2005. A case could be made that the supposedly objective, intelligence-led orientation of fusion centers was actually in tension with the general timbre of aggressive, masculinist intervention that characterized many aspects of the “war on terror” under the Bush administration. In contradistinction, the patient police work done by analysts in fusion centers could be viewed as being much smarter and more reflective, and therefore somewhat feminized compared to other modalities of the “war on terror.” DHS officials have explicitly referred to fusion centers as engaging in “thoughtful analysis” (Riegle, 2009) and have implemented workshops and classes to teach fusion center analysts “critical thinking, analytic tools, techniques, and writing” (U.S. Department of Homeland Security, 2008: 16). These articulations are a far cry from the action-oriented counterterrorism myths circulated by entertainment shows like *24*, which were embraced by former White House deputy chief of staff Karl Rove and former DHS Secretary Michael Chertoff, among others (Monahan, 2010). In this light, the operations and concept of fusion centers resonate better with the crafted image of President Obama as a thoughtful, measured, and intelligent leader.

Surveillance of abstract data—or “dataveillance” (Clarke, 2001)—may be perceived as being less intrusive and less threatening than are video cameras, wiretaps, or other technologies that are traditionally associated with surveillance (Ericson and Haggerty, 1997; Marx, 2006). Provided that the data do not involve information considered sensitive, such as pharmacy or bank records, people definitely do not find dataveillance to be as intrusive as physical searches of individuals or individual property (Slobogin, 2008). Nonetheless, these viewpoints neglect the extent to which personal data are constantly being generated, captured, and circulated by the many information systems and technologies with which people come

in contact (e.g., cell phones, credit cards, the Internet). When “fused,” whether by a marketing firm or a state entity, these data can paint a disturbingly fine-grained representation of individuals, their associations, preferences, and risks. Anyone who has access to such “data doubles” (Haggerty and Ericson, 2006) is in a position to know and act on a great deal of information that might otherwise be considered personal and private. It is perhaps much more personal and private than that which could be gleaned from more traditional surveillance techniques. Even more disconcerting for individuals is the fact that although the data generated by our many information systems are always partial and sometimes grossly inaccurate, they can still negatively affect one’s life experiences and chances (e.g., through one’s credit score or one’s terrorist-risk score).

Therefore, the phenomenon of fusion centers must be situated within the context of surveillance societies. Broadly speaking, surveillance societies operate upon imperatives of data gathering and data monitoring, often through technological systems, for purposes of governance and control (Lyon, 2001; Monahan, 2010; Murakami Wood et al., 2006). These particular logics of surveillance were not invented by U.S. national security agencies in response to the September 11 attacks. Instead, fusion centers and other surveillance-oriented security organizations draw upon existing practices of voracious data collection and fluid information exchange, as exemplified by social networking sites such as Facebook or private-sector data aggregators such as Entersect, a company that actively partners with fusion centers to share its purported “12 billion records on about 98 per cent of Americans” (O’Harrow, Jr., 2008).

Thus, there is also a neoliberal dimension to fusion centers, in that they purchase data from the private sector, sometimes hire private data analysts, and share information with industry partners (Monahan, 2009). By forming information-sharing partnerships, analysts at fusion centers seek to “connect the dots” to prevent future terrorist attacks. Meanwhile, government officials are very interested in figuring out ways in which DHS in general and fusion centers in particular can assist the private sector, presumably by enabling and protecting the ability of companies to profit financially (Monahan, 2010). As DHS Under Secretary Caryn Wagner stated in her 2010 testimony before the House Subcommittee on Homeland Security:

I&A [DHS’s Office of Intelligence and Analysis] will continue to advocate for sustained funding for the fusion centers as the linchpin of the evolving homeland security enterprise. While I&A’s support to state, local and tribal partners is steadily improving, there is still work to be done in *how best to support the private sector*. We intend to explore ways to extend our efforts in this area beyond the established relationships with the critical infrastructure sectors (Wagner, 2010; emphasis added).

In some respects, fusion centers suffer from a mandate that is too open-ended and from guidelines that are too ambiguous. The task of fusing data to produce

“intelligence” that can be used to prevent terrorist acts or respond to “all crimes” or “all hazards” amounts to an invitation for individuals at these centers to engage in almost any surveillance practices that make sense to them. As noted, this flexibility could have the redeeming value of allowing police departments to use DHS and other resources for needs that are perceived as being meaningful for particular jurisdictions (Monahan and Palmer, 2009). However, evidence suggests that people at some fusion centers are also exploiting the significant leeway granted to them to engage in racial profiling, political profiling, illegal data mining, and illegal data collection. The surveillance capabilities of fusion centers enable and invite “mission creep” or “function creep,” whereby analysts draw upon the resources at their disposal to exceed the policies and laws that are intended to govern their activities (*Ibid.*). Moreover, the guidelines for fusion centers are quite ambiguous and there is a general absence of oversight regarding their activities (German and Stanley, 2007). In the following sections, I will review in detail a few cases of abuse by fusion centers and discuss the issues raised by such examples.

Fusion Center Abuses

Given the secretive nature of fusion centers, including their resistance to freedom of information requests (German and Stanley, 2008; Stokes, 2008), the primary way in which the public has learned about their activities is through leaked or unintentionally disseminated documents. For instance, a “terrorism threat assessment” produced by Virginia’s fusion center surfaced in 2009 and sparked outrage because it identified students at colleges and universities—especially at historically black universities—as posing a potential terrorist threat (Sizemore, 2009). In the report, universities were targeted because of their diversity, which is seen as threatening because it might inspire “radicalization.” The report says: “Richmond’s history as the capital city of the Confederacy, combined with the city’s current demographic concentration of African-American residents, contributes to the continued presence of race-based extremist groups...[and student groups] are recognized as a radicalization node for almost every type of extremist group” (Virginia Fusion Center, 2009: 9). Although the American Civil Liberties Union (ACLU) and others have rightly decried the racial-profiling implications of such biased claims being codified in an official document, the report itself supports the interpretation that minority students will be and probably have been targeted for surveillance. The report argues: “In order to detect and deter terrorist attacks, it is essential that information regarding suspected terrorists and suspicious activity in Virginia be closely monitored and reported in a timely manner” (*Ibid.*: 4). Other groups identified as potential threats by the Virginia fusion center were environmentalists, militia members, and students at Regent University, the Christian university founded by evangelical preacher Pat Robertson (Sizemore, 2009).

Another threat-assessment report, compiled by the Missouri Information Analysis Center (MIAC), found “the modern militia movement” to be worthy of

focused investigation. The 2009 report predicted a resurgence in right-wing militia activities because of high levels of unemployment and anger at the election of the nation's first black president, Barack Obama, who many right-wing militia members might view as illegitimate and/or in favor of stronger gun-control laws (Missouri Information Analysis Center, 2009). The greatest stir caused by the report was its claim that "militia members most commonly associate with 3rd party political groups.... These members are usually supporters of former Presidential Candidate: Ron Paul, Chuck Baldwin, and Bob Barr" (*Ibid.*: 7). When the report circulated, many libertarians and "Tea Party" members took great offense, thinking the document argued that supporters of third-party political groups were more likely to be dangerous militia members or terrorists. In response, libertarian activists formed a national network called "Operation Defuse," which is devoted to uncovering and criticizing the activities of fusion centers and is actively filing open-records requests and attempting to conduct tours of fusion centers. Operation Defuse could be construed as a "counter-surveillance" group (Monahan, 2006) that arose largely because of outrage over the probability of political profiling by state-surveillance agents.

Fusion centers have also been implicated in scandals involving covert infiltrations of nonviolent groups, including peace-activist groups, anti-death penalty groups, animal-rights groups, Green Party groups, and others. The most astonishing of the known cases involved the Maryland Coordination and Analysis Center (MCAC). In response to an ACLU freedom of information lawsuit, it came to light in 2008 that the Maryland State Police had conducted covert investigations of at least 53 peace activists and anti-death penalty activists for a period of 14 months. The investigation proceeded despite admissions by the covert agent that she saw no indication of violent activities or violent intentions on the part of group members (Newkirk, 2010). Nonetheless, in the federal database used by the police and accessed by MCAC, activists were listed as being suspected of the "primary crime" of "Terrorism—anti-government" (German and Stanley, 2008: 8). Although it is unclear exactly what role the fusion center played in these activities, they were most likely involved in and aware of the investigation. After all, as Mike German and Jay Stanley (2008: 8) explain:

Fusion centers are clearly *intended* to be the central focal point for sharing terrorism-related information. If the MCAC was not aware of the information the state police collected over the 14 months of this supposed terrorism investigation, this fact would call into question whether the MCAC is accomplishing its mission.

Police spying of this sort, besides being illegal absent "reasonable suspicion" of wrongdoing, could have a "chilling effect" on free speech and freedom of association. The fact that individuals were wrongly labeled as terrorists in these

systems and may still be identified as such could also have negative ramifications for them far into the future.

Another dimension of troubling partnerships between fusion centers and law enforcement was revealed with the 2007 arrest of Kenneth Krayeske, a Green Party member in Connecticut. On January 3, 2007, Krayeske was taking photographs of Connecticut Governor M. Jodi Rell at her inaugural parade. He was not engaged in protest at the time. While serving as the manager of the Green Party's gubernatorial candidate, he had publicly challenged Governor Rell over the issue of why she would not debate his candidate (Levine, 2007). At the parade, police promptly arrested Krayeske (after he took 23 photographs) and later charged him with "Breach of Peace" and "Interfering with Police" (*Ibid.*). Connecticut's fusion center, the Connecticut Intelligence Center (CTIC), had conducted a threat assessment for the event and had circulated photographs of Krayeske and others to police in advance (Krayeske, 2007). The police report reads: "The Connecticut Intelligence Center and the Connecticut State Police Central Intelligence Unit had briefed us [the police] on possible threats to Governor Rell by political activist [*sic*], to include photographs of the individuals. One of the photographs was of the accused Kenneth Krayeske" (quoted in Levine, 2007). Evidently, part of the reason Krayeske was targeted was that intelligence analysts, most likely at the fusion center, were monitoring blog posts on the Internet and interpreted one of them as threatening: "Who is going to protest the inaugural ball with me?... No need to make nice" (*CNN.com*, 2009). According to a CNN report on the arrest, after finding that blog post, "police began digging for information, mining public and commercial data bases. They learned Krayeske had been a Green Party campaign director, had protested the gubernatorial debate and had once been convicted for civil disobedience. He had no history of violence" (*Ibid.*). The person who read Krayeske his Miranda rights and attempted to interview him in custody was Andrew Weaver, a sergeant for the City of Hartford Police Department who *also* works in the CTIC fusion center (Department of Emergency Management and Homeland Security, 2008).

These few examples demonstrate some of the dangers and problems with fusion centers. Fusion center threat assessments lend themselves to profiling along lines of race, religion, and political affiliation. Their products are not impartial assessments of terrorist threats, but rather betray biases against individuals or groups who deviate from—or challenge—the status quo. According to a *Washington Times* commentary that became a focal point for a congressional hearing on fusion centers, as long as terrorism is defined as coercive or intimidating acts that are intended to shape government policy, "any dissidence or political dissident is suspect to fusion centers" (Fein, 2009). Evidence from the Maryland and Connecticut fusion center cases suggests that their representatives are either involved in data-gathering and investigative work, or are at least complicit in such activities, including illegal spying operations (German and Stanley, 2008). The Connecticut case further shows that individuals working at fusion centers are actively monitoring online sources and

interviewing suspects, a departure from the official Fusion Center Guidelines that stress “exchange” and “analysis” of data, not data acquisition through investigations (U.S. Department of Justice, 2006).

One important issue here is that fusion centers occupy ambiguous organizational positions. Many of them are located in police departments or are combined with FBI Joint Terrorism Task Forces, but their activities are supposed to be separate and different from the routine activities of the police or the FBI. A related complication is that fusion center employees often occupy multiple organizational roles (e.g., police officers or National Guard members *and* fusion center analysts), which can lead to an understandable, but nonetheless problematic, blurring of professional identities, rules of conduct, and systems of accountability. Whereas in 2010 DHS and the Department of Justice responded to concerns about profiling by implementing a civil liberties certification requirement for fusion centers, public oversight and accountability of fusion centers are becoming even more difficult and unlikely because of a concerted effort to exempt fusion centers from freedom of information requests. For example, according to a police official, Virginia legislators were coerced into passing a 2008 law that exempted its fusion center from the Freedom of Information Act; in this instance, federal officials threatened to withhold classified intelligence from the state’s fusion center and police if they did not pass such a law (German and Stanley, 2008). Another tactic used by fusion center representatives to thwart open-records requests is to claim that there is no “material product” for them to turn over because they only “access,” rather than “retain,” information (Hylton, 2009).

Although it may be tempting to view these cases of fusion center missteps and infractions as isolated examples, they are probably just the tip of the iceberg. A handful of other cases has surfaced recently in which fusion centers in California, Colorado, Texas, Pennsylvania, and Georgia have recommended peace activists, Muslim-rights groups, and/or environmentalists be profiled (German, 2009; Wolfe, 2009). The Texas example reveals the ways in which the flexibility of fusion centers affords the incorporation of xenophobic and racist beliefs. In 2009, the North Central Texas Fusion System produced a report that argued that the United States is especially vulnerable to terrorist infiltration because the country is too tolerant and accommodating of religious difference, especially of Islam. Through several indicators, the report lists supposed signs that the country is gradually being invaded and transformed: “Muslim cab drivers in Minneapolis refuse to carry passengers who have alcohol in their possession; the Indianapolis airport in 2007 installed footbaths to accommodate Muslim prayer; public schools schedule prayer breaks to accommodate Muslim students; pork is banned in the workplace; etc.” (North Central Texas Fusion System, 2009: 4). Because “the threats to Texas are significant,” the fusion center advises keeping an eye out for Muslim civil liberties groups and sympathetic individuals, organizations, or media that might carry their

message: hip-hop bands, social networking sites, online chat forums, blogs, and even the U.S. Department of Treasury (*Ibid.*).

Recent infiltration of peace groups seems to reproduce some of the sordid history of political surveillance of U.S. citizens, such as the FBI and CIA's COINTELPRO program, which targeted civil rights leaders and those peacefully protesting against the Vietnam War, among others (Churchill and Vander Wall, 2002). A contemporary case involves a U.S. Army agent who infiltrated a nonviolent, anti-war protest group in Olympia, Washington, in 2007. A military agent spying on civilians likely violated the Posse Comitatus Act. Moreover, this agent actively shared intelligence with the Washington State Fusion Center, which shared it more broadly (Anderson, 2010). According to released documents, intelligence representatives from as far away as New Jersey were kept apprised of the spying:

In a 2008 e-mail to an Olympia police officer, Thomas Glapion, Chief of Investigations and Intelligence at New Jersey's McGuire Air Force Base, wrote: "You are now part of my Intel network. I'm still looking at possible protests by the PMR SDS MDS and other left wing antiwar groups so any Intel you have would be appreciated.... In return if you need anything from the Armed Forces I will try to help you as well" (*Ibid.*: 4).

Given that political surveillance under COINTELPRO is widely considered to be a dark period in U.S. intelligence history, the fact that fusion centers may be contributing to similar practices today makes it all the more important to subject them to public scrutiny and oversight.

Transgressive Data Collection

By now it should be apparent that fusion center personnel are neither objectively assessing terrorist threats nor passively analyzing preexisting data. Fusion centers may appear to be more impartial and rational than previous forms of state surveillance. Yet they have incorporated previous surveillance modalities, including their prejudicial beliefs and invasive techniques, and merged them with dataveillance capabilities that amplify the potential for civil liberties violations and personal harm. Even if fusion center activities were restricted to passive data analysis, which they are not, they could still transgress existing laws that are intended to protect people from unreasonable searches. Specifically, Title 28, Part 23 of the Code of Federal Regulations states that law enforcement agencies "shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity" (in German and Stanley, 2008: 2). When fusion center analysts create profiles of risky individuals and then engage in data mining to identify people who match those

profiles, they are effectively bypassing the “reasonable suspicion” requirement for intelligence operations.

Aside from the known cases of abuse, in their official capacity fusion centers are apparently exploiting a technicality in terms of what constitutes “collecting” and “maintaining” criminal intelligence information. The implied reasoning is this: provided that fusion centers merely analyze data stored in databases housed elsewhere, they are not violating the “reasonable suspicion” stipulation even if they are conducting “dragnet” or “fishing expedition” searches that would have been illegal with previous generations of computing technology that did not depend entirely on networks. This rationalization is especially specious when analysts can access police records that are located in the same buildings as the fusion centers. Nonetheless, DHS and Department of Justice guidelines explicitly encourage fusion centers to access as much data as possible, extending “beyond criminal intelligence, to include federal intelligence as well as public and private-sector data” (quoted in German and Stanley, 2007: 7). In an unusually candid statement, Sheriff Kevin Rambosk, who is associated with the Florida fusion center, justifies widespread data sharing as a way to compete with criminals who similarly move across jurisdictional lines:

We know as law enforcement professionals that there are no jurisdictional boundaries for criminals.... And we historically and intuitively know that the more information that we can share with one another, the more cases can be solved, the more crimes can be prevented, and the more information each of our agencies will have to continue to make Collier County one of the safest places in Florida to live (Mills, 2010).

The implication of this assertion is that there should not be any jurisdictional or legal boundaries for law enforcement to collect and share data either, including data from the private sector, which fusion centers in Florida access through a system called “Florida Integrated Network for Data Exchange and Retrieval” or “FINDER” (*Ibid.*).

Conclusion: Surveillance Iterations

Although criminals or terrorists may be crossing jurisdictional boundaries and breaking the law, state agencies and agents do more harm than good when they ignore existing legal constraints or seek out exemptions from public oversight. The few problematic cases reviewed in this article illustrate that without due respect for the “reasonable suspicion” provision on police intelligence-gathering activities, fusion center personnel engage in or endorse racial, political, and religious profiling; they perceive challenges to the status quo as threatening and possibly “terrorist”; they support the investigation and arrest of law-abiding individuals, marking them as “terrorists” in official databases, perhaps in perpetuity; and they

exert a chilling effect on free speech in that activists and others are more likely to temper their activities to avoid similar kinds of harmful scrutiny.

It is important to note that the politics of those being targeted by fusion centers spans the spectrum from right-wing militia members to left-wing anti-war activists. Some may be surprised that individuals supporting progressive causes would be seen as threats during a Democratic presidency. Yet these cases underscore that the politics of many environmentalists, anti-war activists, and other progressives are still radical vis-à-vis the mainstream politics of contemporary Washington. Moreover, law enforcement cultures are typically quite conservative (Greene, 2007; Reiner, 2010) and, similar to other organizations, slow to change (Zhao, He, and Lovrich, 1998). Thus, the outcomes of national elections are unlikely to produce discernable near-term changes in the cultures of these organizations.

If today's surveillance state were to fully embody Barack Obama's campaign rhetoric of respect for "the rule of law," fusion centers would differ markedly. The blurring or suspending of the law are supposedly practices that characterized the "war on terror" under the Bush administration. Impatience with bureaucratic constraints upon counterterrorism efforts or frustration with the burden of protecting civil liberties are similarly more readily associated with the masculinist orientation of the previous administration. Fusion centers could strictly follow stipulations on intelligence gathering; they could erect barriers between public and private databases; they could embrace transparency and accountability by complying with, rather than avoiding, freedom of information requests.

Instead of romanticizing the ideals that could have been achieved, or might yet be achieved, I prefer to conclude by highlighting what can be learned from the example of fusion centers. First, fusion centers show the ways in which the logics of "surveillance societies" pervade all aspects of social life, including the operations of government organizations. Imperatives to collect, share, analyze, and act on data increasingly shape the activities of public institutions, private companies, and individuals. The capabilities of new media technologies simply augment this particular drive, which is unchecked or under-regulated in most domains, and the realm of national security is no different. If governments are reluctant to impose serious restrictions on data sharing more generally, except perhaps for particularly sensitive data such as those contained in medical records, one should not be surprised that government agencies would avail themselves of similar data-sharing functions (Regan, 2004). Second, the unstandardized composition and mission of fusion centers may afford them ample flexibility, but it also allows particularistic biases to shape their activities. When made public, such biases may embarrass fusion center officials, but they are undoubtedly more damaging to the targets of unwarranted surveillance and intervention. The latter must contend with legal battles and fees, emotional stress, and perhaps even physical abuse associated with being marked as terrorist suspects (Guzik, 2009). For surveillance states to be more democratic, their police apparatuses should possess and follow clear guidelines

that respect the law, and subject their activities to routine public scrutiny. To do otherwise is a recipe for abuse.

Acknowledgment: This material is based upon a research project being conducted by the author and Priscilla Regan. The work is supported by the National Science Foundation under grant number SES 0957283.

REFERENCES

- Anderson, Rick
2010 "Watching the Protesters." *Seattle Weekly News* (June 9). At www.seattleweekly.com/2010-06-09/news/watching-the-protesters/1.
- Burdeau, Cain
2010 "Holder: Intelligence-Sharing Centers Vital." *Associated Press* (February 23). At www.washingtonexaminer.com/local/ap/holder-intelligence-sharing-centers-vital-85071812.html.
- Churchill, Ward and Jim Vander Wall
2002 *The COINTELPRO Papers: Documents from the FBI's Secret Wars Against Dissent in the United States*. Cambridge, MA: South End Press.
- Clarke, Roger
2001 *While You Were Sleeping...Surveillance Technologies Arrived*. At www.anu.edu.au/people/Roger.Clarke/DV/AQ2001.html.
- CNN.com*
2009 "Are You on the List?" (September 30). At www.cnn.com/video/?/video/crime/2009/09/30/willis.fusion.centers.cnn.
- Department of Emergency Management and Homeland Security
2008 Department of Emergency Management and Homeland Security Coordinating Council Meeting Minutes. Hartford, CT. At www.ct.gov/demhs/lib/demhs/docstploded/cood_council_minutes/cc_mins_9_18_08.pdf.
- Electronic Privacy Information Center
2008 "Information Fusion Centers and Privacy." At <http://epic.org/privacy/fusion/>.
- Ericson, Richard V. and Kevin D. Haggerty
1997 *Policing the Risk Society*. Toronto: University of Toronto Press.
- Fein, Bruce
2009 "Surveilling for Clues of Evil Intent." *WashingtonTimes.com* (April 1). At www.washingtontimes.com/news/2009/apr/01/surveilling-for-clues-of-evil-intent/.
- Geiger, Harley
2009 "Fusion Centers Get New Privacy Orders Via DHS Grants. December 15." At www.cdt.org/blogs/harley-geiger/fusion-centers-get-new-privacy-orders-dhs-grants.
- German, Michael
2009 Testimony in Support of Senate Bill 931 Before the Joint Committee on Public Safety and Homeland Security. Boston. At www.scribd.com/doc/24658143/Mike-German-Former-FBI-testimony-sb931MA-Fusion-Center-2009.
- German, Michael and Jay Stanley
2008 ACLU Fusion Center Update. July. At www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.
- 2007 "What's Wrong with Fusion Centers?" (December). At www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

- Greene, Jack R.
2007 "Human Rights and Police Discretion: Justice Service or Denied?" *Sociology of Crime Law and Deviance* 9: 147–169.
- Guzik, Keith
2009 "Discrimination by Design: Predictive Data Mining as Security Practice in the United States' 'War on Terrorism.'" *Surveillance & Society* 7, 1: 1–17.
- Haggerty, Kevin D. and Richard V. Ericson
2006 "The New Politics of Surveillance and Visibility." K.D. Haggerty and R.V. Ericson (eds.), *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press: 3–25.
- Holder, Eric
2010 "Attorney General Eric Holder Speaks at the Fourth Annual National Fusion Center Conference." New Orleans, LA: Department of Homeland Security. At www.justice.gov/ag/speeches/2010/ag-speech-100223.html.
- Hylton, Hilary
2009 "Fusion Centers: Giving Cops Too Much Information?" *Time.com*. At www.time.com/time/nation/article/0,8599,1883101,00.html.
- Krayeske, Ken
2007 "And Justice for All..." At www.the40yearplan.com/article_052507_And_Justice_For_All.php.
- Levine, Dan
2007 "Arresting Development." *Cal Law* (January 12): 5. At www.the40yearplan.com/pdf/annotation.pdf.
- Lyon, David
2001 *Surveillance Society: Monitoring Everyday Life*. Buckingham, England; Philadelphia: Open University.
- Marx, Gary T.
2006 "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information—'Hey Buddy Can You Spare a DNA?'" T. Monahan (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge: 37–56.
- Mills, Ryan
2010 "Fla. Police Agencies to Start Using Data-Sharing Tools." *Naples Daily News* (February 12). At www.policeone.com/police-products/communications/articles/2003592-Fla-police-agencies-to-start-using-data-sharing-tools/.
- Missouri Information Analysis Center
2009 MIAC Strategic Report, 02/20/09. "The Modern Militia Movement." Jefferson City, MO. At www.scribd.com/doc/13232178/MIAC-Strategic-Report-The-Modern-Militia-Movement.
- Monahan, Torin
2010 *Surveillance in the Time of Insecurity*. New Brunswick: Rutgers University Press.
2009 "The Murky World of 'Fusion Centers.'" *Criminal Justice Matters* 75, 1: 20–21.
2007 "'War Rooms' of the Street: Surveillance Practices in Transportation Control Centers." *The Communication Review* 10, 4: 367–389.
2006 "Counter-Surveillance as Political Intervention?" *Social Semiotics* 16, 4: 515–534.
- Monahan, Torin and Neal A. Palmer
2009 "The Emerging Politics of DHS Fusion Centers." *Security Dialogue* 40, 6: 617–636.

- Murakami Wood, David (ed.), Kirstie Ball, David Lyon, Clive Norris, and Charles Raab
2006 *A Report on the Surveillance Society*. Wilmslow: Office of the Information Commissioner.
- Napolitano, Janet
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. At www.dhs.gov/news/speeches/sp_1236975404263.shtm.
- Newkirk, Anthony B.
2010 "The Rise of the Fusion-Intelligence Complex: A critique of political surveillance after 9/11." *Surveillance & Society* 8, 1: 43–60.
- North Central Texas Fusion System
2009 *Prevention Awareness Bulletin*. At www.privacylives.com/wp-content/uploads/2009/03/texasfusion_021909.pdf.
- O'Harrow, Jr., Robert
2008 "Centers Tap into Personal Databases." *Washington Post* (April 2). At www.washingtonpost.com/wp-dyn/content/article/2008/04/01/AR2008040103049.html.
- Ratcliffe, Jerry H.
2003 "Intelligence-led Policing." *Trends and Issues in Crime and Criminal Justice* 248: 1–6.
- Regan, Priscilla M.
2004 "Old Issues, New Context: Privacy, Information Collection and Homeland Security." *Government Information Quarterly* 21, 4: 481–497.
- Reiner, Robert
2010 *The Politics of the Police*. New York: Oxford University Press.
- Riegle, Robert
2009 Testimony of Director Robert Riegle, State and Local Program Office, Office of Intelligence and Analysis, before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, "The Future of Fusion Centers: Potential Promise and Dangers." Washington, D.C. At www.dhs.gov/news/testimony/testimony_1238597287040.shtm.
- Rollins, John
2008 *Fusion Centers: Issues and Options for Congress*. Washington, D.C.: Congressional Research Service. At www.fas.org/sgp/crs/intel/RL34070.pdf.
- Sizemore, Bill
2009 "Report: Region May Be a Hotbed for Terrorist Recruiting." *The Virginian-Pilot* (April 26). At <http://hamptonroads.com/2009/04/report-region-may-be-hotbed-terrorist-recruiting>.
- Slobogin, Christopher
2008 "Government Data Mining and the Fourth Amendment." *The University of Chicago Law Review* 75, 1: 317–341.
- Stokes, Jon
2008 "Fusion Center Meltdown: Feds Stifling Open Government in VA?" *Ars Technica* (March 24). At <http://arstechnica.com/security/news/2008/03/fusion-center-meltdown-feds-stifling-open-government-in-va.ars>.
- U.S. Department of Homeland Security
2008 "DHS' Role in State and Local Fusion Centers Is Evolving." Washington, D.C.: U.S. Department of Homeland Security. At www.dhs.gov/xoig/assets/mgmt/rpts/OIG_09-12_Dec08.pdf.

- U.S. Department of Justice
2006 "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era." Washington, D.C.: U.S. Department of Justice. At www.iir.com/global/products/fusion_center_guidelines_law_enforcement.pdf.
- Virginia Fusion Center
2009 *Virginia Terrorism Threat Assessment*. Richmond, VA: Department of State Police. At www.rawstory.com/images/other/vafusioncenterterrorassessment.pdf.
- Wagner, Caryn
2010 Testimony of Under Secretary Caryn Wagner before the House Subcommittee on Homeland Security on the President's Fiscal Year 2011 Budget Request for the Department's Office of Intelligence and Analysis. Washington, D.C.: Department of Homeland Security. At www.dhs.gov/ynews/testimony/testimony_1267716038879.shtm.
- Wall, Tyler and Torin Monahan
2011 "Surveillance and Violence from Afar: The Politics of Drones and Liminal Security-Scapes." *Theoretical Criminology* 15, 3: 239–254.
- Walters, William and Jutta Weber
2010 "UCAV Surveillance, High-Tech Masculinities and Oriental Others." *A Global Surveillance Society?* Conference at City University London.
- Wilson, Dean and Leanne Weber
2008 "Surveillance, Risk and Preemption on the Australian Border." *Surveillance & Society* 5, 2: 124–141.
- Wolfe, Gavi
2009 "What We Know about Recent Surveillance of Lawful First Amendment Activity." Massachusetts: American Civil Liberties Union of Massachusetts. At http://aclu.org/sos/aclu_domestic_surveillance_what_we_know.pdf.
- Wood, David, Eli Konvitz, and Kirstie Ball
2003 "The Constant State of Emergency? Surveillance after 9/11." K. Ball and F. Webster (eds.), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press: 137–150.
- Zhao, Jihong, Ni He, and Nicholas P. Lovrich
1998 "Individual Value Preferences among American Police Officers: The Rokeach Theory of Human Values Revisited." *Policing: An International Journal of Police Strategies & Management* 21, 1: 22–37.