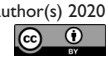
Article

Theoretical Criminology
1–20



DOI: 10.1177/1362480620967020
journals.sagepub.com/home/tcr
SAGE

Surveillance arbitration in the era of digital policing

Peter Fussey
University of Essex, UK

Ajay Sandhu
Ryerson University, Canada

Abstract

This article analyses adoptions of innovative technology into police surveillance activities. Extending the nascent body of empirical research on digital policing, the article draws on qualitative interview data of operational police uses of advanced surveillance technologies. Separate illustrative examples are drawn from social media intelligence gathering, digital forensics and covert online child sexual exploitation investigations. Here, surveillance governance mechanisms, often authored in the 'pre-digital' era, are deemed ill-fitting to the possibilities brought by new technologies. This generates new spaces of interpretation, where regulatory frameworks become renegotiated and reinterpreted, a process defined here as 'surveillance arbitration'. These deliberations are resolved in myriad ways, including perceived licence for extended surveillance and, conversely, more cautious approaches motivated by perceived exposure to regulatory sanction.

Keywords

Governance, policing, regulation, surveillance, technology

Introduction

Paralleling their growing presence in contemporary society, digital surveillance technologies increasingly occupy a central role in police practice. Innovations receiving particular public attention include advances in predictive policing, enhanced online

Corresponding author:
Peter Fussey, Department of Sociology, University of Essex, Wivenhoe Park, Colchester, CO4 3SQ, UK.
Email: pfussey@essex.ac.uk

surveillance and portable digital police hardware among others. With this rapid growth, however, comes a potential 'regulatory lag' where the pace of emerging surveillance possibilities outstrips the capacity for regulators to provide meaningful oversight. This article focuses on these interstitial spaces: between accelerated surveillance possibility and the more ponderous emergence of regulatory controls. It is here that new police subjectivities, inference and discretion are argued to gain growing influence in shaping how digital surveillance technologies are used and how regulatory governance is enacted. As its core theme this article examines how digital policing involves a continual reinterpretation of regulations authored in the 'pre-digital age' to hitherto unanticipated cutting-edge technologies and their attendant possibilities.

Given the importance of police discretion in the operation of surveillance technology (inter alia Bijker et al., 2012) and its rules of deployment, and building on insights from a long tradition of police ethnographies, it is crucial that studies of digital police surveillance engage with the situated operational environments. Moreover, social science analyses of technology have long recognized the vital importance of the social and organizational conditions that shape, and are shaped by, such innovations (e.g. Latour, 1987). Taking these insights as a cue, this article empirically examines how police officers implicated in surveillance activities interpret and negotiate the legal and other regulatory regimes in the emergent landscape of digital policing. To make sense of these complex interactions this article is organized over six main areas of discussion.

The article first examines key literatures to situate the analysis. Here, discussion of the nascent field of digital policing is companioned by attention to germane aspects of more established literatures on technological surveillance and related police practices. The article then examines these surveillance practices within rapidly shifting legal and regulatory environments, the contours of which are understood unevenly by practitioners, as our later analysis demonstrates. The article then sets out the methodological approach governing the research. Key findings covering the complex ways officers engage with regulatory frameworks during digital surveillance activities are then presented in section four. These findings are subdivided into three areas of discussion. The first identifies and analyses new spaces of interpretation generated by adoptions of advanced technology into police practices. This engenders a milieu where surveillance actors continually negotiate their roles relating to the affordances of such technologies and perceptions of ill-fitting regulatory environments. These complex negotiations are defined as 'surveillance arbitration'. The outcome and resolution of such negotiations are captured in two antagonistic approaches: some participants resist the constraints of regulation while others are highly sensitized to rights-based implications and tread with greater caution. These categories of responses are discussed respectively in the following two subsections. Each position is revealed as highly nuanced, varied and ultimately mediated through subjective negotiations. Discourses of technological surveillance, so often cast into binary frames ('nothing to fear, nothing to hide', 'privacy versus security', 'utopian or dystopian' and so on), attain more complex expression among those engaged in its operation. The article concludes with conceptual clarification of the 'surveillance arbitration' processes among law enforcement professionals.

Digital policing and the surveillance society

Modernity is consistently identified as a catalysing agent in the long history of surveillance in human societies (inter alia Hintz et al., 2018; Sennett, 1990). The period saw the coercive potential of surveillance heighten as the visibility of suspects and offenders increased, developments captured particularly prominently in the criminological imagination through Lombroso's use of photographic representation, Bertillon's standardization of 'mug shots' in 1888 and, later and entirely separately, Foucault's (1977) panoptic metaphor for micro-level articulations of disciplinary power. Despite their standing in criminological commentary, however, such landmarks appear anachronistic in the midst of today's digital data rich society. Growing availability of digital technology, partially fuelled by accelerated globalization and the cheapening of consumer electronics, not only drove the ubiquity of surveillance, but also radically altered its operation, reconfiguring the relationships and proximities between subjects and observers (Virilio, 1994).

While surveillance practices have a long history, scholarship over the last 30 years has pointed to its increasing centrality in police work (Ericson and Haggerty, 1997; Marx, 1988). Surveillance techniques have also become progressively technological in character. Perhaps most familiar has been the proliferation of surveillance cameras across Britain's public spaces during the 1990s. While ubiquitous to the point of 'banality' (Goold et al., 2013) and largely operated by local municipalities, these public cameras offered new capabilities to observe the minutia of everyday life in search of crime and disorder (Norris and Armstrong, 1999). Advances in miniaturization, processing and storage capacity, and gains in optical quality have brought multiple variations to this iconic symbol of surveillance. Innovations include the spread of video analytic techniques—such as the use of facial recognition algorithms (Fussey and Murray, 2019)—and the adoption of vehicular, wearable and mobile cameras (Ariel et al., 2015).

Despite the prominence and heavy symbolism of visual surveillance measures, it is important to contextualize such practices with two observations: police uses of surveillance extend visual images and include text based, numerical and biometric data (Higgs, 2011), sometimes characterized as 'dataveillance' (Clarke, 1988). Additionally, as discussed below, police uses of technology extend beyond the pursuit of surveillance.

The proliferation of digital traces and data richness brought by the growth of 'information capitalism' (Thrift, 2005), ubiquitous computing, 'digital citizenship' (Isin and Ruppert, 2015) and, more latterly, 'surveillance capitalism' (Zuboff, 2019), has been consistently thought of as transformational and has brought new possibilities to data-focused surveillance practices. Notable among these are the online mass surveillance activities, as revealed by Edward Snowden in June 2013, measures that stimulated rapid legislative activity (see later). Recent years have also seen the digital 'data revolution' (Kitchin, 2014) extend to mainstream policing and security practice. Indeed, the importance given to the intelligence potential of big data can be seen in the USA with the CIA's establishment of its first new directorate for half a century, the Directorate for Digital Innovation.

In England and Wales an attempt to order the uneven and sometimes patchy adoption of digital technology across 43 devolved police forces has resulted in an emerging national strategy for digital policing. This is articulated most clearly in the National

Police Chief's Council's (NPCC) attempt to produce a long-term strategy in 2016, the *Policing Vision 2025* project (NPCC, 2016), recently updated in *The National Policing Digital Strategy 2020–2030* (NPCC, 2020). While uses of digital technology are varied, the overall strategic approach is framed through three national schemes. 'Digital Public Contact' focuses on digital communications between police and public. 'Digital First' aspires to integrate police and Criminal Justice System activities, such as case file and evidence handling. Finally, and most germane to the focus of this article, 'Digital Intelligence and Investigation' (DII) is concerned with police uses of technology to detect and disrupt crime as well as gain greater situational awareness for intelligence gathering purposes.

Most criminological commentary on digital (and digitized) policing has focused on this latter area of DII. Such technologies hold a double attraction for criminologists: one of novelty and one of resonance with longstanding criminological preoccupations with futurity, anticipation, pre-emption and risk (e.g. Feeley and Simon, 1992; McCulloch and Wilson, 2016). While critical attention has extensively focused on activities such as online surveillance (Lyon, 2015; Murray and Fussey, 2019), portable police hardware (Sandhu, 2019) and other instruments, these twin concerns—police technologies and futurity—have converged most explicitly in the emerging literature on predictive policing (e.g. Aradau and Blanke, 2016; Maguire, 2018).

Such accounts offer important contributions to longstanding criminological concerns of selective police action, categorical suspicion and ecological bias, and provide a valuable digital nuancing of these concepts. While the emergent literature on digital policing plays a vital role in illuminating a complex and highly dynamic terrain, notwithstanding notable exceptions (inter alia Brayne, 2017; Ferguson, 2017; Maguire, 2018) a large amount of this commentary has not been informed by empirical analysis (Brayne and Christin, 2020; Koper and Lum, 2019). As Brayne (2017: 977, emphasis in original) articulates,

> The use of big data in police surveillance activities is the subject of contentious debate in policy, media, legal, regulatory and academic circles. However, discourse on the topic is largely speculative, focusing on the *possibilities*, good and bad, of new forms of data-based surveillance. The technological capacities for surveillance far outpace empirical research on the new data landscape. Consequently, we actually know very little about how big data is used in surveillance activities.

This tendency towards distanced discussion holds significant ontological implications. It risks under-acknowledging the indispensable role individuals and their settings play in influencing how technology becomes applied and the impact it has. It also risks masking how those same individuals and settings are themselves conditioned by the affordances of such technologies. Additionally, accounts that do not engage with these operational settings not only invite the criticism of being speculative, as Brayne contends, they risk attributing excessive deterministic agency to such technology, as sequential generations of scholarship on the philosophy of science have warned (e.g. Callon et al., 2009; Latour, 2005).

This article aims to contribute to the small and growing collection of empirically informed work on the operational uses of advanced digital policing applications.

However, we contend that, while the problem of insufficient empirical insight holds true for studies of digital data-enabled policing, it is important not to discard the many important and relevant contributions offered by longstanding sociologies of policing and surveillance. Empirical studies that explore how police mediate operational cultures and frameworks, and those that consider the 'negotiated, contested, messy and affective character of supervisory labour' (Smith, 2014: 22) of surveillance offer significant insights for the study of newly digitized policing practices.

Particularly important are ethnographies of camera surveillance, particularly those conducted around the turn of the millennium, that highlight how the introduction of technology creates new subjectivities and discretionary practices. Among these, Goold (2004) revealed wide variations in surveillance practices between police and civilian users of the same surveillance infrastructure in Britain and, crucially, the considerable subjectivities at play in determining who becomes targeted by the cameras. A touchstone in the field, Norris and Armstrong's (1999) ethnography of surveillance camera operators further interrogated how new technologies interact with traditional constructions of suspicion culminating in the reproduction of racial bias through video surveillance practices. McCahill's (2002) study of urban surveillance revealed further influences on surveillance operators' decisions to target individuals, which included the affective states of ennui, apathy and active prejudice. Such analyses challenge the excessive determinism regularly assigned to technological surveillance and, crucially for this article, reveal how technologically mediated environments create new arenas for human discretion.

One area of policing research particularly instructive for the analysis of transformations in digital policing is that addressing the related field of covert policing. Here, Marx's (1988) foundational study detailed intersections between technology, suspicion and covert tactics, revealing the reassertion of 'categorical suspicion' through these practices. More recently, Loftus' (2019) ethnography traced the transition of covert policing from a once niche area of law enforcement to it becoming a 'normalized' activity, where such tactics shifted from last to first resort within investigations. The implications of this mainstreaming of covert policing are manifold and, with a trajectory similar to the rise of digital policing, informative. For example, divisions between intrusive and non-intrusive surveillance and between overt and covert approaches—already poorly delineated in law—become progressively opaque. Additionally, covert settings lead officers to increasingly prize 'becoming invisible' (Loftus et al., 2016), a dislocation aligning with a wider shift towards 'abstract policing' (Terpstra et al., 2019) in some jurisdictions. Like covert policing tactics, advanced digital techniques operate at a distance and away from public scrutiny, creating new asymmetries of surveillance.

Drawing on these insights this article argues that, when operating in such novel and less visible roles, officers implicated in digital policing practices play a crucial role in mediating and shaping applications of technology. This agential role of individuals in shaping the uses and boundaries of these digital tools not only provides an important counterpoint to technological determinism, it also resonates with the longstanding scholarship on police discretion.

Emerging as a key concern within the sociology of policing during the 1960s and 1970s, studies of police decision making emphasized the selective application of police powers, notably via influences exerted by cultural and other organizational frames (Manning, 1978)

among others. Further contributions highlighted subjective formulations of decision making and charted their manifestation across distinct areas of policework. Sites of discretion included the selection of investigative tools, formulations of suspicion and establishment of operational procedures (e.g. Goldstein, 1977). Important for this article is the role of legislation and regulation in facilitating, structuring and, conversely, fettering discretion. Indeed, Kenneth Culp Davis' (1971: 4) foundational definition of police discretion points to *boundary limits on police powers*, yet it is fundamentally important to recognize the role of legislation in generating *new latitude for police discretion* to flourish.

Overall, this article contends that police uses of advanced digital surveillance technology have generated several arenas of negotiation which include deliberations over the possibilities and permissible limits of such tools. Regarding the latter, this article examines how accelerated adoption of digital technology engenders new procedural ambiguities, where poorly fitting 'pre-digital' regulations and statutes themselves become extra-procedurally renegotiated and reinterpreted in the context of digital operations. What is at stake, therefore, are not only technological uncertainties, but managerial and bureaucratic ones too.

Regulating innovation

Digital policing operates within a shifting regulatory terrain. As this article argues, surveillance practitioners navigate these regulatory landscapes in varied ways. To contextualize these changes, this section reviews relevant legislative and regulatory landmarks, and considers pertinent socio-legal analysis of how such interventions have impacted in parallel police surveillance activities.

Surveillance practices are largely governed by a blend of legislation, case law and 'softer' regulatory levers. Regarding the former, domestic legislation, police surveillance is governed by a range of statutory mechanisms. Particularly important among these are the Human Rights Act 1998 (HRA), Regulation of Investigatory Powers Act 2000 (RIPA), Protection of Freedoms Act 2012, Investigatory Powers Act 2016 (IPA) and Data Protection Act 2018. While it is beyond the scope and focus of this article to explore each in depth, it is useful to rehearse a number of key features germane to the digital policing regulatory landscape.

Particularly important for digital surveillance practices is RIPA and the institution of the IPA, a replacement for key provisions of Part I of RIPA and authored in the wake of Edward Snowden's 2013 revelations of state sponsored mass surveillance in the UK and the USA. RIPA and the IPA govern the authorization of surveillance warrants and set out procedures for managing directed, intrusive and covert surveillance practices. RIPA gained assent very shortly after the Human Rights Act 1998 became law in the UK and established a legal basis to oversee the engagement of citizens' rights (particularly 'Article 8' privacy rights) during intrusive state surveillance activities. Relevant provisions include the establishment of a surveillance authorization regime and the requirement to evidence necessity and, by extension, proportionality calculations in advance of warrants being issued. RIPA has garnered many controversies. These include its overzealous disproportionate application by local authorities for minor infractions, such as littering and dog fouling, and its inability to govern excessive surveillance activities of some state agencies, as revealed by Snowden.

For the purposes of this article, further shortcomings of RIPA include ambiguity over boundaries between intrusive and non-intrusive surveillance and how the recent ubiquity of digital data challenges longstanding notions of proportionality.

Socio-legal research has critiqued the institution of RIPA into police practice. Notably, empirical studies have highlighted widespread misunderstandings over RIPA procedures by its users. Particularly prone are conflations of necessity and legitimacy and, separately, risks and rights (Bullock and Johnson, 2012; Harfield and Harfield, 2018). Moreover, scope exists to classify invasive surveillance measures as non-intrusive, and thus not requiring authorization, with little scrutiny over this designation (Fussey and Murray, 2019). Critics have also argued that RIPA compliance is consistently gestural and symbolic, operating as a bureaucratic process that enables officers to repackage existing activities without any meaningful engagement with fundamental rights issues. Such accounts see RIPA—and its 'parent', the HRA—as, 'allowing officers to justify their decision making' amid a legitimating discourse of rights, thus providing 'a safety net in the event that they are asked to account for their actions' (Bullock and Johnson, 2012: 632). Human rights considerations thus become relegated to matters of procedure rather than operating as foundational principles. Discourses of ethics and rights become highly performative in such settings. Reflecting Manning's (2003) recognition of how self-indemnification prevails in US policing cultures, UK studies have noted the utility of RIPA in servicing a police '"cover your arse" mentality' (Loftus et al., 2016: 641). As such, while the purported operationalization of human rights through instruments such as RIPA are often characterized as obstructing 'real' police work, in reality they *enable and extend* surveillance by conferring a sense of legitimacy and indemnity to such practices (Bullock and Johnson, 2012; Loftus, 2019; Loftus et al., 2016).

One of the most intriguing recent legislative developments affecting the use of digital surveillance in the UK has been the 2018 Data Protection Act, an instrument that implemented (and, after Brexit, replaces) the EU General Data Protection Regulation into UK law. This legislation makes specific reference to the role of police discretion, stipulating 'significant' human intervention within algorithmic and other automated decision making. However, given its recency, and a commensurate absence of relevant case law, what is meant by a 'significant' intervention remains open to interpretation.

These intersections between regulatory frameworks, police discretion and the possibilities brought by new technologies raise important questions over how digital surveillance practices are conducted. Building on these insights this article explores a further dimension of surveillance activity in the era of digital policing. Here, it is argued, new possibilities brought by advanced digital surveillance technologies allow users to additionally question the applicability of existing regulatory frameworks. These deliberations occur in new sites of reflexivity, where regulation and statute themselves become renegotiated and reinterpreted. This article empirically analyses how technological capability and regulatory structures are negotiated in the crucible of operational policing practice.

Methodology

Research was conducted through qualitative semi-structured interviews with 57 participants involved in digital surveillance practices within four major UK police forces.

Surveillance practices included the collecting, storing, analysing and application of digital data in addition to more familiar surveillance tasks of monitoring specific subjects and spaces. Interviews were conducted between January 2017 and March 2019 and supplemented by sustained engagement with participants' operational cultures and settings. Research questions addressed the following issues: the kinds of data collection and surveillance practices conducted; the incorporation of technology into diverse surveillance tasks; how regulatory frameworks are understood and mediated; meanings ascribed to regulatory instruments; and how such interpretations relate to practice.

Multiple strategies were deployed to gain access and recruit participants. Cultivating trust was central to this endeavour and extensive negotiations were crucial, both in terms of relationship development and for understanding how police organizations considered these issues at senior levels. Strategically placed gatekeepers were initially identified and engaged, and a snowball sampling method adopted to recruit further participants. Two of the researched force areas shared significant parts of their digital capability and police leaders were keen to understand the adoption of technology through their organizations. Offering to communicate high-level findings back to these individuals proved useful for the researchers when identifying key individuals and in cultivating trust and acceptance in these organizations. No editorial intervention was offered by or requested of the authors.

Sustained engagement and accumulated trust enabled opportunities to deploy in-field strategies such as requests for documentation and follow-up interviews for clarification. Moreover, these interactions led to invitations to attend meetings, police planning discussions, strategy events and professional conferences, where further recruitment and data collection took place while allowing researchers to identify and approach individuals holding digital police leadership roles. These contexts constitute a meeting point for negotiations on digital capabilities, operational practice and regulatory constraints. Several further interviews were conducted with experts on the use and regulation of surveillance technology across wider security fields. These included a former head of GCHQ and members of Edward Snowden's legal team in the USA.

While fieldwork emphasized frontline operational surveillance officers involved in collecting and managing data for intelligence and evidential purposes it also engaged individuals responsible for the design of policy and strategic implementation of surveillance technologies. Among those occupying more recognizable investigation roles, interviews included members of digital forensic units who analyse confiscated computer equipment, open source intelligence units who collect social media and social network data, and general intelligence units collecting and managing data from external parties such as social services organizations and internet service providers. The individual value-laden and subjective experience of participants, combined with the way that the structures designed to frame their professional activities became reinterpreted, signifies the interpretivist character of the research. Analysing subjectivity and interpreting responses of those operating within varied and ambiguous techno-regulatory spaces yielded data that were complex and convoluted. Notes and audio recordings were transcribed and coded following each interview using computer software. In accordance with the wider project's research ethics commitments, no participants, organizations or indirect identifiers are offered unless anonymity was explicitly waived.

Findings

The data are heuristically grouped around three core discussions. First, the data reveal how digital innovation generates new spaces of interpretation for surveillance practitioners. A response among many participants was one of disorientation and an attempt to find meaning amid an ambiguous setting. This provides a counter to notions of technological inevitability. Moreover, the act of interpreting and negotiating these ambiguities stimulated new activities, explored in the following sections. For some, perceived regulatory ambiguity was interpreted permissively as licence to extend surveillance activities into new domains. Conversely, other surveillance practitioners adopted a more cautious tone. Variously motivated by (self) indemnification or (selfless) ethical concerns, among other reasons, regulatory ambiguity encouraged these officers to be more restricted in their use of advanced digital surveillance practices.

Spaces of interpretation and surveillance arbitration

Echoing a view frequently encountered in other police research, most participants were critical of existing regulatory frameworks, particularly those focused on upholding citizens' privacy rights. Overwhelmingly convinced of the policing benefits of surveillance technologies, a view reinforced by the dividend of convenience, participants repeatedly expressed concerns over the perceived regulatory constraints imposed on their work. However, the complexities and uncertainties brought by novel technologies, and the increasingly specialized nature of digitally focused policing adds further nuance to these narratives of resistance.

In particular, admissions of confusion were common and candid. These vagaries manifested in several ways and included new uncertainties over the appropriate boundaries for separating intrusive and non-intrusive surveillance, and between overt and covert practices. Relatedly, one Chief Inspector and lead of several digital innovation projects expressed exasperation over limited understandings of privacy across his force area, despite repeated training. Reluctant to search inwardly for the source of confusion, blame was placed externally on the perceived ambiguous formulation of regulatory processes. Notable here is the ontological search for objective certainty. Such certainties are arguably unachievable and run counter to the intentions underpinning much surveillance law. By contrast, formal surveillance authorizations are usually formulated on a more procedural basis, whereby measures are selected for particular operations and judged permissible depending on a series of tests, such as legal basis, legitimate aim, necessity, proportionality, collateral intrusion and so on.

In a variation of this theme, one participant responsible for investigating internet-enabled crime suggested that limited understandings among officers invited them to (illegally) 'look up the system while off duty to check their hillbilly neighbours' or 'people who are "of interest"'. Such accounts suggest that 'excessive surveillance' may not result from the vagueness of regulatory frameworks, but a more limited understanding of the law among individuals undertaking surveillance practices. As digital surveillance tools become increasingly instituted into everyday policing, a tendency potentially following the mainstreaming of covert strategies identified by Loftus (2019) and others, these perceived uncertainties and resultant uneven and intrusive practices are set to grow.

Dilemmas also arose because innovative technologies created new surveillance possibilities unaddressed by existing regulatory provision. Here, a detailed, rather than deficient, understanding of such regulations was key to revealing these ambiguities. A common lament here concerned the outdatedness of legislation used to conduct surveillance activities. Among these were the RIPA, the standard tool for authorizing directed surveillance, and the Police and Criminal Evidence Act 1984, the framework for public–police street encounters. Both were authored in comparatively pre-digital times. At face value it could be argued that these criticisms overlook the subsequent iterative refinement of both mechanisms and, also, the influence of case law. However, further examination of the specifics of operational practice reveal further tensions between the adoption of advanced technologies into policing and the 'pre-digital' regulations that govern it. Three separate illustrative examples of this tension are offered here, drawn from the digital policing practices of social media intelligence gathering, digital forensics practices and covert online child sexual exploitation investigations.

Taking these in turn, members of one police social media monitoring unit drew clear distinctions between the clarity of rules concerning directed surveillance in wholly offline settings and their relevance for online contexts, 'if someone launches a covert operation, say watching a suspect's house, the rules are pretty clear, if you're repeatedly checking their social media, it's more of judgement call'. While substantive guidance has been developed to grade the level of intrusion when monitoring social media data,[1] boundaries over when activities adopt features of covert operations—requiring more stringent authorization and oversight—hold a significant degree of interpretation. Added to this is the 'service' function provided by many police social media monitoring units, functioning to process requests for material from detectives assigned to a specific case. These arrangements often mean adjudication over the level of collateral intrusion. As one participant occupying a similar role stated, 'detectives will often ask for *all* the data on a suspect and their networks'. Because social media activity largely involves interpersonal connection with others, such requests generate necessary deliberations over the degree of information to offer on non-suspects. Elaborating this point through reference to social media intelligence tradecraft, the same participant explained, 'one approach is to draw on lists of friends and associates to confirm a subject's identity and behaviour, but don't pass the full lists back to the requesting officer'.

These activities confer a 'surveillance arbitration' role onto social media intelligence operatives as they perform tasks of gatekeeping and filtering data flows. Moreover, while much scholarship on the harms of surveillance is rightly focused on the rights of surveilled subjects, these incidences demonstrate heightened collateral intrusion, or 'surveillance collateral' (Murray and Fussey, 2019: 47), on non-targets in digital surveillance operations. Underscoring a central theme, these surveillance arbitrators consider their activities to exist in a regulatory lacuna, a vacuum created in the slipstream of accelerated digital innovation: 'It would be fantastic if we had case law to guide our decisions. As long as it's not me that gets done of course! [laughs].' The humour in this response also reveals an enduring theme repeated throughout the data: ambiguities over regulation heightened surveillance officers' sensitivities to legal exposure, a theme explored in additional detail below.

Officers from another area of digital policing, digital forensics, identified similar regulatory gaps and how these also became mediated through new forms of surveillance

arbitration. A repeated complaint concerned the outmoded standards governing the evidential use of forensic material. The main national operating standard for forensic science, ISO17025, was repeatedly cited as focused on more traditional 'offline' physical forensic material, 'the standard is geared to wet forensics [blood, saliva, DNA, etc.] and we can't operate without it . . . We are beholden to it but it does not provide a close fit to digital forensics.' The preservation of evidential fidelity differs between physical and digital forms of forensic material, particularly when it comes to moving evidence from one place to another. DNA samples are hermetically sealed, hard-drives are cloned. Also notable are different interpretations of pre-digital standards to new technological capabilities. For the social media intelligence units discussed above this difference was burdensome, for these digital forensics operatives, it was seen in a more positive light, 'it gives us space to develop our own approach'. Thus, even in this comparatively focused area of work—the extraction of evidence from seized electronic equipment—considerable spaces of discretion exist. Participants reported the need to make constant individual decisions over what was permissible to access. For example, several participants described making judgements when searching email logs to assess whether communications with other individuals were part of client–lawyer dialogue, and therefore subject to restrictions over legal privilege. Others reported practical and jurisdictional ambiguities in accessing messaging stored on (US owned) cloud-based systems, and the need to continually operate in an agile and ad hoc manner.

Ambiguities also surfaced in a third area of digital police work: online child sexual abuse investigations. In this field of covert policing digital technology alters the temporalities of suspect group infiltration. As one officer explained, traditional practices of covert infiltration were hugely time consuming. A covert officer was required to spend significant time and effort to gain access to criminal conspiracies, and the approach usually required painstaking incremental engagement with suspects. One benefit of this measured pace was the opportunity for supervisory authorization of likely next steps in an investigation. By contrast, participants reported how infiltration processes became greatly accelerated in the online world. One participant explained how, for the online-based conspiracies in his caseload, reflective time becomes compressed and decisions often needed to be made instantly. This created problems for written authorizations to define the permissible boundaries of an investigation in advance, and subject them to tests of necessity and proportionality. While authorizations for 'offline' covert operations can develop incrementally as investigations evolve, this option is not always available for faster online operations. To allow undercover officers scope to make decisions in real-time authorizations for covert online investigations therefore necessarily requires greater emphasis on the projected, and potentially speculative, eventualities. To accommodate diverse eventualities, warrants become more likely to request in advance more intrusive, and possibly disproportionate, measures than potentially necessary.

Critical theoretical studies of criminology and surveillance have long exercised on issues of futurity. These enquires have followed a diverse range of concerns but largely cohere around how risk-based and actuarial approaches have been utilized as a means of ordering the social world, articulating diverse modalities of power (e.g. Rose et al., 2006) and anticipating future offending. Yet the activities identified above reveal a further nuancing of these processes. Well-documented practices of categorizing, actuarializing

and managing the future cumulatively aspire to *narrow* ambiguity by making it knowable and actionable. The digital practices outlined here, however, point to an additional principle at play, one that *dilates, accommodates and embraces* uncertainty.

These future-oriented surveillance authorizations involve inferences that recognize many potential outcomes. These approaches are also hewn into a specific form of reasoning: an informed speculation, a logic of abduction. As Lury (2009 cited in Ruppert, 2012: 121) explains, abductive regimes of precaution such as these are predicated on 'neither induction nor deduction . . . [a]nd abduction does not involve even metaphors or tools—but speculative reason or reasonable guesses'.

Moreover, this form of precaution, replete with 'reasonable inferences' and 'informed guesses', becomes a staging post for many other conditions of possibility that invite further action. It constitutes the acceptance of an 'arraying of possibilities such that they can be acted upon', as Amoore (2014: 23) puts it. Rather than standard forms of probability to constrict and 'tame chance in the landscape of fear' (Ericson and Haggerty, 1997: 450), such digital practices *embrace* uncertainties.

These spaces of surveillance arbitration also invite subjective responses. These reactions are varied yet loosely captured here in two antagonistic heuristics. In the first, surveillance actors viewed perceived regulatory gaps as licence to extend their activities. Others adopted a more cautious approach. Particularly notable here is officers' unease over their perceived exposure to regulatory sanction. This in turn motivated a tendency for practitioners to self-regulate and restrict their own surveillance work.

Ambiguity and digitally enabled permissibility

Many participants saw significant operational potential in new surveillance technology, and interpreted regulatory ambiguity as licence to extend their activities. One example of this interpretation was offered by an officer specializing in collecting data from suspects' social media accounts. Amid repeated criticism of what he considered excessive constraints of legislation, this officer confidently outlined a strategy for gathering as much data as he deemed necessary to prevent crime, 'My concerns about a suspect's privacy are quite minimal. My job is to investigate, not to worry about privacy. I will happily gather whatever I bloody well can. I am in favour of gathering as much as I can.' This ideal of unrestricted surveillance was repeated by several research participants, some of whom argued that there was 'no reason' officers should be limited from collecting information given their duty was to protect the public. Complaints over their inability to match the data harvesting capabilities of US technology giants Google Alphabet, Amazon and Facebook were common, as was the failure to account for differences in consent issues and the coercive capabilities of the police compared to corporations. While both RIPA and the IPA institute clear processes for authorization and review of intrusive, covert and directed surveillance practices, the abundance of social media data makes possible a more ambiguous category of surveillance, one that is not easily separated into directed/non-directed and covert/overt binaries. These digitally enabled surveillance opportunities do not fit easily into prior regulatory frameworks and, in turn, allow surveillance practitioners to re-evaluate such instruments in more limited terms.

Sensitized to potential objections over their views, participants sharing this 'permissive' view regularly offered exaggerated characterizations of their opponents. Particularly prominent were constructions of straw men civil libertarians promulgating tired Orwellian tropes. Perceived comparisons to repressive state actors were dismissed by participants as naive and uninformed. Among these participants, one commonly cited, if tautological, safeguard against unethical practice was a normative belief in surveillance officers' inherent honesty and ethical orientation. Relatedly, one member of a force cybercrime unit deployed the Manichean and highly performative (Maguire and Fussey, 2016) language of 'good' against 'bad', to legitimate extra-procedural requests for communications data that could be deemed unethical and potentially illegal:

> I am an honest cop, so I should be able to access data. I should be able to call up companies and get data on anyone if I have a legitimate reason . . . It's ridiculous! I have to go through all the bureaucracy and wait months before I can get data . . . It is hugely frustrating. I am an honest cop and I just want to catch the baddies! Privacy is a block to that. I can't see the big deal.

Here, recourse to subjective ethical codes *and* a more general, utilitarian, 'public good' are judged sufficient grounds for licentious surveillance practices and dismissal of legal safeguards. Such justifications hold multiple implications. Particularly prominent is the instrumental and ironic way personal 'ethics' are used as justification that unethical extra-procedural practices are somehow ethical.

These appeals to a higher purpose, the maintenance of public safety over the protection of citizens' rights, build on a theme identified in other policing research. In their analysis of police responses to the Human Rights Act 1998, for example, Bullock and Johnson (2012: 637) identify common misunderstandings of differences between risk and rights and a 'consistently conflated necessity with legitimacy'. The former fails to acknowledge the circumstances and safeguards governing rights interferences in specific circumstances, while the latter merges two separate elements of the standard three-part human rights test. Such tendencies are apparent in this digital policing context alongside a further misconstruction: here proportionality becomes characterized in terms of achieving policing aims rather than addressing the degree of rights interference.

Extra-procedural uses of digital surveillance tools manifest in other respects. This included negotiation of evidence rules in criminal trials. As one member of a digital forensics unit stated,

> I would break every rule if I could get the data I needed to earn a conviction or, quote, 'seek justice' [laughs]. Because I don't want to go to court and then fail to get a conviction just because I didn't check something. I'd rather put him away.

This sentiment provides an interesting counterpoint to recent legal challenges against digital evidence handling by UK police forces. For example, in *R v Allan* 2017 London's Metropolitan Police Service were criticized for supplying insufficient digital information 'which could reasonably be considered capable of undermining the prosecution case or of assisting the case for the accused' (Crown Prosecution Service, 2018: 2), a requirement under Director of Public Prosecution rules on charging suspects. Yet the above

quote and the fallout from *R v Allan* both reveal how the abundance of digital data, and the infeasibility of submitting its totality to the courts, necessarily means material for investigations and prosecutions becomes selectively sampled.

Uncertainties over how regulations apply to novel digital settings also generate potential for extra-procedural practices. As one senior officer engaged in tackling organized crime in his region stated, 'amateur sleuths [among my unit] doing detective work on social media at home are the bane of my life'. This practice was reflected elsewhere. For example, the head of a gang unit in another part of the country described ICT-savvy peers using their personal computers to trawl suspects' Facebook accounts. Adopting a similar affective vocabulary to that above, this officer labelled these colleagues 'ethical hackers' because, while 'needing to ignore privacy policies' (and potentially operating outside the law), their work was ultimately contributing to the goal of policing gangs. With further apparent disregard for the legislative basis regulating targeted surveillance activities (e.g. RIPA), this officer described such surveillance as 'off the record', comparing it to an off-duty detective following a suspected criminal.

A related and common claim was that rapacious information gathering practices became ethical and rights respecting by virtue of the inability of police to analyse such quantities of data. As one cybercrime investigator explained, 'Yeah, we might have people's data, but bugger me, we don't have the time to look at it all', a position that inevitably raises questions over the necessity of these surveillance measures. Justifications that digital surveillance was rate limited by the capacity of humans to assess the data were present for other forms of surveillance. As one officer holding a senior national counterterrorism role articulated,

> almost all bulk data is never used, it is not sifted through nor analysed. It just sits there unexamined. This is something that's lost in the political discussion . . . Surveillance is expensive and resource intensive. So that limits the intrusion naturally.

Yet the frequency with which such opinions are rehearsed does not erase the successful legal challenges to these activities in UK and European courts. Moreover, these sentiments were not shared by all in senior positions, as a former head of GCHQ explained, 'privacy rights of [suspects] are engaged from the very moment an intelligence agency or police service contemplates an operation to access their data'.

Caution and indemnification

Ambiguities brought by digital policing technologies and varied understandings of their regulatory environments stimulated additional and oppositional responses. Here, surveillance officers expressed significantly greater caution. This wariness was motivated by multiple concerns. While often dressed in the language of rights and ethics, deeper analysis reveals how such concerns often shrouded more instrumental motivations. These included questions over the operational benefits and anxieties over vulnerability to legal sanction. These are discussed in turn.

Regarding efficacy, one common concern emphasized the consequences of collecting excessive data. For example, one social media analyst noted that some peers' permissive

approach to surveillance work generated 'chatter' constituting excessive data and little guidance concerning their relevance. This marked an interesting tension between separated roles of data collection and data analysis, the latter of which regularly involved re-considering privacy issues anew for the same data sets.

Exemplifying this line of thought, one police intelligence unit data analyst claimed that most frontline police officers tended to naively ask surveillance officers to collect and analyse 'any and all' information they could access. Echoing a familiar objection to data collection habits of signals intelligence agencies, this participant used the imagery of a growing data 'haystack' further submerging the 'needle' of useful information. Similarly, one experienced detective superintendent criticized colleagues for their approach, 'because it's available to them, some detectives just think, "let's get some open source [data]" when they start their investigation without saying what they want'. A police digital investigations team leader offered the same criticism, 'if we were searching a home, we don't rip up the bloody floorboards and take them. We are looking for specific things and take only those. I don't know why we think we can take everything from a phone.' A colleague from the same unit doubted motivations for large-scale data consumption were 'malicious'. Rather, she claimed that many officers were not aware of operational consequences from their 'collect it all' mentality, 'often, we'll get detectives asking us for all social media data on a suspect. I'd ask, "what, all of it?", and you'd be amazed how often they reply with "yes" without any understanding of what they're asking for.' Appetites for online communications data thus outstrip surveillance officers' ability to effectively digest it. Such exchanges challenge common claims over the efficiencies of digital surveillance. As this same participant relayed, overwhelmed intelligence units would then have to engage in protracted negotiations with investigators to narrow down and agree which information should be analysed.

These accounts reveal a key element of thinking among these more cautious approaches to digital surveillance. While many criticized the 'collect it all mentality' of their more 'permissive' peers, this was often steeped in concerns over the practical difficulties brought by abundances of data. Consequently, it would be mistaken to describe these more cautiously inclined participants as necessarily more rights-conscious. Rather, these participants expressed similar criticisms of regulatory structures designed to uphold citizens' rights. For example, descriptions of regulatory structures as 'minefields' and 'overly bureaucratic' were common. These lamentations over inconvenient regulation overlook the fundamental basis for human rights focused interventions and oversight: the restriction on arbitrary interference by the state. As Edward Snowden's lawyer expressed in an on-the-record interview for this research, 'the whole point of democracy is to prevent states doing whatever they like, points of friction are essential for surveillance practices'. Overall, what distinguishes the 'cautious' from the 'permissive' participants discussed above are largely instrumental concerns over the effectiveness of unregulated surveillance.

Other surveillance officers adopting this more cautious line were apparently motivated by self-indemnification. For example, one member of a cybercrime unit outlined a 'play it safe' culture, suggesting that peers rarely pushed the boundaries of privacy laws:

> it is not RIPA that holds us back, it's the internal issues. We are risk averse. We don't push policy enough and we don't have case law to guide us. We have plenty of ways to get people's data, but we are too afraid to do it.

Expressing this common sentiment, another member of the unit criticized peers adopting a rigid interpretation of regulations as too 'nervous' to engage in 'perfectly legal' surveillance work. Similar views were expressed by those in comparable roles in a different constabulary, with one officer responsible for investigating online offences viewing what he saw as unregulated surveillance intrusions as 'justifiable' and that more cautious officers 'don't do this out of fear'.

These views were reflected among officers engaged in more traditional forms of policing. Here, one detective inspector specializing in investigating drugs and burglary argued that some surveillance officers become reluctant to tell peers about the data they can collect:

> we want [to] gather data on who has been where, what they did, and use it to track people . . . But people are reluctant to tell us what we could do because they want to be careful . . . People might find out. We might be criticized.

Self-indemnification is a powerful shaper of behaviour and drives ethical practices more than concerns over fairness. Invoking an anatomical imagery familiar to policing researchers, this issue was illustrated by officers in a digital forensics unit:

> requests [from officers for digital searches] always have two components: their suspicions and the reasons why they've carried out a particular request. The section justifying actions is always far more substantial and complete than the requests for specific information. They're 'arse covering'.

Such self-indemnification demonstrates how this enduring theme of police culture (Loftus et al., 2016; Manning, 2003) is reproduced in the digital age. Overall, these accounts demonstrate how rights and ethics concerns are regularly deployed to perform the dual tasks of avoiding analysing excessive quantities of data and, separately, reducing risks of exposure for wrongdoing.

Conclusions: Surveillance arbiters in the digital age

The introduction of technological policing tools amid a regulatory environment developed in a largely pre-digital era has created new uncertainties for surveillance operators. Early scholarship on police discretion and later analyses of how supervisory frameworks become instituted into policing both identify that, while regulatory ordinances are perceived by police as restrictive, they generate spaces for discretion to flourish. These circumstances bring many outcomes, including the paradoxical extension of intrusive practices by legitimizing and indemnifying applications for covert and asymmetric surveillance.

This article has identified how the context of digital policing brings a further dynamic to these processes. Specifically, because digital capability outpaces the more ponderous development of regulatory governance, surveillance operators become implicated in continuous evaluations over the applicability of such frameworks. Additional to the gestural compliance and legitimation of extended surveillance

activities correctly identified in other studies, digital policing constitutes a reflexive milieu where regulation and statute themselves become renegotiated and reinterpreted in a more fundamental sense.

In some senses, this might be expected, given that the era of 'digital memory' (Mayer-Schönberger, 2011) has only recently begun. Yet the practices identified here represent a tension, one that stretches the connection between technology and its regulatory frameworks: a digital anomie whereby the capability expectations of technology are seen to outpace the regulatory means governing its use. These processes confer a 'surveillance arbitration' role onto surveillance operatives as they interpret regulatory environments, mediate institutional goals and adapt their surveillance practices accordingly. In essence, they become key interlocutors positioned at crucial junctures within networks of surveillance governance. These are the spaces where surveillance arbitration takes place.

Those practising digital surveillance navigate these interpretative spaces through myriad subjective and affective approaches. These include a professed vulnerability to rights-focused legal sanction as well as concerns over the efficacy of these surveillance instruments. Contrasting this was a belief that these digital tools offer significant surveillance possibilities and could be used licentiously. This belief consistently incorporated disregard of what were seen as rights and ethics-based 'obstacles' to effective police work. Occasionally accompanied by a crusading rhetoric, such sentiments further underscored the performative qualities of security work. Audiences for this 'crime fighting' discourse ranged from a wider and undefined 'general public' to the interior domain of self-justification.

The activities identified above invite a further nuancing of our understanding of the role of technology in policing. Complementary scholarship in criminology and surveillance studies have accurately documented the growing role of technology to categorize, capture and frame the future, with the ultimate aim of managing risk. In doing so, technologies weight and ascribe probability with the aim of *narrowing* ambiguity, by making it knowable and governable. The digital practices outlined here, however, point to an additional principle at play, one that *dilates, embraces and accommodates* uncertainty. Marking a subtle shift in the politics of temporality, these future-oriented actions do not necessarily reduce uncertainty but infer myriad potentialities and outcomes. In doing so, there is a certain irony where measures and techniques to bring certainty to police practices generate new ambiguities that invite negotiation and, ultimately, arbitration.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship and/or publication of this article: This work was funded by the UK Economic and Social Research Council (ESRC) for the project Human Rights, Big Data and Technology [ES/M010236/1].

ORCID iDs

Peter Fussey https://orcid.org/0000-0002-1374-7133

Ajay Sandhu https://orcid.org/0000-0003-4154-308X

Note

1. Police in England and Wales operate a national 'open source data model' that categorizes types of data and officer access to it into one of five categories. The mid-point of this categorization roughly demarcates a general threshold between overt and covert activity.

References

Amoore L (2014) *The Politics of Possibility: Risk and Security beyond Probability*. Durham, NC: Duke University Press.

Aradau C and Blanke T (2016) Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory* 20(3): 373–391.

Ariel B, Farrar W and Sutherland A (2015) The effect of police body-worn cameras on use of force and citizens' complaints against the police: A randomized controlled trial. *Journal of Quantitative Criminology* 31(3): 509–535.

Bijker W, Hughes T, Pinch T, et al. (2012) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press.

Brayne S (2017) Big data surveillance: The case of policing. *American Sociological Review* 82(5): 977–1008.

Brayne S and Christin A (2020) Technologies of crime prediction: The reception of algorithms in policing and criminal courts. *Social Problems*. Epub ahead of print 5 March 2020. DOI: https://doi.org/10.1093/socpro/spaa004.

Bullock K and Johnson P (2012) The impact of the Human Rights Act on the Police Service in England and Wales. *British Journal of Criminology* 52(3): 630–650.

Callon M, Lascoumes P and Barthe Y (2009) *Acting in an Uncertain World: An Essay on Technical Democracy*. Cambridge, MA: MIT Press.

Clarke R (1988) Information technology and dataveillance. *Communications of the ACM* 31(5): 498–512.

Crown Prosecution Service (2018) A joint review of the disclosure process in the case of *R v Allan*: Findings and recommendations for the Metropolitan Police Service and CPS London. Available at: https://www.cps.gov.uk/sites/default/files/documents/publications/joint-review-disclosure-Allan.pdf.

Davis K (1971) *Discretionary Justice: A Preliminary Inquiry*. Baton Rouge, LA: Louisiana State University Press.

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

Feeley M and Simon J (1992) The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology* 30(4): 449–474.

Ferguson A (2017) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.

Foucault M (1977) Discipline and Punish: The Birth of the Prison. London: Penguin.

Fussey P and Murray D (2019) *Independent report on the London Metropolitan Police Service's trial of live facial recognition technology*. Colchester: Essex Human Rights Centre.

Goldstein H (1977) Categorizing and structuring discretion. In: Goldstein H (ed.) *Policing a Free Society*. Pensacola, FL: Ballinger.

Goold B (2004) *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*. Oxford: Oxford University Press.

Goold B, Loader I and Thumala A (2013) The banality of security: The curious case of surveillance cameras. *British Journal of Criminology* 53(6): 977–996.

Harfield C and Harfield K (2018) *Covert Investigation*. Oxford: Oxford University Press.

Higgs E (2011) *Identifying the English: A History of Personal Identification 1500 to the Present*. London: Bloomsbury.

Hintz A, Dencik L and Wahl-Jorgensen K (2018) *Digital Citizenship in a Datafied Society*. Cambridge: Polity.

Isin E and Ruppert E (2015) *Being Digital Citizens*. London: Rowman & Littlefield.

Kitchin R (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. London: SAGE.

Koper C and Lum C (2019) The limits of police technology. In: Weisburd D and Braga A (eds) *Police Innovation: Contrasting Perspectives*. Cambridge: Cambridge University Press.

Latour B (1987) *Science in Action: How to Follow Scientists and Engineers through Society*. Cambridge, MA: Harvard University Press.

Latour B (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. New York: Oxford University Press.

Loftus B (2019) Normalizing covert surveillance: The subterranean world of policing. *British Journal of Sociology* 70(5): 2070–2091.

Loftus B, Goold B and Mac Giollabhui S (2016) From a visible spectacle to an invisible presence: The working culture of covert policing. *British Journal of Criminology* 56(4): 629–645.

Lyon D (2015) *Surveillance after Snowden*. Cambridge: Polity.

McCahill M (2002) *The Surveillance Web: The Rise of Visual Surveillance in an English City*. Cullompton: Willan.

McCulloch J and Wilson D (2016) *Pre-Crime: Pre-Emption, Precaution and the Future*. London: Routledge.

Maguire M (2018) Policing future crimes. In: Maguire M, Rao U and Zurawski N (eds) *Bodies as Evidence: Security, Knowledge and Power*. Durham, NC: Duke University Press.

Maguire M and Fussey P (2016) Sensing evil: Counterterrorism, techno-science, and the cultural reproduction of security. *Focaal: Journal of Global and Historical Anthropology* 75: 31–44.

Manning P (1978) Rules, colleagues and situationally justified actions. In: Manning P and Van Maanen J (eds) *Policing: A View from the Streets*. New York: Random House.

Manning P (2003) *Policing Contingencies*. Chicago, IL: Chicago University Press.

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

Mayer-Schönberger V (2011) *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

Murray D and Fussey P (2019) Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data. *Israel Law Review* 52(1): 31–60.

Norris C and Armstrong G (1999) The Maximum Surveillance Society. Oxford: Berg.

NPCC (2016) *Policing Vision 2025*. London: NPCC.

NPCC (2020) *The National Policing Digital Strategy 2020–2030*. London: NPCC.

Rose N, O'Malley P and Valverde M (2006) Governmentality. *Annual Review of Law and Society* 2: 83–104.

Ruppert E (2012) The governmental topologies of database devices. *Theory, Culture and Society* 29(4–5): 116–136.

Sandhu A (2019) 'I'm glad that was on camera': A case study of police officers' perceptions of cameras. *Policing and Society* 29(2): 223–235.

Sennett R (1990) *The Conscience of the Eye: The Design and Social Life of Cities*. New York: WW Norton.

Smith G (2014) *Opening the Black Box: The Work of Watching*. London: Routledge.

Terpstra J, Fyfe N and Salet R (2019) The abstract police: A conceptual exploration of unintended changes of police organisations. *The Police Journal: Theory, Practice and Principles* 92(4): 339–359.

Thrift N (2005) *Knowing Capitalism*. London: SAGE.

Virilio P (1994) *The Vision Machine*. Bloomington, IN: University of Indiana Press.
Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Author biographies

Peter Fussey is a professor of Sociology at the University of Essex.

Ajay Sandhu holds a doctorate in Sociology and specializes in the study of Crime and Technology.