ORIGINAL RESEARCH ARTICLE

Police Investigations in Smart Cities: Personal Information and Policy Implications

Étienne F Lacombe*

Abstract: Smart cities have the potential to disrupt the relationship between privacy and policing by providing police officers with new sources of personal information. This article challenges recent literature that suggests this risk should be mitigated through judicial oversight. Viewed holistically, the varying severity of privacy intrusions in smart cities, the technical workings of information collection and processing, and fading logistical limits on public surveillance make reliance on judicial oversight untenable. Instead, this article suggests ways of reshaping extrajudicial safeguards to prevent arbitrary or abusive interference with privacy in the context of smart cities. Building on examples from England and Wales, the author draws on a version of privacy protection that often escapes North American commentators. Ultimately, the author calls on provincial legislatures to develop statutory parameters for the exercise of police discretion that are tailored to various smart city technologies and suggests how oversight should be embedded within policing bodies, both at the structural and individual decision-making level.

Creative Commons License

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License.

* BCL, LLB, LLM.

CONTENTS

Introduction

By 2041, the municipality of Techtown had proudly branded itself a "smart city". It invested heavily in technological initiatives, outfitting its neighbourhoods with sensors and equipping its citizens with data-gathering devices. Techtown's streets are embedded with technologies that capture residents' movements, and residents use their devices to report what they see around them. Collectively, this arrangement exposes information that was always in plain sight, but that was never comprehensively collected or analyzed. It allows for more information on what occurs in public to be captured, and for more facts that may individually reveal very little to be recorded and combined so as to paint a clearer picture of the city as a whole. Among its many uses, the information can be harnessed to complement traditional intelligence-gathering. Faced with this prospect, one question that leaders in Techtown and beyond must address is how to regulate police access to the smart city's valuable, yet potentially intrusive, information collected in the smart city.

By focusing on smart cities, this article presents an evocative example of a wider privacy protection issue. Many technologies already generate retrievable data about individuals, such as their online activity and physical movements. Focusing on smart cities shows that the amount of data being recorded in urban environments will only increase, and accentuates the need to review how modern privacy-infringing investigations are regulated.

This article complements recent literature that suggests the privacy issues smart city policing raises can be addressed through judicial oversight. It emphasizes the need to reshape proactive nonjudicial safeguards within policing bodies and calls on provincial legislatures to lead this reform. Although the label "smart city" could be applied to some contemporary urban environments, this article's focus is forward-looking and contemplates a horizon of about 20 years. A 20-year timeframe exposes the increasing strain under which existing police oversight might be placed as emerging technologies become mainstream. It also avoids looking so far ahead as to speculate about the future of sensor integration and technological development.

Building on examples from the fictional city of Techtown, this article proceeds in three parts. Part I situates the concept of privacy in relation to policing and outlines why the law has long sought to reconcile the protection of personal information with policing powers. It argues that smart cities disrupt the relation between policing and privacy by providing police with a new source of personal information. Part II addresses the promotion by some authors of judicial interpretation and court-based oversight to regulate smart city policing. The severity of privacy infringements caused by information collection and processing in smart cities will vary considerably. Expanding current privacy protections through judicial interpretation would not be responsive to this reality, and greater technical specialization than that which judicial oversight can offer will be required. These concerns, combined with fading logistical limits on the monitoring of public spaces, underscore the need for new forms of oversight, particularly in cases where police behaviour is neither subject to prior judicial authorization nor to post-hoc scrutiny. Part III sketches how some of those reforms may look by drawing on the influence European privacy protections have had in England and Wales. Ultimately, it calls on provincial legislatures to develop statutory parameters for the exercise of police discretion that are tailored to various smart city technologies, and suggests how oversight should be embedded within policing bodies, both at the structural and individual decision-making levels.

I. Situating Smart Cities and Their Privacy Implications

Considered in the abstract, "privacy" and "smart city" are elusive concepts. Both serve as shorthand in such disparate settings as to deprive them of a shared, universal meaning. Referring to privacy, Thomas McCarthy explains, is akin to invoking freedom: "it means so many different things to

so many different people that it has lost any precise legal connotation."[1] The expression "smart city" is similarly dynamic. Its intended meaning varies between authors and disciplines, generating inconsistencies across the literature.[2]

Accordingly, there is value in approaching privacy and smart cities contextually. Situating them within the context to which they are being applied—here, policing—is instrumental to elucidating each concept's meaning and significance. Beyond narrowing what is understood by each term, juxtaposing privacy, smart cities and policing sheds light on their interconnectedness. Explained differently, approaching privacy, smart cities, and policing relationally reveals how developments in one field often provoke changes in the others.

1. Privacy in the Policing Context

Turning first to privacy, this concept can be contextualized by identifying specific interferences with daily life. In his influential work on privacy contextualization, Daniel Solove explains that privacy "enables people to engage in worthwhile activities in ways they would otherwise find difficult or impossible."[3] As a consequence, privacy concerns arise when certain practices—"activities, customs, norms and traditions"—are disrupted.[4] The nature of these disruptions and the means of addressing them vary from one setting to another. Situating privacy in relation to a given context therefore entails "focusing on the specific types of disruption and the specific practices disrupted."[5]

In the policing context, focusing on specific disruptions and practices invites attention to the functions police perform and the civilian practices those functions disrupt. Of the many functions in which police engage, the theme of this article centres on investigations. Police investigations involve "the process of discovering, collecting, preparing, identifying and presenting evidence to determine what happened and who is responsible."[6] Returning to the language proposed by Solove, and as

1. J Thomas McCarthy, *The Rights of Publicity and Privacy*, 2d ed (New York: Clark Boardman Callaghan, 2015) at § 5.59. See also Julie C Inness, *Privacy, Intimacy, and Isolation* (Oxford: Oxford University Press, 1996) at 3 (describing the search for privacy's meaning as chaotic).
2. Victoria Fernandez-Anez, "Stakeholders Approach to Smart Cities: A Survey on Smart City Definitions" in Enrique Alba, Francisco Chicano & Gabriel Luque, eds, *Smart Cities: Proceedings of the First International Conference, Smart-CT 2016, Málaga, Spain, June 15-17, 2016* (Cham, Switzerland: Springer, 2016) 157-168; Arkalgud Ramaprasad, Aurora Sánchez-Ortiz & Thant Syn, "A Unified Definition of a Smart City" in Marijn Janssen et al, eds, *Electronic Government: Proceedings of the 16th IFIP WG 8.5 International Conference, EGOV 2017, St. Petersburg, Russia, September 4-7, 2017* (Cham, Switzerland: Springer, 2017) 13 at 15, 21; Vito Albino, Umberto Berardi, & Rosa Maria Dangelico, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives" (2015) 22:1 J Urban Technology 3 at 4.
3. Daniel J Solove, "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477 at 484.
4. Daniel J Solove, "Contextualizing Privacy" (2002) 90 Cal L Rev 1087 at 1129.
5. *Ibid* at 1130.
6. Kären M Hess, Christine Hess Orthmann & Henry Lim Cho, *Criminal Investigation*, 11th ed (Boston: Nelson Education, 2017) at 8.

the following pages will explain, investigating may produce at least two types of disruption. Police may disrupt civilian practices through *information collection*, which includes conducting surveillance and acquiring records, and through *information processing*, such as the retention and aggregation of data.[7]

The first type of police disruption, information collection, can interfere with a number of practices. Given this article's focus on establishing responsive safeguards, it is noteworthy that many such disruptions are not overseen by courts as they do not require prior judicial authorization and, unless they result in a charge or a complaint, they are not reviewed after the fact. Street checks are a contemporary example of how police information collection can interfere with civilian practices. A street check occurs when police record personal information about a civilian in public so that it can be stored in a law enforcement database.[8] Officers complete a check to gather information of intelligence value, such as suspicious behaviour, or a known offender's location or association. While often associated with stopping individuals in public, street checks include logging information from visual observations of civilians without direct contact.[9] Regardless of whether charges ensue from a street check, this type of information collection by police raises important privacy considerations.

Broadly speaking, knowing that one may be observed, or that personal information may be retrieved, produces a chilling effect. It pushes the person to act in accordance with how their behaviour will be perceived.[10] While this controlling effect may be beneficial—perhaps even desirable—for law enforcement, it jeopardizes certain societal norms and activities. Most evidently, information collection interferes with individuals' interest in being left alone.[11] As Julie Cohen explains, "respite from visual scrutiny affords individuals an important measure of psychological repose [since] we are accustomed to physical spaces within which we can be unobserved, and intrusion into those spaces is experienced as violating the boundaries of self."[12] At a minimum, information collection by police may disturb our sense of wellbeing.

Aside from interfering with an interest in being left alone, information collection by police also poses a threat to personal and interpersonal development. Because surveillance acts as a form of control by discouraging unconventional behaviour, the amount of surveillance that a person experiences influences whether and how they express their identity. When surveillance becomes

7. Solove, "A Taxonomy of Privacy", *supra* note 3 at 489.

8. Ruth Montgomery et al, *Vancouver Police Board Street Check Review* (Vancouver: Vancouver Police Board, 2019), online (pdf): BCCLA <bccla.org/wp-content/uploads/2020/02/VPD-Street-Checks-Final-Report-17-Dec-2019.pdf> at 127.

9. Scot Wortley, *Halifax, Nova Scotia: Street Checks Report* (Halifax: Nova Scotia Human Rights Commission, 2019), online (pdf): <humanrights.novascotia.ca/sites/default/files/editor-uploads/halifax_street_checks_report_march_2019_0.pdf> at 101-102.

10. Robert S Gerstein, "Intimacy and Privacy" (1978) 89:1 Ethics 76 at 78.

11. Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harv L Rev 193 at 193.

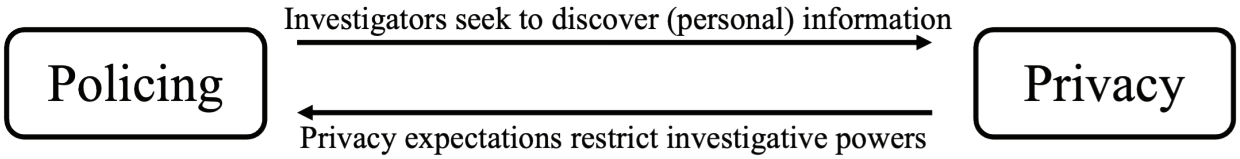
12. Julie E Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52:5 Stan L Rev 1373 at 1425.

perpetual, it risks "corrupting" a person's choices about which aspects of their identity they develop.[13] Similarly, pervasive surveillance may disrupt interpersonal development. Intimate relationships, which involve exclusive sharing between participants, simply cannot exist when information is susceptible to interception.[14] Ordinary social relationships also cannot be formed or maintained absent a level of concealment and discretion.[15] Beyond a certain threshold, information collection limits personal and social development.

The second type of police disruption, information processing, is a more novel form of interference. It can be traced to the proliferation of computers, which record and store an ever-greater assortment of information. The availability of these records, combined with the computing power to process them, has enabled law enforcement to move investigations beyond the simple observation and acquisition of information, and toward the creation of new data.[16] Increasingly, police have the means to combine and analyze seemingly trivial data to discover information that the data, individually, did not reveal. This ability interferes with the structural norms of society by upsetting the balance of power between citizens and the authorities and granting additional power over individuals.[17]

This overview of police functions, and the civilian practices they disrupt, helps shed light on the meaning of privacy in the policing context, as well as the effect of privacy on policing itself. Privacy, in relation to policing, is concerned with interferences at the individual and societal levels. In addition to disrupting personal freedom and individuals' interest in being left alone, police investigations may impact the way members of society build bonds with one another. Owing to the gravity of these possible disruptions, the desirability of controlling certain police practices has long been recognized. Figure 1 begins to explain how policing and privacy influence one another.

Figure 1



Because police investigations serve an important purpose but also risk interfering with valuable privacy interests, there has long been a need to reconcile this tension. This need is etched into the law itself. For instance, the right to be secure against unreasonable search or seizure under s 8

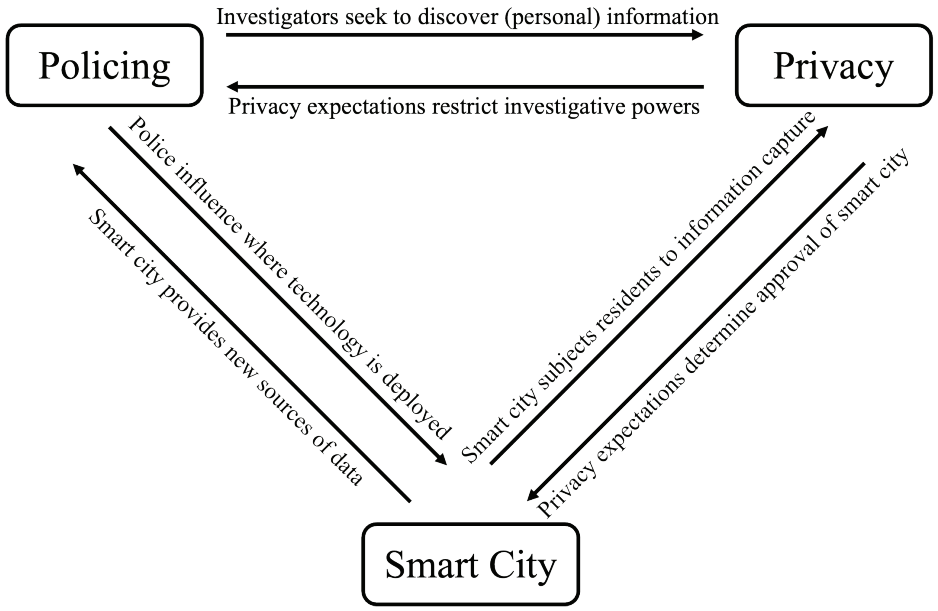
13. Paul M Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52:6 Vand L Rev 1607 at 1657, 1665.
14. Gerstein, *supra* note 10 at 76.
15. Debbie VS Kasper, "Privacy as a Social Good" (2007) 28 Social Thought & Research 165 at 175.
16. Orin S Kerr, "Use Restrictions and the Future of Surveillance Law", *The Future of the Constitution* (19 April 2011), online (pdf): The Brookings Institution <brookings.edu/wp-content/uploads/2016/06/0419_surveillance_law_kerr.pdf> at 3-4.
17. Solove, "A Taxonomy of Privacy", *supra* note 3 at 507-08.

of the *Charter of Rights and Freedoms*[18] reflects the interrelation depicted in Figure 1. It restricts investigative powers by controlling disruptive police practices, and it permits such disruptions when the investigation offers a sufficiently compelling reason to tolerate them.[19]

2. Smart Cities as a Disruptive Force

Given the law's concern for reconciling policing and privacy, it must remain attuned to developments in either field. When technology changes the nature of policing or of privacy concerns, how the law manages the interaction between these two concepts must be reassessed. As Figure 2 illustrates, smart cities trigger the need for such a reassessment by affecting both how investigations may be conducted and how privacy may be engaged.

Figure 2



In terms of their effect on investigations, smart cities have the potential to supply police with unprecedented amounts of information. Because they feature large networks of interconnected technologies with sensing capabilities, the extent to which smart cities monitor and record urban environments is without parallel. Added to these sensor networks are means of harnessing insights at the grassroots level by tasking citizens with data collection responsibilities.[20]

18. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s 8.

19. By its very wording, s 8 of the *Charter* guards against privacy intrusions by prohibiting unreasonable searches, thus tolerating *reasonable* police searches, be they disruptive or not.

20. Oliver Gassmann, Jonas Böhm & Maximilian Palmié, *Smart Cities: Introducing Digital Innovation to Cities* (Bingley, UK: Emerald Publishing, 2019) at 28.

As regards sensing technologies, smart cities will likely feature devices that exist in a more or less developed form today. Concretely, these might include closed-circuit television (CCTV) with facial recognition capabilities, automating recognition of individuals as they move about the city.[21] Increased smart card integration through the deployment of card readers—a common feature of smart cities—may serve as a further source of information. By logging data such as cashless transactions and public transport use, smart cards and their networks will record details of users' mobility and habits and may reveal links between users when this data is correlated.[22] Even the growth of public Wi-Fi infrastructure holds the potential to make information on individuals' movements available, by logging which devices enter a given coverage area and when.[23] While much of this equipment is not entirely novel, privacy concerns will be amplified once such technologies are thoroughly interconnected.[24]

Smart city networks are also likely to capture information from technology that is currently in its infancy. Intelligent vehicles are an example of devices whose widescale deployment could generate new forms of data. In order to facilitate autonomous driving, intelligent vehicles must transmit their location to nearby cars and to traffic lights and other nodes making up the smart city infrastructure.[25] The vehicle's identifier, location, direction and speed must be broadcast in unencrypted form to be intelligible to others in the area.[26] With the right equipment, these unencrypted broadcasts create an opportunity to record vehicular movement within a smart city with great precision.[27] It is even conceivable that as autonomous vehicles become mainstream, governments will require that they report their location to a central oversight body to ensure road safety.[28]

21. Lisbet van Zoonen, "Privacy Concerns in Smart Cities" (2016) 33:3 Gov Inf Q 472 at 475.
22. Gassmann, Böhm & Palmié, *supra* note 20 at 43; David Eckhoff & Isabel Wagner, "Privacy in the Smart City—Applications, Technologies, Challenges and Solutions" (2017) 20:1 IEEE Communications Surveys & Tutorials 489 at 492, 502; Daniel Belanche-Gracia, Luis V Casal -Ariño & Alfredo Pérez-Rueda, "Determinants of Multi-Service Smartcard Success for Smart Cities Development: A Study Based on Citizens' Privacy and Security Perceptions" (2015) 32:2 Gov Inf Q 154 at 154.
23. Maša Galič, *Surveillance and Privacy in Smart Cities and Living Labs: Conceptualising Privacy for Public Space* (PhD Dissertation, Tilburg University, 2019) at 80 [unpublished].
24. Trevor Braun et al, "Security and Privacy Challenges in Smart Cities" (2018) 39 Sustainable Cities and Society 499 at 500.
25. Eckhoff & Wagner, *supra* note 22 at 493, 507.
26. *Ibid* at 507.
27. For a contemporary example of traffic management technology being repurposed to record movement, consider reports of New York City E-ZPasses being read throughout the city instead of only at toll booths: Kelsey Finch & Omer Tene, "Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town" (2016) 41:5 Fordham Urb LJ 1581 at 1598.
28. Ric Simmons, "The Mirage of Use Restrictions" (2017) 96 NCL Rev 133 at 144.

As for examples of information generated through citizen participation, smart cities encourage residents to download data-gathering applications on their mobile devices. Applications enable residents to report street litter or road defects by uploading pictures of issues they discover.[29] Potholes, for example, can be detected by retrieving a phone's GPS and accelerometer data.[30] The data generated by this mode of citizen participation, however, often contains personal information in the form of metadata that users may not intend to share or even be aware is being transmitted.[31] Left unchecked, this source of data, independently or in combination with the sensor technologies mentioned above, is capable of providing police with new forms of information.[32]

While most of these smart city technologies are not geared toward crime detection or surveillance, the data they collect may serve that purpose. This is because policing, like operating a smart city, relies on the collection and analysis of information. Kaja Prislan and Boštjan Slak identify a "natural symbiosis" between smart cities and criminal investigations owing to the shared goals of gathering facts, reconstructing what has occurred, and acting accordingly.[33] Based on these overlapping functions, Elizabeth Joh goes so far as to conclude that policing is embedded into smart city infrastructure and therefore inherent to smart cities.[34] In some cases, there can even be a form of feedback between policing and smart cities given that police may influence which smart city technologies are deployed and where.[35]

As with policing, privacy is at once impacted by, and influential on, smart cities. Notably, smart cities accentuate the loss of "privacy in public" by reducing the possibility of finding reprieve from observation in communal spaces.[36] Traditionally, being observable in public entailed little risk of being observed, at least in an intrusive fashion. If an individual was noticed at all, the person making the observation could only see and retain disparate fragments of information. As Jeffrey Reiman summarized before the turn of the century, "privacy results not only from locked doors and closed

29. Sunil Choenni et al, "Privacy and Security in Smart Data Collection by Citizens" in J Ramon Gil-Garcia, Theresa A Pardo & Taewoo Nam, eds, *Smarter as the New Urban Agenda: A Comprehensive View of the 21st Century City* (Cham, Switzerland: Springer, 2016) 349 at 350; Finch & Tene, *supra* note 27 at 1597.
30. Finch & Tene, *supra* note 27 at 1604.
31. Choenni et al, *supra* note 29 at 354-55; Finch & Tene, *supra* note 27 at 1597.
32. Finch & Tene, *supra* note 27 at 1607, fn 147.
33. Kaja Prislan & Boštjan Slak, "Analysis of the Relationship Between Smart Cities, Policing and Criminal Investigation" (2018) 2:4 Varstvoslovje 389 at 398.
34. Elizabeth E Joh, "Policing the Smart City" (2019) 15:2 Int'l JL in Context 177 at 178.
35. Prislan & Slak, *supra* note 33 at 399-400.
36. Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public" (1998) 17 Law & Phil 559 at 560.

curtains, but also from the way our publicly observable activities are dispersed over space and time."[37] The increasing accessibility of data, a trend that smart cities will perpetuate, leads to previously "scattered and transient" information being "ordered, systematized, and made permanent."[38]

The erosion of privacy in public aggravates the disruptions outlined above by undermining wellbeing and autonomy. Recall that police observation can impede psychological repose when it does not allow reprieve from visual scrutiny. By extension, importing the risk of being systematically observed in public compromises the sense of freedom and relaxation that open spaces are intended to afford.[39] The decline of privacy in public is far from academic. Jurisprudence from the United States (US), in a quote most prominently reproduced by Sotomayor J, evocatively reminds us that data on public movements can reveal such intrusive information as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[40]

Indeed, Canadian law has recognized the importance of privacy in public for some time. More than 30 years ago, the Supreme Court of Canada (SCC) found in *R v Wise* that persistently monitoring the whereabouts of a suspect's vehicle—even though it was being driven in public such that anyone could observe it—violated the suspect's reasonable expectation of privacy.[41] Almost ten years ago, the SCC reiterated that "[t]he mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that, as a practical matter, such a person may not be able to control who observes him or her in public."[42]

As mentioned, and as Figure 2 depicts, the relation between privacy and smart cities is a two-way street. In fact, privacy bears directly on the feasibility of smart city projects because smart city proposals are unlikely to attract sufficient public support without adequate privacy safeguards.[43] Each of the smart city features identified above—sensor network interconnectivity and grassroots data gathering—depends on citizens holding a positive view of their privacy implications. In a recent empirical study, Abdulrahman Habib and others mapped the factors determining whether members

37. Jeffrey H Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future" (1995) 11:1 Santa Clara Comp & High Tech LJ 27 at 29.

38. Nissenbaum, *supra* note 36 at 577.

39. Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 31.

40. *United States v Jones*, (2012) 132 S Ct 945 at 955 (Sotomayor J, concurring), quoting *People v Weaver*, (2009) 909 NE 2d 1195 at 1199.

41. *R v Wise*, [1992] 1 SCR 527, (1992) 133 NR 161 (SCC).

42. *R v Spencer*, 2014 SCC 43 at para 44.

43. See Braun et al, *supra* note 24 at 500, contending that privacy protections "are paramount to the success of a smart city."

of the public are willing to accept smart city technologies and found that perceived privacy (the belief that personal information will be protected) is a strong determinant of trust in smart city technology.[44] The authors conclude that "residents are willing to use smart-city technologies, provided they are assured their information is safe and their right to privacy guaranteed."[45]

As for grassroots information gathering, Sunil Choenni and others' research on the security and privacy implications of data collection by citizens points in the same direction.[46] Their findings suggest that citizens' willingness to act as data collectors is also tied to addressing privacy concerns.[47] The very prospect of developing smart cities, therefore, depends on residents feeling that their personal information is protected. If privacy concerns are not adequately addressed, including those relating to policing, they may have a chilling effect on the public's approval of smart cities and, in turn, on the feasibility of smart city projects.

3. An Emerging Legal Problem

Smart cities' effects on policing and privacy call for external safeguards. Designing smart city technology with built-in privacy protections and promoting responsible data collection have a role to play, but they cannot offer a complete solution. In light of these limitations, the gap forming at the intersection of privacy, policing and smart cities is, in part, a legal one.

While the most secure way to protect privacy is to avoid collecting personal information altogether, not all data generated in smart cities can be dissociated from personal identifiers. To complement technical means of anonymizing data at the source, additional privacy safeguards are required for data that cannot be anonymized. For instance, recall that intelligent vehicles must broadcast unencrypted details of their movements to facilitate autonomous driving. Consequently, by technical necessity, anyone within range of the vehicle's transmission, including police, is capable of intercepting this information.[48] The same inability to anonymize information at the source arises with respect to data collected by smart city residents. Choenni and others report that, practically speaking, it is not possible to predict how data sourced from residents' devices may reveal personal information when combined with other data.[49]

44. Abdulrahman Habib, Duha Alsmadi & Victor R Prybutok, "Factors that Determine Residents' Acceptance of Smart City Technologies" (2020) 39:6 Behaviour & Information Technology 610.
45. *Ibid* at 619.
46. Choenni et al, *supra* note 29.
47. *Ibid* at 350-51. For studies suggesting that a smart city's success is predicated on the public holding a positive view of its privacy implications more broadly, see van Zoonen, *supra* note 21 at 474; Eckhoff & Wagner, *supra* note 22 at 490.
48. Eckhoff & Wagner, *supra* note 22 at 507.
49. Choenni et al, *supra* note 29 at 355.

When data cannot be reliably anonymized, trusting that personal information will only be collected and used to benefit residents may be short-sighted. Smart cities are intended to enhance quality of life, improve resource management, and promote economic growth.[50] It follows that the host of public and private entities collecting data in smart cities should be expected to act for diverse but beneficial purposes, without intending to unnecessarily compromise privacy.[51] However, relying on responsible frontline data collection does not guard against police repurposing data. Absent oversight mechanisms, data collected by private entities and other branches of government with the intention of benefitting a given individual risks being repurposed to that individual's detriment. The potential repurposing of smart city data speaks to the importance of implementing legal privacy controls to guard against abuses after collection.

Naturally, specific legal initiatives that complement responsible data collection and processing may vary from one city to the next. Municipalities can choose to entrust different entities with fulfilling smart city functions, including various forms of public and private organizations. Depending on their nature, these entities may be subject to distinct legislative or contractual obligations concerning privacy. Differences in smart city governance will be relevant to promoting privacy interests in individual municipalities, but the choices each city might make are difficult to predict and lessons for general application are difficult to draw. Thus, the balance of this article focuses on the role existing Canadian oversight structures can play in anticipating smart cities' disruptive forces on privacy and policing.

Lastly, while some intrusive policing techniques pose a more immediate threat to privacy than repurposing information from smart cities, the need for external safeguards should not be discounted. Much could be learned about a person of interest in a criminal investigation by monitoring their personal devices or tracking their wearable accessories rather than sifting through smart city data.[52] Yet, if recourse to smart city data for investigatory purposes is not comprehensively regulated, it risks becoming a convenient alternative to investigatory techniques that do involve robust oversight.

50. Eckhoff & Wagner, *supra* note 22 at 490; Martina Fromhold-Eisebith, "Cyber-Physical Systems in Smart Cities – Mastering Technological, Economic, and Social Change" in Houbing Song et al, eds, *Smart Cities: Foundations, Principles, and Applications* (New York: Wiley, 2017) 1 at 2.

51. See, however, Braun, *supra* note 24 at 500, arguing that many businesses collecting smart city data are hesitant to offer greater privacy protection than what external forces require of them.

52. Prislan & Slak, *supra* note 33 at 404.

II. Complementing Calls for Enhanced Judicial Oversight

Part I outlined the importance of reconciling the tension between the need for police investigations and the need to protect privacy. Recognizing that police will sometimes be justified in infringing individuals' privacy requires officers to discern cases where interference is warranted from those where it is not. Properly regulating this exercise of discretion mitigates the chances that officers will choose to interfere with privacy arbitrarily or on improper grounds.[53]

Court-based and nonjudicial safeguards are complementary ways of regulating investigatory discretion. Court-based controls are premised on judicial review of police action. By measuring police action against statutory and common law thresholds, judicial decisionmakers make binding determinations on the legality of policing decisions. As part of this process, they also interpret existing constraints on police discretion and determine their applicability to novel situations. Nonjudicial safeguards can regulate discretion through means such as officer training, internal policies, and command structures.

Court-based solutions have proven adaptable to new information-driven investigations, and a growing body of literature suggests addressing the privacy issues that smart city policing raise through judicial oversight. As this Part contends, when the issues raised by smart city policing are considered holistically, the limits of court-based controls become more apparent. Accordingly, nonjudicial safeguards can, and in fact, must evolve to regulate smart city policing.

1. Invitations to Rely on Judicial Oversight in Smart Cities

Section 8 of the *Charter* is a pillar of court-based privacy safeguards. Behind its modest wording, which provides that "[e]veryone has the right to be secure against unreasonable search or seizure," lies an adaptable tool in the regulation of intrusive investigative conduct. The provision makes no mention of privacy, and yet, through successive judicial interpretations, s 8 has been used to regulate new information-gathering practices as they emerge.

The SCC recognized and even encouraged s 8's expansion from as early as *Hunter v Southam*.[54] Distancing itself from past formulations of privacy premised solely on protecting property, the Court found that s 8 protects "people, not places"[55] and, later, that s 8 is concerned with safeguarding individuals' dignity, integrity, and autonomy.[56] Anticipating the need to apply s 8 in unforeseen future situations, the unanimous *Hunter* Court ruled the provision "capable of growth and development over time to meet new social, political and historical realities."[57]

---

53. See Loraine Gelsthorpe & Nicola Padfield, "Introduction" in Loraine Gelsthorpe & Nicola Padfield, eds, *Exercising Discretion: Decision-Making in the Criminal Justice System and Beyond* (Uffculme Cullompton: Willan Publishing, 2003) 1 at 4 (suggesting that legal systems that provide little guidance on how to exercise discretion increase the risk that discrimination will creep into decision-making).

54. *Hunter et al v Southam Inc*, [1984] 2 SCR 145, (1984) 55 AR 291 (SCC) [*Hunter*].

55. *Ibid* at 159.

56. *R v Plant*, [1993] 3 SCR 281 at 292-93, (1993) 157 NR 321 (SCC).

57. *Hunter, supra* note 54 at 155.

Following *Hunter*, any activities conducted by the state can qualify as a "search" so long as they interfere with a reasonable expectation of privacy.[58] As courts began adjudicating claims based on informational rather than territorial privacy, the "totality of circumstances" that suggest whether claimants have a reasonable expectation of privacy grew from a list centred on ownership to one weighing factors wholly removed from property considerations.[59] Most notably, perhaps, the nature of the information revealed (i.e., whether the search exposes intimate details of the claimant's lifestyle or biographical information) is now a factor influencing the reasonable expectation of privacy assessment.[60]

Section 8 claims divorced from property considerations have already begun to regulate technologically assisted investigations. In particular, the SCC has shown an openness to recognizing that claimants may have a reasonable expectation of privacy over surveillance conducted in public and data gathered or held by third parties. With respect to surveillance, the SCC recently distinguished visual recordings in public from mere observation. Recordings, it found, have a greater potential to interfere with privacy expectations because of their permanency and the level of detail that can be gleaned from their subsequent study.[61] As for data held by others, the past decade spawned a string of cases recognizing that claimants may have a reasonable expectation of privacy with respect to data stored by third parties, over which the claimants have no control.[62]

Some authors propose continuing to develop s 8 jurisprudence in a direction that would recognize the privacy concerns that smart city policing raises.[63] The scholarship at this stage is not concerned with smart cities specifically, but its focus on privacy concerns in the digital age touches on the same broad themes. In particular, proposed reforms include strengthening the recognition that public surveillance engages important privacy considerations and recognizing that information processing should be subject to oversight as well. These proposals identify important areas for reform but, as the remainder of this article contends, their attempts to situate those reforms within s 8 need to be accompanied by other novel solutions to policing in smart cities and similar environments.

Some proposals invite courts to address modern privacy issues by continuing to move beyond property safeguards and toward weighing the effects of police conduct on individuals. George Dolhai argues that the totality of circumstances list has become so unworkable that courts should recentre

58. *Ibid* at 160.

59. *R v Edwards*, [1996] 1 SCR 128 at paras 45, 31, (1996) 192 NR 81 (SCC).

60. *R v Patrick*, 2009 SCC 17 at para 27 [*Patrick*].

61. *R v Jarvis*, 2019 SCC 10 at para 62.

62. See e.g. *R v Cole*, 2012 SCC 53 (child pornography stored on a work-issued laptop); *R v Marakah*, 2017 SCC 59 (text messages from the sender stored on the recipient's cellphone); *R v Jones*, 2017 SCC 60 (text message conversation held by telecommunications service provider).

63. See *infra* notes 64-74 and accompanying text.

the analysis on the notions of dignity, integrity, and autonomy.[64] Specifically, Dolhai asserts that protection under s 8 should focus on how best to serve the personhood of an individual by engaging with how a given attempt to collect information impairs their dignity, integrity, and autonomy.[65]

Complementary proposals would see the s 8 framework expand to recognize that information processing can engage reasonable expectations of privacy. Legal scholar Jane Bailey argues that the "nature of the information revealed" factor in the totality of circumstances assessment ought not to be framed so narrowly.[66] Currently, the nature of the information revealed militates in favour of recognizing a reasonable expectation of privacy, therefore triggering s 8 if a given search exposes intimate personal details.[67] This attention to how an individual search may expose personal information stops short of acknowledging that aggregating less intrusive non-biographical data may also reveal intimate lifestyle information.[68]

Although writing from an American perspective, the broad strokes of Emily Berman's argument align with ideas found in the Canadian literature.[69] Berman's proposal seeks to address a narrower issue than Bailey's: that of combining information in databases to which police already have access. Berman suggests that if this form of data processing reveals information that engages a reasonable expectation of privacy, it ought to be protected under search and seizure rights. Concretely, aggregation would be considered a "search" if the nature of the intrusive information it reveals could only otherwise have been obtained through information collection.[70]

Mathew Johnson proposes a greater departure from how the SCC has applied s 8 to novel search technologies. In Johnson's view, the dictionary definition of the word "search" should determine whether s 8 is engaged.[71] His proposal would shift the focus of the analysis from the subject matter of the search and the information revealed to the nature of the police action. In other words, a "search" within the meaning of s 8 would be triggered when police look through or examine something to find information.[72] Johnson notes that his approach would facilitate the recognition of privacy infringements in public, since conducting surveillance amounts to examining something to find information and therefore meets the definition of a search.[73]

64. George Dolhai, "Why a New Approach to Privacy Rights and Section 8 of the Chapter [*sic*] is Required in the Cyber Age and What It Could Look Like" (2020) 68:1 Crim LQ 29 at 44.
65. *Ibid* at 30.
66. Jane Bailey, "Framed by Section 8: Constitutional Protection of Privacy in Canada" (2008) 50:3 Can J Corr 279.
67. *Patrick*, *supra* note 60 at para 27.
68. Bailey, *supra* note 66 at 295.
69. Emily Berman, "When Database Queries Are Fourth Amendment Searches" (2017) 102:2 Minn L Rev 577.
70. *Ibid* at 612.
71. Mathew Johnson, "Privacy in the Balance – Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8" (2012) 58:3&4 Crim LQ 442 at 487.
72. *Ibid* at 488.
73. *Ibid* at 489-90.

Turning to the US again, Rebecca Lipman proposes a similar approach, also aimed at overseeing the manipulation of data in databases to which police already have access. For Lipman, general acts that do not involve aggregation, including merely accessing these ever-expanding databases, ought to be considered a "search" based on the plain meaning of that word.[74] According to her construction, simply retrieving personal information that is already accessible would suffice to trigger constitutional search and seizure rights.

The above proposals attest to a movement in the literature that relies on judicial interpretation and court-based controls to address smart city policing issues, namely, information collection in public and information processing. As important as these emerging privacy concerns are, the remainder of this Part will outline why they can only be addressed if court-based controls are accompanied by developments in the area of nonjudicial safeguards as well.

2. Inadequacies of Judicial Oversight in Smart Cities

As smart city technology becomes mainstream, the ability of court-based controls to prevent unjustified privacy intrusions will likely diminish. Upfront judicial oversight is already limited to instances where a warrant is required to access information. The oversight of warrantless searches and submissions by the affected party of any search only occurs after the fact, if the matter proceeds to court at all. While the need to obtain a warrant before accessing certain information acts as an upfront check, this check is undermined when the person or entity holding the information shares it voluntarily.[75] As smart cities develop and relevant information is increasingly held by government partners, instances where judicial approval mechanisms operate may decline. Early smart card integration on the Greater Toronto Area's public transit networks illustrates this point. Over the past years, officers have obtained a warrant in fewer than 20 per cent of cases where fare card data was disclosed to facilitate or further a police investigation.[76]

---

74. Rebecca Lipman, "Protecting Privacy with Fourth Amendment Use Restrictions" (2018) 25:2 Geo Mason L Rev 412 at 456-57.

75. For a discussion of third parties voluntarily turning over data to police, see *R v Cole*, 2012 SCC 53, where school authorities turned over the computer that a teacher used to store nude photographs of a student. While the Court held that police could not access the personal information without a warrant in this case, it added that "[t]he school board was, of course, legally entitled to inform the police of its discovery of contraband on the laptop. This would doubtless have permitted the police to obtain a warrant to search the computer for the contraband." (at para 73)

76. See memorandum from Sara Azargive, Senior Privacy Officer, to Metrolinx Board of Directors, "2018 PRESTO Law Enforcement Requests Data Transparency Report" (7 February 2018), online (pdf): Metrolinx <assets.metrolinx.com/image/upload/Documents/Metrolinx/20190207_BoardMtg_PRESTOLawEnforcementRequests_EN.pdf> at 4, reporting that 22 of the 26 disclosures to law enforcement for investigatory purposes were provided without a court order; Memorandum from Fawad Ebraemi, Chief of PRESTO (Acting), to Metrolinx Board of Directors, "PRESTO Report" (25 March 2021), online (pdf): Metrolinx <assets.metrolinx.com/image/upload/Documents/Metrolinx/20210325_BoardMtg_PRESTO_Quarterly.pdf> at 5, reporting that 44 of the 54 disclosures were provided without a court order.

Where court-based controls do continue to operate, judicial officers' lack of specialization risks undermining their effectiveness. On the one hand, judicial oversight is ill-suited to the complexity and pervasiveness of sensing technologies in smart cities. It is conceivable that judges, like most generalists, will find the workings and privacy ramifications of information processing technologies difficult to appreciate. Orin Kerr fleshes out this concern by contrasting courts' ability to regulate dynamic technologies with traditional technologies that do not change significantly over time, such as automobile stops, which judges can readily comprehend and therefore regulate.[77] Even if monitoring information processing were brought into the fold of court-based controls, as some of the literature described here suggests, judicial officers may be at pains to appreciate the effects of practices like data manipulation and aggregation on privacy.

On the other hand, an important component of overseeing information collection and processing in smart cities will be foreign to the courts. As legal scholar Craig Forcese explains, settings where the government itself collects and stores a large share of intrusive information may be a poor fit for traditional judicial oversight.[78] In such environments, "there is a less pronounced adversarial relationship between information-seeker and information-possessor."[79] Determining whether law enforcement interests are strong enough to justify accessing the information is only one part of providing oversight. Oversight is also concerned with leakage between different government branches, which courts can do little to prevent or control.[80]

Lastly, the idea of developing judicial oversight by adopting a broader interpretation of s 8 in particular is problematic. If novel forms of privacy intrusion qualify as searches, the framework through which courts assess their legality in a given case would likely lack context. Whereas some smart city policing decisions will have far graver impacts on privacy than others, s 8's justificatory framework has crystallized in a way that takes few contextual factors into account. To find that a search is justified, courts require that officers either have a reasonable belief or a reasonable suspicion that their search will uncover evidence of an offence. That is, courts perform a balancing of law enforcement and privacy interests based largely on how confident officers are that a search will reveal evidence of an offence.[81] This weighing exercise places strong emphasis on how likely it is

77. Orin S Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102:5 Mich L Rev 801 at 863.

78. Craig Forcese, "The Limits of Reasonableness: The Failures of the Conventional Search and Seizure Paradigm in Information-Rich Environments" (Paper delivered to the Privacy Commissioner of Canada, 1 July 2011), online (pdf): Social Science Research Network <ssrn.com/abstract=1945269> at 11.

79. *Ibid*.

80. *Ibid*.

81. For an argument that framing privacy and security as a balance oversimplifies the relationship between both concepts, see Bernadette Somody, Máté Dániel Szabó & Iván Székely, "Moving Away from the Security-privacy Trade-off: The Use of the Test of Proportionality in Decision Support" in Michael Friedewald et al, eds, *Surveillance, Privacy and Security: Citizens' Perspectives* (New York: Routledge, 2017) 155-176. The argument is compelling but, in order to track the language and methodology that courts have developed in Canada, this article refers to weighing privacy and law enforcement interests as a "balancing" exercise.

that an intrusive investigative technique will uncover evidence, with comparatively little regard for other fact-specific considerations such as necessity and proportionality. In smart cities, the severity of privacy intrusions will greatly vary and require a more flexible approach to justifying breaches than s 8 can offer. An example may help clarify this concern.

Returning to the fictional city of Techtown with which this article opened, one can imagine a situation where local police have come to learn of a mid-level drug dealer whom they suspect traffics prohibited substances around town. Before making an arrest, police want to find out whether their suspect works with an accomplice and, if so, learn the accomplice's identity. Smart city technology would enable police to investigate with relative ease. Subject to any legal requirements, by correlating data from facial recognition, licence plate readers, or Wi-Fi logs, they could establish which individuals frequently attend the same events as their suspect or who can often be seen with him.

Many variations that bear on whether the state's law enforcement interest supersedes the public's privacy interest are possible within this scenario. By way of example, the nature of events where attendance may be revealed influences privacy considerations. If processing the data would engage scores of individuals' privacy interests because it identifies a large number of people, or if it would reveal people's repeated attendance at a medical facility, for instance, the impetus to restrain the state's action increases. Conversely, if the data is sourced from one location or from a limited period of time, the effect on privacy interests may be relatively weak. Once police have correlated attendance at different events, whether they will retain data and how they will restrict access to it also informs the gravity of privacy intrusions.

All of these variations impact privacy interests in a way that requires guarding against abuses. Even recording individuals' attendance outside an underground party and later deleting the data is detrimental to privacy interests. Experience shows that surveillance technology often becomes a form of control over marginalized groups by monitoring behaviour that is unconventional, but not criminal.[82] Discouraging participation in non-mainstream movements through the controlling force of surveillance can have a chilling effect on personal and social development. Returning to Solove's terminology, discouraging attendance by recording identifiers is a policing action that disrupts worthwhile practices.

That is not to say that recording attendance at public or semi-public events should be disallowed altogether. Society is willing to accept a level of public information collection and processing that compromises privacy to enable police investigations. Officers can choose to engage in public information collection and processing so long as that behaviour fits within the constraints privacy interests place on policing. In less intrusive scenarios such as this one, where the privacy concern

82. Gérard La Forest, "Opinion by Justice Gérard La Forest" (writing extrajudicially to Privacy Commissioner of Canada George Radwanski, 5 April 2002), online: Office of the Privacy Commissioner of Canada <priv.gc.ca/en/opc-news/news-and-announcements/2002/opinion_020410>.

involves recording attendance at public events, s 8 cannot be the privacy framework that guides police discretion when its justificatory mechanism will not tolerate any police actions without at least a reasonable prospect of uncovering evidence of an offence. The levels of privacy infringements that smart city technology will enable require a more contextual approach.

Section 8's justificatory mechanism is unlikely to undergo the necessary change. Recent case law rejects the adoption of a different threshold in public, where privacy interests are lower, to say nothing of a contextual or proportionality threshold. In *R v Kang-Brown* and *R v A.M.*, the SCC discussed the possibility of a *Charter*-compliant "generalized suspicion" standard[83] that would have permitted officers to use invasive investigative techniques if they suspected criminality in certain locations or at certain events.[84] A generalized suspicion standard would have established a more permissive threshold for tolerable police conduct by allowing "random, generalized searches" in situations where individuals have a lesser expectation of privacy, such as travelling through a public transportation hub.[85] The SCC firmly rejected the more permissive standard, recognizing that a generalized search power would give insufficient regard to individuals' privacy interests.

Leaving aside the likelihood of change, any solution that imports more flexibility into the test would risk compromising existing collection restrictions.[86] Section 8 currently provides a simple and robust mechanism for protecting individuals' homes, communications, and data that independently discloses intimate personal details. Those interests should continue to benefit from the strictest protection and only be infringed when state intrusion is likely to produce evidence of an offence. Creating a parallel flexible privacy framework outside of s 8 ensures that existing privacy protections will not be compromised.

3. Renewed Importance of Nonjudicial Oversight in Smart Cities

Nonjudicial controls are often the only safeguards that apply to police decisions. Intrusive investigatory decisions that do not result in criminal charges and discriminatory decisions where no complaint is brought are never litigated, and are therefore only subject to out-of-court controls. These controls take many forms. They include the guidance officers receive through training and policies as well as internal approval processes before conducting certain actions.

Recent studies on the use of street checks in Canada, such as those examining practices in Ontario,[87] Halifax,[88] and Vancouver,[89] exemplify the importance of responsive nonjudicial controls. As mentioned, officers perform a street check by gathering information of intelligence value about

83. *R v Kang-Brown*, 2008 SCC 18 [*Kang-Brown*]; *R v AM*, 2008 SCC 19.

84. *Kang-Brown*, *supra* note 83 at para 245.

85. *Ibid* at paras 246, 253.

86. Simmons, *supra* note 28 at 184.

87. Michael H Tulloch, *Report of the Independent Street Checks Review* (Toronto: Ministry of Community Safety and Correctional Services, 2018).

88. Wortley, *supra* note 9.

89. Montgomery et al, *supra* note 8.

civilians and storing it in a law enforcement database. Street checks often involve stopping individuals in public, but they can occur from logging information about civilians without direct contact. Importantly, street checks do not permit police to collect information randomly.[90]

Without proper oversight, intrusive investigative practices like street checks yield discriminatory results. Reviewing the relationship between race and street checks in Halifax, Scot Wortley found considerable disparities in the collection of information on Black and White residents. Halifax's policing policies provide "a strong theoretical foundation for the delivery of fair, unbiased and impartial police services,"[91] Wortley concludes. Yet, based on 2016 census data, he found that Black Haligonians were five times more likely to undergo a street check than their proportion of the population would suggest, and were 5.7 times more likely to undergo a street check than White residents.[92] Adjusting for newer population estimates, Wortley found Black residents' share of street checks may be closer to 5.33 times greater than their share of the population and 6.1 times greater than the White rate.[93]

The recent findings on street checks serve as a starting point for thinking about nonjudicial controls in smart cities. Despite differences between the application of street check policies and the investigatory use of smart city technologies, we can identify important parallels. The misapplication of street check policies results in unjustified physical stops and differential treatment of racialized residents. Smart city policing is less likely to reproduce these issues. Like street checks, however, investigations based on smart city technology are potentially intrusive practices affecting large portions of the population. They need responsive safeguards so that decisions to use the powers conferred on police officers are properly supported.

Beyond this universal observation that all police powers need responsive out-of-court controls, technological integration will further increase the importance of nonjudicial safeguards. Currently, when investigations involve more than an interaction or stop, such as aggregating several sources of information, police are incentivized to dedicate resources to instances of serious criminality and to deploy them no more widely than necessary. In smart cities, the pervasive monitoring of public spaces will afford access to more information with less effort.[94] The city's sensor network will provide extensive coverage at all hours, collecting information for public safety purposes and for other applications from which the data can be repurposed to investigate crime. Subject to restrictions on their discretion, officers could choose to investigate an offence using greater or lesser amounts of data without encountering logistical obstacles like deploying surveillance teams or setting up additional monitoring equipment.

90. Tulloch, *supra* note 87 at 35-36.

91. Wortley, *supra* note 9 at 166.

92. *Ibid* at 104.

93. *Ibid* at 105.

94. Joh, *supra* note 34 at 180.

Returning to the Techtown drug trafficking example, where police sought to identify a suspect's accomplice, helps illustrate this point. In correlating attendance outside events where drug trafficking is suspected, police could process CCTV footage with facial recognition technology and aggregate licence plate scans, or Wi-Fi hotspot use, to identify who has often been in the same area as their main suspect or who can often be seen with him. In using those techniques, police would need to make choices that impact the severity of privacy infringements. Facial recognition and analysis of the Wi-Fi logs might be applied to a small public area or a large one, over a short or a long period of time by using a database containing few or many faces and mobile device identifiers. Another choice could be what police will do with the data after its initial use. They may choose to delete the information, if it does not prove immediately relevant, or retain it, expecting that it will become useful or not even knowing whether it will ever be of use. With smart city technology already in place and increasingly affordable storage, neither broadening the search nor retaining the data would require significant cost or effort, but each variation would influence how much the investigation impacts privacy.

Absent traditional logistical constraints, how much to infringe upon privacy will depend on the leeway privacy safeguards afford. Nonjudicial safeguards will therefore need to play an even greater role in deciding the level of intrusion that should be tolerated in a given police investigation.

III. Implementing Responsive Safeguards

The final Part of this article suggests avenues for reflection and further research. It does so by building on the conclusion that front-end out-of-court controls will take on a renewed importance in addressing the privacy issues raised by smart city policing. As those issues are part of a broader trend, the following suggestions may also be adapted to other instances where data collection and processing by police raise privacy concerns. This Part begins by drawing on examples from England and Wales, a common law jurisdiction that is different but comparable to Canada, which places less emphasis on court-based controls to regulate the increasing public information collection and processing by police. Using initiatives in that jurisdiction as a starting point, the following pages suggest how provinces could play a greater role in crafting statutory oversight mechanisms and how day-to-day oversight might be embedded within the investigative process itself.

1. Comparative Outlook

Those well versed in Canadian criminal law will recognize *Charter* rights as being flexible and expansive provisions capable of regulating an array of privacy-engaging police conduct. Familiarity with this flexibility and expansiveness encourages creative proposals around how judicial safeguards may one day address the sorts of privacy issues that arise in smart cities, but it also diverts attention from nonjudicial solutions that have emerged in other jurisdictions.

Naturally, applying rights like security against unreasonable search or seizure to the digital age is not the only way of confronting privacy concerns posed by technological change. The laws of England and Wales provide a useful counterpoint. While English and Welsh law has long applied a set of requirements similar to Canada's before physical searches can be authorized[95]—indeed, it has done so for far longer[96]—the interpretation of those protections has not expanded to include intangible information. Obtaining and processing data are governed by a wholly separate, often front-end set of rules developed to safeguard personal information in the digital age.

The balance of this article draws on certain initiatives adopted in England and Wales to suggest nonjudicial safeguards that would benefit smart city policing and how they may apply in Canada. Before exploring these proposals, England and Wales's uneasy relationship with privacy rights bears unpacking. There is a certain irony to holding English and Welsh law out as an example of privacy protection. Over the past four decades, the United Kingdom (UK) has embraced public surveillance technology to become, by some estimates, the country with the most CCTV cameras per capita in the world.[97] As the UK Supreme Court recently explained, the right to privacy "fell on stony ground in England" and developed domestically in response to the European Convention on Human Rights' (ECHR) incorporation at the turn of the century.[98] More than 20 years later, the ECHR's future role in domestic law remains uncertain.[99]

Despite England and Wales's uneasiness with the right to privacy and the considerable European influence on its development, English and Welsh law serves as a useful building block. It illustrates how a version of privacy protection that often escapes North American commentators has developed in the very common law system from which Canadian criminal law originated. Based on that model, lessons can be drawn about developing detailed legislative responses and embedding oversight within the investigative process itself.

---

95. See e.g. *Police and Criminal Evidence Act 1984* (UK), c 60, s 8.

96. *Entick v Carrington* (1765) 19 St Tr 1029, 1 Wils KB 275.

97. Benjamin J Goold, *CCTV and Policing: Public Area Surveillance and Police Practices in Britain* (Oxford: Oxford University Press, 2004) at 1-2.

98. *R (Catt) v Commissioner of Police of the Metropolis*, [2015] UKSC 9 at para 2. See also Dimitrios Giannoulopoulos, *Improperly Obtained Evidence in Anglo-American and Continental Law* (Oxford: Hart, 2019) at 88, arguing that the right to privacy was either inexistant or unimportant in England and Wales's legal culture until the *Human Rights Act 1998*.

99. After Brexit, the UK government launched a review of the *Human Rights Act* to make recommendations on the European Court of Human Rights' influence over domestic courts and on how domestic courts' oversight role under the *Act* impacts legislative and executive power. Reviewers were not tasked with recommending changes to substantive rights, but the review signalled a discomfort with how European human rights law and judicial oversight have constrained domestic state action. See Independent Human Rights Act Review, *The Independent Human Rights Act Review 2021* (December 2021), online (pdf): <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1040525/ihrar-final-report.pdf>.

2. Addressing a Legislative Deficit

In Canada, some privacy-infringing police practices are already framed by statute, including aspects of technologically assisted investigations. For example, the *Criminal Code* provides that intercepting private communications is an offence and, in carving out an exception for police, codifies the steps and thresholds required to obtain authorization.[100] Some aspects of data management by police also benefit from codified boundaries. Returning to the street checks example, Ontario has codified approval processes and limits on accessing the data collected through street checks.[101] These safeguards are distinct from warrant obligations: they outline when an officer may exercise their discretion to collect personal information, govern the retention of that data, and provide for ongoing internal audits within the police service.

While detailed limits to police discretion exist in some areas, there is room to expand the coverage that federal and provincial privacy statutes afford. At the federal level, and in each of the provinces, there are general privacy statutes that regulate information collection and processing by most government entities, including law enforcement bodies.[102] However, as it stands, the provisions that apply to policing tend to create exemptions from privacy restrictions. For instance, many privacy statutes prohibit collecting personal information about an individual from third parties without that individual's consent, but create a blanket exemption for police.[103] Kate Robertson and others posit that police exemptions may have seemed appropriate decades ago, when legislative drafters only had traditional policing activities in mind.[104]

The result is a legislative deficit. To comprehensively regulate smart city investigations, legislatures will need to develop detailed oversight schemes that are responsive to the variety of smart city privacy concerns. As will be discussed, the responsibility for developing these schemes currently falls largely to the provinces.

Using legislation to regulate criminal investigations that involve rapidly changing technologies holds many advantages, especially compared to legislating broadly worded protections and relying on judicial interpretation. Legislatures can enact statutes with an eye to a technology's evolution and wider application by seeking submissions from a broad group of experts and stakeholders, such as

100. *Criminal Code*, RSC 1985, c C-46, ss 184(1), 185-186.

101. O Reg 58/16, s 9.

102. The federal government's legislation is the *Privacy Act*, RSC 1985, c P-21. For an example of similar provincial legislation, see Ontario's *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31 [*FIPPA*].

103. See e.g. *FIPPA, supra* note 102, s 39(1)(g); *Privacy Act, supra* note 102, s 5(3)(b).

104. Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (2020), online (pdf): Citizen Lab <citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>.

"law enforcement, industry, advocacy groups, academics, technical experts and the general public."[105] Moreover, legislatures can act with flexibility, while new technologies are emerging. Unbound by *stare decisis*, they can adapt regulations quickly, to try out different rules and to amend those rules frequently as technology changes.[106]

Pursuing smart city policing restrictions through legislative reform would enable the adoption of tailored and specific rules. In regulating new technologies, legislatures could set clear guidelines on the use of different investigative techniques as new technologies become available or the use of existing technologies becomes more extensive. Concretely, legislation regulating novel search technology could set its own standards of reasonableness for different technologies in the form of a Police Powers Act, similarly to how England and Wales submit their officers to a more detailed set of procedural rules.[107] Such legislation could also apply varying thresholds to justify data processing based on the nature of the information being examined. For example, the *Data Protection Act 2018* establishes distinct justificatory requirements for processing data that would reveal any individual's sexual orientation or religious beliefs.[108] Since this legislative framework would operate outside the protections developed through judicial interpretation, it would not be bound by the strictures of existing justificatory mechanisms. Privacy and policing incentives could be reconciled based on considerations that are tailored to the gravity and context of different infringements.

Further discretionary guidance is possible through the use of police codes. In England and Wales, the Home Secretary develops codes of practice in consultation with police and judicial stakeholders, and must obtain Parliamentary approval before bringing them into operation.[109] Once the codes are in force, they provide guidance for which officers must have regard. Such documents help address the difficulty that those without legal training may face in understanding statutes. They assist by providing a government-sanctioned resource that expands on key definitions and concepts using

105. Steven Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?" (2014) 67 SCLR 505 at 531.

106. Kerr, *supra* note 77 at 871.

107. Johnson, *supra* note 71 at 507. Johnson cites the *Police and Criminal Evidence Act 1984* as an example of legislation detailing police powers, to which one could add the *Investigatory Powers Act 2016* and Part 3 of the *Data Protection Act 2018*.

108. *Data Protection Act 2018* (UK), c 12, s 35.

109. *Police and Criminal Evidence Act 1984* (UK), c 48, s 67. The *Police and Criminal Evidence Act 1984* codes of practice govern core police powers. For equivalent provisions on the development of practice codes in other legislation, see e.g. *Police Act 1996* (UK), c 16, s 39A; *Investigatory Powers Act 2016* (UK), c 25, sched 7.

simple terms and practical examples. Importantly for smart cities, codes of practice can apply to specific areas and, conceivably, to particular technologically assisted investigative techniques. Existing codes in England and Wales such as those governing the acquisition of data from third parties or the retention and deletion of data by police serve as starting points for developing guidance that is responsive to smart city policing.[110]

Adopting police codes or a similar form of government-sanctioned guidance is particularly advisable in complex and dynamic investigatory environments. In his review of Ontario's street check regulation, Justice Michael Tulloch (as he then was) recommended implementing a UK-inspired code of practice. The recommendation rests on the "somewhat confusing and convoluted" rules governing street checks.[111] In smart cities, the interaction between privacy statutes, jurisprudence, and technological developments will present a similarly difficult set of considerations to navigate. Perhaps the main benefit motivating Justice Tulloch's recommendation is to enhance police officers' understanding through aids that do not feature in legislation, such as practical examples and diagrams. Moreover, as with street check practices, smart city data collection and processing is a source of public apprehension. As Justice Tulloch notes in his report, the online availability of a police code would help the public develop an understanding of what is in fact allowed and what is not.[112]

3. Integrating Upfront Oversight

Aside from establishing detailed guidance and justificatory schemes tailored to different technologies, promoting a legislative response to smart city policing facilitates the creation of proactive oversight mechanisms. These mechanisms should include novel monitoring structures as well as checks and guidance for individual investigators.

First, by developing measures to promote compliance with privacy standards at the systemic level, legislatures can reduce the chance of individual infringements. One measure could involve creating a proactive oversight body like the Inspectorate of Constabulary in England and Wales. Among other oversight responsibilities, the Inspectorate monitors compliance with the *Code of Practice on the Management of Police Information* and its associated guidance and standards.[113] The province of Ontario recently announced the creation of an Inspectorate of Policing to monitor police compliance with statutory obligations.[114] If detailed legislative guidance develops as smart cities grow,

110. See e.g. UK Home Office, "Communications Data: Code of Practice" (November 2018), online (pdf): <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf>; National Centre for Policing Excellence, "Code of Practice on the Management of Police Information" (July 2005), online (pdf): <library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf>.

111. Tulloch, *supra* note 87 at 176.

112. *Ibid* at 179.

113. "Code of Practice on the Management of Police Information", *supra* note 110 at § 1.3.1.

114. Solicitor General of Ontario, News Release, "Ontario's First Inspector General of Policing Appointed" (2 October 2020), online: <news.ontario.ca/en/release/58643/ontarios-first-inspector-general-of-policing-appointed>.

legislatures could task arms-length nonjudicial bodies like Ontario's new Inspectorate with upholding privacy standards at an organizational level. Individual police officers would then benefit from structured controls on their discretion through legislated guidance on specific technologies and from active on-the-ground monitoring of how privacy-infringing decisions are being made within their organization.

Second, to compensate for the inadequacies of judicial oversight in smart cities, nonjudicial actors should be integrated into investigations from the outset to provide monitoring and advice. So long as they are sufficiently independent, such actors could offer the expertise and guidance on decision-making that court-based initiatives cannot provide.

In England and Wales, the *Data Protection Act 2018* governs the processing of personal data and serves as an example. This Act establishes that independent experts in data protection, known as data protection officers, must monitor compliance with the legislation's law enforcement provisions.[115] Data protection officers must be knowledgeable in the legal and practical dimensions of data protection,[116] operate without interference,[117] and report to the policing authority's highest management level.[118] Their compliance monitoring does not depend on a case proceeding to court. As applied to smart cities, data protection officers would have the technical expertise to assess risks that others may not foresee, such as the impact of unintended metadata acquisition on privacy interests. Moreover, unlike the judges, who provide oversight in a framework like Canada's search and seizure model, data protection officers give guidance. In addition to monitoring compliance, they advise policing authorities and their employees on how to exercise their discretion within the legislative restrictions.[119]

Guidance from independent data protection specialists would encourage police to minimize privacy disruptions even where greater interference may be legally permissible. Under the *Data Protection Act 2018*, data protection officers must advise on and monitor the use of data protection impact assessments. These assessments are carried out before information is processed to identify, inter alia, the risks to rights and freedoms, the measures through which those risks will be addressed, and the safeguards, security measures, and mechanisms that will ensure the protection of personal data for all those concerned.[120] That is, data protection officers' guidance encourages individual investigations to limit privacy disruptions beyond the minimum legal requirement where possible, and foregrounds the interests of third parties who are not being investigated but whose information may nonetheless be revealed.

115. *Data Protection Act 2018* (UK), *supra* note 108, s 69(1).

116. *Ibid*, s 69(2)(a).

117. *Ibid*, s 70(3).

118. *Ibid*, s 70(5).

119. *Ibid*, s 71(1).

120. *Ibid*, s 64.

The *Investigatory Powers Act 2016* provides another example of how arms-length specialists could be embedded within policing bodies. In regulating police access to communications data, this Act establishes a single point of contact (SPoC) requirement.[121] To make an application for retained communications data from a service provider, police must consult a SPoC who has specialist training and who is able to provide advice as well as monitor the legality of applications to acquire communications data.[122]

Early monitoring and advice from embedded specialists would complement existing sources of guidance. In Canada, courts have shown an openness to setting guidelines for police practices that are not comprehensively regulated. For instance, in *R v Rogers Communications Partnership*, the Court developed a series of non-binding guidelines regarding "tower dumps."[123] Tower dumps occur when police obtain an order for records of all cellular traffic through a specified tower at a given time. Before crafting its guidelines, the Court remarked that although privacy legislation was being developed in other areas, there was none addressing the retention of tower dump records.[124] The Court's guidelines were intended not as conditions precedent for obtaining a production order—that procedure being established by the *Criminal Code*—but as a way of promoting incrementalism and minimal intrusion.[125] Therefore, the Court recommended police practices, such as providing details that would enable the production order recipient to produce fewer records by conducting a narrower search, and confirming that the quantity and the type of data being requested can be meaningfully reviewed.[126]

A combination of upfront specialist advice and detailed legislative guidance on police practices would complement the role courts have played in cases like *Rogers*. As mentioned, legislative limits on police discretion can be developed based on submissions from a host of experts and stakeholders. In *Rogers*, guidelines were established in response to submissions from Crown prosecutors and counsel for the telecommunications companies. Furthermore, safeguards developed by legislatures and advice from embedded experts may influence privacy-engaging investigations as new technologies and practices emerge, rather than once an intrusive investigative technique is sufficiently commonplace to be disputed in court.

In essence, there are many ways of addressing privacy issues in smart cities without unduly relying on court-based safeguards. On the one hand, legislatures should assume a greater role in tailoring police powers and in issuing accessible guidance to account for the range of privacy infringing actions that can be expected from smart city policing. On the other hand, the limited role that courts can play in monitoring smart city investigations, particularly at the front end, militates in favour of embedding arms-length specialists in the investigative process.

---

121. *Investigatory Powers Act 2016* (UK), c 25, s 76.

122. UK Home Office, *supra* note 110 at § 4.4, 4.6.

123. *R v Rogers Communications Partnership*, 2016 ONSC 70.

124. *Ibid* at para 60.

125. *Ibid* at para 63.

126. *Ibid* at para 65.

Making the sorts of changes that smart city policing requires will largely fall to provincial legislatures. There is room for the federal government to further specify investigative processes through statutes such as the *Criminal Code*. In particular, the federal government can act by legislating authorization schemes for police practices that would otherwise be criminal offences or unreasonable searches.[127] However, as discussed, much of what is required by way of legislation is the regulation of practices that engage privacy without rising to the level of a criminal offence or a *Charter* breach. That sort of legislative response falls to the provinces, given their responsibility over policing. The same is true of proposals to embed specialists within policing bodies. Aside from the relatively narrow fields in which policing is a federal responsibly, and despite the inconsistent initiatives this may spawn between jurisdictions, it will be for the provinces to craft laws and oversight structures that are responsive to smart city policing. Absent initiative by provincial lawmakers to fill the current legislative gap and supplement judicial oversight, privacy interests risk being subsumed by smart city policing practices.

Conclusion

Technological developments can disrupt the relationship between privacy and policing by providing police officers with new sources of personal information. The focus of this article has been on smart cities as one example of disruptive technological change that requires regulation to guard against arbitrary or abusive interferences with privacy.

Given the novel settings in which courts have applied existing privacy schemes, the push in the North American literature to rely on these protections is understandable. Viewed holistically, however, the changes in police practices that smart cities will facilitate create a renewed need for proactive nonjudicial safeguards. With some smart city policing decisions likely to have far graver impacts on privacy than others, the means that have developed through judicial interpretation to distinguishing between reasonable and unreasonable infringements will be insufficiently contextual. Moreover, compared to traditional surveillance, acquiring smart city data will involve fewer resource considerations because a permanent monitoring infrastructure will already be in place. Greater specialized oversight in the early stages of investigations would help counterbalance this development in a manner court-based oversight cannot.

Responsive smart city policing regulation can be achieved by supplementing existing privacy legislation and by embedding additional oversight within policing bodies. In terms of legislation, an opportunity exists for lawmakers to develop statutory parameters and accessible guidance on the exercise of police discretion that are tailored to various smart city technologies. As regards embedded oversight, specialists, if they are sufficiently independent, have the potential to not only promote compliance through monitoring but to educate police officers as smart city technology evolves. While all governments have a role to play in regulating smart cities, provincial legislatures, given their responsibility over most policing activities, will need to be particularly active in ensuring the law develops in line with smart city technology.

127. See e.g. *Criminal Code, supra* note 100, s 184 (exception to criminal liability for intercepting a private communication where a police officer conducts a wiretap to prevent imminent harm, subject to certain conditions).