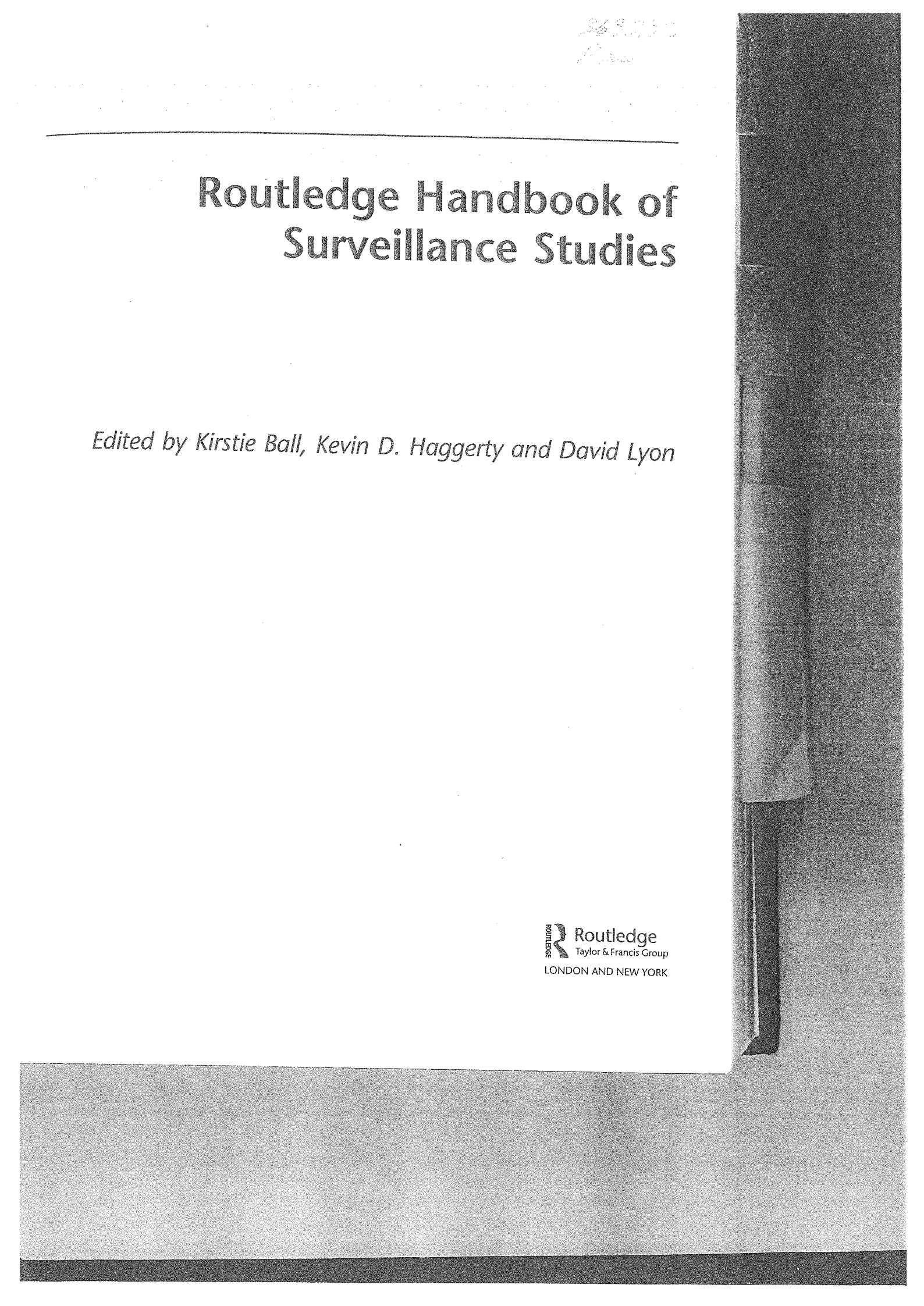
Routledge Handbook of Surveillance Studies

Edited by Kirstie Ball, Kevin D. Haggerty and David Lyon



Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2012
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

Simultaneously published in the USA and Canada
by Routledge
711 Third Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging in Publication Data
Routledge handbook of surveillance studies / edited by David Lyon, Kevin D. Haggerty and Kirstie Ball.
p. cm.
Includes bibliographical references and index.
1. Privacy, Right of. 2. Electronic surveillance–Social aspects. 3. Information technology–Social aspects. 4. Social control. I. Lyon, David, 1948- II. Haggerty, Kevin D. III. Ball, Kirstie.
JC596.R68 2012
363.2'32–dc23
2011041478

ISBN: 978-0-415-58883-6 (hbk)
ISBN: 978-0-203-81494-9 (ebk)

Typeset in Bembo
by Taylor & Francis Books

MIX
Paper from responsible sources
FSC® C004839
www.fsc.org

Printed and bound in Great Britain by
CPI Antony Rowe, Chippenham, Wiltshire

a. Surveillance, crime and the police

Kevin D. Haggerty

Popular depictions of the police tend to portray an action-packed and often violent profession. In the routine operation of policing, however, a considerable volume of an officer's time is consumed with filing, not fighting. The police are information workers, concerned with collecting, analyzing and communicating a diverse array of intelligence within and outside of the police's formal institutional boundaries (Ericson and Haggerty 1997). Indeed, the police are remarkably enthusiastic collectors of information, displaying a desire to amass and secure access to volumes of data that can far surpass their ability to make it pragmatically useful.

That the police conduct surveillance is not a particularly startling insight. Surveillance, in its various forms, is now the preferred institutional response for dealing with any number of social problems. The police, who have an extremely wide organizational remit, are called upon to deal with a bewildering range of issues (some of which are criminalized, while others are not), so it seems appropriate that they might engage in different forms of surveillance and have access to specialized surveillance technologies and databases (Coleman and McCahill 2011).

Despite this long-standing affinity between the police and surveillance, there is much that is new in the scope and operation of police surveillance, something that can be attributed to such things as new organizational models, information technologies, political ideologies, public fears, developments in crime politics, trends in criminal behavior, and so on. Combined, such factors have significantly strengthened and expanded the police's surveillance mandate across the globe.

Concerns about police surveillance sit at the fulcrum of two of modernity's great nightmares. On the one hand is the fear of routine victimization, with crime becoming an endemic part of daily life. Here, police surveillance is understood to be a necessity, as a bulwark against the prospect of descending into an anarchic world of failed states run by criminal gangs. At the other extreme sits the prospect of a totally controlled society, something that was foreshadowed in several totalitarian regimes during the course of the twentieth century. Here police surveillance is positioned as a more sinister tool that always risks being used to regulate the minutia of human conduct in a manner reminiscent of Orwell's dystopic vision of total control (Cohen 1985).

This chapter details some of the issues pertaining to surveillance undertaken by the police for purposes of crime control. In doing so I draw attention to the considerable variability in the police's anti-crime surveillance measures. At the outset, however, it is worth noting that the police are themselves a highly variable institution. Despite many similarities between police forces internationally, policing is not standardized; it displays considerable variation related to local cultures, legal regimes, national histories and

political structures, among other things. Organizational units even within the same police force can operate quite differently, as is apparent in the distinction between uniformed constables and detectives working in civilian clothing. Policing units can themselves often be distinguished one from the other on the basis of the primary (but not necessarily exclusive) forms of surveillance they conduct, with constables relying on informants, detectives on undercover work, cyber police units conducting dataveillance, aerial units combining cameras with forward-looking infrared radar (FLIR), while traffic units use radar and increasingly rely on automated license-plate readers. Such variability means we should be cautious about drawing broad conclusions about surveillance in policing.

In what follows I concentrate primarily on the public police. It should be stressed, however, that policing occurs in a range of institutions, including insurance companies, securities regulators, intelligence agencies, taxation departments, welfare offices and immigration services, to name just a few, with each conducting their own forms of surveillance. The private police (often called "security guards") are also significant players in the dynamics of anti-crime surveillance, and often greatly outnumber state police employees as is the case, for example, in Brazil, South Africa, the United States and many other countries. In the aftermath of the September 11th 2001 terrorist attacks the line which traditionally separated policing from national security has also become blurred in many Western jurisdictions. On top of all of this, officials encourage individual citizens to conduct their own anti-crime surveillance. This includes such things as trying to reduce the risk of home break-ins by maximizing the sight lines around their homes, installing personal surveillance cameras and participating in assorted "crime watch" programs.

The fact that the police exist in a wider institutional matrix is particularly important for understanding police surveillance, as the police increasingly rely on forms of monitoring that are conducted by other government, security and commercial actors, a point I return to below.

A key starting point for understanding the wider politics of police surveillance follows from the social constructionist insight that crime is not a naturally given phenomenon, but that certain acts *become* crimes through highly variable institutional practices of categorization, monitoring and processing. Consequently, the police do not so much detect crime, but deploy assorted measures that selectively draw attention to the behaviors of certain categories and classes of people that *could be*—depending upon a host of contextual factors—processed as crimes. In societies deeply split by race, class and gender divisions, such selective monitoring often gives rise to accusations that the police are discriminatory; that police surveillance is being used to control and criminalize certain groups—something that may result from the police's actions even if it is not their specific intention (see Browne, this volume).

Another analytical issue pertaining to police surveillance concerns the dynamics of "surveillance creep," the process whereby surveillance measures (both "low-tech" and "high tech") introduced for one defined purpose can quickly develop new uses, expanding to focus on new places and populations. This is now a general tendency in the dynamics of surveillance, but the police play a particularly important role here by alternatively reconfiguring surveillance measures used in other domains for police purposes or serving as a launching-off point for the movement of surveillance practices into wider society.

In what follows I introduce some of the different forms of surveillance conducted by the police. I start with the police's more established "low-tech" surveillance practices of snitching and undercover policing, and move to a discussion of some newer and more technological forms of police surveillance. I dedicate one section to surveillance camera technology given how important such devices have become in many urban policing contexts. The concluding substantive section accentuates how the police are not just watchers, but are also themselves monitored.

This is necessarily a selective overview, but the general points about the aims, challenges and political concerns pertaining to specific surveillance measures often generalize to other instances. It is also the case that while I treat these measures separately, one of the most important trends in policing concerns how different surveillance practices are increasingly being aligned and used in concert, something that will undoubtedly only increase in the future.

Snitching

A common expression in policing is that a police officer is only as good as her informants, something that accentuates the centrality of "snitching" in police work. Snitching involves someone trying to gain personal advantage from informing the officials about other's crimes (Natapoff 2009). Or, viewed from a different angle, it involves the authorities positioning a person such that they feel compelled to turn on their criminal collaborators. The typical snitching scenario involves an apprehended (not necessarily charged) suspect providing information about the crimes of their associates. It can also involve informants who have a long-standing relationship with the police, and who are paid for information. The level of snitching in most jurisdictions is impossible to quantify, but it is often pervasive.

Snitching is essentially officially sanctioned punishment bartering. For any barter system to work, both parties must stand to gain from the exchange. For the police, informants can provide access to criminal organizations that they otherwise could not infiltrate. Police also use snitches to try and work up the criminal hierarchy, using an informant's testimony to build cases against more serious offenders. For prosecutors, snitching lubricates the court's wheels, making criminal prosecutions faster and more certain. Indeed, if snitching were eliminated, the courts in many jurisdictions would lurch to a halt, as no snitching would translate into little plea bargaining. For suspects, snitching presents an opportunity to catch a break. This could mean, for example, that in exchange for cooperating they might not be charged, that they will be prosecuted for less serious crimes, that their sentence will be reduced, or that they are incarcerated in a comparatively desirable institution, and so on.

While snitching might not be something that immediately comes to mind when thinking about police surveillance, snitches remain one of the most important ways that the police routinely keep tabs on individual offenders and criminal organizations, as citizens are alternately enticed or coerced to detail the actions of their friends and collaborators. Official reliance on snitches also produces a host of harms. These include how snitching tends to result in a form of secret justice, and produces vastly different outcomes for people charged with the same crimes. Snitching corrodes already strained police/community relations and results in criminals intimidating or punishing informants. To cultivate snitches police will let crimes go unpunished and sometimes even turn a blind eye to serious offences that they know their valuable snitches continue to commit. Perhaps most disastrously, snitching has been a conspicuous factor in many false convictions, as informants with little to lose have indicted innocent individuals in hopes of striking a deal.

Undercover policing

Besides snitching, another long-standing low-tech police surveillance practice involves undercover operations, with officers surreptitiously assuming a host of different roles in hopes of catching criminals. Today this is recognized as a routine and perhaps necessary part of police work, but in the early emergence of the modern Western police institution the prospect that the state would deploy undercover operatives was highly controversial, raising fears of despotic forms of state control. Despite our contemporary familiarity with the general existence of undercover policing, it continues to be plagued by legal and ethical concerns (Marx 1988).

At the most basic level, undercover policing can be unsettling because it involves sometimes extreme levels of deceit and public manipulation. In hopes of collecting intelligence the police have pretended to be, for example, inmates, vagrants, journalists, pornographic book sellers, prostitutes, lawyers, census enumerators, lovers, priests, assorted forms of criminals and many, many more roles. The police will also fake entire social gatherings in attempts to lure reclusive criminals into the open. A classic example of such an operation involves mailing suspects a notice informing them that they have won a prize, or that their social security benefits have been suspended. When the suspect arrives at the appointed "social event" or "welfare office" they are immediately arrested. While such tactics are justified as being necessary, having police officers collect intelligence by posing as journalists or priests also obviously risks undermining public trust.

The internet has created new possibilities for undercover police surveillance, as officers assume virtual identities in hopes of learning about illegal activity. Contemporary revelations that the police and immigration authorities are "friending" people on Facebook in order to access their personal data is an obvious example. Another involves ongoing concerns about sexual predators on the internet, with police organizations across the globe responding to such anxieties by pretending to be paedophiles in order to communicate online with real paedophiles. Alternatively, officers pose as children in youth-oriented chat rooms to entice potential child molesters. As early as 1999 Shari Steele of the Electronic Frontier Foundation estimated that "at least half of the 13-year-old girls in chat rooms are probably policemen." This is undoubtedly a gross overestimation, but it does raise the question of what percentage of the panic-inducing paedophile-related communications on the internet are created entirely by one police officer for eventual consumption by another police officer. How would we know one way or the other?

Such a scenario also points to a recurring problem that undercover work poses for the police; the prospect of "blue on blue" crime. This occurs when a police officer or police organization unaware of a specific undercover operation will swoop in and arrest police officers posing as criminals. Tragically, such mistakes have occasionally resulted in officers shooting other officers who they did not know were working undercover. At a more prosaic level, undercover policing can also put officers in highly stressful situations, breaking up friendships and families and occasionally resulting in emotional collapse. Ethically, undercover policing can straddle a line between catching legitimate criminals and entrapment, where citizens are induced or coerced by the police to engage in criminal acts that they otherwise would not commit.

Police surveillance technologies

As noted, the preceding examples of police surveillance were notably "low tech." Consequently, they contrast with much of what is interesting and occasionally unsettling about contemporary surveillance which involves more "high-tech" surveillance options. The police are now positioned as potential users of almost any new surveillance device. This is particularly apparent when surveillance devices originally produced for military applications are transferred to civilian policing settings, technologies which include satellites, helicopters, drones and sensors (Haggerty and Ericson 2001). Rather than such technologies being a rational response to the practical demands of crime control, they can amount to a form of technological solution in search of a problem, with the police serving as a convenient site for justifying the expanded uses of such devices. Such developments are part of the more general emergence of a surveillance industrial complex (see Hayes, this volume). This general intensification of police surveillance, when combined with the fact that the police's adoption of surveillance technologies can desensitize citizens to the eventual expansion of these devices to other non-policing contexts, gives police surveillance technologies a political significance that extends well beyond issues of detecting or deterring criminals.

While many surveillance technologies have been introduced into policing in recent years it is worth remembering that the police have long sought to rationalize their practices by embracing different technological systems. One of the most important classes of such devices are those that seek to identify people. The early embrace of such practices occurred in the nineteenth century in the context of the rise of a "society of strangers," as rural populations moving to urban centers encountered a litany of unknown others. Such strangers posed a dilemma for the police who sought to keep track of suspect populations and identify known criminals.

A notable early police attempt to address this problem was the Bertillon system. Introduced in France in the 1880s, "Bertillonage" as it was called, combined the emerging archive of police photographic "mug shots" with a series of standardized measurements of several ostensibly unchanging physical attributes of a person's body, storing those details in a coded filing system. Bertillonage was ultimately abandoned with the increasing popularity of fingerprinting, which identifies people by the unique patterns on their fingertips. More accurate than its predecessors, fingerprinting also had the distinct forensic advantage of being

able to position suspects at crime scenes by virtue of the latent prints that they leave behind. Fingerprinting, combined with police "mug shots," remained at the core of police identification practices for approximately a century (Cole 2001), although both saw significant advances during that period which made the data easier to collect, search and distribute.

Efforts to identify criminals (and others) were radically expanded in the 1990s with the emergence of DNA typing, something that allows the authorities to identify unique individuals from trace DNA elements found in saliva, semen, blood, hair, and so on. This gave rise to new investigative practices and also new organizational sections, most notably the "cold case" units that sought to re-examine unsolved cases that might benefit from new forensic techniques.

While DNA testing marks a major scientific advance, to be an effective policing technology DNA systems ultimately require a matched sample. Consequently, there have been recurring calls from the police to expand DNA databases such that they would include ever-larger population groups. DNA identification therefore stands as a clear example of surveillance creep (Nelkin and Andrews 1999), as early proposals for DNA databases came with recurrent reassurances that DNA would only ever be collected from the worst of the worst criminals. Instead, in countries such as Norway, Canada and the United States we have seen a progressive expansion such that more and more classes of offenders are required to submit a DNA sample to be stored on the database. In the UK, one now only has to be a suspect (not even charged with a crime) to have your DNA collected and stored. In other countries the security establishment routinely lobbies for the state to collect DNA from every citizen and all visitors.

Police surveillance is also now being transformed by developments in information technology. Networked computing has allowed for an exponential increase in the amount of information that many institutions collect, analyze and disseminate. While the police collect their own data about myriad phenomena, they are also eagerly eyeing the data amassed by other institutions, recognizing the policing potentials inherent in the data collected by banks, libraries, airlines, telecommunications companies, internet service providers, and others.

To date much of the police's access to and use of such data has been somewhat haphazard and idiosyncratic. Efforts are now underway to change that situation, to find ways for the police to secure regular access to the data collected by other government, police, security and corporate institutions. This is typically referred to as "breaking down information silos," a practice that promises to expand significantly, giving the police more regular access to reams of ever more fine-grained data on citizen's travels, interests, habits, contacts, physical location, and so on. So, the United States, for example, has seen large commercial data brokers such as ChoicePoint prospectively formatting the vast amounts of data they collect on individual American citizens (but also citizens in countries such as Argentina, Brazil and Mexico) and selling it to American law enforcement agencies. This provides the police with "one-stop information shopping" for detailed data about individuals—information that the state is often legally prohibited from collecting itself. In the European Union a spate of "data retention" legislation now mandates that private companies maintain data on their customer's communications (cell phone and internet use) so that it can be made available to the police if deemed necessary.

Such information-sharing efforts became particularly popular after the terrorist attacks of 2001 when the authorities in many countries passed legislation that compelled various organizations to provide the police access to at least some of their data. Ultimately, any success that the police will have in this regard is contingent on a series of local legal and political factors, but there is no denying that the police see accessing such data as a major step forward in their attempt to identify criminals—and people who might become criminals.

This greater ability to link information across institutions for policing purposes promises to dramatically alter people's lived experiences. Marginalized and criminalized populations are most likely to feel the hard end of such initiatives. As information systems become ever more tightly linked we can envision a future where criminalized populations must find alternatives outside of mainstream institutions. One can gain a

glimpse of such a world in Alice Goffman's (2009) excellent ethnography of wanted men living in a Philadelphia ghetto. Almost all of these men have various warrants out for their arrest, usually for non-payment of fines. They are vulnerable to arrest each time they have dealings with state and an increasing number of private institutions as they can only access those services after their personal details are searched on linked databases. The upshot is that they cannot get welfare or travel internationally, and in order to work or acquire medical assistance they must do so in the alternative "grey economy."

Police efforts to access the data collected by other institutions are also subtly changing the dynamics of criminal suspicion. Previously, individuals became suspects or known to the police because of what they did—or were presumed to have done. The police might then initiate formal surveillance measures if they deemed it appropriate. Today, the emergence of policing focused on databases means that the data system itself can generate suspicious populations. Aggregate data can be analyzed using sophisticated data algorithms (see Gandy, Jr, this volume) to single out people with profiles that authorities have deemed "risky"—the classic example involves the work of immigration authorities who use profiles to flag individual travelers as security threats because they are travelling alone, on a one-way ticket bought with cash, have no luggage and are arriving from any number of "high risk" countries. In such instances the data system effectively constructs suspicion on the basis of a combination of weighted data points, serving up "risky" individuals for greater levels of police scrutiny.

In terms of the official response to crime, such dataveillance gives a greater forward-looking dimension to policing. Historically, the crime control apparatus was primarily concerned with events that occurred in the past, punishing offenders for acts that they had already committed. What little consideration of the future there was in crime control came from justifying such measures as potentially preventing or deterring crime. Today, greater attention to potential criminal risk factors for various populations is starting to focus crime control more on reducing risks such that crime might not occur—something that often goes by the name of "pre-emption." This operates by analyzing data for indicators that someone with a specific constellation of attributes is statistically likely to commit crime in the future, and intervening today to try and reduce those risk factors. While we are still in the very early days of such pre-emption efforts, they raise ethical issues about whether the state should be singling out people on the basis of crimes that they have not yet committed—and might never commit.

As noted, many other surveillance devices are rapidly finding uses in policing including helicopters, wiretaps, drones and the like. All such devices are justified as a way for the police to better identify suspects and detect crimes. They can also come with a cost that is difficult to calculate. In particular, such devices can further distance the police from the communities they are supposed to serve, something that is routinely held out as a major dilemma for the prospects of consensual policing.

Surveillance cameras

One of the more significant recent "high-tech" developments in policing has been the introduction of surveillance cameras. These are also often referred to as "closed circuit television" (CCTV), although that terminology is increasingly inappropriate as the cameras no longer use "closed circuit" technology, nor are the images displayed on a television. Whatever they are called, the embrace of these devices marks a notable transformation in police practice and public attitudes.

Surveillance cameras were originally introduced in private settings such as corner stores and retail outlets. Any footage that the police received from those cameras was handed to them at the discretion of the camera owners. It was only in the early 1990s, particularly in the United Kingdom, where public surveillance cameras controlled and operated by public authorities truly took off. Again, it was not the police who installed and operated these devices, but they were and continue to be regularly provided with the images and intelligence they produce. The reasons for this expansion are complex (see Norris in this volume) having been justified for several reasons beyond any ability to catch criminals, including the belief

that they might reassure the public, manage traffic, and be a key element in urban regeneration programs more generally. The exact number of cameras in most countries is debatable, but the unassailable truth is that there are many cameras, their numbers grow daily, they are increasingly integrated, and their technological abilities to see are becoming more sophisticated.

The introduction and expansion of cameras signifies a rather remarkable change in public attitudes. One generation ago the idea that the state would install video cameras to watch its own citizens stood as perhaps the iconic symbol of a totalitarian society. Today, such devices are widely supported.

There remains, however, the vexatious issue of whether the routine use of such cameras actually reduces crime. While most police officers have anecdotal evidence of cameras helping to catch a particular criminal, at the more aggregate level even the most rigorous and comprehensive evaluations typically conclude that any evidence for the camera's crime-fighting power is ambiguous, at best (Gill and Spriggs 2005). The crime-reducing ability of public cameras is blunted by the fact that criminals modify their behavior in order to operate notwithstanding the presence of cameras. Cameras sometimes displace criminal behavior to neighboring areas, something that the camera-equipped community might applaud, but at a broader societal level hardly counts as a progressive development.

There are serious methodological challenges in trying to discern any effect of surveillance cameras. At the most basic level, it can be difficult or impossible to know what the crime rate would have been if the cameras were not installed, making before-and-after comparisons problematic. There is also wide variability in the abilities of such cameras with some being stand-alone systems that provide little more than grainy images of the flow of humanity. More sophisticated systems can digitally scrutinize people with the aid of pan, tilt, zoom and now audio capabilities. Still others are dummies, installed in hopes of deterring unwanted behavior, but which record nothing. Some systems are unmonitored, others are monitored by security guards and still others by police officers. The number of people staffing the cameras, their training and level of professionalism can vary dramatically. The physical location and density of the cameras and the degree to which they are publicized can also distinguish one system from another. These different configurations suggest that there is a world of difference in the operational dynamics of systems, making comparisons of their effects difficult. It seems fair to say, however, that the cameras have not lived up to the early optimistic claims of those who believed that cameras would significantly reduce crime and ease public anxieties about victimization.

In many contexts surveillance cameras also represent another clear example of "surveillance creep." Most cameras were initially justified as a means to counter high-level crimes such as child abductions and terrorism. Once installed, the camera's ability to monitor the minutia of public behavior has encouraged authorities to use them to address a host of low-level regulatory matters. In the UK, for example, local authorities have used cameras that were legally authorized to counter terrorism to regulate such prosaic misdeeds as people putting their garbage out on the wrong day, not cleaning up after their dog, urinating in public, littering, delivering newspapers without a license, smoking under-age, posting flyers and driving in an anti-social manner.

Policing under surveillance

The police are often referred to as a "low-visibility" profession, one where officers work outside of the limelight of public scrutiny and away from the direct oversight of supervisors. It is clear, however, that this image has been inaccurate for some time. Officers are monitored by practices that operate both internally and externally to the police organizations.

Internally, the police are monitored in a range of different ways, from the polygraph tests that they must often take as part of the recruitment process, medical testing and regular re-certification for firearms proficiency. The day-to-day police work of line officers is also scrutinized in detail by supervisors to ensure that they adhere to regulations pertaining to the bureaucratic formatting and dissemination of police-generated information—something that can entail intensive and extensive forms of oversight

(Ericson and Haggerty 1997). Officers are also policed by internal units specializing in investigating police wrongdoing. While questions remain about the efficacy of such internal investigations, officers are always cognisant that their actions might be scrutinized by such units. Occasionally, internal affairs will go to considerable lengths to detect police wrongdoing, as was the case in New York where officials sought to test the integrity of their officers by hiding illegal drugs where police officers would find them and also reporting fictitious instances of drug dealing to test whether officers would respond appropriately.

In a society characterized by a greater prevalence of monitoring devices the police also increasingly find themselves scrutinized by citizens and external institutions. Sometimes this involves instances where inappropriate police actions have been captured by cameras designed by contrast to catch criminals or protect officers, such as those installed in holding cells or on police vehicles. Internationally, officers also find that they are now routinely filmed at public protests, with both sides of any confrontation recording the encounter. On a day-to-day basis, the increasing ubiquity of camera-equipped cellular telephones means that citizens commonly have their actions photographed or recorded. Usually this occurs haphazardly but it can also be a conscious policy of groups concerned about police violence, such as "cop watch" organizations who seek out and record police behavior.

This increasing prevalence of policing in front of the camera poses a host of challenges for the police. For example, it can elevate non-routine and perhaps unrepresentative encounters to the status of highly symbolic political events. This, in turn, makes it increasingly difficult for the police to control the stories that they tell about their actions and ultimately reduces their relative power (Goldsmith 2010). In the process, the issue of "spin control" becomes ever more important for the police, who must be increasingly attuned to how to advance their preferred interpretations of often unflattering or disturbing videos of police behavior. So, surveillance technologies are not only used by the police, but are increasingly directed at police officers by different constituencies, changing the day-to-day practices of policing while increasing the risk of scandal.

Conclusion

The police have long been agents of surveillance, and the consequences of their monitoring are particularly significant given the high value we place on security but also because of how police actions can fundamentally alter an individual's life course or serve to cumulatively marginalize certain populations.

The expansion of new surveillance options is fundamentally altering what it means to do police work, with officers becoming ever more focused on collecting and analyzing reams of data and using assorted surveillance devices that range from DNA to license-plate readers to in-car cameras to wiretaps. None of these developments, however, necessarily works in a seamless fashion. There are always hiccups and localized forms of resistance and failure when new police surveillance measures are introduced. This is particularly apparent in relation to the ongoing calls for the police to share intelligence with other security organizations. As has long been known, the police are eager to collect information and acquire data collected by others, but they are much more reticent about divulging their own data. Questions also remain about the police's ability to effectively manage and use the surveillance data that is now available to them.

We appear to be in the midst of a major recalibration in the public's fears of police surveillance, with citizens and politicians alike being more willing to empower the police with surveillance and dismiss lingering anxieties about the inherently repressive potential of such practices. It remains to be seen how this transformation will shape the scope and operation of police surveillance into the future.

Note

Special thanks to Ariane Ellerbrok for her extensive comments on this chapter and to my co-editors Kirstie Ball and David Lyon for their valuable feedback.

References

Cohen, Stanley. (1985). *Visions of Social Control: Crime Punishment and Classification*, Cambridge: Polity.

Cole, Simon A. (2001). *Suspect Identities: A History of Fingerprinting and Criminal Identification*, Cambridge, MA: Harvard University Press.

Coleman, Roy and McCahill, Mike. (2011). *Surveillance and Crime*, London: Sage.

Ericson, Richard V. and Haggerty, Kevin D. (1997). *Policing the Risk Society*, Toronto: University of Toronto Press and Oxford: Oxford University Press.

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

Goffman, Alice. (2009). "On the Run: Wanted Men in a Philadelphia Ghetto," *American Sociological Review*, 74: 339–57.

Goldsmith, Andrew. (2010). "Policing's New Visibility," *British Journal of Criminology*, 50: 914–34.

Haggerty, Kevin D. and Ericson, Richard V. (2001). "The Military Technostructures of Policing," in *Militarizing the American Criminal Justice System: The Changing Roles of the Armed Forces and the Police*, edited by P. Kraska, Boston, MA: Northeastern University Press.

Marx, Gary T. (1988). *Undercover: Police Surveillance in America*, Berkeley: University of California Press.

Natapoff, Alexandra. (2009). *Snitching: Criminal Informants and the Erosion of American Justice*, New York: New York University Press.

Nelkin, Dorothy and Andrews, Lori. (1999). "DNA Identification and Surveillance Creep," *Sociology of Health and Illness*, 21(5): 689–706.