Surveillance & Society

Towards a Macro-Level Theoretical Understanding of Police Services' Acquisition of Risk Technologies

Dallas Hill and Christopher O'Connor

Volume 22, Number 4, 2024

Open Issue

URI: https://id.erudit.org/iderudit/1115672ar
DOI: https://doi.org/10.24908/ss.v22i4.16486

See table of contents

Publisher(s)

Surveillance Studies Network

ISSN

1477-7487 (digital)

Explore this journal

Cite this article

Hill, D. & O'Connor, C. (2024). Towards a Macro-Level Theoretical Understanding of Police Services' Acquisition of Risk Technologies. *Surveillance & Society*, *22*(4), 395–409. https://doi.org/10.24908/ss.v22i4.16486

Article abstract

Most North American police services have rapidly acquired and implemented a range of emerging and disruptive technologies in recent years. This rapid adoption of technologies has left a significant gap in our theoretical understanding of how police make decisions about which technologies to acquire. While existing research has focused on technology's impact at the organizational level, the macro-level context that shapes technological acquisition by the police is undertheorized. To address this gap in the literature, this article combines theorizing by Ericson and Haggerty (1997) on policing the risk society (PRS) and Zuboff (2019) on surveillance capitalism (SC) to develop a macro-level theoretical framework. We consider technologies acquired by the police to be risk technologies and argue that combining key elements of PRS and SC theorizing offers a macro-level understanding of police decision-making about which technologies to adopt that can complement meso-level organizational theories. While calling for additional empirical research, this article concludes by discussing the potential impacts associated with private-sector involvement in public-sector initiatives and providing directions for future research.

Surveillance & Society

Article

Towards a Macro-Level Theoretical Understanding of Police Services' Acquisition of Risk Technologies

Dallas Hill

Ontario Tech University, Canada
dallas.hill@ontariotechu.net

Christopher O'Connor

Ontario Tech University, Canada
christopher.o'connor@ontariotechu.ca

Abstract

Most North American police services have rapidly acquired and implemented a range of emerging and disruptive technologies in recent years. This rapid adoption of technologies has left a significant gap in our theoretical understanding of how police make decisions about which technologies to acquire. While existing research has focused on technology's impact at the organizational level, the macro-level context that shapes technological acquisition by the police is undertheorized. To address this gap in the literature, this article combines theorizing by Ericson and Haggerty (1997) on *policing the risk society* (PRS) and Zuboff (2019) on *surveillance capitalism* (SC) to develop a macro-level theoretical framework. We consider technologies acquired by the police to be risk technologies and argue that combining key elements of PRS and SC theorizing offers a macro-level understanding of police decision-making about which technologies to adopt that can complement meso-level organizational theories. While calling for additional empirical research, this article concludes by discussing the potential impacts associated with private-sector involvement in public-sector initiatives and providing directions for future research.

Introduction

In recent years, the police have acquired, used, or experimented with a wide range of technologies. This includes facial recognition technology (Hill, O'Connor, and Slane 2022), automated license plate recognition technology (Merola, Lum, and Murphy 2019), big data and machine learning (Brayne 2017), drones and robots (Davis 2019), and artificial intelligence (AI) (Berk 2021). As Hannem et al. (2019) note, these technologies should be considered risk technologies (RT) in the hands of the police. RT are conceptualized as tools equipped with the capabilities to drive human decision-making in the realm of risk assessment (Hannem et al. 2019). These RT are not merely neutral technologies that purport to enhance public safety but instead encapsulate a complex mix of enhanced surveillance techniques, attempts to predict crime before it occurs, and efforts to measure risks that are often unmeasurable. Applying this definition to the scope of this article, all technologies acquired by police services to collect data in mass volumes for the purpose of assessing the risks posed by or to populations are referred to as RT.

At the center of many of these RT is data (O'Connor et al. 2022). Data are collected via RT for immediate but also (unknown) potential future uses (Sanders, Weston, and Schott 2015). The acquisition of RT by police has raised a variety of concerns, particularly around the data being used and collected. For example, the accuracy of facial recognition technology has been called into question due to a lack of quality in the data used to train the algorithms, thus leading to potential bias (Nesterova 2020). Similarly, it is still often unclear how the algorithms used to predict crime via machine learning arrive at their decisions. With this

Hill, Dallas, and Christopher O'Connor. 2024. Towards a Macro-Level Theoretical Understanding of Police Services' Acquisition of Risk Technologies. *Surveillance & Society* 22 (4): 395-409.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

understanding essentially black-boxed, sometimes because of companies' proprietary claims to this information, questions remain as to how much previously collected biased and poor-quality data influenced the future predictions of where and on whom the police should focus their attention (Hälterlein 2021). Given this, research on existing RT within police services has shown mixed results concerning their overall effectiveness, efficiency, and fairness (Haskins and Chapman 2018; Jennings, Lynch, and Fridell 2015; Koper, Lum, and Hibdon 2015; Ozer 2016; Sanders and Sheptycki 2017; White 2014). These technologies are also often acquired without accompanying regulation and oversight (Joh 2017).

When RT acquired by the police have been examined by researchers, the focus has often been on the organizational level. For example, there is much research on the implementation of technology and its subsequent impacts on police services, although much less research and theorizing on police acquisition of RT. Therefore, the theorizing that does exist on police acquisition of technology also tends to focus on the organizational level. However, a few researchers have examined the larger macro-level context in which technological acquisition plays out (Bayerl et al. 2013; Sheptycki 2019). As Bayerl et al. (2013: 804–805) argue, the "view of 'technologies in organizations' needs to be broadened into a wider view on 'technologies in organisations in their macro-context.'" In agreement, Sheptycki (2019) asserts that broader factors should be considered when examining technological advancement. While these acknowledgments have advanced the literature on technology in public safety spaces, a specific focus on technology acquisition has not been presented. Our goal in this article is to provide a theoretical framework for understanding the macro-level theoretical context in which police acquire RT.

This article begins with an examination of previous organizational theorizing that has been used to explain police acquisition of technologies. We then discuss the advantages and limitations of these approaches and illustrate the need for a macro-level theoretical framework that can complement organizational theorizing. More specifically, we make the case for combining key elements of Ericson and Haggerty's (1997) *policing the risk society* (PRS) and Zuboff's (2019) *surveillance capitalism* (SC) to provide a macro-level theoretical context for understanding police adoption of risk technologies. We argue that combining key elements of these theories demonstrates previously ignored macro-level impacts on police decision-making, highlights the potentially problematic relationship between the private and public sectors, and illuminates possible avenues for better oversight of police decision-making around RT. Overall, this article adds to the existing literature by providing a macro-level theoretical framework for understanding the complex reality of technological decision-making by police.

Risk Technologies and Organizational Theorizing

This section discusses three examples of organizational theories that have been used to explain why and how police acquire RT. While we acknowledge that various organizational theories have been undertaken to explore the structure and operations of policing (e.g., contingency theory [Lawrence and Lorsch 1967] and institutional isomorphism [DeMaggio and Powell 1983]), we have chosen three vastly different models to exemplify the breadth of organizational theorizing in both technological decision-making and policing scholarship. These theories include the diffusion of innovations (DOI) model (Rogers 1962, 2003), the behavioural theory of the firm (Cyert and March 1963), and the garbage can model of organizational choice (Cohen, March, and Olsen 1972). These three organizational theories are some of the more frequently cited in the literature when police decisions surrounding technology adoption are examined. Although we would also note that RT acquisition is a substantially under-researched and theorized area of policing. We discuss each of these theories separately before discussing the shortcomings of organizational approaches more broadly.

Diffusion of Innovation Model

One theoretical perspective for understanding the process of technology acquisition within organizations is the DOI model (Hendrix et al. 2019; Pasha 2019; Rogers 1962; Weisburd, Petrosino, and Lum 2003). In

policing, scholars have tethered the DOI model to the examination of body-worn cameras (BWCs) (White and Malm 2020), COMPSTAT/crime mapping (Weisburd and Lum 2005; Weisburd, Petrosino, and Lum 2003), conducted energy weapons (White 2014), and information communication technology acquisition (Skogan and Hartnett 2005). The origins of this model are centered in the discipline of communications and explain how an innovation (an idea or product) is communicated over time through a specific social system or organization (Rogers 2003). The final step of the model is the subsequent adoption of the diffused innovation (e.g., purchasing a new product, acquiring new behaviour). More recently, DOI theory has been specifically tethered to the adoption of technologies by organizations (Rogers 2003). The defining properties of the DOI model acknowledge the hierarchical characteristics of organizational decision-making and suggest that successful persuasion to adopt an innovation (e.g., technology) is dependent on the relative advantage of the technology over the product it is replacing, the compatibility with the values and needs of the adopters, the complexity of the innovation, the testability of the innovation prior to commitment, and the observability of tangible results (Rogers 1962, 2003). However, the processes of the model are not simultaneous or linear, as they can be influenced by various organizational factors leading to differing outcomes.

In the instance where a decision is made to acquire an innovation, adopters of the innovation are categorized into five mutually exclusive classifications including innovators, early adopters, early majority, late majority, and laggards based on their level of innovativeness (Rogers 1962, 2003). Innovators play a significant role in the diffusion process because they are the individuals who are the first to try an innovation. Rogers (2003) characterizes innovators by their venturesomeness on account of their impulsivity. Correspondingly, innovators typically have control of substantial financial resources and can rebound from inevitable unsuccessful adoptions of innovations. In contrast, early adopters are highly respected by their local social systems and are regarded as the central point of reference when considering the adoption of an innovation. Furthermore, early adopters are often discrete and successful with their adoption of new products. Alternatively, the adoption of an innovation by the early majority is a relatively long process. In comparison, the late majority are often skeptical of change and will only choose to adopt an innovation following the early majority. Lastly, laggards refer to those who are conservative, skeptical of change, and difficult to persuade. Consequently, laggards rely on empirical evidence and pressure from other categories of adopters to acquire an innovation (Rogers 1962, 2003).

By focusing specifically on the decision-making process, DOI theorizing provides an understanding of the rate at which police organizations adopt new technologies and the various stages of said adoption. Social media adoption and use by the police offers an illustrative example of DOI theorizing. Police were initially reluctant to adopt social media except for the initial few organizations that could be classified as innovators or early adopters (e.g., Royal Canadian Mounted Police and X [formerly known as Twitter]). After these early stages, social media use by the police substantially expanded (early majority, late majority) with all but a few, typically smaller scale, police services (laggards) not having some form of social media presence (Dekker, van den Brink, and Meijer 2020; Walsh and O'Connor 2019). Police services reflecting on their approach to technology acquisition (i.e., are they innovators, laggards, or somewhere in between) would benefit from understanding where, as an organization, they fall on this spectrum. This could also be reframed as the willingness of police services to take a risk on trying out new technologies that might succeed but could also fail in unknown and potentially damaging ways.

The Behavioural Theory of the Firm

A second theory that is drawn upon to explain police acquisition of RT is the behavioural theory of the firm (Hendrix et al. 2019). Empirically, this rational organizational perspective has been used to examine the role of randomized control trials in police decision-making (Bedford and Neyroud 2021) and COMPSTAT/crime mapping adoption (Willis, Mastrofski, and Weisburd 2007). Originated by Cyert and March (1963), this theory concentrates on explaining the key factors contributing to the decision-making of large-scale organizations focused solely on short-term goals. The behavioural theory of the firm would consider police

organizations to be rational actors that would only acquire technologies that they could use to meet their mission and goals (Hendrix et al. 2019). For example, if a police service was looking to acquire Geographic Information System (GIS) software to direct patrol, it would make sense that they subsequently integrate hot spots policing into their organizational model (Piza and O'Hara 2014).

This theoretical perspective also recognizes that organizations have multiple goals and multi-decision coalitions in which management, workers, stakeholders, consumers, and suppliers have their own sets of goals and demands. For instance, the goals of (technology) suppliers include high profits and monopolization, while the goals of consumers (police) include low purchase prices and good quality products. Thus, the goals of the organization are dependent on the various demands of members within the coalition. Demands are created through several avenues including the availability of information, past achievements, aspirations, expectations, and the achievements demonstrated by other groups (e.g., other police services). For various reasons, the individuals within the coalition bring the selected demands to leadership who then decide which requests help the organization reach their overarching goals and mission (Cyert and March 1963).

The behavioural theory of the firm offers valuable insight into how organizational decision-making by police services is impacted by limited/available resources within a context of potentially unlimited/multi-faceted demands. That is, organizations have a limited number of resources to invest in strategic goals and the varying demands presented by different members compete for the resources of the firm (Cyert and March 1963). By acknowledging the resource component of decision-making, it becomes clear that not all demands that are presented to police leadership will be considered and not all goals will be met satisfactorily. Therefore, despite the perceived efficacy of RT, police services may not acquire and implement them in their organizations partially due to limited resources. Consequently, the decision to acquire RT is not a linear process.

The Garbage Can Model of Organizational Choice

Finally, a third theory that is drawn upon to explain police acquisition of risk technologies at the organizational level is the garbage can model of organizational choice. Rather than being grounded in rational choice, this model is rooted more in entropy (Hendrix et al. 2019). That is, it is argued that complex organizations often do not rely on strategic goals and their missions to make decisions (Cohen, March, and Olsen 1972). Instead, the decision-making processes are equivalent to "A garbage can into which various kinds of problems and solutions are dumped by participants as they are generated. The mix of garbage in a single can depends on the mix of cans available, on the labels attached to the alternative cans, on what garbage is currently being produced, and on the speed with which the garbage is collected and removed from the scene" (Cohen, March, and Olsen 1972: 2).

These types of organizations, also referred to as "organized anarchies," are characterized by their ad hoc decision-making around RT rather than it being linked to meeting the strategic goals of the organizations (Cohen, March, and Olsen 1972; Hendrix et al. 2019). For example, in Canada, several members of police services recently accepted a free trial from Clearview AI to use their controversial facial recognition software (Browne 2020; Hill, O'Connor, and Slane 2022). This technology appears to have been used by officers without any oversight, for unknown purposes, and without the public's and possibly police leadership's knowledge. In other words, there was no clear link between the technology's use and the police services' goals and missions.

The garbage can model of organizational choice clarifies the unique structural and cultural elements that go into the acquisition of RT by complex organizations like police services. That is, there are sometimes no clear directives or formal processes for acquiring RT (e.g., trial and error is used to determine technological usefulness). Also, RT can be acquired as solutions in search of problems to solve (Cohen, March, and Olsen 1972). As Strom (2017) found, technology acquisition by police services in the United States was often

unstructured and independent of the short and long-term goals of the organizations. Similarly, Weisburd and Neyroud (2011) describe technology decision-making by police as a "black box" that is often done without demonstrations of effectiveness or efficiency. By moving away from a rational choice perspective, this theory furthers our understanding of how police services can quickly acquire RT (e.g., body-worn cameras, facial recognition technology) without being guided by a rational plan. It also helps to illustrate that there are internal and external influences on police RT decision-making that go beyond the immediate goals of any police service.

Shortcomings of Organizational Theorizing

Both the DOI model and behavioural theory of the firm discussed above describe a logic to police decision-making around RT. While these organizational theories are enticing for explaining RT adoption by police services because of the logical/rational decision-making procedures they present, there are limitations to framing RT decision-making by police services in this way. First, decision-making around RT is not always rational/logical and linked to the strategic goals of police services. For instance, Hendrix et al. (2019) found that decisions to adopt technology within police services occurred independently of their organizational strategies and goals. Second, the focus on internal decision-making oversimplifies the complexities of police services, which are fluid and ever-changing organizations made up of multitudes of different actors (e.g., officers working with limited supervision and high levels of discretion) and external factors (e.g., politics, interest groups) that lead to less than well thought out decision-making about RT (Sheptycki 2017). Consequently, these theories do not account for instances where goals are not distinctly outlined or when change happens at a rapid pace (e.g., when calls for accountability prompted the adoption of body-worn cameras). The alternative theory offered, the garbage can model of organizational choice, is one grounded in chaos. It describes RT acquisition by police services as less about active and planned decision-making and more about happenstance (Strom 2017). Unfortunately, this tells us little about how RT are acquired (Hendrix et al. 2019). While this theory also hints at external factors influencing how RT come to be acquired by police services, these are not fully explored.

Organizational-level theories have only begun to articulate the complexity inherent in police acquisition of RT. Questions remain as to how different types of RT, the level of risk associated with the RT, and police services' performances impact their decision-making around RT (Hendrix et al. 2019). For example, it has been found that poor performance may encourage police services to adopt riskier technologies earlier than police services that are performing well at achieving their mission (Pasha 2019), but more research explicitly examining RT acquisition is needed. Thus far, the reliance on meso-level organizational theorizing to explain the acquisition of RT by police services has focused mainly on the structural and cultural elements influencing decision-making within police services. For the most part, this has neglected the macro-level influences (e.g., private sector, politics, economics, social movements) that play a crucial role in technological decision-making. Organizational theorizing remains unequipped to explain, or has not yet integrated into their theoretical frameworks, how changes in the external environments that policing agencies inhabit impact decision-making.

Therefore, this has left a very narrow interpretation of how police make decisions about technology. For example, the potential influence of private technology corporations (e.g., marketing, vendor-consumer relationships) remains largely absent from the wider discussion of potential influences on the acquisition of RT within police services. According to Greene (2014: 221), "we seem to have moved the discussion to considerations of aggregate police effects, hot spots, evidence-based, and the like, measuring selectively chosen impacts of police interventions (most at the meso-level)…. [S]uch an approach…ignores what new environments the police face in the twenty-first century (macro-level) and their likely impact on the police." With empirical evidence to suggest that police services do not consider organizational goals during their decisions to adopt RT (Strom 2017; Hendrix et al. 2019), the scope of the analysis must be broadened to

examine the larger societal context that shapes police services' acquisition of RT. Ultimately, this would help provide a more holistic view of the issue.

Macro-Level Theorizing: Policing the Risk Society and Surveillance Capitalism

To provide a more comprehensive theoretical picture of police acquisition of RT, this section draws on Ericson and Haggerty's (1997) work on policing the risk society (PRS) and Zuboff's (2019) work on surveillance capitalism (SC). In this section, we demonstrate the relevance of PRS and SC to explaining police services' technological decision-making beyond, or as an accompaniment to, organizational-level theorizing. We first discuss each theoretical work separately to clarify their perspectives. Ericson and Haggerty's (1997) work has been influential in policing by providing a modern illustration of police work as predominantly knowledge work that facilitates relationships between the private and public sectors. Additionally, Zuboff's (2019) work illustrates the concerns that accompany the consumption of private technology, including how systems of power (i.e., private technology corporations) use information as a tool to control and shape the experiences of their consumers (in this case, the police), which in turn affects how RT impact the public. After each perspective is discussed, we merge key concepts from each theoretical perspective to elucidate the macro-level influences on police decision-making about RT.

Policing the Risk Society

Contrary to what is commonly illustrated by mass media, police spend relatively little time "fighting crime" (Ericson and Haggerty 1997). Alternatively, police work is characterized as knowledge work through the collection of information and the assessment of risk (Chan 2001; Ericson and Haggerty 1997; Manning 1992). The underlying framework of PRS rests on the argument that increased information about risk leads to a more secure world. Respectively, police work is measured in terms of risk and how those risks can be managed more effectively and efficiently. Under a PRS framework, police are no longer considered to be self-governed. Rather, they are governed by demands that are external to the organization. For example, insurance companies shape the data that police need to collect (Ericson and Haggerty 1997; O'Connor and Shon 2019). According to this theorizing, police are continuously faced with the competing demands of other institutions (e.g., social services, health care, technology companies) that influence the rules, technological design, data collected, and RT that are acquired (O'Connor and Shon 2019).

The proliferation of RT throughout police services has transformed police knowledge work by creating new opportunities to collect, manage, and regulate information (Brayne 2017; Ericson and Haggerty 1997; O'Connor and Shon 2019). As such, various empirical works have expanded this characterization. For example, Sheptycki (2017) and Bowling, Reiner, and Sheptycki(2019) expand PRS theorizing by characterizing police as governed by screens and as functioning in plurality with external agencies (e.g., private security). Additionally, Terpestra, Fyfe, and Salet (2019) further this concept with the introduction of "abstract policing." According to Terpestra, Fyfe, and Salet (2019), police work is becoming increasingly distant from the communities they are intended to serve due to increasing knowledge demands and technology use. These new opportunities to collect data have shifted police practices away from traditional reactive policing strategies towards data-driven approaches (e.g., evidence-based policing). Data-driven police practices position information at the forefront of strategic and tactical decision-making (Burcher and Whelan 2018). Correspondingly, data-driven strategies are proactively focused on establishing a pre-crime society that values risk prevention over and above reactive means of addressing crime (Zedner 2007). Further, when crimes do occur, they are likely investigated with the help of RT (e.g., BWCs). The shift in police practices towards data-driven approaches, coupled with increasing external requests for information, has led to the adoption of a unidirectional approach to the intelligence cycle that is dysfunctional for the fluidity of police organizations (Sheptycki 2013). This management-guided approach to intelligence results in the compulsion to collect as much information as possible even if that information might not be initially relevant (Ericson and Haggerty 1997; Manning 1992; Sheptycki 2013).

PRS extends beyond previous organizational attempts to understand police decision-making, as it acknowledges police initiatives as driven by both internal and external demands for information. These influences ultimately impact police decisions to acquire RT that collect the necessary information to satisfy these increasing demands (Terpestra, Fyfe, and Salet 2019). Although police typically decide to adopt RT in hopes of increased organizational effectiveness and efficiency, most of the efforts by police services to incorporate RT are directed by the demands from external institutions (Ericson and Haggerty 1997; Manning 2001). Private sector insurance companies are illustrative of an external entity that demands information about risk from the police. For example, PRS suggests that, while responding to automobile accidents, the main priority of police work is to collect data concerning risk management for insurance companies (e.g., responsible parties, demographic information, incident report). This information demanded by insurance companies allows them to re-calculate a driver's risk score to maintain balance through the re-distribution of risks. Correspondingly, external requests for information have demonstrated a profound impact on how the police think and act as an organization (Gates 2019; Joh 2017; Rogers and Scally 2018).

Additionally, PRS extends current organizational theorizing by acknowledging the inequalities in society surrounding the ownership and control of information via RT (Ericson and Haggerty 1997; Ferguson 2017; Joh 2017). With decreasing control over knowledge production initiatives, police services are often unaware of where the knowledge they produce ends up, let alone how external and powerful industries (e.g., private technology corporations) exploit the collected information (Ericson and Haggerty 1997). As the demands for risk knowledge from external institutions continue to rise, new questions also emerge surrounding the collection, storage, management, and accessibility of information by police services. Specifically, private technology corporations are increasingly involved in police knowledge work through the supply of RT that can collect, store, and manage large volumes of information (Ericson and Haggerty 1997; Joh 2017). As we attempt to illustrate below, combined with surveillance capitalism theorizing, PRS can help to theorize the influence (e.g., marketing tactics) of private technology corporations (e.g., Clearview AI) on police decisions to acquire new technologies.

Surveillance Capitalism

SC is a macro-level economic theory frequently used to explain the negative impacts private sector technology corporations can have on society stemming from their ownership of the means of learning and the control of information (Zuboff 2015, 2019). Zuboff (2019: VII) operationalizes SC as:

> A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales; a parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification; a rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history; the foundational framework of a surveillance economy; as significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth; the origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy; a movement that aims to impose a new collective order based on total certainty; and an expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty.

According to this definition, economic ends are intrinsic to technological development (Zuboff 2019). To achieve these economic ends, surveillance capitalists utilize a convergence of freedom and knowledge to control the market (Zuboff 2019). Therefore, an individual's information is taken and sold to fund the freedom and knowledge of surveillance capitalists while simultaneously oppressing the individual who offered their information for access to various RT. For example, Facebook requires users to agree to a lengthy list of terms and conditions prior to using their platform for social engagement. These terms and

conditions include the extraction of user data that can be shared with third-party companies to personalize advertisements and content. Consequently, users are sacrificing their personal information to access the benefits of the platform, while Facebook profits from the collection of said knowledge.

This theorizing raises potential ethical concerns regarding the relationship between police services and RT companies and the corporate control of information. Presumably, before acquiring RT, police services must also agree, like users of almost any technology, to a lengthy list of terms and conditions, although little is currently known about what has been agreed to in these contracts. Given this, it is often unclear exactly who owns the data collected by and stored in RT (e.g., digital evidence platforms) and how/if these data are being used beyond immediate police use. We do know that surveillance capitalists focus on the collection of information for behaviour modification purposes through the sale of emerging digital technologies. Therefore, regardless of criminal involvement, the historical location information of countless individuals is collected through police RT and may exist in several databases where it can be aggregated and sold to make decisions about consumption habits, health, and creditworthiness (Brayne 2017; Joh 2016).

The complete societal transformation by way of SC has paved the way for a social system without boundaries surrounding privacy and security (Zuboff 2015, 2019). The potential impacts of RT integrating into the public sector have only begun to be addressed in the literature. For instance, Robinson (2019) and Zuboff (2015) both express concern regarding the influence of private sector finances on public sector activities, such as the growing collaborations between government authorities and private technology corporations for surveillance purposes. As previously mentioned, the consumer-vendor relationship poses greater concern when the product itself plays a significant role in the collection, management, analysis, and storage of information by public police services (Joh 2017). However, the literature surrounding the influence of private technology companies on public sector decision-making has circled the broad impacts of SC as a whole and has not been applied to the area of policing.

Discussion

Drawing on PRS and SC theorizing, this section outlines a macro-level theoretical understanding of police services' acquisition of risk technologies. Collectively, insights from PRS and SC provide a more robust understanding of how external private sector influences could impact organizational decision-making in the public sector. Individually, SC and its defining properties do not present a direct link to how the police make decisions regarding what RT to acquire. However, when combined with PRS theorizing, police can be conceptualized as consumers of technologies that are capable of mass data collection and surveillance. Correspondingly, it is imperative to examine how economic factors are specifically impacting the technological decisions of police. As will be demonstrated in subsequent sections, drawing insights from the two theories illuminates the following: (1) police can be categorized primarily as knowledge workers *and* consumers; and (2) several concerns emerge when boundaries are blurred between the private and public sector, specifically surrounding the acquisition of RT.

Police as Knowledge Workers and Consumers

Although the characterization of police as knowledge workers has been extensively theorized and empirically demonstrated (Bowling, Reiner, and Sheptycki 2019; Chan 2001; Ericson and Haggerty 1997; Manning 1977, 1992; Egbert and Leese 2021; Sheptycki 2017, 2020; Terpestra, Fyfe, and Salet 2019), we propose an addition to this role. Specifically, we argue that most North American police services operate as both knowledge workers *and* consumers. Through the lens of SC, we can theorize that the rapid acquisition of private sector technologies in policing spaces has shifted the roles and capabilities of the police to be driven by economic means and the ownership of information rather than by "community consumerism" (Loader 1999; Reiner 1992; Squires 1998). Under SC, police can be characterized as one of the primary consumers of a niche market of RT designed and produced by private technology corporations to collect mass volumes of information used to surveil populations in various contexts. Correspondingly, as

consumers, police services would be privy to typical marketing strategies that the average consumer of technology experiences. By tethering the identity of police as knowledge workers *and* consumers to the foundations of SC, we shift the focus towards understanding how police make decisions to acquire various types of RT. In doing so, the primary point of interest becomes the increasing institutional control that can play into decision-making processes, specifically the overall influence of private technology corporations. Explicitly, aggressive marketing tactics (Dencik, Hintz, and Carey 2018; Hood 2020; Sanders and Sheptycki 2017), market secrecy (Aguilar 2020; Goodfield 2020; Joh 2017; Sanders, Weston, and Schott 2015), and limited access to information (Tashea 2016; Joh 2017) have been highl ighted as influencing police decision-making processes.

As consumers, police services have become privy to private sector marketing. As it stands, a few scholars have noted the influence of aggressive marketing tactics used by private technology corporations on police services' decision-making (Dencik, Hintz, and Carey 2018; Hood 2020; Joh 2017; Sanders and Sheptycki 2017). For instance, within many of these contracts between police services and private surveillance corporations, police services can obtain the marketed product at a discounted rate on the condition that they take part in future marketing by providing testimonials and referrals to other agencies (Sanders and Sheptycki 2017). Additionally, scholars have uncovered instances of the private sector pressuring police services to sign no-bid contracts, thus establishing their monopolized presence in the industry (Joh 2017). Further, police services that invest in the technology can agree to host visiting agencies to demonstrate the "efficiency" of the technology. These marketing tactics can also take the form of joint press conferences between private corporations and police services, web marketing, trade shows, and speaking engagements. Collectively, these tactics and engagements are often used by corporations as evidence that their technology is efficient and effective for police usage, ultimately muddling the line between strategic marketing and empirical evidence (Sanders and Sheptycki 2017). Therefore, regardless of the quality, necessity, effectiveness, and efficiency of RT, market dominance by a handful of private technology corporations can persuade police services to continue with their products and services to avoid competitive bidding (Joh 2017).

Market secrecy has also been identified as a contributing influence on police services' decision-making. Specifically, as a layer of protection for their products, non-disclosure agreements (NDAs) are becoming increasingly common in the purchase of private RT by police services. Police services signing NDAs presented by private corporations are problematic for several reasons. Largely, the acquisition of new and potentially intrusive surveillance technologies can be kept secret from the public and excluded from any judicial authorization. Most notably, the undisclosed use of Stingrays by police organizations throughout the US has been identified as a violation of privacy rights and deemed comparable to a search without a warrant (Joh 2017). Similarly, a handful of Canadian police services have recently been criticized for their undisclosed use of Clearview AI, a facial recognition software that collects publicly accessible images of citizens without their consent (Aguilar 2020; Goodfield 2020; Office of the Privacy Commissioner of Canada 2020). Ultimately, this form of consumerism and layer of secrecy contradicts the amassed standards of transparency and accountability expected of the police and can subsequently result in significant harm to police imagery and public trust (Joh 2017; Sanders, Weston, and Schott 2015).

Blurred Boundaries

Second, we argue that macro-level factors directly influence public institutions through the blurring of public and private financial boundaries via surveillance activities and knowledge requests (Bowling, Reiner, and Sheptycki 2019; Ericson and Haggerty 1997; Robinson 2019; Zuboff 2015, 2019). As a result, police services are becoming increasingly embedded into the digital economy. By undertaking a macro-level theoretical approach to understanding police decision-making on RT, scholars have recently discussed the negative consequences that can accompany the blurring of boundaries between private technology companies and police services (Joh 2017; Robinson 2019). In doing so, it becomes clear that corporations that provide police with various RT can possess significant control over policing decisions and initiatives.

One notable method of control surrounds the storage and management of data by police services and private technology corporations (Brayne, Levy, and Newell 2018; Fan 2018; McNeal 2015; Rogers and Scally 2018. Alongside the introduction of emerging RT, police services were presented with the ability to record mass amounts of data instantaneously. For example, BWCs allow police personnel to record all their daily work, including all interactions with the public. As a result, mid-sized police services are likely to record approximately five to seven terabytes of data per month (Fan 2018; Joh 2016). Once this volume of data is created, it generates issues regarding where the data are stored, the associated costs of data management and storage, data retention procedures, and ownership of the data (Brayne, Levy, and Newell 2018; Fan 2018; White 2014). The successful adoption of RT hinge on the successful resolution of these data issues.

One solution typically offered by corporations is cloud-based digital evidence management systems (DEMS) provided to police services at an annual subscription cost (White 2014). For example, in hopes of increased service efficiency, several Canadian police services have opted to store their data through Axon's Evidence.com, a cloud-based DEMS that can store police data recorded through supporting RT. According to Axon (n.d.b), DEMS are more effective and efficient than traditional policing methods in terms of data access, sharing, and cost. However, recent evidence has demonstrated that DEMS can have severe financial and organizational constraints on police services (Brayne, Levy, and Newell 2018; Fan 2018; Hung, Babin, and Coberly 2016; Strom 2017; White 2014). Although a police department may also choose to store the data themselves, the current storage technologies used by police are not adequately equipped to handle such large quantities of visual data and supplementary information (Fan 2018). Additionally, departments that have decided to store the data internally have found that additional staff members were needed to manage the sheer amount of data being collected (Fan 2018). Thus, the acquisition of any data-heavy RT come with a host of issues that are not easily resolved and often require additional planning, subscriptions, and costs. With increasing calls to defund the police and for police to curtail spending, this raises questions about whether these RT investments are justified and can be maintained long-term.

For police services that decide to invest in DEMS, the decision to migrate to a new department-wide system has demonstrated to be much more expensive than originally anticipated (Brayne, Levy, and Newell 2018; Fan 2018; Strom 2017; White 2014). For example, US police services often reported the high initial costs of DEMS as being unreasonable (Strom 2017). Of the agencies that had the budget to implement RT and DEMS, there were several reports of hidden costs during or after the initial purchase. The unplanned costs of DEMS and supporting technologies can have significant impacts on the budget of a police service, which subsequently impacts the overall success of the technology's implementation. Although these services promise to increase efficiency and effectiveness, the demands of police services are constantly changing, and long-term contracts might make police services less nimble in responding to the public's needs. For example, Axon's Evidence.com price plan states that police services must subscribe to a minimum of a five-year contract to receive the optimal services of the software, which includes unlimited storage (Axon n.d.a). Presumably, police services would need to meet their contract obligations despite any funding cuts that might occur or would need to pay to adjust the parameters of their contract to address any public safety challenges that emerge during the timeframe of the contract.

The blurring of boundaries between private technology companies and police services also extends to who makes the decisions around data storage and management procedures (Hung, Babin, and Coberly 2016). For instance, according to Axon's Officer Safety Plan, to obtain unlimited data storage, police services must choose from a selection of plans starting at $99 USD per user per month (Axon n.d.b). Subscribing to a plan any lower than Axon's Officer Safety Plan results in severe restrictions on data storage and security, therefore exacerbating the issue of discretion surrounding data retention, as services are forced to either restrict how much data they collect or delete data that are already stored in the cloud. Further, in an examination of US police services' BWC policies, Fan (2018) reported little attention was being paid to data storage and management beyond its use in criminal prosecutions. Thus, data and video footage that might place police services in a bad light could be deleted under the guise of clearing up storage space.

Thus, the discretionary power that is afforded private technology companies and police services around the rules of RT adoption, as well as the data these RT produce, raises a host of ethical concerns (Newell and Greidanus 2018).

With increasing external demands for information generated from RT controlling a substantial portion of policing agendas (Ericson and Haggerty 1997), there is a need for effective data management and storage (Joh 2017). Ideally, effective data management and storage would ensure the security of confidential information, prevention of lost/misused data, high quality of data, and accessibility to data for authorized personnel. However, managing the sheer quantity of data associated with the adoption of RT while maintaining privacy, reliability, security, and accessibility is one of the biggest challenges for police services (Strom 2017). For instance, in an audit of the Los Angeles Police Department's use of automated license plate reader (ALPR) technology, three out of four precincts that used a cloud storage vendor to hold their data lacked contract guarantees that the vendor could appropriately protect the data (Howle 2020). These challenges are further complicated by the fact that private corporations frequently own the rights to the data collected and managed by DEMS and the supporting RT utilized by police services (Brayne, Levy, and Newell 2018; Joh 2017).

According to Brayne, Levy, and Newell (2018), permissive Freedom of Information Acts in certain US jurisdictions can be detrimental to people's privacy. That is, the data collection and storage of sensitive data by private technology corporations and police services run the risk of mass distribution after an individual has interacted with RT (Bennett Moses et al. 2022). For instance, in sensitive cases (e.g., domestic violence responses) where police services are required to wear BWCs, survivors run the risk of identification following a data breach/hack if those data were recorded and held by RT (Newell and Greidanus 2018). Similarly, Dryer and Stroud (2015) highlight the secondary use of police data collected via RT as an issue. Specifically, the simultaneous increase in public and private sector databases alongside the increased use of ALPR by police services raises data surveillance, privacy, and access concerns as license plate information is frequently retained and stored regardless of whether a hit is present. Ultimately, the quick adoption of RT by police services has resulted in very few guidelines regarding safeguards against discriminatory and other rights-violating uses of data, data protection obligations, ownership, and accessibility (boyd and Crawford 2012; Joh 2017).

Private corporations have had a large influence not only on the RT adopted by police but also on the decision-making around the data produced by these RT. Recently, some contracts between private technology corporations and police organizations have given private technology corporations the ownership rights to all data that are collected and stored using their technology. For instance, ShotSpotter (a gunshot location software) demands ownership over all the information collected by police organizations that use their technology. Subsequently, when police wish to share this information, there is the possibility that they will be unable to, or that there will be a fee associated with retrieval (Tashea 2016). According to Joh (2017), this has left police organizations confused as to what information they own and what degree of control they have over the data produced by the RT they purchased. Further, restrictions on the accessibility of data have only come to light after contracts between private technology vendors and police organizations have terminated (Joh 2017). Most notably, there have been reports of vendors returning data to police services in encrypted forms without proper decoding materials after the completion of contractual obligations (Alden 2017). Collectively, these concerns point to the potential influence of private technology corporations on police services' acquisition of RT.

Conclusions and Future Directions

Overall, understandings of how police make decisions regarding which RT to adopt are scarce. Organizational models have attempted to further our understandings by asserting that police make decisions through logical means (i.e., DOI and the behavioural theory of the firm) or through none at all (e.g., the

garbage can model of organizational choice). While these theories offer important insights, they have not been able to account for how different types of technologies get adopted in different ways and for varying reasons across police services. Also, these meso-level approaches appear inadequate for explaining how external influences, such as technology corporations, impact police decision-making on RT acquisition. Therefore, developing a more comprehensive and macro-level approach is paramount.

In this article, we have argued that combining key elements of PRS and SC provide a macro-level theoretical framework that can help explain the larger context in which police adopt RT. These two macro-level approaches help to define the role of the police, their intended uses of RT, and the role they play as consumers in the private sector. The increasing pressure to fulfill knowledge demands from external institutions and the "collect all data mantra" that has become embedded within modern police practices illustrate how macro-level factors (e.g., economics, risk, digital innovation, surveillance capitalism, politics) play a role in police decisions about RT. Although we have only begun to examine these macro-impacts, through the lens of PRS and SC theorizing it has been illustrated that resources, marketing tactics/secrecy, data access, data ownership, hidden costs, and data retention have all been identified as harnessing the potential to influence police decision-making regarding the acquisition of RT. It would also be fruitful to explore how PRS and SC intersect with the pluralization of policing (Bowling, Reiner, and Sheptycki 2019). Without the acknowledgement of these macro-level factors, it is difficult to properly assess the applicability, efficiency, and effectiveness of RT for police services.

With that said, more empirical research is required to assess the utility of the proposed theoretical framework provided in this article. Therefore, this paper recommends additional macro-level theorizing, particularly expanding the combined PRS and SC framework and examining if it is supported by empirical research. Additionally, future research should focus on an array of influences (e.g., corporate involvement, effectiveness, efficiency) that could impact the decision-making stages of the acquisition of RT by police services. More research needs to explore how police make decisions about which technologies to acquire, the impacts of acquiring and implementing technologies on police personnel, what technologies are efficient and effective to use and to what ends, and how police services can best acquire and implement new technologies to meet their technological needs and mission goals. While we narrowly examined some of the organizational theories associated with technological *acquisition* by police, future theorizing and research should examine the wealth of tangentially related literature on police technology *use* (Bowling, Reiner, and Sheptycki 2019) and how it is applicable to the PRS and SC frameworks discussed in this paper. That is, there are many reasons police acquire technologies beyond the ones we explicitly focused on. Ultimately, additional research and theorizing on police technology acquisition can help police navigate the increasingly complex nature of contemporary policing and the involvement of privately-owned RT and their associated companies that have an ever-increasing presence in shaping people's day-to-day lives. Shining a light on these influences on police decision-making could also help to develop better oversight for the acquisition of RT.

References

Aguilar, Bryann. 2020. OPP Admit to Using Controversial Facial Recognition Software Clearview AI. CTV News, March 1. https://toronto.ctvnews.ca/opp-admit-to-using-controversial-facial-recognition-software-clearview-ai-1.4834043 [accessed January 23, 2021].

Alden, William. 2017. There's A Fight Brewing Between the NYPD And Silicon Valley. Buzzfeed News, June 28. https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley [accessed January 25, 2021].

Axon. N.d. Axon Evidence. https://www.axon.com/products/axon-evidence [accessed November 12, 2024].

———. N.d. Evidence.com Plans. https://prismic-io.s3.amazonaws.com/tasr/84ab50c9-f70e-4481-aef8-23caa6155437_axon+evidence.com+plans.pdf [accessed January 21, 2022].

Bayerl, P. Saskia, Gabriele Jacobs, Sebastian Denef, Roelof J. van den Berg, Nico Kaptein, Kamal Birdi, Fabio Bisogni, et al. 2013. The Role of Macro Context for the Link Between Technological and Organizational Change. *Journal of Organizational Change Management* 26 (5): 793–810.

Bedford, Laura, and Peter Neyroud. 2021. Organizational Learning from Field Research in Policing: How Police Can Improve Policy and Practice by Implementing Randomized Controlled Trials. In *Enhancing Police Service Delivery: Global Perspectives and Contemporary Policy Implications,* edited by James F. Albrecht and Garth den Heyer, 359–377. Cham, CH: Springer.

Bennett Moses, Lyria, Jan Breckenridge, Joshua Gibson, and Georgia Lyons. 2022. Technology-Facilitated Domestic and Family Violence: Protecting the Privacy and Safety of Victim-Survivors. *Law, Technology and Humans* 4 (1): 1–17.

Berk, Richard A. 2021. Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement. *Annual Review of Criminology* 4 (1): 209–237.

Bowling, Benjamin, Robert Reiner, and James WE Sheptycki. 2019. *The Politics of the Police*. Oxford, UK: Oxford University Press.

boyd, Danah, and Kate Crawford. 2012. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication & Society* 15 (5): 662–679.

Brayne, Sarah. 2017. Big Data Surveillance: The Case of Policing. *American Sociological Review* 82 (5): 977–1008.

Brayne, Sarah, Karen Levy, and Bryce Clayton Newell. 2018. Visual Data and the Law. *Law & Social Inquiry* 43 (4): 1149–1163.

Browne, Rachel. 2020. Toronto Police Service Confirms some Members tested Clearview AI's Controversial Facial Recognition Tool. Global News, February 13. https://globalnews.ca/news/6547256/toronto-police-service-confirms-some-members-tested-clearview-ais-controversial-facial-recognition-tool/ [accessed March 10, 2023].

Burcher, Morgan, and Chad Whelan. 2018. Intelligence-led Policing in Practice: Reflections from Intelligence Analysts. *Police Quarterly* 22 (2): 139–160.

Chan, Janet B. L. 2001. The Technological Game: How Information Technology Is Transforming Police Practice. *Criminal Justice* 1 (2): 139–159.

Cohen, Michael D., James G. March, and Johan P. Olsen. 1972. A Garbage Can Model of Organizational Choice. *Administrative Science Quarterly* 17 (1): 1–25.

Cyert, Richard M., and James G. March. 1963. *A Behavioral Theory of the Firm*. Englewood Cliffs, NJ: Prentice-Hall.

Davis, Oliver. 2019. Theorizing the Advent of Weaponized Drones as Techniques of Domestic Paramilitary Policing. *Security Dialogue* 50 (4): 344–360.

Dekker, Rianne, Puck van den Brink, and Albert Meijer. 2020. Social Media Adoption in the Police: Barriers and Strategies. *Government Information Quarterly* 37 (2): https://doi.org/10.1016/j.giq.2019.101441.

DiMaggio, Paul J., and Walter W. Powell. 1983. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review* 48 (2): 147–160.

Dencik, Lina, Arne Hintz, and Zoe Carey. 2018. Prediction, Pre-emption and Limits to Dissent: Social Media and Big Data Uses for Policing Protests in the United Kingdom. *New Media & Society* 20 (4): 1433–1450.

Dryer, Randy L., and S. Shane Stroud. 2015. Automatic License Plate Readers: An Effective Law Enforcement Tool or Big Brother's Latest Instrument of Mass Surveillance? Some Suggestions for Legislative Action. *Jurimetrics Journal of Law, Science and Technology* 55 (2): 225–274.

Egbert, Simon, and Matthias Leese. 2021. *Criminal Futures: Predictive Policing and Everyday Police Work*. New York: Routledge.

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

Fan, Mary D. 2018. Body Cameras, Big Data, and Police Accountability. *Law & Social Inquiry* 43 (4): 1236–1256.

Ferguson, Andrew Guthrie. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Gates, Kelly. 2019. Policing as Digital Platform. *Surveillance & Society* 17 (1/2): 63–68.

Goodfield, Kayla. 2020. Canadian Privacy Officials Will Investigate Controversial Facial Recognition Tool Used by Toronto Police. CTV News, February 21. https://toronto.ctvnews.ca/canadian-privacy-officials-will-investigate-controversial-facial-recognition-tool-used-by-toronto-police-1.4822198#:~:text=The%20investigation_%20into%20Clearview%20AI,Privacy%20Commissioner%20of%20Canada%20said [accessed February 1, 2021].

Greene, Jack R. 2014. New Directions in Policing: Balancing Prediction and Meaning in Police Research. *Justice Quarterly* 31 (2): 193–228.

Hälterlein, Jens. 2021. Epistemologies of Predictive Policing: Mathematical Social Science, Social Physics and Machine Learning. *Big Data & Society* 8 (1): 1–13.

Hannem, Stacey, Aaron Doyle, Christopher J. Schneider, and Carrie B. Sanders. 2019. Introduction. In *Security and Risk Technologies in Criminal Justice: Critical Perspectives*, edited by Stacey Hannem, Carrie B. Sanders, Christopher J. Schneider, Aaron Doyle, and Tony Christensen, 19–34. Toronto, CA: Canadian Scholars.

Haskins, Paul A., and Brett Chapman. 2018. *Harmonizing Police Technology Acquisitions with Policing Strategy*. Washington, DC: US National Institute of Justice.

Hendrix, Joshua A., Travis Taniguchi, Kevin J. Strom, Brian Aagaard, and Nicole Johnson. 2019. Strategic Policing Philosophy and the Acquisition of Technology: Findings from a Nationally Representative Survey of Law Enforcement. *Policing and Society* 29 (6): 727–743.

Hill, Dallas, Christopher D. O'Connor, and Andrea Slane. 2022. Police Use of Facial Recognition Technology: The Potential for Engaging the Public through Co-constructed Policy-Making. *International Journal of Police Science & Management* 24 (3): 325–335.

Hood, Jacob. 2020. Making the Body Electric: The Politics of Body-Worn Cameras and Facial Recognition in the United States. *Surveillance & Society* 18 (2): 157–169.

Howle, Elaine M. 2020. *Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement must Increase its Safeguards for the Data it Collects.* Report No. 2019-118. Auditor of the State of California, February 13. https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf [accessed March 13, 2022].

Hung, Vivian, Steven Babin, and Jacqueline Coberly. 2016. *A Market Survey on Body Worn Camera Technologies*. Washington, DC: US Department of Justice.

Jennings, Wesley G., Mathew D. Lynch, and Lorie A. Fridell. 2015. Evaluating the Impact of Police Officer Body-Worn Cameras (BWC) on Response-to-Resistance and Serious External Complaints: Evidence from the Orlando Police Department (OPD) Experience Utilizing a Randomized Controlled Experiment. *Journal of Criminal Justice* 43 (6): 480–486.

Joh, Elizabeth. 2016. Beyond Surveillance: Data Control and Body Cameras. *Surveillance & Society* 14 (1): 133–137.

———. 2017. The Undue Influence of Surveillance Companies on Policing. *New York University Law Review* 92: 101–130.

Koper, Christopher S., Cynthia Lum, and Julie Hibdon. 2015. The Uses and Impacts of Mobile Computing Technology in Hot Spots Policing. *Evaluation Review* 39 (6): 587–624.

Lawrence, Paul R., and Jay W. Lorsch. 1967. Differentiation and Integration in Complex Organizations. *Administrative Science Quarterly* 12 (1): 1–7.

Loader, Ian. 1999. Consumer Culture and the Commodification of Policing and Security. *Sociology* 33 (2): 373–392.

Manning, Peter K. 1977. *Police Work: The Social Organization of Policing.* Cambridge, MA: MIT Press.

———. 1992. Information Technologies and the Police. *Crime and Justice* 15: 349–398.

———. 2001. Theorizing Policing: The Drama and Myth of Crime Control in the NYPD. *Theoretical Criminology* 5 (3): 315–344.

McNeal, Gregory S. 2015. Government-operated Drones and Data Retention. *Washington & Lee Law Review* 72 (3): 1139–1159.

Merola, Linda M., Cynthia Lum, and Ryan P. Murphy. 2019. The Impact of License Plate Recognition Technology (LPR) on Trust in Law Enforcement: A Survey-Experiment. *Journal of Experimental Criminology* 15 (1): 55–66.

Nesterova, Irena. 2020. Mass Data Gathering and Surveillance: The Fight against Facial Recognition Technology in the Globalized World. *SHS Web of Conferences* 74: https://doi.org/10.1051/shsconf/20207403006.

Newell, Bryce Clayton, and Ruben Greidanus. 2018. Officer Discretion and the Choice to Record: Officer Attitudes Towards Body-Worn Camera Activation. *North Carolina Law Review* 96 (5): 1525–1578.

O'Connor, Christopher D., John Ng, Dallas Hill, and Tyler Frederick. 2022. Police Analysts on the Job in Canada: Work Experiences, Data Work, and the Move Towards Evidence-Based Policing. *Police Practice & Research* 23 (4): 458–472.

O'Connor, Christopher D., and Phillip C. Shon. 2019. Civilising the Police: Reconceptualising the Role of the State in Theories of American Policing. *Global Crime* 20 (1): 45–64.

Office of the Privacy Commissioner of Canada. 2020. OPC Launches Investigation into RCMP's Use of Facial Recognition Technology. February 28. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200228/ [accessed March 13, 2021].

Ozer, Murat. 2016. Automatic Licence Plate Reader (ALPR) Technology: Is ALPR a Smart Choice in Policing? *The Police Journal* 89 (2): 117–132.

Pasha, Obed. 2019. Does Substandard Performance Encourage Innovation Adoption? *American Review of Public Administration* 49 (5): 572–584.

Piza, Eric L., and Brian A. O'Hara. 2014. Saturation Foot-Patrol in a High-Violence Area: A Quasi Experimental Evaluation. *Justice Quarterly* 31 (4): 693–718.

Reiner, Robert. 1992. Police Research in the United Kingdom: A Critical Review. *Crime and Justice* 15: 435–508.

Robinson, William I. 2019. Accumulation Crisis and Global Police State. *Critical Sociology* 45 (6): 845–858.

Rogers, Everett M. 1962. *Diffusion of Innovations*. 1st edition. New York: Free Press.

———. 2003. *Diffusion of Innovations.* 5th edition. New York: Free Press.

Rogers, Colin, and Emily Jayne Scally. 2018. Police Use of Technology: Insights from the Literature. *International Journal of Emergency Services* 7 (2): 100–110.

Sanders, Carrie B., and James Sheptycki. 2017. Policing, Crime and "Big Data"; Towards a Critique of the Moral Economy of Stochastic Governance. *Crime, Law and Social Change* 68 (1–2): 1–15.

Sanders, Carrie B., Crystal Weston, and Nicole Schott. 2015. Police Innovations, "Secret Squirrels" and Accountability: Empirically Studying Intelligence-led Policing in Canada. *The British Journal of Criminology* 55 (4): 711–729.

Sheptycki, James. 2013. To Go Beyond the Cycle of Intelligence-led Policing. In *Understanding the Intelligence Cycle*, edited by Mark Phythian, 99–118. New York: Routledge.

———. 2017. The Police Intelligence Division-of-Labour. *Policing and Society* 27 (6): 620–635.

———. 2019. The Police Intelligence Division-of-Labour. In *Policing Across Organisational Boundaries*, edited by Benoit Dupont, Chad Whelan, and Peter K. Manning, 39–54. New York: Routledge.

———. 2020. Liquid Modernity and the Police Métier; Thinking about Information Flows in Police Organisation. In *The Policing of Flows*, edited by Anthony Amicelle, Karine Cote-Boucher, Benoit Dupont, Massimiliano Mulone, Clifford Shearing, and Samuel Tanner, 122–138. New York: Routledge.

Skogan, Wesley G., and Susan M. Hartnett. 2005. The Diffusion of Information Technology in Policing. *Police Practice and Research* 6 (5): 401–417.

Squires, Peter. 1998. Cops and Customers: Consumerism and the Demand for Police Services. Is the Customer Always Right? *Policing and Society: An International Journal* 8 (2): 169–188.

Strom, Kevin. 2017. *Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report*. Washington, DC: US Department of Justice.

Tashea, Jason. 2016. Should the Public Have Access to Data Police Acquire through Private Companies? *ABA Journal,* December 1. https://www.abajournal.com/magazine/article/public_access_police_data_private_company [accessed February 12, 2021].

Terpstra, Jan, Nicholas R. Fyfe, and Renze Salet. 2019. The Abstract Police: A Conceptual Exploration of Unintended Changes of Police Organizations. *The Police Journal: Theory, Practice and Principles* 92 (4): 339–359.

Walsh, James P., and Christopher O'Connor. 2019. Social Media and Policing: A Review of Recent Research. *Sociology Compass* 13 (1): https://doi.org/10.1111/soc4.12648.

Weisburd, David, and Cynthia Lum. 2005. The Diffusion of Computerized Crime Mapping in Policing: Linking Research and Practice. *Police Practice and Research* 6 (5): 419–434.

Weisburd, David, and Peter Neyroud. 2011. Police Science: Toward a New Paradigm. *New Perspectives in Policing*, January. Washington, DC: National Institute of Justice and Harvard Kennedy School.

Weisburd, David, Anthony Petrosino, and Cynthia M. Lum. 2003. *Assessing Systematic Evidence in Crime and Justice: Methodological Concerns and Empirical Outcomes*. Thousand Oaks, CA: Sage.

White, Michael D. 2014. *Police Officer Body-Worn Cameras: Assessing the Evidence*. Washington, DC: Office of Community Oriented Policing Services.

White, Michael D., and Aili Malm. 2020. *Cops, Cameras, and Crisis: The Potential and the Perils of Police Body-Worn Cameras*. New York: New York University Press.

Willis, James J., Stephen D. Mastrofski, and David Weisburd. 2007. Making Sense of COMPSTAT: A Theory-based Analysis of Organizational Change in Three Police Departments. *Law & Society Review* 41 (1): 147–188.

Zedner, Lucia. 2007. Pre-Crime and Post-Criminology? *Theoretical Criminology* 11 (2): 261–281.

Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75–89.

———. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.