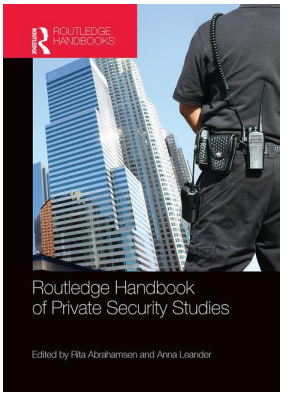

Routledge Handbook of Private Security Studies

Rita Abrahamsen, Anna Leander

Private Eyes

Publication details
https://www.routledgehandbooks.com/doi/10.4324/9781315850986-11
Ajay Sandhu, Kevin D. Haggerty
Published online on: 20 Oct 2015

10
PRIVATE EYES
Private policing and surveillance

Ajay Sandhu and Kevin D. Haggerty

Surveillance is a key attribute of contemporary life (Bennett *et al.* 2014). To appreciate the prevalence of surveillance we must recognize that it is not confined to draconian practices of social control, but entails any effort to collect information in order to further governmental ambitions. Here 'governmental' does not refer exclusively to state activities, but to public, private and individual efforts to advance different agendas. This is a necessarily broad definition, but one that usefully moves us beyond the usual focus on espionage and video cameras. Surveillance includes such things, but also extends to interpersonal scrutiny as well as to an expanding list of new technologies, including DNA databases, drones, metal detectors, satellites, biometrics, radio frequency identification (RFID) chips, online dataveillance, facial recognition, GPS tracking, identity cards, and the like. These varied devices and practices are changing how we raise our children, fight wars, deliver healthcare, educate students, socialize, conduct research, secure national borders, and conserve wildlife. Indeed, there are few realms of contemporary life that are not being transformed by new developments in surveillance (Ball *et al.* 2012).

This chapter focuses on the surveillance that is operative in private policing. In line with most researchers working in this field, we recognize that policing is accomplished through complex networks of private and public actors. These networks are composed of combinations of individuals and organizations that we might not immediately identify as 'the police,' but that nonetheless perform official and unofficial regulatory functions (Johnston and Shearing 2003). Readers should therefore bear in mind that while we single out some surveillance dynamics in private policing, surveillance on the ground typically involves heterogeneous interweavings of public/private organizations, individuals, texts, practices, and technologies (Haggerty and Ericson 2000).

In the following we emphasize both commonalities and differences in the dynamics of surveillance in private policing. In terms of the commonalities, the overriding point is that surveillance is central to the mandate and day-to-day operation of all policing. The second point is that such activities are remarkably diverse, and involve starkly different actors, technologies, and objectives.

To make these points we outline the relationships concerning surveillance among (a) private security officers who watch surveillance cameras, (b) private financial regulators responsible for monitoring financial markets and corporate activity for signs of fraud and other forms of

manipulation, and (c) everyday citizens who are increasingly encouraged to be the police's 'eyes and ears'. We conclude with a brief discussion of the symbolic dimensions of such surveillance.

Camera operators

Not long ago citizens in democratic countries tended to see the prospect of surveillance cameras trained on the public streets as a characteristic feature of totalitarian societies. Today, however, many Western nations cannot seem to install cameras fast enough (Doyle *et al.* 2011). It has reached the point that surveillance cameras have become a banal aspect of urban life (Goold *et al.* 2013). The individuals watching all of these screens are often private security officers, tasked with deciding, on a moment-by-moment basis, exactly what to monitor. In North America and Europe this typically involves looking for crime or disorder, but in other contexts camera operators are attuned to signs of political unrest or lack of conformity to religious dictates (Alhadar and McCahill 2011).

When contemplating the surveillance conducted by the private police, most people probably immediately conjure up images of security guards scrutinizing camera screens. These individuals use increasingly sophisticated technologies. Even rudimentary cameras can now digitally record in colour, and can tilt, pan, and zoom. These systems are easily networked and integrated into wider communication systems, allowing camera operators in many jurisdictions to communicate with other security personnel in real time. Advanced systems can zoom in to read a text message on a smartphone from hundreds of meters away. The newest devices allow for audio recording and facial recognition.

An increasing percentage of the private security sector now spends their entire shift staring at the feeds from dozens of different cameras. In the United Kingdom the British Security Industry Authority suggests there might be as many as one camera for every 11 people (5.9 million cameras) (Barrett 2013), and this only represents one component of a global camera industry slated to grow from US$11.5 billion in 2008 to $37.5 billion in 2015 (Electronics Research Network 2011). This embrace of cameras has occurred in a neoliberal political environment where officials routinely proclaim that they are committed to 'evidence-based policy'. The reality, however, is that surveillance cameras are a clear example of how crime policy is, in fact, often developed in an empirical vacuum. In the United Kingdom, where cameras first made serious inroads, camera systems were initially introduced as part of the 'ring of steel' established around London's financial district to protect against IRA bombings. In the 1990s the Conservative government, eager to reinforce its 'law and order' agenda and develop high-profile ways to 'do something' about crime, established a Home Office programme to encourage local councils to install camera systems. These efforts gained added public support in the aftermath of a series of high profile horrific crimes, most notably the murder of the toddler James Bulger in 1993.

However, perhaps the greatest factor contributing to the appeal of cameras was the commonsense assumption that surveillance cameras trained on public areas would inevitably reduce crime. Notwithstanding this belief, it remains unclear whether the cameras fulfil that promise. While it can be hard to develop sound methodological studies to measure the effects of surveillance cameras (Farrington and Painter 2003), the existing research suggests that camera systems work best in highly controlled environments – such as car parks – but are not particularly good at deterring the more spontaneous forms of urban disorder fuelled by the combustible combination of alcohol and machismo. Dedicated criminals appear to simply move to other nearby locations, or develop sophisticated techniques to commit crimes even in plain view of the cameras. A prominent meta-analysis of the impact of surveillance cameras on crime commissioned by the British Home Office could therefore only conclude – after studying many years'

worth of research – that it was too soon to come to a definitive conclusion as to the cameras' effectiveness (Gill and Spriggs 2005).

One of the most notable pragmatic problems camera operators face is that the cameras actually show too much. Any single camera shot will display far more than an individual could ever hope to scrutinize. Consequently, operators employ visual heuristics to help them identify what types of people and things are potentially 'out of order', and therefore deserving of greater scrutiny. The danger here is that these heuristics can be based upon deeply held prejudices and stereotypes. Research conducted in camera control rooms, for example, shows that in Western settings where the young black male has come to stand for criminal danger, camera operators typically use race as a primary discriminating category. The result is greater unwarranted camera attention being directed at black men (Norris and Armstrong 1999). Young people in general also tend to be monitored more closely, irrespective of their actions (or inaction). Daniel Neyland's (2006) study of surveillance camera operators captures a sense of how all-encompassing such suspicions can become in his chapter entitled 'Who are These Kids, and Why are They Standing Still?'. The cameras can also often reproduce a sexualized male gaze, with (predominantly) male camera operators objectifying women, but remaining oblivious to the types of harassment, intimidation, and dangers women face (Wright *et al*. 2014).

The fact that camera operators can have considerable discretion about who and what to watch can foster the impression that they are in positions of considerable power. In fact, these individuals tend to be among the most marginal actors in the criminal justice system. Gavin Smith's (2009) research on the occupational realities of camera operators shows them to be poorly paid, poorly trained, and have little job security. While watching the screens offers the occasional voyeuristic thrill, the reality is that most of the time the job is tremendously tedious. Being positioned near the bottom rung in the criminal justice division of labour also means that camera operators can find themselves bossed around and disrespected by the public police, who are their ostensible allies. Such occupational stresses can be compounded when monitoring becomes a psychological ordeal, as can happen when camera operators must helplessly watch people being beaten or committing suicide.

Financial surveillance

For decades we have seen the spectacle of corporate executives bilking taxpayers and investors of billions of dollars through a recurrent series of high profile economic crimes and misdeeds. Beyond the immediate financial losses, such activities are particularly hazardous to capitalist economies because they can undermine public trust in financial markets.

While the state has final authority to prosecute financial crimes, a complex network of public and private agencies is now responsible for investigating and regulating financial markets and business practices. These amount to quite different forms of surveillance conducted by private authorities. Such organizations sometimes conduct targeted surveillance, but also coordinate more rudimentary documentary and bureaucratic practices designed to make something as inscrutable as 'the market' into a phenomena that can be represented, analysed and managed (Ericson and Haggerty 1997). Private agencies provide forms of financial expertise that often cannot be found among the public police, including highly specialized auditors, lawyers, and forensic accountants.

As part of our dual emphasis on the centrality of surveillance in private policing – and the extreme diversity in what that surveillance entails in different contexts – we briefly identify some surveillance-related attributes of the private policing of economic crimes. Such efforts have created distinctive ways to visualize financial markets that, paradoxically, are also blinkered to certain varieties of economic wrongdoing.

Over the past two decades financial markets have become digitized. This allows massive amounts of financial instruments to be exchanged almost instantaneously, while also giving rise to new trading strategies designed to use the speed of these systems to capitalize on minute pricing differences (Lewis 2014). For regulators, computerization disconnected them from their previous personal relationships with traders who worked the stock market floors and who could offer clues about suspicious transactions (Thrift 2000). At the same time, digitization provided regulators with enormous amounts of data about market activity. Those data are the foundation of the distinctive contemporary financial surveillance modus operandi. Regulators now strive to create forms of computerized market legibility, whereby banks and other financial institutions must conform to 'know your customer regulations' and other standards for reporting and record keeping, all designed to make the movement of funds easier to trace using computers.

A prime example of this trend occurred in the aftermath of 9/11, when existing efforts to monitor financial activity for signs of money laundering by organized crime were quickly transformed into a heightened focus on trying to trace 'terrorist finances'. The upshot has been efforts to mandate that banks, international money transfer services, and other private financial institutions enhance the documentation of their customer's activities, and to routinely make that information available to the state (de Goede 2008). This amounts to a form of surveillance 'deputization' (Michaels 2010), whereby private agencies do the front-line collection of massive amounts of information which they share with the state, and which then serves as the informational backbone of state surveillance efforts. Edward Snowden's revelations make it clear that this type of surveillance deputization is now a key aspect of security efforts more widely, as communications service providers and internet service providers (ISPs) have been alternately enticed, threatened, or compelled to make their customer's data available to security agencies (Lyon 2014). Occasionally state security agents will simply hack into private corporate databases to obtain the desired information, without the corporation's (or client's) knowledge or consent (Gallagher 2014).

In the everyday operation of financial markets, traders are expected to buy and sell financial instruments according to a series of well-established trading rules and principles of market integrity. These are designed to prohibit such things as insider trading, wash trading, and other more complicated financial manipulations. Research conducted by James Williams (2009, 2013) in Canada stands out as some of the only criminological works that give us a sense of how surveillance operates in this world. As Williams demonstrates, the Toronto Stock Exchange contracts with the private organization Investment Industry Regulation Organization of Canada (IIROC) to identify forms of market manipulation, improper trade execution, and front-running. IIROC is then given access to the massive amounts of transactional data produced by the Toronto Stock Exchange.

Rather than making them omniscient, the volume of data available to regulators means that they face serious challenges in making sense of an almost unmanageable data glut. The solution has been for investigators to design computer algorithms to identify suspicious activities. These algorithms monitor the movement of funds between accounts, and the purchase and sale of stocks, bonds and other financial instruments, and automatically trigger an alert when they identify suspicious activity. That might happen, for example, when a trading rule has been violated – say a designated company 'insider' has traded some of his or her stocks. Alternatively, an alert might sound when trading occurs outside of established norms for a stock's price or for the volume of that stock traded in the recent past. In essence, these algorithms monitor for dramatic spikes in stock prices and trading volumes that occur outside of a statistically determined normal range. These statistical norms are themselves based on one month rolling

averages. So, if a stock that last week traded at comparatively leisurely rate starts to sell rapidly, the computer produces an alert. Thousands of such alerts can sound in a single day, which the IIROC staff then try and decipher to determine whether they are explainable aberrations, or if they warrant further investigation.

While finance has become digitized, the actual understanding regulators have about the markets depends almost entirely on what data are scrutinized, and the design of the algorithms used to make sense of that information. The result is a series of notable regulatory blind spots. For example, the fact that the alert system only monitors a small number of market indicators, including volume, price, and volatility, provides a comparatively thin and rudimentary view of markets. Second, jurisdictional issues mean that the IIROC regulators only focus their attention on equities-based markets and cannot monitor activities on the bond, derivatives, and commodities markets. Consequently, they cannot detect the common practice of cross-market manipulation. Finally, the fact that the alert system is based on detecting statistical variations based on one-month averages means that financial actors involved in more long-term market manipulations are invisible to the regulations. All of this leads Williams to this conclusion:

> While it may be true that digitized financial markets are more transparent than ever, they are rendered surprisingly opaque by virtue of the superficiality of these representations and the surfeit of information relative to the paucity of 'true' market knowledge.
>
> *(Williams 2009: 481)*

Moreover, it is the established powerful actors who are best positioned to take advantages of these regulatory blind spots.

Citizens' eyes and ears

Security officials usually fear that vigilantes will violate a suspect's legal rights and safeguards. Nonetheless, in recent years, officials have championed new efforts to invigorate, direct, and coordinate everyday citizens as part of anti-crime and anti-terrorism efforts. The aim is for citizens to be the police's 'eyes and ears', as people are encouraged to scrutinize their local environment. These efforts represent instances of private policing surveillance in that they seek to integrate the primal human proclivity to watch one another (Locke 2010) into the state's security agenda.

Attempts to champion the surveillance potentials of everyday citizens find support in recent criminological research that advocates for extremely pragmatic strategies to make it more difficult, or even impossible, for potential offenders to commit crime. This is most apparent in Felson's (2002) routine activities theory, which sees crime as resulting from the combination of a potential offender, suitable target, and a lack of a competent guardian. It is also a component of Newman's (1973) early work advocating for the creation of 'defensible space' – an ambition embraced by advocates of crime prevention through environmental design (CPTED; Jeffery 1971).

All of these approaches assume that we can reduce crime by enhancing the public's ability to routinely monitor their environment, often referred to as 'natural surveillance'. Typically, the emphasis is on creating unencumbered sight lines in workplaces, neighbourhoods, and on city streets. One example might involve increasing the sight lines for a convenience store clerk by having him or her stand on an elevated platform while also reducing the height of merchandise shelves. Officials trained in CPTED encourage homeowners to install more lighting, cut

down tall shrubs, and replace brick or wooden fences (that block people's views) with fences made of wrought iron bars that neighbours can see through. Planners now design entire subdivisions on these principles, populating suburbs with cul-de-sacs because of how they enhance the ability of neighbours to unconsciously monitor one another (Desyllas *et al*. 2003). All such initiatives enhance the public's surveillance abilities, often without people even knowing that this has happened, or that it is the result of explicit design decisions.

In the aftermath of the terrorist attacks of 9/11 the state turned to more direct attempts to empower and embolden citizens to actively scrutinize one another. Security officials from across the Western world nurtured a form of 'participatory surveillance' by urging citizens to watch out for suspicious individuals and activities. Many of these schemes were modelled on the longstanding Neighbourhood Watch programme (McConville and Shepherd 1992), which has homeowners mark their property for identification, conduct local street patrols, and display signage to announce their anti-crime vigilance. Comparable American terrorism-inspired developments include: 'If you see something, say something', TIPS, Marine Watch, Eagle Eyes, CAT Eyes, Talon, Real Estate Watch and Highway Watch (Stanley 2004). All such programmes exhort citizens to report suspicious activities to the authorities, and help them to do so through dedicated phone numbers and websites.

Similar ventures train citizens to search for and respond to terrorist threats. For example, the United States Department of Homeland Security supports the 'Citizen Corps' programme, which aims to 'harness the power of every individual through education, training, and volunteer service to make communities safer, stronger, and better prepared to respond to the threats of terrorism, crime, public health issues, and disasters of all kinds' (US Department of Homeland Security 2015). Citizen Corps teaches citizens how to look for threats, organize and create dedicated groups, and create defence strategies in case of a disaster or attack. It has a course specifically designed for children called 'youth preparedness' (FEMA undated) to teach kids how to be ready for emergencies by contributing to 'family disaster supply kits' and making escape plans.

The Texas Virtual Border Watch stands as one of the more fascinating of these recent 'watch' programmes. Now discontinued, this pilot initiative built upon an intriguing mix of computers, webcams, voyeurism, patriotism, and xenophobia to encourage citizens to use their home computers to remotely monitor cameras trained on the US border with Mexico in search of criminals or drug dealers illegally entering the US. People from anywhere in the world could register to become one of these virtual video vigilantes, and click on a button to alert the authorities if they saw anyone crossing the border illegally. While it did not meet its intended quotas for locating threats and making arrests (Koskela 2011), the virtual border watch provides an intriguing glimpse into how participatory surveillance can be technologically augmented.

All of these initiatives involve a form of 'reponsibilization', whereby the state's role in countering crime and terrorism is subtly transferred onto individual citizens who are encouraged to play a greater role in managing such risks. They are also examples of what Mathiesen (1997) refers to as 'synoptic' surveillance, which is characterized by 'the many' watching 'the few'. This is to be contrasted with forms of 'panoptic' surveillance famously identified by Foucault (1977), where 'the few' watch 'the many'.

Notwithstanding their official embrace, serious questions remain about the efficacy and desirability of such initiatives. Most basically, it is not clear that these programmes reduce crime. Typically introduced with a flourish in the aftermath of a high profile criminal or terrorist event, public enthusiasm for participatory surveillance tends to quickly wane, leaving behind only the signs proclaiming the existence of programmes that are effectively defunct. More

problematically, empowering citizens to act on ill-defined notions of 'suspicious people' or 'suspicious activity' can encourage them to draw upon their own prejudices and unfounded anxieties as the basis for identifying who to watch. It is therefore not surprising that these programmes have been plagued with false reports and phony tips (Neumann 2008). Citizen watchers often target youths deemed to be in the wrong place at the wrong time, and individuals who conform to modern stereotypes of post-9/11 terrorism, which includes having brown skin or displaying markers of the Muslim faith (Chan 2008). For those being watched, such scrutiny can be a form of aggressive and stigmatizing exclusion that reminds them of their marginal status. So while these initiatives aim to protect citizens, there is also the danger that they can instead corrode the types of mutualism, respect, and trust that is intrinsic to the functioning of any healthy community.

Conclusion

The above three examples are so different that it might be hard to bear in mind that they are all instances of surveillance conducted by private policing. That, in part, is our point. Private policing is a remarkably varied enterprise, employing practices of surveillance and visualization that involve dramatically different actors, technologies, and routines. While such complexity can make it challenging to develop a comprehensive understanding of surveillance and private policing in all its different guises, it also presents valuable research opportunities. Studying surveillance provides a rewarding entrée for researchers seeking to understand the aims, objectives and practical strategies operative in private policing.

Much of the existing criminological research on surveillance concerns the question of whether it actually reduces crime and disorder. Such evaluative research is a well-established criminological enterprise (Sherman *et al.* 2006), although one with the tendency to produce frustratingly inconclusive results that prompt heated ideological debates about how to interpret those findings. Evaluative research, however, also risks making the mistake of accepting the stated aims of surveillance advocates at face value. Reducing crime is often only one of the ultimate aims or social consequences of surveillance – and sometimes not a particularly important ambition in comparison to surveillance's numerous other accomplishments. That is because surveillance, like policing itself (Manning 2012), is a highly symbolic activity that conveys a diverse set of meanings to quite different audiences.

Consider, for example, the participatory surveillance of citizens watching other citizens. While not particularly useful in identifying terrorists, this form of private policing involves rich drama whereby citizens literally perform a simulated police role. In the process, they align themselves with the state's security agenda while effecting an insider/outsider social cleavage – one where real or imagined enemies are positioned as external threats. Marginalized groups are stigmatized as 'outsiders', while 'insiders' are bonded together. Likewise, surveillance cameras perform important symbolic work irrespective of whether they actually reduce crime. For the private security sector, who often must struggle for official legitimacy, sophisticated cameras can signal their modernity and professionalism. By using cameras these organizations also convey to external agencies, such as the courts, that they are performing their anti-crime due diligence (Haggerty and Tokar 2012). For everyday citizens the cameras can themselves come to stand for safety, security, and urban renewal.

In terms of the surveillance of financial markets, regulatory efforts to fashion a bureaucratic and documentary field of visibility amenable to computerized scrutiny and other forms of representation actually help constitute the market itself (Williams 2009). In the process this surveillance conveys the reassuring – and perhaps completely false – impression that markets

are amenable to meaningful understanding and regulation, and that such regulation is not capricious, but rooted in rational processes. In a charged political environment, financial surveillance by private actors also serves the basic but vital role of allowing politicians to appear to be addressing the persistent problem of corporate wrongdoing, again, irrespective of the efficacy of such financial oversight.

Bibliography

Alhadar, I. and McCahill, M. (2011) 'The Use of Surveillance Cameras in a Riyadh Shopping Mall: Protecting Profits or Protecting Morality', *Theoretical Criminology* 15(3): 315–30.

Ball, K., Haggerty, K. and Lyon, D. (2012) *The Routledge Handbook of Surveillance Studies*, Abingdon: Routledge.

Barrett, D. (2013) 'One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey', *The Telegraph* 10 July, www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html.

Bennett, C., Haggerty, K., Lyon, D. and Steeves, V. (2014) *Transparent Lives: Surveillance in Canada*, Athabasca: Athabasca University Press.

Chan, J. (2008) 'The New Lateral Surveillance and a Culture of Suspicion', in M. Deflem and T. Ulmer (eds), *Surveillance and Governance: Crime Control and Beyond*, Bingley: Emerald, pp. 223–39.

Coleman, R. and McCahill, M. (2011) *Surveillance and Crime*, London: Sage.

De Goede, M. (2008) 'Risk, Preemption and Exception in the War on Terrorist Financing', in L. Amoore and M. de Goede (eds), *Risk and the War on Terror*, Abingdon: Routledge, pp. 97–111.

Desyllas, J., Connoly, P., and Hebbert, F. (2003) 'Modelling Natural Surveillance', *Environment and Planning B* 30(5): 643–55.

Doyle, A., Lippert, R. and Lyon, D. (2011) *Eyes Everywhere: The Global Growth of Camera Surveillance*, Abingdon: Routledge.

Electronics Research Network (2011) 'Global Video Surveillance Market to reach US $37.7 Billion by 2015', *Semiconductor Research News*, www.marketresearchworld.net/content/view/3884/77.

Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.

Farrington, D. and Painter, K. (2003) 'How to Evaluate the Impact of CCTV on Crime', in M. Gill (ed.), *CCTV*, Leicester: Perpetuity Press, pp. 67–79.

Felson, M. (2002) *Crime and Everyday Life* (3rd edn), Thousand Oaks, CA: Sage.

FEMA (undated) *Youth Preparedness: Implementing A Community-Based Program*, Washington, DC: Federal Emergency Management Agency, www.fema.gov/media-library-data/20130726-1903-25045-5654/youth_preparedness_implementing_a_community_basesd_program_v5_508.pdf.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison* (trans. A. Sheridan), New York: Vintage.

Gallagher, R. (2014) 'Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco', https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story.

Gill, M. and Spriggs, A. (2005) *Assessing the Impact of CCTV*, London: Home Office Research, Development and Statistics Directorate.

Goold, B., Loader, I. and Thumala, A. (2013) 'The Banality of Security: The Curious Case of Security Cameras', *British Journal of Criminology* 53 (6): 977–96.

Haggerty, K. and Ericson. R. (2000) 'The Surveillant Assemblage', *British Journal of Sociology* 51(4): 605–22.

Haggerty, K. and Tokar, C. (2012) 'Signifying Security: On the Institutional Appeals of Nightclub ID scanning Systems', *Space and Culture* 15(2): 124–34.

Jeffery, R. (1971) *Crime Prevention Through Environmental Design*, Beverly Hills, CA: Sage.

Johnston, L., and Shearing C. (2003) *Governing Security: Explorations in Policing and Justice*, Abingdon: Routledge.

Koskela, H. (2011) 'Don't Mess With Texas: Texas' Virtual Border Watch Program and the (Botched) Politics of Responsibilization', *Crime, Media, Culture* 7(1): 49–65.

Lewis, M. (2014) *Flash Boys: A Wall Street Revolt*, New York: W. W. Norton.

Locke, J. (2010) *Eavesdropping: An Intimate History*, Oxford: Oxford University Press.

Lyon, D. (2014) 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique', *Big Data and Society* 1(1): 1–13.

Manning, P. (2012) 'Drama, the Police and the Sacred in Policing', in T. Newburn and J. Peay (eds), *Policing: Politics, Culture, and Control,* Oxford: Hart, pp. 173–94.

Mathiesen, T. (1997) 'The Viewer Society: Michel Foucault's "Panopticon" Revisited', *Theoretical Criminology* 1(2): 215–34.

McConville, M. and Shepherd, D. (1992) *Watching Police Watching Communities*, London: Routledge.

Michaels, J. D. (2010) 'Deputizing Homeland Security', *Texas Law Review* 88: 1435–73.

Newman, O. (1973) *Defensible Space: Crime Prevention Through Urban Design*, New York: Collier.

Neuman, W. (2008) 'In Response to M.T.A.'s "Say Something"' Ads, a Glimpse of Modern Fears', *New York Times* 7 January, www.nytimes.com/2008/01/07/nyregion/07see.html?pagewanted=all&_r=0.

Neyland, D. (2006) *Privacy, Surveillance and Public Trust*, Basingstoke: Palgrave.

Norris, C. and Armstrong, G. (1999) *The Maximum Surveillance Society: The Rise of CCTV*, Oxford: Berg.

Sherman, L., Farrington, D. Welsh, B. and MacKenzie, D. L. (2006) *Evidence-Based Crime Prevention* (revised edition), Abingdon: Routledge.

Smith, G. J. D. (2009) 'Empowered Watchers or Disempowered Workers? The Ambiguities of Power Within Technologies of Security', in K. F. Aas, H. Oppen Gundhus and H. Mork Lomell (eds), *Technologies of (In)security*, Abingdon: Routledge, pp. 125–46.

Stanley, J. (2004) *The Surveillance Industrial Complex*, New York: American Civil Liberties Union.

Thrift, N. (2000) 'Pandora's Box: Cultural Geographies of Economies', in G. L. Clark, S. Gertler and M. P. Feldman (eds), *The Oxford Handbook of Economic Geography*, Oxford: Oxford University Press, pp. 689–704.

US Department of Homeland Security (2015) 'Citizen Corps', www.dhs.gov/citizen-corps.

Williams, J. (2009) 'Envisioning Financial Disorder: Financial Surveillance and the Securities Industry', *Economy and Society* 38 (3): 460–91.

Williams, J. (2013) 'Regulatory Technologies, Risky Subjects, and Financial Boundaries: Governing "Fraud" in the Financial Markets', *Accounting, Organizations and Society* 38(6–7): 544–58.

Wright, J., Glasbeek, A. and van der Meulen, E. (2014) 'Securing the Home: Gender, CCTV, and the Hybridized Space of Apartment Buildings', *Theoretical Criminology* 19(1): 95–117.