The Emerging Politics of DHS Fusion Centers

TORIN MONAHAN & NEAL A. PALMER*

Department of Human & Organizational Development, Vanderbilt University, Nashville, TN, USA

This article explores public concerns about the US Department of Homeland Security's data 'fusion centers'. These centers, which are proliferating across all US states, coordinate data-sharing among state and local police, intelligence agencies, and private companies. The primary goal of fusion centers is to engage in intelligence-sharing for counter-terrorism purposes. However, they have been used for a variety of other purposes, such as basic policing, spying on social movement organizations, or restricting legal public activities such as taking photographs. Drawing upon a comprehensive analysis of media publications from 2002 to 2008, we identify and discuss three primary categories of concern with fusion centers: (1) their *ineffectiveness*, particularly given the financial expense, the statistical unlikelihood of terrorist attacks, and the pressing need for other law enforcement support; (2) the potential for *mission creep*, where the functions of fusion centers expand beyond their originally intended purposes to encompass things like all-hazards preparedness; and (3) the *violation of civil liberties*, especially through racial profiling or First Amendment violations.

Keywords fusion centers • Department of Homeland Security • mission creep • surveillance • media • counter-terrorism • privacy

THE PROVISION OF NATIONAL SECURITY is a constant challenge for modern states. In the era of the 'War on Terror', the United States has radically restructured security agencies and relationships in pursuit of that goal. Whereas a great deal of attention has been given to the formation of the US Department of Homeland Security (DHS) in 2002 (see, for example, Firestone, 2002; Altheide, 2006; Monahan, 2006a), which effectively absorbed and restructured 22 federal agencies, there is much less awareness about public–private partnerships in the quest for national security. Given the dominance of a neoliberal orientation toward governance, outsourcing

SECURITY DIALOGUE

SAGE Publications, http://sdi.sagepub.com
Vol. 40(6): 617–636, DOI: 10.1177/0967010609350314

to private contractors has become a privileged response by US policymakers for meeting public needs (Duggan, 2003; Giroux, 2004). The realm of national security is no different. Security contractors are hired to police war zones such as Iraq, disaster zones such as New Orleans after Hurricane Katrina, and places of transport and shipping such as airports and docks (Engelhardt, 2007; Lipsitz, 2006). Additionally, the USA currently devotes roughly 70% of its intelligence budget to private contractors, amounting to $42 billion annually (Scahill, 2007, 2008). In some cases, contractors have even been given 'shoot to kill' authorization by the US Federal Bureau of Investigation (FBI) for domestic security provision (Rothschild, 2008). Obviously, there is a need to document and critically evaluate this trend in the privatization of security.

One key mechanism often employed in the pursuit of security is that of technological surveillance, whether of borders, critical infrastructures, populations, or data. For some time, scholars in the field of surveillance studies have been deconstructing the myth that state-level surveillance and security operations should be the sole focus of public concern (see, for example, Ball & Webster, 2003; Lyon, 2003a; Monahan, 2006b). Rather than the risk of an authoritarian state – or Big Brother – trampling civil liberties, a greater and more likely threat is the systematic generation, integration, and sharing of vast quantities of personal data that can be harnessed to sort, control, and discriminate against people or groups (O'Harrow, 2005; Lyon, 2003b; Regan, 2004; Gandy, 2006). This is not to say that state-led surveillance operations do not violate the rights of people: they clearly can and do. Instead, this orientation highlights the fact that routine surveillance, in the form of data-collection and data-mining, is key to the operations of private companies, and that these organizations can also impinge upon the rights of people or collaborate with government agencies to do so. This conclusion is supported, for instance, by revelations in 2006 that major telecommunications companies had illegally shared data on individual customers with the US National Security Agency (NSA) (Electronic Frontier Foundation, 2006).[1]

Drawing upon these insights, this article explores one dimension of the privatization of national security: the formation of DHS 'fusion centers', which coordinate data-sharing among state and local police, intelligence agencies, and private companies. The stated goal of fusion centers is to 'blend relevant law enforcement and intelligence information analysis and coordinate security measures to reduce threats in their communities' (US Department of Homeland Security, 2006). Although there is evidence that some fusion centers existed before the formation of the DHS,[2] they became formalized under the aegis of state-level DHS offices in direct response to the recommendations of the 9/11 Commission. Put simply, after the attacks of 9/11, there

[1] The passage of an amended Foreign Intelligence Surveillance Act in 2008 granted retroactive immunity to those telecommunications companies.

[2] The Los Angeles County Terrorism Early Warning Center (LACTEW), established in 1996, is often referenced as being the first fusion center (German & Stanley, 2008).

was widespread consensus within the intelligence community that various agencies had not been able to work in concert to 'connect the dots' and prevent the attacks. Fusion centers are one response to this identified problem. According to a congressional report on the subject: 'the DHS State, Local, and Regional Fusion Center Initiative is key to Federal information sharing efforts and must succeed in order for the Department to remain relevant in the blossoming State and local intelligence community'.[3] As of 2009, there were 58 such centers across the USA funded by the DHS at a cost of $380 million dollars (US Department of Homeland Security, 2009). Because they enroll local police in their activities, it is estimated that there are 800,000 operatives involved with fusion centers (German & Stanley, 2008). Far from being restricted to the sharing of data among government agencies, fusion centers also facilitate cooperative efforts among government agencies and private industries, although the details of these relationships are shrouded in secrecy (Monahan, 2009b).

Concretely, most fusion centers are located within state and local police departments (Milloy, 2008). They employ intelligence analysts provided by the DHS, along with civilian analysts and police intelligence officers (Ebbert, 2005; Hall, 2006). In addition, these centers seek to utilize potentially relevant information obtained by other public employees, such as firefighters and sanitation workers, and many also operate tip hotlines where members of the public can report suspicious activities (Sheridan & Hsu, 2006). Fusion centers engage in a range of practices, including following up on hotline-reported tips and analyzing crime data from multiple databases for trends that could be indicative of larger criminal activity (Ebbert, 2005). We will provide further details and examples in subsequent sections.

Given that fusion centers are entities that coordinate the sharing of disparate data across multiple networks with the goal of enabling the pre-emptive identification of risky individuals for law enforcement intervention, they effectively actualize what Kevin Haggerty & Richard Ericson (2000) refer to as *the surveillant assemblage*. The characteristics of surveillant assemblages are that they abstract individuals and practices from social contexts, translating them into 'data' that can be analyzed in discrete form, exchanged freely, and recombined to provide a seemingly objective representation – or 'data double' – of individuals (Haggerty & Ericson, 2000; Monahan & Wall, 2007). At least in theory, fusion centers thrive upon the production and exchange of data and the sorting of individuals based on their assigned risk. As we will show, however, fusion centers engender a politics that has the potential to also do much more than this.

[3] See 'Conference Report on H. R. 1, Implementing Recommendations of the 9/11 Commission Act of 2007', in the US Congressional Record for 25 July 2007 (House); available at http://www.fas.org/irp/congress/2007_cr/hr1-info.html (accessed 1 September 2009).

In this article, we map the contours of fusion centers primarily by analyzing media reports that make reference to them. The material available on fusion centers is sparse, however. There are a few well-crafted, critical reports by civil society organizations (German & Stanley, 2008; EPIC, 2008). Otherwise, while there are many industry and government documents that argue for the need for such centers or offer recommendations for how to improve their functions, there are relatively few academic or media articles dedicated to fusion centers. Rather, as information comes to light about the activities of fusion centers or the costs associated with them, journalists tend to make passing remarks about or allusions to these entities. We used LexisNexis to locate all unique references to DHS fusion centers between 2002 and 2008, coding these into analytic categories. Because the majority of reports identify concerns with fusion centers, we present three dominant categories of concern related to such centers: (1) their *ineffectiveness*, particularly given the financial expense, the statistical unlikelihood of terrorist attacks, and the pressing need for other law enforcement support; (2) the potential for *mission creep*, where the functions of fusion centers expand beyond their originally intended purposes to encompass things like all-hazards preparedness; and (3) *violation of civil liberties*, especially through racial profiling or First Amendment violations. These areas of concern represent a nascent politics of fusion centers in the public realm. In analyzing them, we unveil some of the emerging problems associated with fusion centers but also obtain insight into the kinds of public values that are seen both as important and as threatened by new security arrangements.

Methods

For our methods, we employed qualitative document analysis (Altheide, 1996) of print media sources to locate and track emergent meanings attached to fusion centers. We conducted a LexisNexis search for articles mentioning both 'homeland' and 'fusion center', or those mentioning both 'terrorism' and 'fusion center', published between November 2002 and December 2008.[4] November 2002 was chosen as a start date because the Department of Homeland Security was created then. The search returned 90 newspaper and magazine articles, 56 of which were deemed relevant, 49 of which were unique. The majority of these appeared in newspapers between 2005 and 2008. Articles were eliminated that referred to fusion centers not as physical, inte-

[4] We also conducted Google Scholar searches on the same terms and for the same time periods. Here we found many industry and government reports, but almost no academic articles. Accordingly, for the purpose of focusing on media representations of fusion centers, we opted to exclude the Google Scholar results from the analysis presented in this article.

grative entities designed to counter terrorism but instead borrowed the term to describe technologies that integrate information that may or may not be used in DHS fusion centers. Many of the articles provided only general information on the creation of fusion centers and on their basic purpose. Similarly, a few articles provided information only on new personnel hires at centers. A limitation of this methodological approach is that concerns with fusion centers are restricted to information in the public domain and identified by journalists as being important. Obviously, different, complementary research approaches are needed. However, given the difficulties involved in achieving access to fusion centers or their representatives, qualitative document analysis serves as an important first step toward achieving an empirically informed understanding of such centers.

Ineffectiveness

The rise of fusion centers has brought with it criticisms of their effectiveness, especially given their financial expense. By 2008, the DHS had provided states with up to $23 billion for overall security provision (Schmitt & Johnston, 2008), including $380 million dedicated to establishing and operating fusion centers to prevent terrorist attacks (US Department of Homeland Security, 2009). Nonetheless, because much of the money has been implemented in more of an all-crimes approach, federal funds are being employed in ways that were initially unforeseen. For instance, in Massachusetts, funds have been used to bolster fire departments with basic equipment rather than for terrorism prevention (Helman, 2005). Thus, critics contend that fusion centers are as useful for procuring grants as they are for preventing crime (Ebbert, 2005).

Local and state authorities rationalize this all-crimes approach by arguing that terrorists may have a propensity to participate in other criminal activities prior to terrorist acts, so authorities lobby to use DHS funds for alternative purposes. Others take a related approach in applying for funds, acknowledging that although funds might upgrade existing anti-terrorism bomb squads, for instance, equipment purchased, such as new hazardous-material suits, could also be used for highway cleanups unrelated to terrorism (Schmitt & Johnston, 2008).

From a local perspective, directives on how funds should be spent may limit what local and state fusion centers are able to accomplish. Whereas funds for fusion centers initially had few restrictions connected to their use (Belluck, 2004), this policy has shifted more recently. In 2007, for instance, Massachusetts received funding that required the state to develop a plan for responding to improvised explosive devices (IEDs), even though local and state authorities had no existing intelligence pointing to such a threat.

According to reports, 'the demand for plans to guard against improvised explosives is being cited by state and local officials as the latest example that their concerns are not being heard, and that national officials continue to push them to spend money on a terrorism threat that is often vague and undefined' (Schmitt & Johnston, 2008). Similarly, on the West Coast, authorities were charged with developing hurricane-evacuation plans in reaction to the muddled government response to Hurricane Katrina on the Gulf Coast, even though states in the West face little danger from hurricanes (Schmitt & Johnston, 2008). These measures are in the spirit of emergency preparedness for any crisis. Nonetheless, states and local governments see too heavy an emphasis on national issues that are not obvious threats in every locality, and states argue that money awarded to fusion centers could be used more effectively if states had more say in the allocation process.

Federal stipulations on fusion-center funds may also proscribe uses that local authorities deem relevant and necessary. As awareness of fusion-center funding has spread, some departments assert that they are not receiving as much money as they need. For instance, medically related projects, such as mass-casualty response and hospital-patient tracking in the event of an attack, were bypassed in a Virginia grant application to the DHS to the chagrin of hospital representatives (Sheridan, 2007). Indeed, much criticism has focused on the federal emphasis on prevention instead of response (Sheridan, 2007). Concerning criticisms of cost, some authorities argue that fusion centers may nonetheless save money by more efficiently responding to threats and determining the extent to which these threats should be investigated for terrorist ties, especially if so doing eliminates the need to involve multiple potentially relevant agencies (Hall, 2007).

Unfunded mandates represent an additional criticism by state and local governments of fusion centers. Though federal funds have become increasingly available to establish and improve fusion centers, much of the onus of funding salaries for public- and private-sector analysts and other fusion-center personnel rests with state and local authorities (Ebbert, 2005; Sheridan & Hsu, 2006). States and localities feel the need to cut budgets in other departments in order to fund fusion centers, even if threats of terrorism appear minimal, and this may weaken their ability to respond adequately to other crimes or maintain other socially necessary programs (Schmitt & Johnston, 2008; Belluck, 2004). If local and state agencies choose not to direct as much money to fusion centers, the fusion center may not operate at full strength (Hall, 2007). Ironically, then, inadequate funding at the federal level may mean that fusion centers cannot establish coordinated counter-terrorism activities throughout the country.

Though the stated goal of fusion centers is to integrate information from the Central Intelligence Agency (CIA), the FBI, the Pentagon, the Department of Defense, the DHS, and other federal, state, and local agencies, their ad

hoc construction means that many agencies are still unable to draw upon information from multiple sources (DeYoung, 2006b; Lipowicz, 2006b). At the federal level, intelligence information is still not coordinated into a single system within agencies such as the FBI and the DHS (Lipton, 2007), making its use by local authorities more difficult (Goodman, 2006; Hsu, 2006). According to a 2006 survey of the National Governors Association and the Government Accountability Office, the extensiveness of the data available, coupled with access restrictions, makes much of the information useless (Lipowicz, 2006b; Hall, 2006, 2007).

Additionally, federal agencies often have competing missions, and turf wars are well documented. For instance, the CIA may seek to maintain an open information channel in monitoring terrorist activities, while the FBI's intention to capture leaders of terrorist plots may close these channels down (Maloof, 2005). The field has been further crowded by the introduction of the DHS (Lipton, 2007). Problems in cooperation at the federal level trickle down to the state and local levels, and the lack of central authority makes those in other agencies reluctant to work with one another (Lipton, 2007). Some assert that if federal entities had made it their mission to share information, utilize common databases, and mine data, the need for federal funds to establish more local fusion centers could have been minimized (Maloof, 2005), and that perhaps a single national security entity could have served a similar purpose (Belluck, 2004).[5]

With or without fusion centers, problems of sharing information come down to mismatches between security clearances and incorrect assumptions about whom to include in the information loop. Thus, information-sharing may be hindered because public- and private-sector analysts lack appropriate security clearances, are not sufficiently integrated into agencies, or simply presume that others do not need to know given information (Belluck, 2004; Lipowicz, 2006a,c; Sheridan & Hsu, 2006). Additionally, there is evidence to suggest that those conducting necessary background checks for employees cannot keep up with the demand; as a result, much information still goes unanalyzed (Sheridan & Hsu, 2006). As White House Homeland Security Advisor Frances Fragos Townsend explained: 'It remains unclear just how much fusing of information is going on day to day. Existing efforts are insufficient and to blame for "mixed and at times competing messages" from US officials and limited contributions from state and local leaders' (cited in Sheridan & Hsu, 2006).

Variations in the size, staffing, and local missions of fusion centers lead to a general lack of communication between and coherence among centers. Some fusion centers may be little more than places where officers are paid to

[5] Indeed, the frustration expressed by state governors in relation to obtaining federal intelligence can be seen in their increasing desire to create fusion centers (Lipowicz, 2006b). According to Washington's Acting Police Chief Cathy L. Lanier, 'Information doesn't get to me because they don't believe I have a need to know' (cited in Lipton, 2007).

examine databases, while others may take a much more active approach in linking information (Kaplan, 2006). Because of insufficient training, local and state authorities still lack substantial instruction on what to observe and to whom they should report it (Sheridan & Hsu, 2006). Finally, though federal officials have begun providing intelligence analysts to fusion centers, these are still not present in every fusion center (Hall, 2006; Lipton, 2007), meaning that much coordination between federal and state and local levels often fails to occur.

Given these constraints, many centers have found it easier to rely on old-fashioned practices than on emerging technological systems, as the lack of uniform standards for all fusion centers prevents them from working together as effectively as they might (DeYoung, 2006a). At the local level, court records may not be linked with prison records even in the same county (Kaplan, 2006). With the immense quantity of data now available, a simple phone call to relay information can be more effective than computer systems designed to mine data, as such systems are often incompatible with one another (DeYoung, 2006b). This seemingly intractable situation is recognized by the DHS: 'The DHS inspector general reported that the federal Homeland Security Information Network, the department's premier information-sharing network, is ineffective in supporting information-sharing among federal, state and local officials. The network is not being used regularly because there is lack of trust among users. Users are confused and frustrated, the report said' (Lipowicz, 2006a). In addition, the tendency of federal databases to be overlapping and outdated makes information analysis even more difficult (Sheridan & Hsu, 2006).

Clearly, significant obstacles exist for fusion centers to function as intended. Nonetheless, the fact that they are largely ineffective at 'fusing' data in a way that demonstrably increases security does not mean that they are without effects. They institute an approach to national security that allows for significantly more fluid exchange of data than existed previously, across government and private-sector organizations. They also grant considerable leeway to localities to adapt the given resources to their perceived needs – or target the resources at their perceived threats. As will be described in the following sections, this flexibility can both lead to mission creep and increase abuses.

Mission Creep

Mission creep is common to most surveillance systems and practices, so it is not surprising that it is present at fusion centers too. Because the development of new technological systems simultaneously introduces valences for new social practices, organizational configurations, and cultural identi-

ties, it can be understood as partially determining social spheres and values (Winner, 1977, 1986; Bush, 1997). In the domain of surveillance, systems of monitoring, tracking, identification, and analysis lend themselves to a panoply of 'secondary' uses that often extend beyond their primary intended or legally sanctioned functions (Marx, 1988; Lyon, 2001; Monahan, 2007). Thus, with fusion centers, mission creep occurs mainly when these centers use federal funds for activities unrelated, or tenuously related, to counter-terrorism. This has not gone unnoticed by the US federal government: a 2007 congressional report found that fusion centers were more often being used for all-crimes and all-hazards functions than for counter-terrorism investigations (Hall, 2007). This criticism is often at odds with how fusion centers operate, though, because most are centered in state or municipal police headquarters and therefore might be expected to prioritize this local orientation (Milloy, 2008). The DHS also envisions fusion centers as being all-encompassing. For instance, Charles E. Allen, chief intelligence officer for the Department of Homeland Security, identified the centers' purpose as '"all hazards, all crime, all threats," targeted not just at terrorism but also at transnational gangs, immigrant smuggling and other threats' (cited in Sheridan & Hsu, 2006). O'Harrow & Nakashima (2008) further relate:

> That wall [between law enforcement information-gathering, relating to crimes and prosecutions, and more open-ended intelligence, relating to national security and counter-terrorism] is fast eroding following the passage of laws expanding surveillance authorities, the push for information-sharing networks, and the expectation that local and state police will play larger roles as national security sentinels.

DHS authorities argue for a more comprehensive approach to minimizing the threats of terrorism, and this has translated into a focus on observable patterns at local levels as well as intelligence regarding terrorist organizations at the international level (Connors, 2008). Such an approach is summed up by a report from the International Association of Chiefs of Police: 'All terrorism is local' (Kaplan, 2006). Thus, while some fusion centers focus exclusively on traditional models and definitions of terrorism, most also incorporate all-crimes approaches into their operation, addressing problems such as fraud, racketeering, computer hacking, and gang activity (Kaplan, 2006; Schmitt & Johnston, 2008).

As alluded to above, some of this mission creep represents creative appropriation on the part of state and local governments, such as when 'hazmat' suits purchased for bomb squads are employed for the dual purpose of cleaning up highway spills (Schmitt & Johnston, 2008). Other times, though, the creep can be more controversial, as in Rhode Island police officials' use of a truck whose designated purpose was to haul a patrol boat for port security, to haul a horse trailer unrelated to security matters (Schmitt & Johnston, 2008). The gearing of fusion centers toward all crimes makes sense for localities, however. The proliferation of federal dollars linked to combating terror-

ism signifies a huge resource for local and state agencies, and such agencies adapt to include counter-terrorism activities to access these resources. At the same time, local governments and police forces recognize the need to protect immediate vicinities and engage in locally appropriate work (Schmitt & Johnston, 2008). The all-crimes framing allows them to do both.

While many localities have adapted their missions to pursue additional funds, the idea that uncovering local crimes may also uncover global networks of crime and terrorism has also been adopted at the local level (Ebbert, 2005). Fusion centers have embraced this idea perhaps more strongly than have federal officials: as federal funding has become burdened with restrictions, demands, and qualifications, fusion-center representatives have argued aggressively for greater lenience in the use of funds as a means of more effectively preventing terrorism. If states must develop plans in accordance with federal stipulations, they say, such as in developing plans for IEDs, then they should be able to use the resources provided for other crimes, such as gun violence, drug trade, and gang activity (Schmitt & Johnston, 2008). Still, these applications have been criticized by groups that have failed to secure DHS funding. For instance, hospital administrators have been advocating for greater funding as well as better integration of public health information in responses to possible terrorist attacks or natural disasters (Sheridan, 2007; Welsh, 2006).

The way fusion centers are organized also appears to encourage mission creep. Minimal guidelines at the federal level mean that fusion centers develop with different foci and different organizational emplacements. Because police personnel and other employees at fusion centers draw upon their local contexts and perceptions of need, this has led to greater police involvement in counter-terrorism development, as well as to police agencies utilizing counter-terrorism tools against more traditional crimes. Every law enforcement entity is being charged with creating some level of intelligence capability, though (Kaplan, 2006). Fusion centers are designed to combine information from multiple intelligence and crime agencies, so participating agencies strategize to benefit in some way. For example, some centers feature hi-tech video walls and dashboards with constantly updated information on crimes and emergencies as well as on terrorist threats (Klein, 2007; Milloy, 2008). New Jersey, upon opening its fusion center in 2006, hailed its future success at enabling all levels of government to access information more efficiently not just for terrorism but also for emergencies and other crimes (*Philadelphia Inquirer,* 2006).

Intelligence operations are also being significantly reorganized. Perhaps the greatest focus of post-9/11 intelligence reform pertained to the integration of intelligence into streamlined databases intended to facilitate easier access and use (Kaplan, 2006). The Justice Department has created the National Data Exchange, also known as N-DEx (O'Harrow & Nakashima, 2008), to enable a

'one-stop shop' for this purpose. Federal officials have access to more information at state and local levels than they have ever had, and state and local officials, as well as private contractors, also have access to more federal information than before, regardless of how reluctant federal agencies have been to distribute this information (O'Harrow & Nakashima, 2008). When states have laws prohibiting the access of credit reports on individuals, for example, officials can simply call fusion centers in other states to tap that information, effectively circumventing state law (German & Stanley, 2008).

In addition to technologies developed to integrate information, other technologies developed for counter-terrorism measures find application in other domains. Thus, the recent emphasis on biometric technologies to more comprehensively police borders also has implications for more civilian aspects of life (Magnet, 2009). States are implementing or considering the use of such technology for drivers' licenses, and more surveillance on workplaces could eventually prevent undocumented immigrants from finding jobs or receiving social services (Lipowicz, 2005, 2006c). This is also consistent with findings in the field of surveillance studies that new systems are ratcheted up, harmonized across jurisdictions, and locked in. For instance, biometric- and RFID-enabled passports are being required by the USA of citizens in other countries that are participating in the US waiver program, meaning that there are political pressures for countries that have the privilege of visa-free access to the USA to adopt so-called e-passports in order to maintain that privilege, and this international standard is being codified as well under the auspices of the International Civil Aviation Organization (Stanton, 2008). That some people may be affected more than others is part of the 'social sorting' functions of most forms of contemporary surveillance, especially surveillance that draws upon databases (Lyon, 2003b).

Finally, the way fusion centers are staffed increases the tendency toward mission creep. The responsibility of state and municipal governments rather than the federal government for staffing fusion centers means that fusion centers respond not just to federal needs but also to local ones. At times, this relationship can tilt heavily toward local interests, such that officers may limit investigation to the local level and fail to make broader connections to possible terrorism-related threats (Hall, 2007), which is something that can become exacerbated by obstacles to intelligence-sharing from the federal level to the state or local level, as referenced above.

Elements of mission creep can be expected when personnel working in fusion centers have multiple, and sometimes competing, commitments and concerns (Ebbert, 2005). In the past, intelligence analysts and advisers came from the emergency management sector, but they are increasingly from state and local police agencies (Welsh, 2005) or from the private sector (German & Stanley, 2008). In addition to police personnel, centers are bringing together personnel from public health, intelligence communities, and other law

enforcement sectors (Lipowicz, 2006a). The much greater numbers of local law enforcement officials, public health representatives, and others over federal agents makes the tailoring of fusion centers to local needs unsurprising.

The premise of fusion centers, that information must be connected across multiple domains, tends to justify the use of funds across a spectrum of purposes (Helman, 2005), and national calls to identify local terrorist threats encourage local authorities to examine more closely groups that heretofore have been described as being mere agitators or annoyances to local authorities, as will be discussed in the next section. The promise of new funding means that authorities will continue to have the resources and motivation to engage in such activities (Kaplan, 2006).

Violations of Civil Liberties

Perhaps the most resounding criticism of fusion centers has been of their potential for impinging upon civil liberties. The intensification of surveillance since 9/11 has been conspicuous, evident in the proliferation of surveillance cameras in public places, heightened security at borders and airports, and overzealous crackdowns on public protests and policing of public space (Ball & Webster, 2003; Fernandez, 2008; Monahan, 2006b; Salter, 2004). Evidence of abuses by fusion centers and lack of guidelines for their oversight has, in turn, heightened fears of surveillance (Kaplan, 2006). Mitt Romney, a prominent supporter of fusion centers, has openly called for fusion centers to wiretap mosques and spy on foreign students (Helman, 2005). In Georgia, vegetarian protesters at the premises of a baked-ham retailer were covertly photographed (Milloy, 2008; Sheridan & Hsu, 2006), while union and labor activists, environmentalists, and animal-rights protesters have also been documented targets of surveillance under the dubious rationale of preventing terrorism (Kaplan, 2006). Even web surfers have been confronted for viewing inappropriate content on public servers, something ill advised but not necessarily illegal or related to terrorism (Kaplan, 2006).

Nonviolent public protest – whether against wars, globalization, the death penalty, or the Republican Party – has been a particular focus of new counterterrorism surveillance (German & Stanley, 2008; Fernandez, 2008). For example, a 'temporary' fusion center utilized to limit protests near the Republican National Convention's 2004 proceedings in New York City was defended as a preventative measure against terrorism, even though the Democratic National Convention's meeting in Boston was not equipped with similar measures (O'Shaughnessy, 2004). Of course, antiwar activists are known to begin meetings by welcoming undercover cops (Kaplan, 2006); because undercover cops have been embedding themselves more frequently in protests and

mass demonstrations and acting as agent provocateurs, this suspicion is not unwarranted (Marx, 1988; Fernandez, 2008; German & Stanley, 2008).

Though the Justice Department requires a level of 'reasonable suspicion' to warrant intelligence-gathering, these guidelines are not followed closely at local levels (Lipton, 2007). 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' (quoted in German & Stanley, 2008: 2). However, with unclear distinctions between terrorism and traditional crimes, the potential for abuse of power also increases. For instance, local officials are being instructed to pay more attention to individuals than they previously have, being particularly observant of 'suspicious patterns' in the behavior of and interactions among individuals. Thus, local police departments collect 'suspicious activity reports' on individuals and share them with fusion centers without the burden of first proving 'reasonable suspicion' (German & Stanley, 2008). The Los Angeles Police Department (LAPD), for instance, now requires officers to report activities such as 'using binoculars', 'taking pictures or video footage with no apparent esthetic value', 'taking notes', or 'espousing extremist views' (German & Stanley, 2008: 2). People previously viewed as innocuous citizens or tourists can now be perceived as security threats in need of immediate mitigation and prolonged investigation. These policing and intelligence activities are illegal under federal law, which requires proof of reasonable suspicion; nonetheless, the LAPD's program is heralded by the Office of the Director of National Intelligence as a model for other cities to follow (German & Stanley, 2008: 2).

The range of people who now have access to sensitive information, and the expansion of access to people who previously did not have access to files without concurrent ethics guidelines, particularly at local and state levels, provides further credence to fears of intelligence abuse and privacy violations (Vascellaro, 2004; Welsh, 2005). Officers are now working on terrorism task-forces embedded within more traditional agencies, and the designation of their work as related to terrorism or more traditional crimes can become blurred as officers transition between different aspects of their job. This is particularly the case if they are employed by fusion centers as well as by more traditional agencies. More than 6,000 officers at the state and local levels now have federal-level security clearance, which provides them with access to credit reports and banking histories that were previously restricted (Kaplan, 2006). Additionally, many analysts are contractors who are less accountable than more traditional officers because they do not report directly to agency officials or adhere as stringently to agency requirements (Rose & Berlet, 2005). Private contractors have fewer requirements related to ethics training and

face fewer potential punishments for ethics violations (Lipton, 2007).

Notwithstanding the obstacles to data access enumerated in this article's section on ineffectiveness, much of the information fusion centers analyze has been publicly available in the past but has not been as readily accessible (Flynn, 2005). One police-department database trainer asserts about fusion-center activities: 'If people knew what we were looking at, they'd throw a fit' (cited in Kaplan, 2006). Therefore, beyond the number of people with access to private information about individuals, the emphasis on access to sensitive information raises additional privacy concerns. Citizens supplying biometric information to federal authorities may not approve of its dissemination internationally, particularly if it limits travel or is provided to nations with less stringent security requirements or to entities whose actions they do not support (Bowcott, 2004). As agencies are demonstrating, having too much access to information can result in too much power. As civil liberties attorney Richard Gutman warns: 'You've got all this money and all this equipment – you're going to find someone to use it on' (cited in Kaplan, 2006).

The tying together of databases has allowed officers to more easily compile case files on persons who heretofore had not been viewed as terrorist threats (Kaplan, 2006), what some have identified as 'fishing expeditions'. Such data-mining can lead to targeting civilians when they have indeed done nothing wrong (O'Harrow & Nakashima, 2008), which is a practice that appears more likely in the light of recent spying by the US National Security Agency (Pincus, 2006). For instance, the Matrix system (Multi-State Anti-Terrorism Information Exchange program), which was discontinued in 2005, instantly created files on 120,000 people with 'high terrorist factor scores' (Kaplan, 2006; Lipowicz, 2006a) by combining information, as suggested by DHS guidelines, from databases containing motor-vehicle registrations and drivers' license information, housing records, criminal records, and other public sources as well as private ones (Lipowicz, 2005). Other software is being developed to hypothesize potential next steps for people suspected of criminal and/or terrorist behavior (O'Harrow & Nakashima, 2008). This potential on the part of fusion centers for anticipating crimes before they occur represents one more component of the larger movement toward pre-emptive policing and risk management, which tends to ignore root causes of crime (Haggerty & Ericson, 2006; Simon, 2006; Garland, 2001).

The expansion of intelligence beyond criminal matters, along with the proliferation of private agencies profiting from sharing information with public agencies, for which citizens pay, also raises criticism across the board. Citizens question such sharing of information, both in the government's right to private data and in private companies' profiting at citizens' expense. The N-DEx software mentioned above, for instance, was developed by Raytheon, leading to questions about how much personal information private companies have access to (O'Harrow & Nakashima, 2008), particularly as such access

would appear to have little value in countering terrorism. Furthermore, private companies may have a more lax orientation to privacy protection than do government agencies (Rose & Berlet, 2005), so fusion centers can circumvent some privacy protections by working with them. In addition to software development, commercial enterprises sell information to police agencies on Americans' housing histories, financial circumstances, social and familial networks, arms purchases, and other information deemed relevant. The fusion centers at individual states then draw upon those data as they see fit (Lipowicz, 2006a; O'Harrow, 2008).

Fusion centers raise privacy concerns as well because of the role of third parties and their access to information. Agencies have been slow to develop privacy protections (Kaplan, 2006), partly as the result of the ever-changing nature of technology, and again partly because of the lack of federal guidelines for fusion centers. The centralization of information and intelligence into single databases is particularly troublesome because of the vulnerability of such an approach to hackers or employee negligence. Hackers may now gain access to a wealth of additional, potentially damaging information (Kaplan, 2006). Identity theft is one relevant concern (Rose & Berlet, 2005), especially as private information is now kept in fusion-center databases. Credit-card companies have been particularly susceptible to past hacks or employee negligence (Ryan, 2005; Whitson & Haggerty, 2008; Monahan, 2009a), so these problems will surely persist.

Finally, many question the role of civilians in fusion-center and counterterrorism surveillance. Most fusion centers operate tip lines for citizens to report suspicious behavior (Ebbert, 2005; Sheridan & Hsu, 2006), and these can distract police agencies and result in unfounded investigations of innocent citizens. While fusion centers have been praised for identifying potential terrorist threats, in part through public–private cooperation, to date most of these leads have proven fruitless (Sheridan & Hsu, 2006).

Conclusion

Not a lot is known about DHS fusion centers. Undoubtedly, this is due in part to efforts by those involved to keep the activities of fusion centers secret. As with most state-run surveillance and security operations, the ready-made rationale for such secrecy is that the state must hide its intelligence operations from potential terrorists so that such people will not modify their behavior to avoid detection.[6] This explanation lacks persuasive force, though, especially because people who engage in terrorist activities may be 'new recruits' who

[6] See 'Homeland Security Act of 2002' in the US Congressional Record for 17 September 2002 (Senate); available at http://fas.org/sgp/congress/2002/s091702.html (accessed 1 September 2009).

would not necessarily have any data record to give them or their intentions away (Privacy International, 2004). What is more likely behind fusion-center secrecy is that authorities learned their lesson about how powerful opposition could be to 'total information awareness' (TIA) programs and have elected to hide practices of widespread intelligence-gathering and data-mining on US citizens and others. Indeed, the TIA program of the US Defense Advanced Research Project Agency, which was announced to the public after 9/11 and was rapidly scuttled in the face of vocal opposition, was in fact a centralized data fusion center of the very kind that has now been quietly reinvented as state-level 'fusion centers' (EPIC, 2008).

Another reason for secrecy has to do with the liberal 'sharing' of private information across public and private sectors. This dimension of fusion centers is conspicuously absent from most official DHS publications and statements, but it is readily acknowledged by DHS representatives at conferences and other venues (Monahan, 2009b). Some of the nongovernmental entities involved with fusion centers are banks, universities, hotels, telecommunication companies, healthcare providers, and private security firms (EPIC, 2008). If the public received word that their personal information was being shared to enhance the profit of private industries and expand the intelligence databases of government agencies, this could jeopardize the lucrative – if legally and ethically problematic – arrangements in place.

This article has explored three dominant themes of concern found in popular media sources about fusion centers: ineffectiveness, mission creep, and violation of civil liberties. As with most surveillance systems, the potential threats are great, but fusion centers do not seem to work as promised, intended, or advertised by the DHS. Because of incompatibilities in technological infrastructures, resistance by local law enforcement, and territoriality by intelligence agencies, the objective of total information awareness and the ideal of unguarded sharing of intelligence are not achieved in practice. Fusion centers may be ineffectual at their primary tasks, but they still alter the field of security provision. They reprioritize police, intelligence, and even public health agencies toward counter-terrorism objectives; they shift funding toward such objectives, even when state and local governments and police forces object to these priorities; they enable data-sharing with private companies, further widening and tightening the surveillance net in which people are caught; and they complement and encourage surreptitious monitoring of 'suspicious' others, such as nonviolent protesters or amateur photographers. Through mission creep of this sort, fusion centers enable privacy violations and may have a 'chilling' effect on free speech and the legal use of public space.

Fusion centers provide a window into dominant forms and logics of contemporary securitization. They clearly embody an all-hazards orientation that pervades emergency-preparedness discourses and operations today (Lakoff,

2006) and they develop within – and contribute to – a risk-management approach to policing and governance that seeks to control rather than eliminate threats and social problems (Simon, 2006; Wacquant, 2009). Moreover, even as highly secretive organizations, fusion centers embrace neoliberal rationalities of privatization and responsibilization. Public–private partnerships are key to fusion-center operations, as is the use of private security analysts. Whereas responsibilization is typically theorized in terms of individuals who must consume security products and services not provided by the state (Rose, 1999; Katz, 2006; Monahan, 2009a), in this case it is state and local governments that are burdened with unfunded mandates and concomitant pressures to staff fusion centers even while cutting other social services. One could proffer a generous reading of mission creep by fusion centers and say that these are laudable efforts by state agents and others to make their work relevant to the perceived needs of their communities. Be that as it may, this article suggests that such efforts lend themselves to the violation of civil liberties and privacy, while rendering ambiguous laws and policies governing intelligence operations.

* Torin Monahan is an Associate Professor of Human & Organizational Development and an Associate Professor of Medicine at Vanderbilt University. His main theoretical interests are in social control and institutional transformations with new technologies. His recent books include *Surveillance and Security: Technological Politics and Power in Everyday Life* (Routledge, 2006), *Schools Under Surveillance: Cultures of Control in Public Education* (Rutgers University Press, 2010), and *Surveillance in the Time of Insecurity* (Rutgers University Press, 2010). Neal A. Palmer is a doctoral student in the Department of Human & Organizational Development at Vanderbilt University.

References

Altheide, David L., 1996. *Qualitative Media Analysis*. Thousand Oaks, CA: Sage.

Altheide, David L., 2006. *Terrorism and the Politics of Fear*. Lanham, MD: Altamira.

Ball, Kirstie & Frank Webster, eds, 2003. *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. Sterling, VA: Pluto.

Belluck, Pam, 2004. 'States and Cities Must Hunt Terror Plots, Governor Says', *New York Times*, 15 December.

Bowcott, Owen, 2004. 'Biometrics: Helping the Fight Against Terror, Hindering the Hope for Privacy – British Police Ready To Link Up to Databases of US Intelligence', *The Guardian*, 18 June.

Bush, Corlann Gee, 1997. 'Women and the Assessment of Technology', in Albert H. Teich, ed., *Technology and the Future*, 7th edn. New York: St. Martin's Press (157–179).

Connors, Tim, 2008. 'Cities, Police and Terrorism', *New York Times*, 29 July.

DeYoung, Karen, 2006a. 'In Arizona, Officials Share Data the Old-Fashioned Way', *Washington Post*, 9 August.

DeYoung, Karen, 2006b. 'A Fight Against Terrorism – and Disorganization', *Washington Post*, 9 August.

Duggan, Lisa, 2003. *The Twilight of Equality? Neoliberalism, Cultural Politics, and the Attack on Democracy*. Boston, MA: Beacon Press.

Ebbert, Stephanie, 2005. 'Fusion Center Takes Aim at Terror', *Boston Globe*, 26 September.

Electronic Frontier Foundation, 2006. 'EFF Sues AT&T To Stop Illegal Surveillance', 31 January; available at http://www.eff.org/news/archives/2006_01.php#004369 (accessed 1 September 2009).

Electronic Privacy Information Center (EPIC), 2008. 'Information Fusion Centers and Privacy'; available at http://epic.org/privacy/fusion/ (accessed 1 September 2009).

Engelhardt, Tom, 2007. 'What "Progress" in Iraq Really Means', *The Nation* (online), 13 August; available at http://www.thenation.com/doc/20070827/engelhardt (accessed 1 September 2009).

Fernandez, Luis, 2008. *Policing Dissent: Social Control and the Anti-Globalization Movement*. Brunswick, NJ: Rutgers University Press.

Firestone, David, 2002. 'Traces of Terror: The Reorganization', *New York Times*, 27 July.

Flynn, Edward, 2005. 'In Defense of Mass. Fusion Center', *Boston Globe*, 20 June.

Gandy, Oscar, Jr., 2006. 'Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment', in Kevin D. Haggerty & Richard V. Ericson, eds, *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press (363–384).

Garland, David, 2001. *The Culture of Control: Crime and Social Order in Contemporary Society*. Chicago, IL: University of Chicago Press.

German, Mike & Jay Stanley, 2008. 'ACLU Fusion Center Update', July; available at http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf (accessed 1 September 2009).

Giroux, Henry A., 2004. *The Terror of Neoliberalism: Authoritarianism and the Eclipse of Democracy*. Boulder, CO: Paradigm.

Goodman, Melvin A., 2006. 'America Is Safer Since 9/11', *Christian Science Monitor*, 18 September.

Haggerty, Kevin D. & Richard V. Ericson, 2000. 'The Surveillant Assemblage', *British Journal of Sociology* 51(4): 605–622.

Haggerty, Kevin D. & Richard V. Ericson, 2006. 'The New Politics of Surveillance and Visibility', in Kevin D. Haggerty & Richard V. Ericson, eds, *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press (3–25).

Hall, Mimi, 2006. 'Feds Move To Share Intelligence Faster: Teams Being Sent To Work Alongside Local Agents', *USA Today*, 27 July.

Hall, Mimi, 2007. 'State-Run Sites Not Effective vs. Terror: Report Blasts Costly Intelligence Centers', *USA Today*, 24 July.

Helman, Scott, 2005. 'Wiretap Mosques, Romney Suggests', *Boston Globe*, 15 September.

Hsu, Spencer S., 2006. 'Allen: Chief Intelligence Officer', *Washington Post*, 11 January.

Kaplan, David E. (with Monica M. Ekman & Angie C. Marek), 2006. 'Spies Among Us', *US News and World Report*, 30 April; available at http://www.usnews.com/usnews/news/articles/060508/8homeland.htm (accessed 1 September 2009) .

Katz, Cindi, 2006. 'The State Goes Home: Local Hypervigilance of Children and the Global Retreat from Social Reproduction', in Torin Monahan, ed., *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge (27–36).

Klein, Allison, 2007. 'The City's Critical Link to All First Responders', *Washington Post*, 11 October.

Lakoff, Andrew, 2006. 'Techniques of Preparedness', in Torin Monahan, ed., *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge (265–273).

Lipowicz, Alice, 2005. 'Justice Department Releases Fusion Center Guidelines', *Newsbytes*, 31 August.

Lipowicz, Alice, 2006a. 'To Be or Not To Tell', *TechNews*, 21 July.
Lipowicz, Alice, 2006b. 'Intelligence Fusion Centers Catching On', *TechNews*, 7 April.
Lipowicz, Alice, 2006c. 'Four Key Questions Greet DHS in 2006', *TechNews*, 16 January.
Lipsitz, George, 2006. 'Learning from New Orleans: The Social Warrant of Hostile Privatism and Competitive Consumer Citizenship', *Cultural Anthropology* 21(3): 451–468.
Lipton, Eric, 2007. 'C.I.A. Veteran Races Time To Rescue Fledgling Agency', *New York Times*, 16 February.
Lyon, David, 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
Lyon, David, 2003a. *Surveillance After September 11.* Malden, MA: Polity.
Lyon, David, ed., 2003b. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. New York: Routledge.
Magnet, Shoshana, 2009. 'Bio-Benefits: Technologies of Criminalization, Biometrics and the Welfare System', in Sean P. Hier & Josh Greenberg, eds, *Surveillance: Power, Problems, and Politics.* Vancouver: UBC Press (169–183).
Maloof, Michael, 2005. 'Fractured Flow of Intelligence?', *Washington Times*, 22 November.
Marx, Gary T., 1988. *Undercover: Police Surveillance in America*. Berkeley, CA: University of California Press.
Milloy, Courtland, 2008. 'Lanier's D.C. Is One Big Unruly Family', *Washington Post*, 26 March.
Monahan, Torin, 2006a. 'Securing the Homeland: Torture, Preparedness, and the Right To Let Die', *Social Justice* 33(1): 95–105.
Monahan, Torin, ed., 2006b. *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge.
Monahan, Torin, 2007. '"War Rooms" of the Street: Surveillance Practices in Transportation Control Centers', *The Communication Review* 10(4): 367–389.
Monahan, Torin, 2009a. 'Identity Theft Vulnerability: Neoliberal Governance Through Crime Construction', *Theoretical Criminology* 13(2): 155–176.
Monahan, Torin, 2009b. 'The Murky World of "Fusion Centres"', *Criminal Justice Matters* 75(1): 20–21.
Monahan, Torin & Tyler Wall, 2007. 'Somatic Surveillance: Corporeal Control Through Information Networks', *Surveillance & Society* 4(3): 154–173.
O'Harrow, Robert, Jr., 2005. *No Place To Hide*. New York: Free Press.
O'Harrow, Robert, Jr., 2008. 'Centers Tap Into Personal Databases: State Groups Were Formed After 9/11', *Washington Post*, 2 April.
O'Harrow, Robert, Jr. & Ellen Nakashima, 2008. 'National Dragnet Is a Click Away: Authorities To Gain Fast and Expansive Access to Records', *Washington Post*, 6 March.
O'Shaughnessy, Patrice, 2004. 'Intel Op Center Fuses 20 Units', *Daily News* (New York), 30 August.
Philadelphia Inquirer, 2006. 'N.J. Official Pushes Homeland Security Centers', 8 September.
Pincus, Walter, 2006. 'NSA Gave Other U.S. Agencies Information From Surveillance: Fruit of Eavesdropping Was Processed and Cross-Checked With Databases', *Washington Post*, 1 January.
Privacy International, 2004. 'Mistaken Identity: Exploring the Relationship Between National Identity Cards and the Prevention of Terrorism'; available at http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf (accessed 1 September 2009).
Regan, Priscilla M., 2004. 'Old Issues, New Context: Privacy, Information Collection and Homeland Security', *Government Information Quarterly* 21(4): 481–497.
Rose, Carol & Chip Berlet, 2005. 'Romney's Spy Center', *Boston Globe*, 14 June.

Rose, Nikolas S., 1999. *Powers of Freedom: Reframing Political Thought*. New York: Cambridge University Press.

Rothschild, Matthew, 2008. 'FBI Deputizes Private Contractors With Extraordinary Powers, Including "Shoot To Kill"', *The Progressive*, 8 February; available at http://www.alternet.org/story/76388/ (accessed 1 September 2009).

Ryan, Nancy, 2005. 'Governor Is Using the Fear Factor', *Boston Globe*, 22 June.

Salter, Mark B., 2004. 'Passports, Mobility, and Security: How Smart Can the Border Be?', *International Studies Perspectives* 5(1): 71–91.

Scahill, Jeremy, 2007. *Blackwater: The Rise of the World's Most Powerful Mercenary Army*. New York: Nation Books.

Scahill, Jeremy, 2008. 'Blackwater's Private Spies', *The Nation* (online), 5 June; available at http://www.thenation.com/doc/20080623/scahill (accessed 1 September 2009).

Schmitt, Eric & David Johnston, 2008. 'States Baffled By Strings on U.S. Security Funding: Roadside Bombs? In Massachusetts?', *International Herald Tribune*, 27 May.

Sheridan, Mary Beth, 2007. 'Anti-Terrorism Grant To Fund Upgrades, New Projects', *Washington Post*, 3 August.

Sheridan, Mary Beth & Spencer S. Hsu, 2006. 'Localities Operate Intelligence Centers To Pool Terror Data: "Fusion" Facilities Raise Privacy Worries As Wide Range of Information Is Collected', *Washington Post*, 31 December.

Simon, Jonathan, 2006. *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. New York: Oxford University Press.

Stanton, Jeffrey M., 2008. 'ICAO and the Biometric RFID Passport: History and Analysis', in Colin J. Bennett & David Lyon, eds, *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective.* New York: Routledge (253–267).

US Department of Homeland Security, 2006. 'DHS Strengthens Intel Sharing at State and Local Fusion Centers', press release. Washington, DC: US Department of Homeland Security; available at http://www.dhs.gov/xnews/releases/press_release_0967.shtm (accessed 1 September 2009).

US Department of Homeland Security, 2009. 'State and Local Fusion Centers'. Washington, DC: US Department of Homeland Security'; available at http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm (accessed 1 September 2009).

Vascellaro, Jessica E., 2004. 'Openness of Single Security Network for US Spurs Debate', *Boston Globe*, 25 June.

Wacquant, Loïc J. D., 2009. *Punishing the Poor: The Neoliberal Government of Social Insecurity*. Durham, NC: Duke University Press.

Welsh, William, 2005. 'States To Focus on Fusing Threat Information', *Newsbytes*, 3 February.

Welsh, William, 2006. 'Public health Is Part and Parcel of Homeland Security', *TechNews*, 5 January.

Whitson, Jennifer R. & Kevin D. Haggerty, 2008. 'Identity Theft and the Care of the Virtual Self', *Economy and Society* 37(4): 572–594.

Winner, Langdon, 1977. *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Cambridge, MA: MIT Press.

Winner, Langdon, 1986. *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago, IL: University of Chicago Press.