The murky world of 'Fusion Centres'

Torin Monahan critiques the emergence of data-sharing 'Fusion Centres' intended to reduce crime and prevent terrorism.

Public-private partnerships are often extremely well hidden arrangements in the ongoing privatisation of national security. In the United States, the Department of Homeland Security (DHS) has supported the creation of 'Fusion Centres' to share data across government agencies and across public and private sectors. According to DHS these centres are designed for state and local governments 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). By early 2008, there were 58 such centres across the US funded by DHS and costing $380 million dollars (US Department of Homeland Security, 2008). Fusion Centres can be thought of as part of a crime- and terrorism-prevention approach known as 'intelligence-led policing'. This involves a triage-like system where specific criminal activities, or suspected criminals or terrorists, are explicitly targeted for monitoring and intervention because of the assumption that focusing on high-risk activities or people will reduce crime or terrorism across the board. As a US Department of Justice report simply puts it: 'Good policing is good terrorism prevention' (Bureau of Justice Assistance, 2005).

One is hard pressed to find out any information about the function of these centres – neither who, exactly, is participating nor what information they are sharing. According to Robert O'Harrow Jr, who is an investigative journalist at the *Washington Post*, these centres are sifting through drivers' license records, identity-theft reports, financial information on individuals, firearms' licenses, car-rental information, top-secret FBI databases and more. This is all being done in partnership with private sector 'data brokers', such as 'Entersect, which claims it maintains 12 billion records on about 98 per cent of Americans' (O'Harrow Jr, 2008). There are no clear mechanisms for oversight or accountability with Fusion Centres, in spite of the fact that private companies are likely obtaining unprecedented access to government data on individuals, and vice versa.

Whereas DHS press releases are evasive about the functions of Fusion Centres at security conferences government representatives are more forthright about the rationales for these organisations. For instance, at the '9th Annual Technologies for Critical Incident Preparedness Conference and Exposition' in San Francisco in 2007, which I attended, DHS spokesperson Matthew Skonovd was quite clear that the purpose was to obtain data from the private sector and to share government intelligence with them so that private companies could become full partners in security provision (Monahan, forthcoming). Fusion Centres, he explained, are part of the federal government's efforts to respond to recommendations by the 9/11 Commission, which is a point seconded by a congressional report from which he quoted: 'the DHS State, Local, and Regional Fusion Centre 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' (Congressional Record, 2007). State funds invested in the private intelligence community, broadly speaking, are stunning: 'Washington spends some $42 billion annually on private intelligence contractors, up from $17.5 billion in 2000. That means 70 per cent of the US intelligence budget is going to private companies' (Scahill, 2008).

As Skonovd explained, in this 'blossoming' intelligence-sharing field, 'harvesting' and sharing information, it is necessary for the community to 'connect the dots' in order to avoid future terrorist attacks. When I asked what kinds of information are shared, and with what private industries, he responded that any information about risks to critical infrastructures, such as electricity plants and water-treatment facilities, which are increasingly privately-owned utilities in the USA, would be conveyed to those companies, and DHS would request co-operation in return. (It should be noted that this is a clear departure from public DHS documents, which emphasise coordination with local law-enforcement agencies, not with the

. . . specific criminal activities, or suspected criminals or terrorists, are explicitly targeted for monitoring and intervention because of the assumption that focusing on high-risk activities or people will reduce crime or terrorism across the board.

10.1080/09627250802699715

private sector.) If industry partners in Fusion Centres do not have appropriate classified clearance levels, Skonovd hinted that there are always 'work arounds' to facilitate sharing, such as having individuals sign 'non-disclosure agreements'. Industry representatives on the panel added that their companies were in a good position to co-operate with DHS because the US Safety Act of 2002 protected them from liability if they did so. Since then, the passage of an amended Foreign Intelligence Surveillance Act in 2008 granted retroactive immunity to telecommunications companies that illegally shared data on individual customers with federal intelligence agencies, confirming that businesses will likely be shielded from liability when sharing with Fusion Centres or any other government organisations.

A number of public critiques of Fusion Centres have emerged over the past few years. First, there is a concern that these centres are a waste of taxpayer-dollars that might be better spent on more pressing law-enforcement needs. Because federal security grants regularly come with cost-sharing requirements for states, they effectively institute unfunded mandates for programmes that might be low priorities for state or city governments. Large-scale systems that are funded have questionable utility. For example, a vast 'Homeland Security Information Network' has been implemented to foster information sharing, but it remains largely ineffectual because only two per cent of its 9,500 registered users log on each day, due to overwork or a commitment to more organic social networks and face-to-face interactions (DeYoung, 2006).

Second, the potential is high for Fusion Centres to be used to violate privacy rights, or civil liberties of citizens and others. There has been outrage over the use of Fusion Centres in the racial profiling of Muslim Americans, most notably in Massachusetts, under Governor Mitt Romney's direction. Moreover these centres are implicated in the investigation of activists or protestors engaged in legal domestic activities that have nothing to do with the stated mission of combating terrorism, such as individuals protesting at the 2008 Republican National Convention. The orientation of these centres towards collaboration with the private sector has further alarmed privacy advocates, who note the extremely lax data protection policies and practices of private companies handling sensitive data on individuals.

Finally, and related to the last critique, there is evidence of mission creep with these centres as they mutate into 'all-crimes' and 'all-hazards' organisations. Some reports have pointed to the intentional expansion of the mission of Fusion Centres – from anti-terrorism to general all-hazards preparedness – in order to ensure their continued existence in the face of future budget cuts. There is evidence, as well, that states are simply altering the missions of Fusion Centres because they are not perceived as being relevant.

As with most surveillance systems lacking clear guidelines and accountability mechanisms, Fusion Centres are inevitably employed for purposes other than those for which they were originally intended. In this instance, though, Fusion Centres may be reincarnating the data-mining aspirations of the infamous 'Total Information Awareness' (TIA) programme of the USA, which was scuttled in 2003 after vocal public protest. TIA was intended to integrate disparate databases and to facilitate data mining, so as to identify terrorist threats. These objectives persist in the form of Fusion Centres, airline passenger-prescreening systems and related international efforts to stockpile, mine and share data. Such schemes exist elsewhere. In the United Kingdom, for example, it was recently reported that the Home Office was seeking to collect information on all phone calls, email and websites visited by its residents. This data mining would be carried out under the authority of the proposed 2009 Communications Data Bill. Whether implemented as part of official public policy, or through covert means, governments are revealing their predilections for amassing data and establishing public-private partnerships without clear data-protection safeguards, accountability measures, public support or even proven efficacy. ■

Torin Monahan is Associate Professor of Human and Organizational Development and Associate Professor of Medicine at Vanderbilt University.

References

Bureau of Justice Assistance (2005), *Intelligence-Led Policing: The New Intelligence Architecture*, Washington, DC: US Department of Justice.

Congressional Record (2007), *Conference Report on H.R. 1, Implementing Recommendations of the 9/11 Commission Act of 2007*, Washington, DC: US House of Representatives. www.fas.org/irp/congress/2007_cr/hr1-info.html (accessed 7 December 2008).

DeYoung, K. (2006), 'In Arizona, officials share data the old-fashioned way', *Washington Post*, 9 August. www.washingtonpost.com/wp-dyn/content/article/2006/08/08/AR2006080801007.html (accessed 29 November 2008).

Hall, M. (2007), State-run sites not effective vs terror; Report blasts costly intelligence centers. *USA Today*, 24, July 2007, 1A.

Monahan, T. (forthcoming), *Insecurity: Surveillance, Fear, and Inequality in America*, New Brunswick, NJ: Rutgers University Press.

O'Harrow Jr., R. (2008), 'Centers tap into personal databases', *Washington Post*, 2 April. www.washingtonpost.com/wp-dyn/content/article/2008/04/01/AR2008040103049.html (accessed 8 December 2008).

Scahill, J. (2008), 'Blackwater's private spies', *The Nation*, 5 June. www.thenation.com/doc/20080623/scahill (accessed 8 December 2008).

US Department of Homeland Security (2006), *DHS Strengthens Intel Sharing at State and Local Fusion Centers*, Washington, DC: US Department of Homeland Security. www.dhs.gov/xnews/releases/press_release_0967.shtm (accessed 9 December 2008).

US Department of Homeland Security (2008), *State and Local Fusion Centers*, Washington, DC: US Department of Homeland Security. www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm (accessed 9 December 2008).