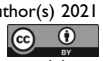
Original Research Article

International Journal of
Police Science
& Management

Technological innovation in policing and crime prevention: Practitioner perspectives from London

International Journal of
Police Science & Management
2022, Vol. 24(2) 190–209



DOI: 10.1177/14613557211064053
journals.sagepub.com/home/psm


Julian Laufs and Hervé Borrion
UCL Jill Dando Institute of Security and Crime Science, London, UK

Abstract
Digital technology now plays a critical role in policing and security management, with policing apps, drones and body-worn cameras potentially being game-changers. Adoption of such technologies is, however, not straightforward and depends upon the buy-in of senior management teams and users. This study examines what obstacles practitioners face in the procurement, deployment and use of crime prevention and detection technologies. The issue is explored through a number of expert interviews conducted with practitioners in London between August 2019 and March 2020. This work expands previous, more theoretical, literature on the topic by adding a practical perspective and advances the understanding of issues faced in innovation processes and their management. We identified a variety of issues and obstacles to technological innovation for policing. These include the deployment of new systems at the cost of old ones, lack of financial and political support, issues in public–private partnerships, and public acceptability. Although individual practitioners may have the expertise and willingness to unleash the full potential of surveillance and crime-reduction technologies, they are usually restrained by institutional rules or, in some cases, inefficiencies. In terms of the latter, this study especially highlights the negative impact of a lack of technical interoperability of different systems, missing inter- and intra-agency communication, and unclear guidelines and procedures.

Keywords
Technological innovation, expert interviews, police management, crime prevention, policing, technology management

Submitted 14 Sep 2021, Revise received 14 Sep 2021, accepted 15 Nov 2021

Introduction

Technology has become prevalent in most areas of society and, in a struggle to keep up with recent advances, public agencies are forced to innovate at an ever-increasing rate. The use of technology has, however, been an important part of police work, and technological innovation has gone hand-in-hand with the evolution of police practice (Borrion, 2018). Improving effectiveness and efficiency to keep up with growing demand while remaining within tight budgetary constraints is a core driver of this symbiotic relationship (Chan, 2001; Laufs et al., 2020b). Moreover, the 'entrepreneurial revolution' has increasingly left many organisations involved in policing internally scrutinised by management systems and internal audits and externally under the eye of 'watchdogs', public complaints systems and central auditors. Chan (2001) goes as far as to suggest that 'technology has redefined the value of communicative and technical resources, institutionalised accountability through built-in formats and procedures of reporting and restructured the daily routines of operational policing'. The effect of technological innovation on

Corresponding author:
Julian Laufs, UCL Jill Dando Institute of Security and Crime Science, 35 Tavistock Square, London WC1H 9EZ, UK.
Email: julian.laufs@ucl.ac.uk

organisations can vary depending on the nature and the design of the technology and the way in which change is managed. The impact of information technologies is considered to be especially substantial, because officers increasingly cannot complete their tasks without them (Chan, 2001). With additional challenges brought on by the COVID-19 pandemic, the overall dependence of the police on technological innovation to improve their operations increased manifold (Azoulay and Jones, 2020; Laufs and Waseem, 2020).

Today many police forces are more 'tech-savvy' than ever before (National Police Chief's Council, 2016). With industry standing ready to satisfy this appetite with crime analysis software, drones and body-worn cameras, among others, there is an increased use of technological products (Higgins, 2016; McQuade, 2001; Rogers and Scally, 2018). This development is not hard to understand because both crime and policing co-evolve with technology in what Ekblom (1999, 2005) has called an 'arms race'.

Because this is such an important issue for the future of policing and crime prevention, it is not surprising to see public and academic discussions on this topic. However, these are generally dominated by a focus on theoretical and philosophical aspects of technological innovation in the field. With an overwhelming focus on the implications for wider society, there is limited research approaching the topic from practitioners' perspectives and discussing the impact on those who actually use those technologies.

This article addresses this gap by examining the institutional realities of technological innovation in policing and public security. In doing so, it specifically focuses on the use of so-called surveillance-oriented security technologies (SOSTs), which refer to all technological solutions aimed at detecting or preventing crime by gathering data and monitoring citizens (Pavone and Esposti, 2012). Although not all new security technologies are surveillance-oriented, the term is still useful because a large proportion of technologies for crime prevention and detection include, or rely on, some form of monitoring or sensing component (Laufs et al., 2020a). The most commonly known form of a SOST is arguably closed-circuit television (CCTV), which is implemented widely across London and the UK (Dixon et al., 2003). As such, the innovation and deployment of new CCTV systems and the improvement of existing (and possibly more intrusive) systems are a key focus of this article. In addition, other technological solutions (both software and hardware) are considered that may support police in overcoming operational challenges in their day-to-day activities. Here, however, a special focus is placed on smart devices and those aimed at automating tasks.

Similar to many other police forces in the UK and around the world, police and crime prevention services in London have faced austerity and budget cuts over the past decade, with severe detrimental effects across almost all areas of activity (Brown, 2020; Greig-Midlane, 2019).

At the same time, London is at the forefront of digital transformation and modernisation, and on the path to becoming a 'smart city'. Briefly defined, this means any city that uses new information and communication technologies to improve the well-being of its citizens and make services more resource-efficient (Elmaghraby and Losavio, 2014). This also includes improvements to citizens' safety and security and, as such, by default, police and surveillance in the city (Laufs et al., 2020a). The 'smartification' of the city infrastructure and the rapid deployment of new technologies means that practitioners are confronted with new solutions and also new problems on a daily basis. A large part of this process are the aforementioned SOSTs and the deployment of technological solutions to tackle resource insufficiencies.

To explore practitioner perspectives and the practical issues encountered in the procurement and deployment of new SOSTs, a series of expert interviews were conducted with 20 London-based senior crime-reduction practitioners. Their views were elicited about the utility of smart and emerging digital technologies for crime prevention and detection, and specifically SOSTs. Further questions probed the obstacles that are most likely to impede effective procurement and operation. Specifically focused on a group of stakeholders underrepresented in the literature (D Liu et al., 2018), this study offers a glimpse into practitioners' perceptions of smart infrastructures. The findings contribute to a richer picture of SOSTs in smart cities and their future use, and inform the ongoing debates on their likely risks and benefits.

In the following, we discuss why technological innovation is necessary and how the debate on policing and surveillance is often one-sided. We then lay out the methodological foundations before identifying and discussing themes emerging from the interviews.

Background

Innovation and practitioner perspectives – beyond theoretical issues

The first important question to answer is why focusing on practical issues of the deployment of new SOSTs and especially practitioners' perspectives is important. Although discussing overarching and often philosophical issues of security versus privacy and questions of individual rights is crucial, it rarely provides direct insight into how new technologies are actually used on the ground, and therefore perhaps into the types of outcomes they can be expected to achieve. In many instances, the voices of those working in the field and using new technological solutions in their

daily work are not part of the discussion when examining issues of surveillance and crime prevention. As such, this article does not seek to discuss the broad issues where public discussion often invokes images of a surveillance state and 'big brother'. An example of this is the controversial issue of facial-recognition technologies for policing and security purposes. The heated discussion surrounding the deployment of facial recognition around a large multimodal transport hub in London (Sabbagh, 2019) and trials by London's Metropolitan Police Services between 2016 and 2020 are just the tip of the iceberg (Bradford et al., 2020; Fussey and Murray, 2019). Against this dystopian backcloth of public debate, academics have been assessing the societal impacts of smart technology and technological innovation in general, often framing them as conflicts between security and privacy or between public order and individual rights. In many instances, however, these discussions have neglected the fact that technological innovation can be instrumental in bridging the gaps between increasing demand for police services and decreasing public funding. In the past decades, for example, many organisations, including police forces across the world, have initiated a digital 'transformation' (ICT) in the hope of reducing operating expenses and improving service effectiveness, accountability and procedural regularity (Adams et al., 2009; Chan, 2001; Crow and Smykla, 2019; Ekblom, 2005; Laufs et al., 2020b; Lum et al., 2017; Weisburd and Braga, 2019).

This shows that technological innovation in policing and crime prevention is not an obscure scenario in the distant future, but rather a necessity that dictates routines and day-to-day activities for practitioners. Indeed, digitalisation and technological innovation play a key role in the Policing Vision 2025 published by the National Police Chief's Council (2016) and the Metropolitan Police Service (2017a, 2017b), which stresses that more must be done to exploit the operational benefits of advances in technology in coming years. This highlights that it is crucial to go beyond the broad philosophical discussions and to explore questions of practical realities in the deployment of new technologies for crime prevention and policing.

Privacy versus security – an outdated debate?

Public support for crime-reduction measures fluctuates over time and often as a result of critical events. Deployment of new surveillance technologies or the introduction of new surveillance powers, for example, often occur in the aftermath of tragedies or mass-casualty events, when the perceived need for increased security within the population is highest (Dinev et al., 2008; Thompson et al., 2020), or as a way to cope with otherwise scarce resources by means of automation (Joh, 2019; Leese, 2021; D Wilson, 2019). By contrast, public support is lowest after data leaks and surveillance scandals such as the Snowden revelations (Hintz and Dencik, 2016; Lischka, 2017; Murata et al., 2017).

As a result, the introduction of more technology-oriented security policies and increasingly intrusive SOSTs has provoked two main reactions in most countries, ranging from those who support increased surveillance in the name of (national) security and efficiency to those who argue that restrictions are undemocratic, unjustified or plain useless (Tsoukala, 2006). This dichotomy goes back to the age-old debate of security versus privacy. Often, this discussion is portrayed as a cost–benefit problem and as a trade-off where one has to choose between security improvements gained through better SOSTs or privacy (Pavone and Esposti, 2012; Pavone et al., 2016).

Several studies examine different angles of this trade-off discussion (Bowyer, 2004; Davis and Silver, 2004; Riley, 2007; Strickland and Hunt, 2005). Nevertheless, pitting privacy and security against each other, and viewing the debate as a zero-sum game, is far from uncontroversial (Pavone and Esposti, 2012). One important criticism of the framing is that it oversimplifies an otherwise highly complex discussion (Monahan, 2006; Tsoukala, 2006). At the same time, it deepens the divide between practitioners aiming to improve security and civil society organisations and citizens concerned about their privacy rights. Although both issues are important and should work in balance, the way the debate is framed has negative consequences for both sides.

In addition, it is questionable to what extent this debate applies today and whether it is still timely in its current form. As discussed before, both security and privacy are conceptually shifting. New SOSTs and smart capabilities growingly blur the lines between private and public, between volunteered and mandated data. With the rise of the age of data and information, the trade-off between security and privacy becomes increasingly blurry. Today, privacy of one's information and personal data also means security from at least some forms of crime in both the online and offline realms (Braun et al., 2018; Sen et al., 2013; van Heek et al., 2017).

Potential issues in the deployment of new technologies

This study discusses known issues that can substantially hinder or even stop the use of new technologies in an organisation. For enterprise risk assessment, the |ISO31000 (2018) standard distinguishes between internal factors (that pertain to the organisation) and external ones. In the following, we focus especially on internal factors because these were overwhelmingly identified by the participants.

This section not only provides background about the topic, but also lays out a reference frame for the subsequent analysis. The issues and themes discussed herein will guide the analysis and help to contextualise the experiences and information gathered from participants.

A key issue that may occur when deploying a new technology is the impact it can have on the working practices and the working culture within an organisation (Rogers and Scally, 2018). This goes especially for law enforcement environments, with often complex subcultures, as discussed by Reiner (2010). New technologies that promise to change the status quo of individual labour realities can be seen as threatening and potentially be rejected by workers (Eugene III, 2001; Hassell, 2006; Nhan, 2014). An example is the introduction of computer-aided dispatch in many US law enforcement agencies in the 1970s and 1980s (Rogers and Scally, 2018). The system was initially widely disliked because of the significant changes it brought to the way police operated. Although police agencies have made significant strides in changing attitudes towards new technologies, there might still be some concern, especially in light of the significant potential offered by smart applications and artificial intelligence (Bartsch, 2011).

Another pitfall that might occur when deploying new security technologies is the tendency to impose them on existing structures instead of taking more holistic approaches and ensuring they are integrated into existing systems and can be used to their full potential (Rogers and Scally, 2018). In addition, the use of new technologies in existing systems (both physical and organisational) can lead to the improper use of technologies because they are used to solve problems in the traditional way rather than innovate processes as a whole (Chan, 2001). This issue is especially hard to tackle in countries like the UK and the USA due to the decentralised and, to some extent, fragmented nature of the policing system. Although some constabularies might be frontrunners in deploying new technologies, many of the deployed smart technologies cannot live up to their full potential until inter- and intra-force structures change. This is especially the case in areas such as common databases or county lines where intelligence and information-exchange structures between forces often require common standards (Allen et al., 2008; Elliott-Davies et al., 2016; Grace, 2019; Newell, 2013).

In addition, a lack of training and experience can be a significant obstacle to the usability of new technologies (Chan, 2001; White and Escobar, 2008). Because urban, societal and demographic developments do not stop, adequate training is much needed for police to be successful in the future (Taylor et al., 2014).

Lastly, budgetary and legislative constraints in particular can have a negative effect on the attitude practitioners have towards the deployment and use of new security technologies (Rogers and Scally, 2018). Although to some extent, these constraints can be reasonable or even act as important safeguards, practitioners may feel as if they lack support from their superiors or the general legitimisation to employ new technologies (Kirmeyer and Dougherty, 1988).

Much research and also practical evaluations that integrate user focus and usability issues do not make the effort to identify practical user requirements and institutional restraints (Brell et al., 2018). Lack of understanding of practitioners' perspectives makes it difficult to improve the usability of new technologies, which in turn can hinder the work of security professionals (Werlinger et al., 2009). This is reiterated by Botta et al. (2007) and Werlinger et al. (2008), who argue that, in addition to human and organisational factors, technological factors can also have a major influence on professional performance.

Academically, these issues are rarely discussed in terms of security or policing work, especially not with regard to deployment and use of new technologies. This is problematic for two main reasons. First, police work can often set a precedent for organisations with strong and highly intricate group and social dynamics (Hirschmann and Christe-Zeyse, 2016; Ingram et al., 2018). Second, it is a field in which day-to-day operations can change significantly due to the use of new technologies (Chan, 2001). Thus, exploring the perspectives of security professionals with regard to the use of new technologies is an important topic that should have a more prominent place in the agenda of policing research.

Why expert interviews

The aim of this research was to gain insights into the planning, procurement and use of new security technologies for policing. Complementing studies that have analysed policy documents or measured the success or failure of outcomes, this work focuses on practitioners and the issues they face in day-to-day operations.

Furthermore, official record keeping, position papers or policy documents do not tell us much about the precise tactics and strategies of their deployment or capture more informal interactions and processes (Beyers et al., 2014). Another caveat of simple policy analysis lies in the fact that, in some instances, the official position of the organisation may differ from that of those directly working on the issue (Beyers et al., 2014).

Thus, to understand practitioners' perspectives, this study followed the method proposed by Brell et al. (2018). In their article, the authors carry out qualitative expert interviews to discuss possible use-cases of new technologies and identify the benefits and barriers of new traffic-monitoring technologies. Other authors such as

Beyers et al. (2014) discuss the rationale of interviewing as a data collection instrument in more detail and highlight the merits of it for the purpose of exploratory studies.

Experts can provide 'inside' information that is especially crucial when examining the reality of policy planning processes and day-to-day operations (Dorussen et al. 2005). As such, they bridge the gap between single in-depth case studies and large-N comparisons (Dorussen et al., 2005).

Method

Between August 2019 and March 2020 (pre-COVID), we conducted in-depth interviews with 20 practitioners involved in the deployment and use of new technologies for policing and public security in London. This section discusses how we selected the experts, the interview process and the steps taken to analyse the data.

Preparation, process and issues of validity

Semi-structured interviews were chosen as because they offer a balance between the issue-focus of structured surveys and the flexibility of open-ended questions (Dorussen et al., 2005). Interviews were conducted in situ to maximise the comfort of participants and minimise strain on their time (Werlinger et al., 2009). In addition, being on-site meant that participants were able to show the researchers what they were talking about and, in several instances, this allowed for the direct referral of further participants who were working at the same time.

Before the interviews, questions were formulated and clustered by theme (Appendix 1). The latter was done to hold participants' attention and obtain fully thought-out responses (Beyers et al., 2014; Schuman and Presser, 1996). In formulating the interview questions, we consciously avoided using academic language, jargon and leading or assumptive statements (Schwarz et al., 1999). Similarly, open questions were prioritised to allow stakeholders to freely express their views.

Recruitment and participants

Population boundaries were set using Christopoulos's (2009) seven-question checklist, and only officials and experts working directly with security technologies for public safety in crime prevention or detection in London were considered eligible for the study. The population of interest was not limited to police or those in enforcement capacities, but included those working with CCTV, e.g. councils and other public officials. Involving those working with CCTV was considered appropriate because it has become a mainstream crime prevention strategy in many countries around the world (Piza, 2018). It is especially prevalent in the UK, with an estimated over 4.2 million cameras across the country (Norris and McCahill, 2006; Piza et al., 2019) and more than half a million in London alone (Skogan, 2019; Webster, 2019).

To find participants, this study used the peer-esteem snowball technique (PEST) presented by Christopoulos (2009), which combines network analysis, snowball sampling and elite interview methods to confidently construct pseudo-representative samples of experts. Not only did this reduce the risk of selection bias, but it also helped to take into account network boundaries, provided an estimate of the population size and allowed for clustering of expert opinions on the basis of their nomination network. As such, applying the technique contributed to addressing known weaknesses of snowball sampling, including selection bias, population clustering and the difficulty in motivating expert participants, as discussed by Erickson (1979).

In an initial step, the researchers identified gatekeepers to the expert population (Christopoulos, 2009). Although PEST suggests using a number of unbiased informants, this was not applicable to our case because the pool was already restricted through the limited number of public institutions working in the field. In a second stage, participants were asked to provide further nominations in a series of snowball waves. The generic stages of PEST are outlined in Table 1.

Interviews with security professionals present several challenges (Botta et al., 2007; Kotulic and Clark, 2004). Practitioners often do not have time to participate, may not be willing to disclose sensitive information, and there is often no publicly available contact information (Werlinger et al., 2009). To overcome these challenges, this study leveraged professional connections of the researchers to find initial contacts.

Sampling dimensions included the participant's role within their organisation as well as their level of seniority (Bartsch, 2011). Table 2 gives an overview of the (anonymised) participants along with their affiliation and position within their organisation.

Participants were grouped according to their affiliation and professional role. Affiliations were either policing organisations or CCTV control rooms[1]. Professional roles included participants with management and planning duties, as well as officers who conducted day-to-day policing operations on the ground (e.g. patrolling) or generally those working directly with security technologies for crime detection and prevention in their day-to-day work. The exact affiliations of the participants (see also Table 2) could not be disclosed due to confidentiality reasons.

Interview protocol

In total, 20 experts were interviewed, varying from one to seven experts per organisation. Each interview lasted

Table 1. Generic stages of peer-esteem snowball technique (adapted from Christopoulos, 2009).

	1st stage	2nd stage	Subsequent stages	Final stage
Primary scope	Selection of seed nominators	Approach first-wave nominees	Approach all new nominees and non-respondents	Reach population saturation or significant sample size
Validity considerations in expert interviews	Estimate the degree of fragmentation of the population and include all sub-clusters of experts	Non-response bias. Authority of sponsoring organisation affects non-response. Centrality within the sub-clusters of nominated actors	Approach individuals who have not responded	Unlikely to reach saturation. Sampling may not sufficiently capture diversity of views. Not a good instrument for capturing dissent

between 30 and 60 minutes. This qualitative approach produced rich data that were subsequently analysed using a systematic approach (Halperin and Heath, 2017; Miles and Huberman, 1984).

Although the interviews did not ask for sensitive information per se, the first participants who were interviewed requested for their answers not to be recorded. As a result, the researchers followed the example by Chong (2008) and resorted to taking detailed notes and writing down specific quotes during the interviews. These notes were then transcribed and revised shortly after the interviews, as suggested by Beamer (2002). Upon completion, the interview notes were discussed with the interviewees to ensure accuracy and awareness of the interviewers' work (Bryman and Cassell, 2006).

Although this approach was not ideal and recordings would have provided a range of benefits[2], the researchers followed best practice from the literature. In fact, the literature suggests that such an approach delivers comparable results with regard to data quality to directly recorded interviews with few drawbacks (Rutakumwa et al., 2020).

Nevertheless, this also means an increased role for the researcher in the recording of the data, resulting in a need for increased sensitivity to the significance of the researcher for the research process (reflexivity) (Bryman and Cassell, 2006). In other words, the increased involvement of the researchers in the data collection and interpretation process (i.e. the taking of notes as opposed to simple recording) increases the implications of the researcher in the generated data (Bryman and Cassell, 2006). Defending such an approach, Rutakumwa et al. (2020) write that 'choosing not to use an audio recorder […] should not be viewed as a weakening of research conduct but rather as a successful indicator of the researchers' sensitivity to the integrity of the research project'.

Interviews were only conducted if participants provided informed consent to take part in the study as per UCL ethics regulations.

Table 2. Affiliation and role of participants. For confidentiality purposes, all participants are anonymised.

Affiliation	Senior leadership	Front-line practitioners
CCTV control rooms	3	3
Police	7	7

Coding and analysis method

To analyse the rich data, the detailed interview notes were synthesised, and common themes were identified (Huberman and Miles, 2002). The coding frame was not derived purely from the data themselves but rather previously defined research questions were used to shape the analytical lens (Halperin and Heath, 2017). This helped reduce the amount of data to be processed and allowed for more efficient extraction of the most important and meaningful parts. Setting a predefined coding frame allowed us to summarise patterns of similarities and variability better and identify differences between the different groups of participants. The study maintained enough flexibility to explore the explanations given by the participants in more depth (Glaser et al., 1968).

Responses were broken down into single statements that were then clustered around common concepts and themes. This was done iteratively within each interview, and related statements were then grouped together (Appleton, 1995; Bartsch, 2011). In addition, this study organised statements based on the participant's position within their organisation. This allowed us to determine whether responses to a single question differed between participants of different levels of seniority or affiliation.

The analysis followed the pattern of clustering answers within the following four categories: (a) what knowledge practitioners had about recent technological developments; (b) what benefits and issues experts could identify with regard to these new technologies (e.g. benefits to their

day-to-day work); (c) what obstacles they had met previously and were likely to face in the deployment and use of new security technologies; and (d) what they would emphasise in the design of new security technologies. In the following, each theme is discussed, and the responses pertaining to it analysed. The analysis also reports some of the comments that were discussed by only one or two experts but that the researchers found particularly useful in thinking about the use of new security technologies or generally representative of the consensus among experts.

Results

Presentation of the results is structured around the interview topics to allow a better overview and easier comparability when replicating this study in other settings. This section gives insights into not only the most important findings, but also the lack thereof in some of the categories. A contextualisation and evaluation of the importance of individual results along with the resulting implications follow in the subsequent discussion.

What knowledge did practitioners have about technological innovation in crime prevention and policing?

This first category of questions served to assess the participants' knowledge, categorise their responses to other questions and ensure that answers were given on the basis of a sufficient knowledge base (Halperin and Heath, 2017; Tourangeau and Smith, 1996). All but one participant showed knowledge about new security technologies and smart cities. The participant that did not show much knowledge in this area was retained because of their role within the Metropolitan Police Service. The concrete technologies mentioned ranged from smart streetlights to autonomous cars and parking, as well as the use of smart drone technology and urban surveillance:

> I know about smart streetlights and smart parking. (Police)

> It is happening increasingly. They recently started a smart city initiative in my area. (Police)

> As police, we need to go with the times. My smartphone has great capabilities, and I think we could really use better technology to improve police work. (Police)

All participants confirmed that they had acquired this knowledge in a work-related context, with one participant stating that they had to '[…] constantly evolve in order to stay ahead'. Participants were also able to describe situations in which they had previously encountered the deployment and use of new technologies. They were able to recount numerous examples from their professional and personal lives, and many were up to date with regard to new technological innovations and smart capabilities.

Differences between groups. Overall, answers were largely homogenous, with all participants showing knowledge of new security technologies and, at least to some extent, about smart cities. Despite the rather homogenous knowledge demonstrated by the participants, the specific technologies that each practitioner recounted depended heavily on their work. Although all participants were asked the same questions about their knowledge of new SOSTs and smart cities, their interpretation of these terms was highly subjective. No further explanation or clarification was given at first to avoid priming the participants. Whereas many CCTV operators described SOSTs, including the use of wireless mobile cameras, sound surveillance as well as smart street lighting systems, police officers described primarily wearable devices or new technologies for patrol vehicles:

> Mobile camera units can help us with watching new hot spots and to see whether we need permanent cameras. (CCTV)

> We could really use something like [smart] glasses that allow us to see an augmented version and information of the suspects. (Police)

> [We need] a mobile tracker to point us in the right direction when on foot. (Police)

This divide, however, was not only seen horizontally between participants from different organisations, but also was nuanced depending on the level of seniority within the same organisation. Whereas front-line participants and operators recounted practical interventions to help in day-to-day operations, participants who worked in management positions often interpreted the question to include technologies for personnel management and more efficiency-improvement tasks.

What benefits and issues did practitioners identify in interventions?

The second set of questions aimed to discuss which benefits and issues practitioners identified with regard to new security technologies and what impact this could have on their day-to-day operations. Two themes emerged from the stated benefits: efficiency and effectiveness. Besides these, practitioners described operational concerns, but did not mention issues of social acceptability or privacy risks to the same extent.

Benefits for efficiency. The first sub-theme of efficiency emphasised that the bottom line of all innovation should be to make police work more efficient and to reduce administrative and staffing work:

> Clocking in and out from a shift should be digital. Sometimes we start our shifts before, for example, if we come to help with an incident before clocking in. A digital system would make this much easier. (Police)

> Especially for managing staff and the organisation we need better digital systems. (Police)

Participants agreed almost unanimously that a key priority should be to reduce the time individual employees spend on non-crime-related tasks. All of the participants in the CCTV control rooms noted, for example, that they were often understaffed and faced a growing work load of requests from both public and private bodies. Although one might argue that most public bodies are always underfunded and short-staffed (Barnes and Henly, 2018; Vinod Kumar, 2014), interviewees were able to give very specific examples in which this became a security issue. One participant working in a CCTV control room noted that:

> [W]hile at high times four staff are on watch, this is often reduced to two. This means that [the control room] is often understaffed, and operators have to complete multiple tasks at once.

Conditions like these are problematic in terms of the occupational health of the operators (Laufs and Waseem, 2020) but are also a threat to public safety and crime prevention if there are too many incidents for operators to respond to (Rankin et al., 2012). This is a known problem and has been identified previously in the literature (Keval and Sasse, 2010). As a result, participants suggested that smart technologies would offer new avenues to cope with the work load and help optimise staff performance. In particular, they automatic video classification and person/video re-identification as promising tools for the future. Both technologies refer to the use of artificial intelligence to automatically classify the content of video data (Boukerche et al., 2017; Brezeale and Cook, 2008; Laufs et al., 2020a).

Another advantage that operators saw in technology was that maintenance and troubleshooting could be improved as most software issues could be fixed remotely and only required one call to the company running the system. This advantage, especially prevalent in cloud-based systems (Valentín et al., 2017), meant that lengthy repair processes could in many cases be foregone and issues of data storage and loss to a large extent ruled out.

Issues of interoperability. Participants stressed that the deployment of new technologies had downsides too:

> If we get a new system, it won't work with the existing ones. (CCTV)

> We got a new system to manage staffing and clocking in and out, but it did not work and was not as flexible as the way we did things before, so we stopped using it. (Police)

> We have a brand-new communication system, but we cannot use it because some of the other agencies are not on the same system. (CCTV)

The most common issue named by participants was that new and old systems were often incompatible. Many described day-to-day practices in which new systems did not match existing application programming interfaces (APIs) and thus were not usable. Participants reported that this slowed down their work significantly. Not only did software and integration issues make single tasks harder, but they contributed to a less productive and more tense work environment:

> Everyone got annoyed because we had to use the new system, but it took much longer than how we did things before. (Police)

Even the installation of new hardware elements such as cameras was not always straightforward. One CCTV operator recounted how the procurement of new cameras had been highly problematic because they were not compatible with the current software and that the procurement of new software was pricey and much discussed within the organisation. The participant lamented that there were no larger studies exploring the feasibility of new features or which software would be most sustainable in the future. Because the subscription to new software was too expensive, an interim solution was decided, and old cameras were integrated into the old system, which ultimately limited their functionality. Although the academic literature proposes some solutions to this problem, such as customisable plug-and-play solutions (Baldoni et al., 2017), they rarely reflect the realities of CCTV control rooms as bottlenecks of multi-agency collaboration. Proposals of single system architectures or platforms for smart interventions as proposed by de Diego et al. (2018) or Valentín et al. (2017) are thus often hard to set up under real conditions.

Compatibility issues are present even in the more modernised CCTV control rooms. In contrast to the first CCTV control room visited by the interviewer, the second had just undergone a complete refurbishment. The entire borough had been equipped with 70 new high-definition cameras, and additional smart technologies such as smart lampposts[3] had been rolled out. The security-relevant data

from all of these smart interventions converged in the control room, but despite the modernisation efforts, compatibility issues were still prevalent. Although the borough had updated all its systems, the aforementioned bottleneck meant that several other agencies, such as police and other emergency services, had communication channels to this control room. Here, the radio used to keep in touch with the police was older than the other systems and, as such, was not compatible. Although the new digital phone system was able to connect different stakeholders simultaneously and could log incidents automatically, the old radio system only worked one-to-one:

> A very annoying problem […] that despite the investments and modernisations we cannot use the new radios because they are not compatible with the ones the police give us. Now we can only wait till they get on the new system and even then, we won't know if it will be the same. (CCTV)

Similar issues were reported by participants who worked for the police, with some stating that the installation of new patrol car tracking systems had 'disturbed their routines' and 'cost lots of time'. As such, participants showed themselves generally open to the installation and usage of new technologies but were critical towards those that were meant to replace larger parts of the system or had too much of an impact on their daily operations. Although there was no general rejection of new technologies, some practitioners were disillusioned by the new systems that had been put in place. This issue is in itself not new as already two decades ago, Chan (2001) urged that technologies for policing must be compatible with those of other agencies.

Benefits for effectiveness. The focus of this study does not solely lie on CCTV. While those participants working immediately with CCTV (three) primarily described technologies to make their work more efficient, it was police officers who identified technologies with the aim of making crime prevention and detection more effective.

> It would be very useful to get something to find suspects and where they live faster. Maybe even see who lives at a certain address or whether they are there. (Police)

> It would be very useful to be able to see someone's criminal history before approaching them. (Police)

Those in management positions were very conscious of potential benefits for staff allocation and budgeting, whereas front-line participants focused primarily on how technologies could help them identify and apprehend offenders. Within the latter group, whereas CCTV operators placed a larger emphasis on analytical capabilities, police officers clearly highlighted communicative and mobility technologies. Participants stressed that currently, prevention programmes were not reaching the right people and that they would have to 'get in their channels' to make programmes more effective. In contrast to this, the question of whether this would affect personal liberties and the extent to which some suggestions could be considered invasive was not much discussed. This was partly because there were no established structures and that these issues would have to be discussed on a political rather than an operational level.

Issues of social acceptability. Although many of the technologies identified and discussed by the experts have undeniable benefits, issues of ethics and social acceptability were little discussed as potential drawbacks. This could be attributed to a range of reasons (e.g. practitioners' perspective on the issue or their perception that this was not a topic the interviewer wanted to hear from them), but it nevertheless brings up questions with regard to the ethical deployment and usage of these technologies. Most of the practitioners stated that although they were involved in procurement decisions, assessments of social acceptability and possible ethical drawbacks were not up to them. Instead, participants recalled how these issues were 'up to the politicians' (CCTV) and rather 'strategic and political decision' (police) instead of practical ones.

Only one expert, one of the control room managers, stated that the local council had considered 'systems with artificial intelligence and facial recognition software' but had been 'scared off by a possible backlash'. This indicates that issues of social acceptability can have a great impact on the acquisition process, with interventions deemed too risky not selected.

What institutional obstacles did practitioners face in deploying and using new security technologies?

Deployment at the cost of existing systems. One of the biggest obstacles that practitioners identified for the deployment and use of new technologies was that the practical impacts on their work were often not sufficiently considered in the procurement and deployment process:

> We had a system that worked well, but that was replaced. It would have been better to spend that money on something else. (Police)

> It made our work much harder because everyone had to get used to the new interface and the way it worked. It made it much more difficult. (CCTV)

Another example of this is the response from one practitioner about the redesign of a CCTV control room which was moved out of a building shared with the local police unit and into a third location in an effort to streamline police services and increase CCTV capabilities. This redesign of the control room was not discussed with operators or middle management, a fact that was heavily criticised by the participant:

> It made it much harder to communicate with the police because before, they were in the same building and would just come upstairs. Now we have to call them or email them, and it takes up much more time. (CCTV)

As a result of the move, operators had less contact with the police and more work with administrative processes (such as writing emails or phone calls) that would previously have been addressed in person. Although new software was bought to make work in the control room more efficient, it was quickly rendered useless as it was incompatible with other systems used in the control room and by other agencies.

Another participant reported that a new shift management system for the police station causing severe delays in people clocking in and out because it did not allow for the needed flexibility in working hours. Although both moves were meant to improve efficiency and lower the administrative work load within the organisations, they ultimately increased the amount of paperwork and labour needed to deal with problems.

This study suggests that these negative impacts and unintended consequences were, to a large extent, limited to the use of efficiency-oriented technologies, i.e. those aiming to reduce administrative work and increasing productivity.

Although most organisations may go through a transitional phase, the cases described by participants indicated more severe structural issues as unintended consequences (see also Chan, 2001; Patel et al., 2018). The current study also found a sharp discrepancy between the answers provided by front-line practitioners and those with management responsibilities. The latter emphasised the positive effect of new technologies in managing their workforce and accomplishing their job; the former often highlighted the negative impacts and unintended consequences of the deployment of new systems. Although this had to do with their respective roles, it showed at least some disconnect between managers and front-line participants.

Financial and political commitments. Within the police as well as the CCTV control rooms, managers showed a keen interest in deploying and using a variety of new technologies to enhance efficiency and effectiveness:

> We are already behind with digitalisation. We need to do better. (CCTV)

> There are not many projects where this is not discussed. It seems to be everywhere now, so we try to use it to make things better. (Police)

However, participants identified a lack of political commitment and financial support as significant obstacles, particularly with regard to the use of smart surveillance systems and more far-reaching and comprehensive approaches. One participant formulated his disagreement like this:

> [Politicians] don't want to put all of their eggs in one basket. They make small commitments rather than large ones that would bind them in the future.

This echoes the concern that several practitioners did not feel fully supported in their roles by their superiors and the institutions they worked for. In many cases, the use of new technologies was not governed by clear regulations. The resulting ambiguity led to frustrations amongst many practitioners.

Public–private partnerships. Practitioners identified the interaction with private partners such as private security companies, real estate developers and private land/building owners as potential obstacles. This was particularly the case in scenarios in which private entities limited the control of police or crime prevention and policing depended on their approval or cooperation:

> On one hand, we need to work with them, but they also can become a headache. (CCTV)

> There is a lack of communication between them and us, and they usually use their own systems instead of relying on us. (CCTV)

Participants working in the control rooms stated that rapidly constructed new developments in particular were increasingly becoming a problem for existing CCTV infrastructure. Newly planted trees obstructed cameras, and many new developments relied on private CCTV services that did not allow access to their cameras. This created more and more 'blind spots', which intensified issues such as person or vehicle re-identification. As a solution, the participant suggested that increased dialogue between developers and CCTV would be needed.

Issues with this regard were exclusive to participants working with CCTV and those remotely controlling surveillance technologies. They also mentioned that while the deployment of a new communication system with local security guards had been set up to reduce the work load of police, it had only increased the work load for control rooms where more and more lines of communication converged.

Social acceptability. Lastly, several practitioners identified either implicitly or explicitly social acceptability[4] and the public's trust as a limiting factor:

> We have to be careful what the public think we do with this. (Police)

> There is a lot of debate, and we want a system that works and not something controversial. (CCTV)

Participants from the newly renovated CCTV control room in particular mentioned that whereas more advanced surveillance technologies had been considered before the modernisation, only a few had ultimately been deployed. Practitioners in this control room stated that they:

> … had to reject a few [surveillance technologies] because of financial reasons. They were simply too expensive. […] we could not do most of them because people would not have liked it.

Participants from the police made similar suggestions, stating that public acceptability of the technologies would be a significant obstacle and that people would consider many interventions to be an invasion of privacy. However, none of the practitioners was able to provide specific metrics that were or could be used to evaluate how the public felt about a certain crime prevention or detection tool.

Even though some participants referred to public opinion surveys on facial recognition and other more advanced technologies (Bradford et al., 2020; Bromberget al., 2019; Fussey and Murray, 2019), they highlighted that there were no specific surveys for each individual case they referred to. This means that although social acceptability and the view of the general public can hinder or even fully stop the deployment and use of new crime prevention and detection tools, the threshold for this is often arbitrary and rarely follows an evidence base.

Discussion and recommendations

This article identified a variety of issues and obstacles to technological innovation for policing and the deployment of new SOSTs. These include the deployment of new systems at the cost of old ones, lack of financial and political support, issues in public–private partnerships, and public acceptability. The following discussion groups and contextualises these findings, highlighting the most important ones and laying out implications for further research as well as recommendations for improving innovation practice in the field of security and policing. The section first discusses the institutional and technological foundations needed for technological innovation before examining discrepancies and synergies between the academic debate and practice, especially with regard to issues of social acceptability and ethics.

Institutional and organisational requirements for successful innovation

The expert interviews conducted in this study indicate that there are two possible areas that need to be examined specifically when troubleshooting technological innovation in policing. These are institutional foundations and organisational support to enable practitioners to work effectively and technological coordination and interoperability.

With regard to the former, this research found that practitioners are often more open-minded and eager to increase technological innovation than initially assumed. If solely considering the general characterisation of security practitioners and police in the literature as usually not tech-savvy individuals, such a result would have been unexpected (Sheng et al., 2009; Werlinger et al., 2009). Many of these studies are, however, decades-old, and this research finds that those working with technologies today are often not only knowledgeable in their field, but also seem to keep up to date with trends and recent developments.

Nevertheless, there is a significant amount of scepticism, and many practitioners believe that technologies would make their work more difficult in some respects. Despite this, many interviewees suggested that they were in favour of increasing innovation and were actively bringing in ideas.

One important take-away message is that there is a lack of institutionalisation of technological innovation in policing. Strict hierarchies and inflexible structures create bottlenecks for innovation that make bottom-up innovation often impossible and can reduce the effectiveness of top-down innovation (Borins, 2002). Instead, efficient leadership and institutional structures that allow innovation are needed to enable both top-down and bottom-up initiatives. This includes political leadership that provides clear rules and regulations but does not interfere with day-to-day operations (Borins, 2002).

In several cases, participants felt that they did not have the support of their superiors for deploying or using smart technologies to the fullest. This disconnect may indicate an obstacle to effective change management (Campbell et al., 2003; Hirschmann and Christe-Zeyse, 2016). A lack of support from superiors can have several negative effects on the motivation of staff and the overall work environment (Kirmeyer and Dougherty, 1988). Insecurities felt in the (middle-) management of an organisation will inevitably translate to the lower ranks, and can severely hinder the widespread deployment and use of new technologies, and ultimately foster a general rejection of them, as described by McQuade (2001) or Chan (2001).

This creates a circle of problems that hinder innovation, especially as with limited budgets and increased public attention, political support and budgetary commitments come under increased scrutiny, and decision processes become longer (Abramovaite et al., 2018; Schmidt et al., 2015). As such, this project suggests that clear guidelines are needed that emphasise coherence in dealing with technologies and discourage managers from undermining organisation-wide initiatives directly or indirectly.

It is important to note here that throwing technology at the problem is not an answer, as studies such as the one by Garicano and Heaton (2010) find that the use of new technologies alone has neutral, and at worst detrimental, effects on police productivity, if not accompanied by appropriately flexible organisational and management practices. This is further supported by the findings of Mastrobuoni (2020) which suggest that the success of technological innovation depends largely on the surrounding institutional framework.

Change is often wanted by police forces and other agencies but rarely institutionalised. This is problematic because innovation (especially technological) does not bring about exclusively benefits, but also unexpected drawbacks. A lack of standardised processes and the capacity of practitioners to foresee them is therefore problematic (de Diego et al., 2018). Because public agencies are often not set up to follow the fast-paced, dynamic environment that technological innovation requires, many practitioners stated that they were faced with bureaucratic challenges in almost all of their actions, not only restricting their ability to do their job, but also negatively impacting their work morale. Front-line participants working for the police suggested, for example, that tools for demand prediction and management would be useful to streamline organisational structures and free up resources. Although demand is extremely difficult to predict, some tools exist to make or at least improve predictions (Borrion et al., 2020; Boulton et al., 2017; Davies and Bowers, 2019; Laufs et al., 2020b).

In many instances, practitioners voiced concerns about the chronic need for additional staff and resources. Although one might argue that a lack of funding is a common frustration, especially in public agencies, that does not necessarily advance the understanding of their view on the procurement and deployment of new SOSTs, this is not the case. A key aim of this article was to explore practitioner perspectives on technological innovation in their organisations and the priorities when procuring and deploying new SOSTs. The aforementioned frustrations with resources and financing were often mentioned and thus should not be discounted, but rather seen as an important part of the practitioner perspective.

Working conditions as described by some of the practitioners are problematic in terms of the occupational health of the operators (Laufs and Waseem, 2020) and can also constitute a threat to public safety and crime prevention if there are too many incidents for operators to respond to (Rankin et al., 2012). This is a known problem and has been identified in the literature previously (Keval and Sasse, 2010).

This, and the fact that budgetary and resource constraints were so often mentioned, highlights the need for new technologies to manage increasing work loads and more diverse ranges of tasks in times of austerity and shrinking resources. Particularly with even tighter budgetary constraints as a result of the COVID-19 pandemic, public agencies will need to embrace innovation to manage resource shortfalls and maintain effectiveness (Azoulay and Jones, 2020). Nevertheless, practitioners also saw potential in the use of new technologies to deal with resource shortages and staffing problems. This echoes the findings by JM Wilson and Weiss (2014), who examined how individual staffing and individual work load can affect policing operations.

Interoperability of systems and the way to smartness

In addition to the lack of support and institutional structures to enable effective work, practitioners also identified technological issues that were hindering progress. This included specifically the interoperability of systems both between those of different providers and between different agencies.

A common theme across all participants, regardless of their level of seniority or affiliation, was that new solutions should be compatible with existing systems or, as one participant put it: ‘new technologies should be fluid and should piggyback on what is already there’. This echoes the findings of several authors, such as Datta and Sarkar (2017) and Patel et al. (2018), who propose that, especially in a public context, systems compatibility should be prioritised. This issue is in itself not new because two decades ago, Chan (2001) urged that technologies for policing must be compatible with those of other agencies.

Although the academic literature proposes some solutions to this problem, such as customisable plug-and-play

solutions (Baldoni et al., 2017), they rarely reflect the realities of CCTV control rooms as bottlenecks of multi-agency collaboration. Proposals of single system architectures or platforms for smart interventions, as proposed by de Diego et al. (2018) or Valentín et al. (2017), are thus often hard to set up under real conditions.

This study recommends a more coordinated and collaborative approach to ensure interoperability and harmonisation of systems. This is especially important in the context of future smart cities, where the fragmented deployment of smart technologies can have significant impacts on their usefulness (Fernandez-Anez et al., 2018; Libbe, 2018). Chmutina and Bosher (2017) repeatedly emphasise the importance of a holistic approach to smart infrastructure, especially with regard to security. Even though the literature discusses this issue primarily with regard to achieving broad coverage of smart technologies across a city, the examples above give insights into the potential side effects on a micro-level (i.e. the effects of just one change to one office).

In addition, the results indicate that issues with private stakeholders lead to increased inefficiencies in the new systems, which echoes the findings of T Liu et al. (2020). Issues of public–private partnerships are not new (Cvrtila and Perešin, 2014; Purtova, 2018), but they are more relevant than ever in the context of smart cities, for instance, as future urban infrastructure is likely to be increasingly privatised (T Liu et al., 2020). Most models of the smart city rely heavily on the harmonious interplay of private and public agents and on the mutually beneficial use of each other's infrastructures (Ankitha et al., 2017; Choi and Na, 2017). To foster such a mutually beneficial relationship, we suggest an inclusive forum encouraging relevant stakeholders to take a more unified approach to crime prevention and the deployment of smart technologies in an area, as suggested by Borrion et al. (2019).

Ethical concerns and social acceptability

The findings also indicate a disconnect between practitioner needs and those issues dominating the public discourse on the matter. At the same time, however, ethical and normative debates are necessary to maintain a balance in the procurement and use of new SOSTs.

Although individual practitioners may have the expertise and willingness to deploy SOSTs to their full potential, they are usually restrained by institutional rules and regulations (or, in some cases, inefficiencies). Indeed, practitioners are bound by codes of practice and their actions are limited by laws and guidelines to ensure no actions are taken unlawfully (Germain et al., 2011). As such, this form of restraint is a crucial and reassuring element of a functioning security system in a liberal democracy. However, once legal and ethical requirements are satisfied, practitioners also face the issue of social acceptability when deploying new crime prevention and detection technologies. Because the evidence base on this is still insufficient and because many organisations rely on arbitrary thresholds, it is hard to overcome or even define the obstacle that social acceptability presents.

As a result, considerations of this nature are often only a minor and not institutionalised part of the SOST implementation processes. This may, of course, be attributed to the fact that procurement decisions and considerations of this nature are made by policy-makers rather than those operating or working with the technologies directly. Although this separation of those directly involved in the use of surveillance and those making procurement decisions is essential in a democratic society, it brings about several issues for both sides of the equation. Although most practitioners are likely proponents of the introduction of more advanced SOSTs rather than scrutinising ethical or acceptability concerns, limiting their involvement in the procurement decision to merely practical issues can be problematic. Ethical considerations and also those of social acceptability need to be made when examining the full picture rather than selective opinion snapshots. Here, further research is needed to explore the interplay between day-to-day practice and overarching ethical issues.

This is also highlighted by the before-mentioned concerns about resource constraints, which not only present practical obstacles to policing and surveillance, but also are an important part of the ethics debate. If the budgetary situation is too dire, practical needs may outweigh ethical concerns or those of social acceptability (Pavone and Esposti, 2012). At the same time, those deploying SOSTs might consider their use ethical and proportionate because they are in control and proportionality of surveillance is always relative (Macnish, 2014). This means that leaving ethical considerations up to non-governmental organisations and privacy rights groups, and operational concerns to practitioners pits these groups against each other in a struggle to win political favour either for or against deployment of a new system. At the same time, police rely on an ethical and socially acceptable deployment of new SOSTs because strong opposition to a new technology has the potential to harm police–community relations and trust in police (Bradford et al., 2020; Neyland, 2006). Thus, a better approach would be to engage with both groups and search for acceptable solutions that satisfy ethical standards just as much as operational needs. This echoes the findings of several previous studies, suggesting that more inclusive and nuanced approaches that highlight issues of function creep, data commercialisation, discrimination or privatisation of data are needed (Amoore, 2006; Côté-Boucher, 2008; Liberatore, 2007; Lodge, 2007; Spence, 2005).

Overall, a more distinct evaluation process is needed that includes various perspectives and leaves room to find a compromise. This article suggests that the gap between the practical needs of practitioners and socially acceptable and democratic solutions needs to be bridged by further research and active engagement of citizens by the government.

Limitations

Although expert interviews were considered the most appropriate design for this study, there are still some limitations. In theory, it would be useful to increase the sample size, but the pool of potential experts on this matter is very limited on a local or even national scale. As such, significantly increasing the sample size was not a feasible option in the case of this research.

Because not all experts are equally knowledgeable and may make mistakes, the data are admittedly, to some extent, more diverse and 'messy' than in other modes of research (Dorussen et al., 2005). This, and similar issues of (inter-) expert reliability are often not discussed extensively in much of the current literature, and it is crucial to at least acknowledge them (Dorussen et al., 2005; Halperin and Heath, 2017; Hooghe et al., 2010).

Other issues of validity could be disregarded altogether. Issues such as the time-lag between the interview and the topic or events in question were not relevant in this case because this study aimed to explore the professional opinion and experiences of stakeholders, factors that would likely not change significantly overnight (Beyers et al., 2014).

Future research questions

This research was useful to explore the practical concerns of practitioners about the procurement and deployment of new SOSTs and other smart technologies, however, it also brought up a range of new research topics that should be addressed in subsequent studies.

First, while our research suggests that the police as an institution are often too stiff for the growingly fast-paced technological developments, additional research is needed to understand exactly which institutional dynamics should be changed to increase flexibility and allow for better technological innovation in the police.

Second, future research should pick up findings regarding the arbitrary threshold for social acceptability and the lack of established procedures. This is needed because social acceptability is an essential prerequisite for the success of any new policing technology (Bradford et al., 2020). In addition, a lack of acceptance by the public can not only impact the intervention in question, but also may have a lasting negative impact on police–community relations as a whole (Nam, 2018).

Third, the question remains whether the results of this study can be seen as indicators of a 'smartification of policing'? Although the answers to the first background question were mainly used to categorise the subsequent responses, they also helped to put our findings into the context of the existing literature. Experts showed knowledge of technologies and did not show any direct dislike of their deployment or use. Although this may be expected given most individuals work directly with technology in their day-to-day work, it stands in contrast to previous findings and the general characterisation of crime prevention practitioners and police in the academic debate. This sample was too small to tell much about the wider organisations; however, it would be interesting to identify, through further research, the extent to which we can observe a technologisation or even smartification of policing.

Lastly, this research uncovered possible detrimental effects of increased privatisation in the field of public security and surveillance. It further suggested that the distinct lack of institutionalised measures and the reliance on external agencies hinders technological innovation and prevents police forces from staying up to date. Here, it would be useful for further research to examine the individual steps in public procurement processes and identify opportunities for streamlining them.

Conclusion

Overall, this article identified three key areas for improving current practices of procuring and deploying new surveillance technologies for policing and crime prevention in London. First, institutional set-ups need to be made more flexible and conducive for (technological) innovation. This includes increasing support from policy-makers and leaders, as well as regulatory clarify for the deployment and use of new SOSTs.

Second, this article highlights issues of interoperability as current, but also future obstacles to the use of SOSTs in policing and crime prevention. Here, not only technologically compatible systems should be procured but their deployment should also take practitioner concerns into account to minimise disruptions in day-to-day operations.

Lastly, this article highlighted the current lack of guidelines and evidence with regard to social acceptability. More research is needed to provide a better evidence base for future deployments of new SOSTs. At the same time, evaluation processes should be formalised and made more inclusive to ensure issues of ethics and social acceptability are not overshadowed by budgetary constraints and resource shortages.

These results only partially corroborate the findings of previous studies or the characterisation of police and crime prevention practitioners in the academic debate and, as a result, have several implications for the academic debate on technological innovation in policing and crime prevention. The theoretical discussion often highlights ethical issues and those of social acceptability, even though – in our interviews at least – most practitioners discussed these as rather peripheral issues in the procurement and implementation of new SOSTs.

Instead, practitioners focused on functionality and direct impacts on effectiveness and efficiency in their daily work. The main implications arising from this are that the academic debate needs to place a greater focus on practitioner perspectives and operational and practical issues. This can be done by involving practitioners and those working with SOSTs on a daily basis more and emphasising the importance of ethical and socially acceptable deployment from the onset of the procurement process (Azoulay and Jones, 2020). The overall lack of research reaffirms the urgency of this project. Not only is it important to evaluate the social acceptability level of individual interventions, but the findings of this study also indicate that there is a practical need for general criteria to evaluate to what extent the general public will examine a specific intervention.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Dawes Centre for Future Crime.

ORCID iD

Julian Laufs https://orcid.org/0000-0001-8358-3544

Notes

1. It is also noteworthy that the CCTV control rooms are not run by police forces but by local authorities. Although their primary function is detecting crime and securing evidence (through video recording), they also operate to monitor other factors such as traffic.
2. For a more in-depth discussion of the benefits and drawbacks of different data-recording methods in interviews, we recommend Hayes and Mattimoe (2004).
3. Smart lampposts use sensors to adapt the lighting to the flows of traffic and pedestrians to reduce electricity usage, minimise costs, reduce maintenance and CO_2 emissions, and enhance public safety and well-being (Dizon and Pranggono, 2021). Their utility can go far beyond lighting because smart lampposts can include video-monitoring devices, air pollution sensors, RFID readers, emergency call buttons or charging ports for electric vehicles (Babu et al., 2021).
4. Note that this was not discussed as an ethical or moral dimension but rather as a practical concern for the procurement and use of new technologies.

References

Abramovaite J, Bandyopadhyay S, Bhattacharya S et al. (2018) Alternatives to custody: Evidence from police force areas in England and Wales. *The British Journal of Criminology* 59(4): 800–822.

Adams A, Baer R, Denmon S et al. (2009) Glendale Police Department's strategic approach to staffing. *Alliance for Innovation Management Interns* 1 *October*: 1–87.

Allen D, Wilson T, Norman A et al. (2008) Information on the move: The use of mobile information systems by UK police forces. *Information Research* 13(4): 13–14.

Amoore L (2006) Biometric borders: Governing mobilities in the war on terror. *Political Geography* 25(3): 336–351.

Ankitha S, Nayana K, Shravya S et al. (2017) Smart city initiative: Traffic and waste management. In: *2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. Bengaluru, India, 19-20 May 2017.

Appleton JV (1995) Analysing qualitative interview data: Addressing issues of validity and reliability. *Journal of Advanced Nursing* 22(5): 993–997.

Azoulay P and Jones B (2020) Beat COVID-19 through innovation. *Science* 368(6491): 553. DOI: 10.1126/science.abc5792.

Babu DV, Nisha ASA, Dhasan DB et al. (2021) Intelligent high tech street lightning pole for smart city. *Annals of the Romanian Society for Cell Biology* 25(4): 13752–13759.

Baldoni G, Melita M, Micalizzi S et al. (2017) A dynamic, plug-and-play and efficient video surveillance platform for smart cities. In: *4th IEEE Annual Consumer Communications & Networking Conference (CCNC),* Las Vegas, USA, 8–11 January 2017.

Barnes CY and Henly JR (2018) 'They are underpaid and understaffed': How clients interpret encounters with street-level bureaucrats. *Journal of Public Administration Research and Theory* 28(2): 165–181.

Bartsch S (2011) Practitioners' perspectives on security in agile development. In: *Sixth International Conference* on Availability, Reliability and Security, Vienna, Austria, 22–26 August 2011.

Beamer G (2002) Elite interviews and state politics research. *State Politics & Policy Quarterly* 2(1): 86–96.

Beyers J, Braun C, Marshall D et al. (2014) Let's talk! On the practice and method of interviewing policy experts. *Interest Groups & Advocacy* 3(2): 174–187.

Borins S (2002) Leadership and innovation in the public sector. *Leadership & Organization Development Journal* 23(8): 467–476. DOI: 10.1108/01437730210449357.

Borrion H (2018) Engineering. In: Wortley R, Sidebottom A, Tilley N et al. (eds) *Routledge Handbook of Crime Science*. Oxfordhire, UK: Routledge, 167–178.

Borrion H, Ekblom P, Alrajeh D et al. (2019) The problem with crime problem-solving: Towards a second generation pop? *The British Journal of Criminology* 60(1): 219–240.

Borrion H, Kurland J, Tilley N et al. (2020) Measuring the resilience of criminogenic ecosystems to global disruption: A case-study of COVID-19 in China. *PLoS ONE* 15(10): e0240077.

Botta D, Werlinger R, Gagné A et al. (2007) Towards understanding IT security professionals and their tools. In: *Proceedings of the 3rd Symposium on Usable Privacy and Security,* Pittsburgh, USA, 18–20 July 2007. New York: Association for Computing Machinery.

Boukerche A, Siddiqui AJ and Mammeri A (2017) Automated vehicle detection and classification: Models, methods, and techniques. *ACM Computing Surveys* 50(5): 62.

Boulton L, McManus M, Metcalfe L et al. (2017) Calls for police service: Understanding the demand profile and the UK police response. *The Police Journal* 90(1): 70–85.

Bowyer KW (2004) Face recognition technology: Security versus privacy. *IEEE Technology and Society Magazine* 23(1): 9–19.

Bradford B, Yesberg JA, Jackson J et al. (2020) Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology* 60(6): 1502–1522. DOI: 10.1093/bjc/azaa032.

Braun T, Fung BC, Iqbal F et al. (2018) Security and privacy challenges in smart cities. *Sustainable Cities and Society* 39: 499–507.

Brell T, Philipsen R and Ziefle M (2018) Pictures of You, Pictures of Me - User Acceptance of Camera-technology in Intelligent Transport Systems. In: Gusikhin O (ed.) *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2018)*. Setúbal: Science and Technology Publications, 371–378.

Brezeale D and Cook DJ (2008) Automatic video classification: A survey of the literature. *IEEE Transactions on Systems, Man, and Cybernetics Part C (Applications and Reviews)* 38(3): 416–430.

Bromberg DE, Charbonneau É and Smith A (2019) Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly* 101415.

Brown D (2020) Criminal justice in an age of austerity: The London Bridge killings. *Alternative Law Journal* 45(4): 238–246.

Bryman A and Cassell C (2006) The researcher interview: A reflexive perspective. *Qualitative Research in Organizations and Management* 1(1): 41–55. DOI: https://doi.org/10.1108/17465640610666633.

Campbell JH, Brann J and Williams D (2003) *Officer-Per-Thousand Formulas & Other Policing Myths: A Leadership Model for Better Police Resource Management*. Portland, OR: Campbell DeLong Resources.

Chan JB (2001) The technological game: How information technology is transforming police practice. *Criminal Justice* 1(2): 139–159.

Chmutina K and Bosher L (2017) Rapid urbanisation and security: Holistic approach to enhancing security of urban spaces. In: *The Palgrave Handbook of Security, Risk and Intelligence*. London: Palgrave Macmillan, 27–45.

Choi W and Na J (2017) Relative importance for crime prevention technologies as part of smart city based on spatial information 2017 Smart City Symposium (ed Ruzicka J) 2017. Prague. 1–5.

Chong HG (2008) Measuring performance of small-and-medium sized enterprises: The grounded theory approach. *Journal of Business & Public Affairs* 2(1): 1–11.

Christopoulos D. Peer esteem snowballing: A methodology for expert surveys. In: Eurostat Conference for New Techniques and Technologies for Statistics, Luxemburg, February 2009.18–20.

Côté-Boucher K (2008) The diffuse border: Intelligence-sharing, control and confinement along Canada's smart border. *Surveillance & Society* 5(2): 142–165.

Crow MS and Smykla JO (2019) *Police Body-Worn Cameras: Research Developments on an Emerging Technology*. 44(3): 257–262. DOI: https://doi.org/10.1177/0734016819854789 Los Angeles: SAGE.

Cvrtila V and Perešin A (2014) New security models and public-private partnership. *Collegium Antropologicum* 38(1): 195–204.

Datta S and Sarkar S. Automation, security and surveillance for a smart city: Smart, digital city. In: *IEEE Calcutta Conference (CALCON),* 02-03 December 2017. Calcutta.

Davies T and Bowers K (2019) Patterns in the supply and demand of urban policing at the street segment level. *Policing and Society* 30(7): 795–817. DOI: https://doi.org/10.1080/10439463.2019.1598997.

Davis DW and Silver BD (2004) Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science* 48(1): 28–46.

de Diego IM, San Román I, Montero JC et al. (2018) Scalable and flexible wireless distributed architecture for intelligent video surveillance systems. *Multimedia Tools and Applications* 78(17): 437–459. DOI: https://doi.org/10.1007/s11042-018-7065-3.

Dinev T, Hart P and Mullen MR (2008) Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems* 17(3): 214–233.

Dixon J, Levine M and McAuley R (2004) Street drinking legislation, CCTV and public space: Exploring attitudes towards public order measures. Home Office.

Dizon E and Pranggono B (2021) Smart streetlights in smart city: A case study of sheffield. *Journal of Ambient Intelligence and Humanized Computing*. DOI: https://link.springer.com/article/10.1007/s12652-021-02970-y#citeas.

Dorussen H, Lenz H and Blavoukos S (2005) Assessing the reliability and validity of expert interviews. *European Union Politics* 6(3): 315–337.

Ekblom P (1999) Can we make crime prevention adaptive by learning from other evolutionary struggles? *Studies on Crime and Crime Prevention* 8: 27–51.

Ekblom P (2005) How to police the future: Scanning for scientific and technological innovations which generate potential threats and opportunities in crime, policing and crime reduction. In: Smith MJ and Tilley N (eds) *Crime Science – New Approaches to Preventing and Detecting Crime*. Cullompton: Willan.

Elliott-Davies M, Donnelly J, Boag-Munroe F et al. (2016) 'Getting a battering' The perceived impact of demand and capacity imbalance within the Police Service of England and Wales: A qualitative review. *The Police Journal* 89(2): 93–116.

Elmaghraby AS and Losavio MM (2014) Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research* 5(4): 491–497.

Erickson BH (1979) Some problems of inference from chain data. *Sociological Methodology* 10: 276–302.

Eugene AIII 2001 *Rethinking Police Culture: Officers' Occupational Attitudes*. 1 El Paso, TX: LFB Scholarly Publishing, 1–275.

Fernandez-Anez V, Fernández-Güell JM and Giffinger R (2018) Smart city implementation and discourses: An integrated conceptual model. The case of Vienna. *Cities (London, England)* 78: 4–16.

Fussey P and Murray D (2019) Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology.Available at: https://www.hrbdt.ac.uk/download/independent-report-on-the-london-metropolitan-police-services-trial-of-live-facial-recognition-technology/ (Last accessed: 11 November 2021)

Garicano L and Heaton P (2010) Information technology, organization, and productivity in the public sector: Evidence from police departments. *Journal of Labor Economics* 28(1): 167–201.

Germain S, Douillet A-C and Dumoulin L (2011) The legitimization of CCTV as a policy tool: Genesis and stabilization of a socio-technical device in three French cities. *The British Journal of Criminology* 52(2): 294–308.

Glaser BG, Strauss AL and Strutzel E (1968) The discovery of grounded theory; strategies for qualitative research. *Nursing Research* 17(4): 364.

Grace J (2019) 'Algorithmic impropriety' in UK policing contexts: A developing narrative? *UK Policing Contexts: A Developing Narrative*. DOI: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3487424 .

Greig-Midlane J (2019) An institutional perspective of neighbourhood policing reform in austerity era England and Wales. *International Journal of Police Science & Management* 21(4): 230–243.

Groves R, Singer E, Lepkowski J et al. (2004) Survey methodology. In: House J, Juster R, Khan H et al. (eds) *A telescope on society: Survey research and social science at the University of Michigan and beyond*. Ann Arbor: The University of Michigan Press, 21–64.

Halperin S and Heath O (2017) *Political Research: Methods and Practical Skills*. Oxford: Oxford University Press.

Hassell KD (2006) *Police Organizational Cultures and Patrol Practices*. El Paso, TX: LFB Scholarly Publishing.

Hayes T and Mattimoe R (2004) To tape or not to tape: Reflections on methods of data collection. In: Humphrey C and Lee B (eds) *The Real Life Guide to Accounting Research*. Amsterdam: Elsevier, pp. 359–372.

Higgins GE (2016) Police administration and organisation. In: Jennings WG and Maldonado-Molina MM (eds) *The Encyclopedia of Crime and Punishment (Vol. 1)*. London: Wiley.

Hintz A and Dencik L (2016) The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review* 5(3): 1–16. DOI: https://doi.org/10.14763/2016.3.424 .

Hirschmann N, Christe-Zeyse J (2016) Effective change management in the police Contributions to the 2013 CEPOL European Police Research and Science Conference Nogala D, Neidhardt K, Görgen Th et al. (eds) 11–13. September 2013 Münster, Germany 154–159.

Hooghe L, Bakker R, Brigevich A et al. (2010) Reliability and validity of the 2002 and 2006 Chapel Hill expert surveys on party positioning. *European Journal of Political Research* 49(5): 687–703.

Huberman M and Miles MB (2002) *The Qualitative Researcher's Companion*. Thousand Oaks, CA: SAGE.

Ingram JR, Terrill W and Paoline EAIII (2018) Police culture and officer behavior: Application of a multilevel framework. *Criminology; An Interdisciplinary Journal* 56(4): 780–811.

ISO (2018) ISO 31000 Risk management — Guidelines.

Joh EE (2019) Increasing automation in policing. *Communications of the ACM* 63(1): 20–22.

Keval H and Sasse MA (2010) 'Not the usual suspects': A study of factors reducing the effectiveness of CCTV. *Security Journal* 23(2): 134–154.

Kirmeyer SL and Dougherty TW (1988) Work load, tension, and coping: Moderating effects of supervisor support. *Personnel Psychology* 41(1): 125–139.

Kotulic AG and Clark JG (2004) Why there aren't more information security research studies. *Information & Management* 41(5): 597–607.

Laufs J, Borrion H and Bradford B (2020a) Security and the smart city: A systematic review. *Sustainable Cities and Society* 55: 102023. DOI: https://doi.org/10.1016/j.scs.2020.102023.

Laufs J, Bowers K, Birks D et al. (2020b) Understanding the concept of 'demand' in policing: A scoping review and resulting implications for demand management. *Policing & Society* 31(8): 895–918. DOI: https://doi.org/10.1080/10439463.2020.1791862.

Laufs J and Waseem Z (2020) Policing in pandemics: A systematic review and best practices for police response to COVID-19. *International Journal of Disaster Risk Reduction* 101812. doi: https://doi.org/10.1016/j.ijdrr.2020.101812.

Leese M (2021) Security as socio-technical practice: Predictive policing and (non-) automation. *Swiss Political Science Review* 27(1): 150–157.

Libbe J (2018) Intelligente Steuerung – Zur Umsetzung von Ansätzen smarter Städte und Regionen. In: Veit S, Reichard W and Wewer G (eds) *Handbuch zur Verwaltungsreform*. Wiesbaden, Germany: Springer VS, 571–580.

Liberatore A (2007) Balancing security and democracy, and the role of expertise: Biometrics politics in the European Union. *European Journal on Criminal Policy and Research* 13(1–2): 109–137.

Lischka JA (2017) Explicit terror prevention versus vague civil liberty: How the UK broadcasting news (de)legitimatise online mass surveillance since Edward Snowden's revelations. *Information, Communication & Society* 20(5): 665–682.

Liu D, Lu W and Niu Y (2018) Extended technology-acceptance model to make smart construction systems successful. *Journal of Construction Engineering and Management* 144(6): 04018035.

Liu T, Mostafa S, Mohamed S et al. (2020) Emerging themes of public–private partnership application in developing smart city projects: A conceptual framework. *Built Environment Project and Asset Management* 11(1): 138–156. DOI: https://doi.org/10.1108/BEPAM-12-2019-0142.

Lodge J (2007) Freedom, security and justice: The thin end of the wedge for biometrics? *Annali dell'Istituto Superiore di Sanita* 43(1): 20.

Lum C, Koper CS and Willis J (2017) Understanding the limits of technology's impact on police effectiveness. *Police Quarterly* 20(2): 135–163.

Macnish K (2014) Just surveillance? Towards a normative theory of surveillance. *Surveillance & Society* 12(1): 142–153.

Mastrobuoni G (2020) Crime is terribly revealing: Information technology and police productivity. *The Review of Economic Studies* 87(6): 2727–2753.

McQuade S (2006) Technology-enabled crime, policing and security. *The Journal of Technology Studies* 32(1): 32–42.

Metropolitan Police Service (2017a) The Met's Direction: Our Strategy 2018–2025. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/the-mets-direction—our-strategy-2018—2025.pdf (Last accessed: 09 November 2020)

Metropolitan Police Service (2017b) ONE MET - Digital Policing Strategy. Available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/one-met-digital-policing-strategy-2017-2020.pdf

Miles MB and Huberman AM (1984) Drawing valid meaning from qualitative data: Toward a shared craft. *Educational Researcher* 13(5): 20–30.

Monahan T (2006) *Surveillance and Security: Technological Politics and Power in Everyday Life*. London: Routledge.

Murata K, Adams AA and Palma AML (2017) Following Snowden: A cross-cultural study on the social impact of Snowden's revelations. *Journal of Information, Communication and Ethics in Society* 15(3): 183–196. DOI: https://doi.org/10.1108/JICES-12-2016-0047.

Nam T (2018) Untangling the relationship between surveillance concerns and acceptability. *International Journal of Information Management* 38(1): 262–269.

National Police Chief's Council (2016). Policing Vision 2025. Available at: https://www.npcc.police.uk/documents/Policing%20Vision.pdf

Newell BC (2013) Local law enforcement jumps on the big data bandwagon: Automated license plate recognition systems, information privacy, and access to government information. *Maine Law Review* 66: 397.

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

Nhan J (2014) Police culture. In: Albanese J (ed) *The Encyclopedia of Criminology and Criminal Justice*, 1–6

Norris C and McCahill M (2006) CCTV: Beyond penal modernism? *The British Journal of Criminology* 46(1): 97–118.

Patel J, Wala H, Shahu D et al. Intellectual and enhance digital solution for police station. In: International Conference on Smart City and Emerging Technology (ICSCET), 2018.

Pavone V and Esposti SD (2012) Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science* 21(5): 556–572.

Pavone V, Santiago Gomez E and Jaquet-Chifelle D-O (2016) A systemic approach to security: Beyond the tradeoff between security and liberty. *Democracy and Security* 12(4): 225–246.

Piza EL (2018) The crime prevention effect of CCTV in public places: A propensity score analysis. *Journal of Crime and Justice* 41(1): 14–30.

Piza EL, Welsh BC, Farrington DP et al. (2019) CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy* 18(1): 135–159.

Purtova N (2018) Between the GDPR and the police directive: Navigating through the maze of information sharing in public-private partnerships. *International Data Privacy Law* 8(1): 52–68. DOI: https://doi.org/10.1093/idpl/ipx021.

Rankin S, Cohen N, Maclennan-Brown K et al. CCTV operator performance benchmarking. In: IEEE International Carnahan Conference on Security Technology (ICCST), 2012.

Reiner R (2010) *The Politics of the Police*. Oxford: Oxford University Press.

Riley T (2007) Security vs. privacy: A comparative analysis of Canada, the United Kingdom, and the United States. *Journal of Business and Public Policy* 1(2): 1–21.

Rogers C and Scally EJ (2018) Police use of technology: Insights from the literature. *International Journal of Emergency Services* 7(2): 100–110.

Rutakumwa R, Mugisha JO, Bernays S et al. (2020) Conducting in-depth interviews with and without voice recorders: A comparative analysis. *Qualitative Research* 20(5): 565–581.

Sabbagh D (2019) Facial recognition row: police gave King's Cross owner images of seven people. *The Guardian*. Available at: https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people

Schmidt T, Philipsen R and Ziefle M (2015) From v2x to control2trust In: International Conference on Human Aspects of Information Security, Privacy, and Trust.

Schuman H and Presser S (1996) *Questions and Answers in Attitude Surveys: Experiments on Question Form, Wording, and Context*. Thousand Oaks, CA: SAGE.

Sen M, Dutt A, Agarwal S et al. Issues of privacy and security in the role of software in smart cities. In: 2013 International Conference on Communication Systems and Network Technologies (CSNT), 2013.

Sheng S, Kumaraguru P, Acquisti A et al. (2009) Improving phishing countermeasures: An analysis of expert interviews. In: Paper presented at the 2009 eCrime Researchers Summit 2009 eCrime Researchers Summit.20-21 October 2009. Tacoma, WA. Boston: IEEE.

Skogan WG (2019) The future of CCTV. *Criminology & Public Policy* 18(1): 161–166.

Spence K (2005) World risk society and war against terror. *Political Studies* 53(2): 284–302.

Strickland LS and Hunt LE (2005) Technology, security, and individual privacy: New tools, new threats, and new public perceptions. *Journal of the American Society for Information Science and Technology* 56(3): 221–234.

Taylor RW, Fritsch EJ and Liederbach J (2014) *Digital Crime and Digital Terrorism*. Englewood Cliffs, NJ: Prentice Hall.

Thompson N, McGill T, Bunn A et al. (2020) Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology* 71(9): 1129–1142.

Tourangeau R and Smith TW (1996) Asking sensitive questions: The impact of data collection mode, question format, and question context. *Public Opinion Quarterly* 60(2): 275–304.

Tsoukala A (2006) Democracy in the light of security: British and French political discourses on domestic counter-terrorism policies. *Political Studies* 54(3): 607–627.

Valentín L, Serrano SA, García RO et al. (2017) A cloud-based architecture for smart video surveillance. *International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences* 42(5): 21–33.

van Heek J, Arning K and Ziefle M (2017) *The Surveillance Society: Which Factors Form Public Acceptance of Surveillance Technologies?* Vol. 738. Berlin: Springer, 170–191.

Vinod Kumar T (2014) Differing services, rising expectations, and greater demands: Patterns in variations of police-public dynamics across areas with conventional and community policing in India. *Policing: An International Journal of Police Strategies & Management* 37(1): 170–189.

Webster W (2019) Surveillance cameras will soon be unrecognisable–time for an urgent public conversation The Conversation .Surveillance cameras will soon be unrecognisable–time for an urgent public conversation, The Conversation, Available at: https://theconversation.com/surveillance-cameras-will-soon-be-unrecognisable-time-for-an-urgent-public-conversation-118931 (Last accessed 21 November 2021).

Weisburd D and Braga AA (2019) *Police Innovation: Contrasting Perspectives*. Cambridge: Cambridge University Press.

Werlinger R, Hawkey K and Beznosov K (2008) Human, organizational and technological challenges of implementing IT security in organizations. *HAISA* 8: 35–48.

Werlinger R, Hawkey K, Botta D et al. (2009) Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies* 67(7): 584–606.

White MD and Escobar G (2008) Making good cops in the twenty-first century: Emerging issues for the effective recruitment, selection and training of police in the United States and abroad. *International Review of Law, Computers & Technology* 22(1–2): 119–134.

Wilson D (2019) Predictive policing management: A brief history of patrol automation. *New Formations* 98(98): 139–155.

Wilson JM and Weiss A (2014) Police staffing allocation and managing workload demand: A critical assessment of existing practices. *Policing: A Journal of Policy and Practice* 8(2): 96–108.

APPENDIX 1: Interview questions

Overall aim and objectives

1. Realistic scenarios
   - Are you aware of any smart city initiatives?
   - What are possible deployment scenarios in London?
   - Which alternatives are most feasible? — financially, ethically, practically …?
2. The current process
   - How long does it take to deploy a new technology?
   - What things are primarily considered in the process?
   - What kinds of consultations are being held before?

- Are issues of ethics and social acceptability considered before?
- I know that many councils now try to buy new security technologies in bulk/together, has this changed the evaluation and consultation process in any way?

3. Suggestions for the future
   - Where do you see room for improving the current consultation processes?
   - (This is kind of inevitable.) In an ideal world what would smart security systems look like?

Author biographies

Julian Laufs is a currently a PhD candidate at the UCL Jill Dando Institute of Security and Crime Science where he focuses on the prevention of future crime in smart cities. He also researches the usefulness and cost of smart crime prevention technologies as well their impact on police demand dynamics.

Hervé Borrion is a crime scientist who uses his systems engineering background to better understand and address crime problems across the world. He is an academic advisor on the MoRiLe project (development of a risk model for 80+ law enforcement agencies). Dr Borrion is currently the Deputy Head of Department of the UCL Department of Security and Crime Science.