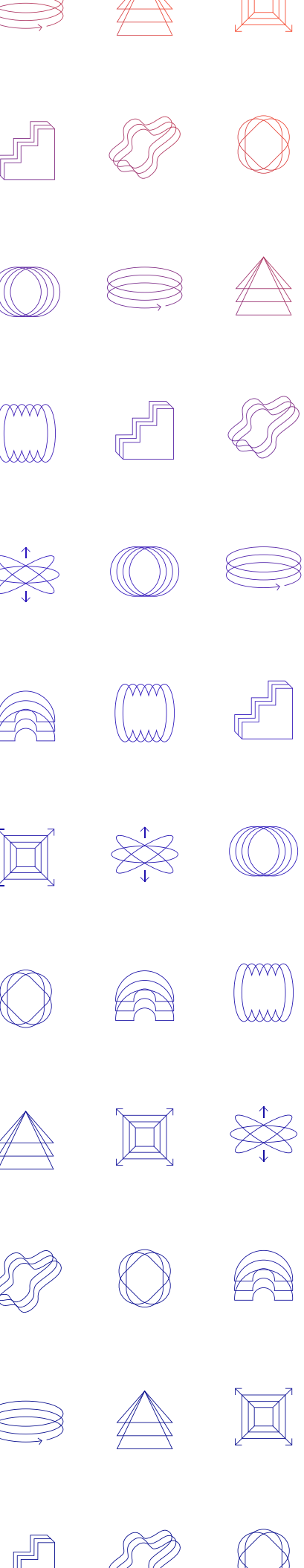

The Intersectional Privacy Risks of Data Sharing Between Law Enforcement and Local Government

A project by Open North

Funded by the Office of the Privacy Commissioner's Contributions Program 2022/23

OPEN NORTH

ACKNOWLEDGMENTS

Recommended Citation

Open North. 2023. "The Intersectional Privacy Risks of Data Sharing Between Law Enforcement and Local Government." Open North.

Disclaimer

If you create an adaptation of this work, please add the following disclaimer along with the attribution: *This is an adaptation of an original work by Open North. The views and opinions expressed in the adaptation are the sole responsibility of the author and the adaptation is not endorsed by Open North.*

Attribution

Authors

Thomas Linder, Merlin Chatwin

Collaborators

This project was made possible by the generous funding provided by the Office of the Privacy Commissioner's Contributions Program. We would like to thank the OPC for their ongoing work to uphold and advance the state of privacy in Canada, and for supporting this project and many others like it.

This project would also not have been possible without Open North's extensive network of friends and collaborators who frequently made time in their busy schedules to provide advice and feedback. In no particular order these include Brenda McPhail, Renee Sieber, Teresa Scassa, Vivek Krishnamurthy, Christopher Parsons, Cristiano Therrien, Jonathan Obar, Bianca Wylie, Daniel Konikof, Alex Luscombe, Ushnish Sengupta, Alok Mukherjee, Meghan McDermott, Katrina Ingram, Nabeel Ahmed, Jamie Duncan, Jagtaran Singh, Kevin Webb, Pierre-Antoine Ferron, and Ana Qarri.

We also thank all the interviewees from local governments and police services from coast to coast to coast. They, too, took the time to speak with us and contribute to a better understanding of how data sharing is governed in Canada.

Collaboration is the foundation for breaking down silos, envisioning better systems, and working to build a better society. We look forward to continuing this work!

CONTENTS

ABSTRACT

There has been a growing realization that while cities can certainly benefit immensely from more granular data collection, algorithmic analytics, platform-based tools, or networked systems, the inherent risks in these techniques necessitate a far greater emphasis on governance policy. Concurrently, a series of public scandals has revealed the degree to which law enforcement has also embraced data technologies, but frequently in secrecy and in contravention of the norms of privacy if not the laws. As the digital transformation of societal systems continues, these dynamics increasingly play out in the same digital infrastructure and data ecosystem – and potentially impact the same residents' privacy rights. In addition, recent developments in so-called 'big data' and 'artificial intelligence' systems have called the adequacy of existing privacy rights into question. This debate has entered the public discourse and contributed to an ongoing decline in trust in government use of data and digital technologies. This report explores the issue of data sharing between law enforcement and municipal bodies, and the intersectional risks this sharing has on communities already facing systemic harm. Based on interviews with 27 decision-makers in law enforcement and municipal government as well as two expert workshops, we outline the ambiguity around data sharing that exists, the heterogeneity in existing governance practices, and detail the calls for reform. On this basis, we recommend establishing a working group including civil society experts, law enforcement professionals, and responsible municipal employees to develop policy proposals to address the issue.

INTRODUCTION

The last few years have seen concurrent yet unnecessarily disconnected developments in the Canadian discourse around the governance of public use of data and digital technologies in cities. There is a growing realization that while cities can benefit immensely from more granular data collection, algorithmic analytics, platform-based tools, or networked systems, a far greater emphasis on pre-emptive governance policy is necessary. While the 'smart city' project of Sidewalk Labs collapsed in 2020, in part under the weight of sustained criticism of its data governance policies (Artyushina, 2020), the federal Smart Cities Challenge emphasized the values and principles of open and responsible governance (Valverde & Flynn, 2020). Subsequently, the cities of Toronto and Montreal have released frameworks outlining their guiding principles for the ethical and responsible use of data and emerging technology and are currently working on operationalizing these frameworks. However, at the same time a series of public scandals has revealed the degree to which law enforcement has also embraced data technologies, but frequently in secrecy and in contravention of the norms of privacy, if not the laws. The most recent such scandal, around the use of the facial recognition technology Clearview, prompted the development of an artificial intelligence governance policy by the Toronto Police Service (Brandusescu et al., 2021).

In Canada there is a long-standing dispute over the relationship between police services and municipalities. Many services, like the Toronto Police Service, are funded by the municipality but are not governed by it, answering instead to a separate entity, the nominally civilian police service board. This has led to tensions around questions of funding and lack of democratic oversight over and insight into what that funding supports. In addition, there are ongoing disagreements over what the police service boards have governance power over, and what remains "operational' purview of the police services themselves (Roach, 2022). These debates over responsibility and governance make it clear that at least in terms of society's rapidly growing data and digital technology ecosystem cities and law enforcement are deeply intertwined (Artyushina & Wernick, 2021; Lorinc, 2021). Not only are they facing similar regulation issues, but their data and technology systems are becoming rapidly integrated: common databases, closed-circuit television (CCTV) access, data-sharing projects, similar analytics tools, all operating in and adding to cities' digital infrastructure (Linder, 2021). The risks these technologies can pose, particularly to marginalized communities, have also become unavoidably apparent: biased data, privacy violations, secretive procurement and use of new technologies, unethical sharing of data, illegitimate use cases, and discriminatory algorithms all have contributed to a decline in public trust in the use of data and technology by government services (Bannerman & Orasch, 2019).

These debates over responsibility and governance make it clear that at least in terms of society's rapidly growing data and digital technology ecosystem cities and law enforcement are deeply intertwined.

This project responds to a dearth of research on this commingled data ecosystem and siloed governance field. Through 27 interviews with practitioners in law enforcement and local government as well as two expert workshops, we shed empirical light on the state of data sharing and governance between law enforcement and municipal authorities. This report documents what is known about this kind of data sharing, the state of data sharing's governance, and the kinds of privacy risk assessment frameworks that are in place. Our goal is to catalyze deeper conversation about how to openly, democratically, and responsibly govern this intersection and to protect residents facing intersectional risks from deeply embedded systemic biases.

Context

The digital transformation of Canadian society and its government has been vigorously underway for well over a decade, driven by the promise of greater knowledge of resident dynamics, needs, and barriers as well as the capacity to act on this knowledge. Such projects touch on a broad cross section of societal issues, from the logistics of public transport management to emergency response, environmental awareness, social services delivery, or public safety – and many of these issues involve both law enforcement and other municipal services. Out of this imbrication we have seen digital transformation projects like the Saskatchewan Hub Model designed to better intake, assess, and triage high risk social service needs through a centralization of data and service providers (P. S. Canada, 2018). Likewise, the launch of the Community Safety and Well-Being Plans specifically promises "a roadmap for how the City and social systems that serve Torontonians, such as community services, healthcare systems, education systems, justice systems, police and businesses, can work collaboratively across different sectors and across governments to support community safety and well-being" (Toronto, 2021). Despite these noble intentions, the reality is frequently one of still-siloed services, fragmented and patchwork governance, and inadequate risk assessment processes and tools.

Open North has been at the leading edge of open and shared data for the common good, and the technology that enables it, since 2011. To us, pursuing the common good means that we prevail past short-term considerations and individual or organizational interests to create healthy, just, and sustainable communities with strong democratic processes. Through our work on data governance and digital transformation, we have observed municipal, provincial, and federal law enforcement being siloed off from best practices designed to protect the privacy, security, and overall well-being of residents. For example, through our participation in the Open Government Multistakeholder forum with the federal government, we observed that the open government commitments for opening and sharing data did not include law enforcement bodies. Similarly, the recently tabled Bill C-27 on privacy and artificial intelligence legislation specifically exempted law

enforcement and security services from the regulation, and the Province of Ontario's Open Government Partnership commitment on Trustworthy Artificial Intelligence did not include the Ontario Provincial Police. At the municipal level, the City of Toronto developed the Digital Infrastructure Strategic Framework that covered all aspects of the city's use of data and digital technology – but could not even mention the Toronto Police Service due to their legal institutional differentiation, even though technologically the two are deeply enmeshed and are responsible to the same residents and accorded the same rights and freedoms.

Problem statement

While many benefits are promised from the further integration and digitization of social services through digital data collection, analysis, dissemination, and decision-making tools, the risk landscape continues to change dramatically. The amount of data collected, its granularity, wide range of sources, and comprehensiveness across so many touch points of individuals' lives, means that existing privacy protections are not adequate – particularly not in the case of already marginalized and discriminated-against groups. Due to systemic racism, sexism, classism, and homophobia such groups are at greater risk than others, and, as study after study has shown (Palmater, 2016; Wortley & Owusu-Bempah, 2011, 2022), are also more threatened by some government institutions, like the police, than others.

This creates a complex landscape of differential threats posed by data production and usage which is largely inadequately reflected in the institutional understanding of the situation as well as in the governance frameworks and policy documents available. In addition, the specific issue of data sharing to and from law enforcement is opaque and hidden from public oversight. This report seeks to shed some light on this particular aspect of governmental digital transformation, and ask of key law enforcement and municipal decision-makers:

1. What they know of the current state of data sharing;
2. How it is governed;
3. What risk assessment frameworks are in place; and
4. Whether governance changes are necessary now or in the future.

With this information we seek to spark a deeper conversation about how institutions can enable data sharing that supports effective service delivery, while also guarding against harms. To this end, we recommend establishing a working group to bring together experts from academia, civil liberties organizations, and municipal and law enforcement bodies to take up the findings, identify innovative alternatives, and chart actionable paths forward.

This report continues by first describing our methodology, then providing a detailed overview of the relevant literature on privacy and intersectionality, the digital transformation of cities, the digital transformation of law enforcement, and how the data governance literature can serve as an analytical frame for these issues. It continues with an outline of the empirical findings and analysis of the data and then concludes by outlining proposed next steps.

METHODOLOGY

Given the dearth of research on the data-sharing practices of government agencies with law enforcement, this project was necessarily exploratory. In order to methodologically account for the exploratory nature of this process we focused on semi-structured interviews as the central method to provide the greatest sampling flexibility. However, gaining interview access to law enforcement is notoriously difficult (Monaghan, 2017), particularly on potentially sensitive topics like privacy and data sharing. By using a snowball sampling approach to develop the widest possible sampling net, we hoped to gather sufficient respondents to achieve our goals. By the end of the data collection phase, we had conducted interviews with 27 individuals across five municipal or regional police services and 10 municipal or regional governments. Almost all interviews were between 30 and 45 minutes long and followed a semi-structured interview guide. Notes and recordings, where consent for recordings was given, were encrypted and password protected.

Due to the resistance of municipal and law enforcement personnel to participating in interviews, and the opaque nature of the responses given by those who did participate, our data analysis focused on what was not being said as much as it focused on what was being said. In order to rigorously identify themes and patterns, we utilized standard content analysis qualitative methods (Anderson, 2007; Roller, 2019) for the interview data, identifying key points and arguments in conjunction with the literature review framework.

After analysis we produced a number of preliminary hypotheses on why details of data governance and ethical frameworks were not emerging from the interview data and added two workshops of experts to the research methods. An invitation to participate in these expert workshops was extended to Brenda McPhail, Renee Sieber, Merlin Chatwin, Teresa Scassa, Vivek Krishnamurthy, Christopher Parsons, Cristiano Therrien, Jonathan Obar, Bianca Wylie, Daniel Konikof, Alex Luscombe, Ushnish Sengupta, Alok Mukherjee, Meghan McDermott, and Jamie Duncan, Akwasi Owusu-Bempah, Jagtaran Singh, Michael Kempa, and Kent Roach. These workshops provided crucial in-depth analysis and contextual assessment of our findings, validating our problem statements, and underscoring the need for serious further work on data-sharing governance innovation and improvement. The results of these workshops are summarized in the second section of the Analysis chapter.

Limitations

While we knew at the onset that gaining a sufficiently geographically representative interview response rate was unlikely, we were surprised by the level of resistance we encountered to responding to our inquiries and participating in interviews. While we were able to conduct interviews with personnel from five different law enforcement agencies, many more turned us down or rescinded initial interest before the interview could take place. The rejection rate was high amongst cities too, although not to the same degree. The non-response rate amongst law enforcement was roughly 75%, while among municipal contacts it was around one third. As such, our results can only be taken as underscoring the existence of the issue, and not as indicative of the representativity of the cases across Canada. While this lack of cooperation and transparency is undoubtedly a limitation, it is itself also stark evidence of inadequate public, accountable, and democratic data governance work being advanced at the intersection of law enforcement and municipalities in Canada.

LITERATURE REVIEW

Privacy, intersectionality, and digital transformation

Privacy law in Canada is well-articulated by numerous resources (Bannerman & Orasch, 2019; Canada. Department of Justice, 2019; O. of the P. C. of Canada, 2014; Grieman, 2019; Robertson, Khoo, & Song, 2020) and does not require extensive repetition here. What is central to this report is that Canadian privacy law is facing ongoing criticism for failing to keep up with the massive changes to the digital landscape. Teresa Scassa, amongst many, has written that "the rapidly changing digital and data landscape has placed increasing pressure on Canada's existing data protection frameworks," and "while data protection law stagnates, data collection continues to increase in volume and variety" (Scassa, 2020a, p. 173). It is not the goal of this report to offer further criticism of Canadian privacy regulations, let alone suggest paths forward. Instead, this section sets the stage for how privacy and risk are currently thought about with regards to data sharing between local government agencies and law enforcement by providing an overview of the key areas of concern in the literature.

In addition to general criticism that Canadian privacy law is no longer adequate to the 'big data' and 'AI' digital economy, more specific concern has been voiced around its ontological focus on individuals' privacy. As has been extensively argued (Bannerman & Orasch, 2019; Scassa, 2020a), privacy rights in Canada (as well as other Organisation for Economic Cooperation and Development countries) take an ontologically individualist approach in giving protection to a very specific kind of data, known as personally identifiable information (PII), under a set of laws that apply to different sectors. The Privacy Act (the Personal Information Protection and Electronic Documents Act, PIPEDA) covers the Government of Canada's collection, usage, and disclosure of PII data; PIPEDA, with some exceptions, covers the private business sector (with substantially similar laws in place in B.C., Alberta, and Quebec); and the provinces have their own public sector privacy laws (O. of the P. C. of Canada, 2008). What constitutes PII differs slightly from law to law, but in general it can be said to cover (O. of the P. C. of Canada, 2014):

- race, national or ethnic origin,
- religion,
- age, marital status,
- medical, education, or employment history,
- financial information,
- DNA,
- identifying numbers such as your social insurance number, or driver's license, and
- views or opinions about you as an employee.

What is not considered PII can include:

- Information that is not about an individual, because the connection with a person is too weak or far-removed (for example, a postal code on its own which covers a wide area with many homes);
- Information about an organization such as a business;
- Information that has been rendered anonymous, as long as it is not possible to link that data back to an identifiable person;
- Certain information about public servants such as their name, position, and title; and
- A person's business contact information that an organization collects, uses, or discloses for the sole purpose of communicating with that person in relation to their employment, business, or profession.

In other words, privacy legislation protects data that relates directly to an individual. In the context of data sharing between local government and law enforcement, what constitutes PII is outlined by provincial privacy legislation (e.g. the Freedom of Information and Protection of Privacy Act, FIPPA, and the Municipal Freedom of Information and Protection of Privacy Act in Ontario), and this legislation forms the basis of the privacy risk determination carried out in a privacy impact assessment (PIAs). PIAs have become the standard tool and procedure by which to assess the potential privacy risk posed by a new digital technology or data collection and analysis system.

However, this PII-based approach to privacy remains under sustained criticism. Computer scientists have shown that in the age of big data, key mitigation techniques like anonymizing or de-identifying data (i.e. stripping data of PII, or through other computational processes rendering it no longer PII) can easily be undone through the correlation of multiple data sets (Bradbury, n.d.; Lomas, 2019; Rocher, Hendrickx, & de Montjoye, 2019). This seriously undermines a key privacy safeguard in Canadian privacy legislation (Ladak, Ladak, & Ladak, 2021; Rosner, 2019). This has led to new calls for implementing so-called Privacy by Design techniques, although the degree to which these are actually adopted versus merely paid lip service to is unclear.

In addition to the insufficiency of this key mitigation technique, PIAs as a whole have been criticized. Scassa (2020a, p. 182) notes that "the BC Commissioner was concerned that "a PIA that only assesses technical compliance fails to account for the wider risks that initiatives can raise for the personal privacy of individuals whose lives and personal information are affected" (OIPC, 2004, p. 26). The most recent assessment of the state of PIA implementation is now a decade old, but the authors (R. M. Bayley & Bennett, 2012, p. 184) noted then that "With regard to implementation, Canadian PIAs also fall short. The extent to which the PIAs are revisited and revised and the promised mitigation measures implemented is unknown. However, privacy regulators have reason to believe that PIA plans are not always carried out."

(1) The rationale for using scare quotes will be explored in subsequent sections

Beyond PII-centric technique, and particularly in the light of the emergence of 'big data' and 'artificial intelligence' technologies,[1] experts have increasingly been arguing that such an individualistic ontology is insufficient to cover all privacy risks (Barocas & Nissenbaum, 2014; Bennett & Bayley, 2016; Taylor, Floridi, & Van der Sloot, 2016). As Taylor et al. argue 2016, p. 10), "much attention is paid to the concepts of anonymisation, of protecting individual identity, and of safeguarding personal information. However, in an era of big data where analytics are being developed to operate at as broad a scale as possible, the individual is often incidental to the analysis. Instead, data analytical technologies are directed at the group level." In other words, if the information is not protected by one of the laws (i.e. is not recognized as 'personal information') then the confidentiality or mitigation obligations laid out in the law do not apply. The inquiry into whether data can be disclosed under the law without the knowledge or consent of the consumer, and whether police need a warrant/production to obtain it, relies in large part on the nature of the data collected. Data that is not identifying, that doesn't track the location of an individual or their device, and that is not about a specific person may not be private enough to fall under the protections of either PIPEDA or section 8 of the Canadian Charter — yet this data also poses significant risks to the freedoms that privacy is intended to safeguard: "Privacy rights are increasingly understood as having collective and not just individual dimensions" (Scassa, 2020a, p. 175).

The rationale for protecting individuals' privacy was not just to protect the sanctity of their personal information per se, but more fundamentally to ensure "autonomy, human dignity, personal freedom or interests related to personal development and identity" (Taylor et al., 2016, p. 14). The UN Office of the High Commissioner for Human Rights (2011, p.5) defined privacy as the "presumption that individuals should have an area of autonomous development, interaction, and liberty"; this freedom is frequently posited as foundational to other rights, for, as Privacy International writes, it "gives us a space to be ourselves without judgement, allows us to think freely without discrimination, and is an important element of giving us control over who knows what about us" (Privacy International, 2017). However, as Barocas and Nissenbaum (p.45) write, "common applications of big data undermine the values that anonymity traditionally had protected" and "even when individuals are not 'identifiable', they may still be 'reachable.'"

Big data technologies enable the analysis of such large and encompassing data sets; for example all cell phone location data throughout a city, that people's autonomy, freedom, and interests could well be infringed upon without any individual understanding of who they are. Taylor et al. (p. 15) write, "policies and decisions are made on the basis of profiles and patterns and as such negatively or positively affect groups or categories." It is on this basis that privacy philosophers like Nissenbaum, Taylor, and Floridi have conceptualized the idea of "group privacy" (Taylor et al., 2016) as a way of positioning groups, even anonymized ones, as being at risk for privacy violations.

In recent years, we have seen numerous examples of how such big data technologies and, more recently, artificial intelligence technologies, have discriminated against groups of people.

In recent years, we have seen numerous examples of how such big data technologies and, more recently, artificial intelligence technologies, have discriminated against groups of people (Barocas & Selbst, 2016). In most cases these have been already marginalized groups, as in the case of such technologies used to make decisions about social welfare (Eubanks, 2018), immigration (Molnar & Gill, 2018), recidivism risk assessment (Mattu, n.d.), advertising and online search results (Noble, 2018), and – most directly relevant to this report – in policing. Extensive research has now shown that 'big data' or 'AI' tools like predictive policing or hotspot analysis (Brayne, 2017; Linder, 2021; Richardson, Schultz, & Crawford, 2019; Robertson et al., 2020; Tulumello & Iapaolo, 2022) use the same pattern-identifying techniques to construct groups of people, or areas in which groups of people live, and single them out for specific action. In an extensive assessment of the situation in Canada, Robertson, Khoo, and Song (2020) came to the conclusion that such technologies would potentially violate the Charter rights of Canadians. Indeed, specifically on the issue of data sharing between law enforcement and other government agencies, they quote the UN Human Rights Council as saying that data sharing between law enforcement agencies and other state agencies risks violating privacy rights "because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another" (UN Human Rights Council, 2014, p. 27).

However, privacy regulations still lag behind this growing awareness. As Bennett and Raab write, "Indeed, this understanding is not entirely absent amongst privacy advocates and regulators as well, although the extent to which they can embrace it is constrained by the persistence of the individualistic and rights-oriented paradigm" (2018, p. 34). Recent policy-making around artificial intelligence technologies has begun to introduce broader thinking on collective or group privacy. In 2022, the Standing Committee on Access to Information, Privacy and Ethics released a report on facial recognition technology that acknowledged the social and collective risks to groups posed by such technologies. Artificial intelligence policies currently being developed by the Toronto Police Service also recognize the potential for these technologies to discriminate against groups. In these developments is the tacit agreement that 'big data' or 'AI' technologies can discriminate intersectionally. In other words they have a history and predisposition to amplifying existing gender-based, racializing, and class-based biases.

The juncture of intersectionality, privacy risk, and emerging technology is an immensely broad subject and has been covered from many angles (Benjamin, 2019; Crawford, 2021; Grzanka, 2018; Rambukkana, 2021). The following two sections will look specifically at the literature around the digital transformation of cities and intersectional risk and at law enforcement.

Digital transformation of cities and risks

Cities have become critical epicenters for responding to systemic risks across the societal spectrum. From poverty to nutrition, from education to aging, from wealth inequality to discrimination, from health to welfare, from technological change to environmental breakdown, or from conflict to immigration, all these issues intersect in cities – and as a result so do many of the undertaken and proposed solutions. It is for this central role that cities play that global bodies like the UN, the World Bank, or the European Union have invested vast sums in rethinking the governance of cities to meet these challenges. One area in which these tensions are brought together most dramatically is the digital transformation of cities. Cities have always been the locus and the testbeds for political projects, and the rapid rise of digital technology and its promises over the last few decades has led to a plethora of theories, discourses, projects, movements, and economic and social interests, all vying to chart a new, technologically based paradigm going forward for municipal structure (Lorinc, 2022; Mosco, 2019).

This technology-focused urban discourse has often been called the 'smart city,' however this term is now widely acknowledged to be creation of private industry public relations and to be more misleading than clarifying – particularly when attempting to delineate the intersectional risks posed (Green, 2019). Instead we refer to the digital transformation of cities through the adoption of smart technologies, a concept that enables a more social science-driven analysis of the structural, policy, social, economic, and political effects that have come about as a result of the use and attempted use of digital technologies in urban governance. There is a vast literature on this topic covering everything from political economy to policy and environmental science. Our goal in this section is to provide a foundational outline of the literature on how data collection and usage is developing in cities and what intersectional risks this poses.

Pre-dating the discourse of 'smart cities,' the technological and computational capacity to collect ever larger amounts of data, and to store, share, and analyze them, drove a "remarkably consistent vision of digital era public management reform" (Clarke, 2020, p. 98). Out of this vision, Clarke argues, developed a self-propelling dynamic in which "when public services and spaces are digitized, they produce and are subsequently shaped by vast troves of data" (105). Data began developing a significance, a value, and function, within municipal governance that was qualitatively as well as quantitatively different from the collection and usage of information in urban history until that point – this came to be known as digital urbanism, the digital city, the smart city, smart urbanism, or a host of similar terms (Brown & Toze, 2017; Lauriault, McArdle, & Kitchin, 2018; Meijer, 2018).

The promises were that increased 'big data' collection and analysis would make the city 'knowable' at greater depth and breadth than hitherto possible, while

Cities have become critical epicenters for responding to systemic risks across the societal spectrum. From poverty to nutrition, from education to aging, from wealth inequality to discrimination, from health to welfare, from technological change to environmental breakdown, or from conflict to immigration, all these issues intersect in cities - and as a result so do many of the undertaken and proposed solutions.

algorithmic and automated analyses and decision-making systems would enable viable responses to this new knowledge at a scale and high speed (Kitchin, 2014a, 2014b). As Tulomello and Iapaolo (2022, p. 6) write,

> *"Grounded in positive visions of data-driven urban omniscience, the epistemological assumption behind smart urbanism is that each city functions, ideally at least, as a complex "system of systems"—including transportation, energy, education, health care, public safety, and security (cf. IBM, 2011, p. 2; Marvin and Luque-Ayala, 2017). As such, cities' overall performance can be optimized by tackling urban problems in a holistic and coordinated fashion through the integrative analysis of geosocial data."*

As the authors and many other researchers argue (Mattern, 2021; Shapiro, 2020), the vision of data-driven governance was one of immense, ongoing data sharing across a fully interconnected and digitally networked city, coupled with as near to real-time analysis of and reaction to the data as possible.

Such a governance system, however, necessitated a significant shift in the loci of power and control. At that scale, at that speed, and at the level of deep embeddedness in information technology systems, many decisions were buried from easy oversight: "In these circumstances, the data steward (the actor or actors that control and manage those data) become de facto or de jure depending on the arrangement, the dominant governance actor wielding policy, oversight, and regulatory controls" (Clarke, 2020, p. 105). Critics also pointed out that the private technology vendors had an outsized impact on what technological solutions were designed for which problems (Green, 2019; Valverde & Flynn, 2020), leading to what some called "policy making by procurement" (Crump, 2016). As Franke and Gailhofer argue, "in the case of smart cities, and digitalization in general, the public sector does not have a leading, let alone monopolistic, control over either data or the tools to use it. Rather, it is confronted with an all-encompassing societal transformation which is dominated by private corporations. Moreover, the relationships between different actors have changed and become more complex" (2021, p. 4). While this research is largely based on the experience of large, global cities, the lobbying of municipalities by private corporations is evident in the Canadian context.

As we began exploring in the section on privacy and intersectional risk, and can concretize with regards to municipalities here, these technological changes were also political, economic, and social changes that brought about a new spectrum of associated risks. A central, and we argue often overlooked, dynamic in thinking about risk – and particularly privacy risks – here is the simultaneous risk resulting from inclusion in the system and from exclusion from it. This has been termed the problem of hypervisibility and invisibility in surveillance studies (Benjamin, 2019; Browne, 2015). Inclusion in the system means exposure to privacy breaches, algorithmic biases, and the effects of data-driven governance measures with a long history of negative, intersectional effects for marginalized communities.

Exclusion from the system can mean avoiding some of these effects, but also means lack of access to needed, beneficial services like healthcare, transportation, security, financial services, etc. These tensions are not a dichotomy, but, rather, frequently overlap and play out along the digital divide: the inequality gap that has opened up dramatically between those who have the privilege and the resources to access a city's high-tech services without risk of either invisibility or hypervisibility and those who do not and thus must contend with both (Abdelaal & Andrey, 2022; Andrey, Masoodi, Malli, & Dorkenoo, 2021).

It is on these lines of tension that intersectionality becomes a crucial lens. The divide, the effects of hypervisibility and invisibility, are not polarized but rather differentially distributed across a range of different groupings by age, gender, sexuality, racialization, and class. If privacy rights serve to safeguard rights and freedoms like autonomy, dignity, expression, freedom from discrimination, etc., then they must start by considering how these rights and freedoms are impinged upon along the intersectional lines of cities digital transformation.

There are innumerable examples of such violation or invasion in cities across the globe, but for the scope of this project around data sharing there are several significant issues. Data, as experts have pointed out, is not found in the world; it is created. It is the fabrication of technological systems responding to economic, political, and social needs, and thus suffers from the same problems of bias, error, and partiality. Further, as a product of interests, data is thus also predominantly the product of powerful interests. What gets measured, how, for which purposes, and to what effect is, to a large extent, determined by power (Beer, 2016; Foucault, 2019). In cities, the marginalization of groups can be caused, at least in part, by whether issues that affect them are poorly datafied (public transport coverage, access to nutritious food, broadband internet access, effects of climate breakdown, etc.), or where the data is removed from their control and used against them with little option for recourse (social services data, financial data, etc.). It is in these differentializing power structures of data that we find the intersectional risk to autonomy, dignity, self-expression, freedom from discrimination, etc. that privacy regulations are supposed to guard us against.

Finally, what the vast literature on the function and governance of cities as well as Open North's own influential work defining a more progressive "Open Smart City" (Open North, n.d.) also teaches us is that cities are not monoliths. Indeed, the very idea of the smart city as a "system of systems" constantly sharing data is predicated upon the understanding that cities are actually heterogeneous assemblages of various actors, each with its own powers, interests, and effects. What intersectional urban studies show us is that historically and ongoingly some of these actors have had markedly more harmful effects on marginalized communities than others. As such, from a data sharing and governance perspective, we must ask ourselves whether a blanket privacy risk assessment can be applied to all actors within a city, or whether some need to be treated with particular caution.

The very idea of the smart city as a “system of systems” constantly sharing data is predicated upon the understanding that cities are actually heterogeneous assemblages of various actors, each with its own powers, interests, and effects.

Digital transformation of law enforcement and risks

In parallel with the digital transformation that cities as a whole have been undergoing, policing has changed dramatically in its use of data and technology. The history of technological change goes back via multiple genealogies to the advent of patrol cars and two-way radio on the one hand and the introduction of centralized computational statistics for crime analysis on the other (Wilson, 2017, 2019a, 2019b). From these developments was born, in the late 90s and through rapid growth post-9/11, a massive and far-reaching transformation of the collection, analysis, and communication of data within police services and between police services and others government entities (Brayne, 2020; Ericson & Haggerty, 1997; Ferguson, 2019; Linder, 2021). Many of the same ideas around governing, or policing, on the basis of 'big data' collection and analysis emerged in law enforcement as well – driven in part by many of the same private vendors like Microsoft, IBM, or Motorola intensely lobbying police services to procure and implement their technologies (Linder, 2021).

Surveillance and security studies researchers have detailed extensively how, in the wake of 9/11 and the subsequent pressure and funding in the United States for police to engage in massive counter-terrorism surveillance (Ajana, 2013; Muller, 2010), vast systems of data collection, analysis, and sharing were set up (McQuade, 2015). The development of the infrastructure and computational technologies to conduct such surveillance, collect and store the data, analyze and share it, brought about the construction of a vast system of policing data that stretched far beyond the U.S. into similar developments in the U.K. and Canada and the rest of the Five Eyes global surveillance network ("Five Eyes | Privacy International," n.d.). On a more local, municipal policing level, Ferguson (2019) and Brayne (2020) have laid out in detail how police services began acquiring and using numerous new surveillance tools to collect data on cellphone locations, vehicle locations, social media, CCTV networks, and biometrics and to tap into databases held by other government agencies like social services, vehicle registration, traffic departments, other emergency services, and urban planning. As Linder (2021) described in detail, in Canada (as well as the U.S. where the trend began) these technologies continue to be used by police long after whatever terrorism threat that might have existed has disappeared and are now frequently centralized in so-called Real-Time Operations Centres (RTOCs). RTOCs serve as central command and control units for real-time big data collection, analysis, and dissemination. Their function is to access, analyze, and share data from the wide suite of CCTV, databases, algorithmic data mining, and automated decision making tools in order to, like cities, process and respond to data on a scale and at a speed that was previously impossible.

In Canada, as well as the U.S. and elsewhere, the last decade has seen numerous examples of police services breaching privacy regulations with tools like

In Canada, as well as the U.S. and elsewhere, the last decade has seen numerous examples of police services breaching privacy regulations.

international mobile subscriber identity (IMSI) catchers or ClearviewAI or operating in unregulated areas that were later deemed unacceptable (Bennett, Haggerty, Lyon, & Steeves, 2014). Compounding this disregard for privacy laws, it has been argued by numerous policing scholars that these surveillance and data analytics technologies exacerbate existing tendencies towards intersectional discrimination. Significant research has now shown that Canadian policing's historical discrimination against racialized communities (Maynard, 2017; Roach, 2022) and other marginalized groups like the homeless continues to this day (CBC News, 2022; Kwon & Wortley, 2022; Palmater, 2016; Stelkia, 2020; Wortley & Owusu-Bempah, 2011). Technologies like predictive policing, hot spot analysis, facial recognition, gunshot detection, or social network analysis have all been credibly accused of amplifying biases that already exist in data, enabling the hypervisibilization of already-discriminated against groups, obscuring discriminatory practices behind a false veneer of technological objectivity, and introducing further discrimination through biased algorithms (Brayne, 2017; Ferguson, 2019; Linder, 2021; Richardson et al., 2019; Tulumello & Iapaolo, 2022). An extensive analysis of these systems within the Canadian legal system came to the conclusion that these technologies and practices have "the potential to violate fundamental human rights and freedoms that are protected under the Canadian Charter of Rights and Freedoms ('the Charter') and international human rights law" (Robertson et al., 2020, p. 3).

What researchers like Brayne (2020) and Linder (2021) have shown is that these potentially harmful technologies frequently rely on data acquired through data sharing with municipal agencies. It is well past time that the siloing of thinking about the ethical and responsible digital transformation of cities and law enforcement be broken down. The next section takes a closer look at these intersections and provides an analysis of the legal situation for those intersecting technologies that have been treated in court.

Convergence of municipal and law enforcement digital transformation and emergent risks

From the perspective of the developments in data and digital technology usage, cities and law enforcement over the last decade are almost indistinguishable in terms of means. As Tulumello and Iapaolo write, "thus, put into perspective, the city-scale implementation of smart solutions, including predictive policing, as tools to solve otherwise intractable problems can be understood as part of a broader trend towards algorithm-based policymaking, and must be framed within the context of the smart city's global discourse and imaginary" and "crime control and prevention are interconnected with virtually every domain of urban policy, thus working as a synecdoche for urban policy more generally" (2022, p. 5). Joh offers the same analysis, saying "as cities become 'smart', connected and watchful, policing will become a less visible and a more embedded aspect of the urban environment. These developments represent but one more step in

When asked about specifics aspects of smart cities, study participants expressed the the greatest amount of concern about data sharing with police, with 76% saying that it shouldn’t be permitted or only with appropriate safeguards.

the rapid changes brought to policing by the increasing use of digitized data and artificial intelligence" (Joh, 2019, p. 181).

This convergence of law enforcement and municipal governance is causing a widespread erosion in public trust, as Bannerman and Orasch (2019) detail. Their survey found that 88% of Canadians were concerned about their privacy in smart city contexts. When asked about specifics aspects of smart cities, study participants expressed the the greatest amount of concern about data sharing with police, with 76% saying that it shouldn't be permitted or only with appropriate safeguards. In their legal analysis of this intersection, Robertson et al. (2019) found that "problems may arise when data is shared between law enforcement agencies, other government bodies, and the private sector" (p. 74) and "such data sharing arrangements could also erode public trust in essential social services and public service employees or deter vulnerable individuals from accessing such services" (p. 83).

A clear example of this convergence was provided by Thunder Bay's proposal for the Federal Smart Cities Challenge. The bid called for the use of smart city funding to support the development of an extensive police surveillance apparatus (DUNCAN & BARRETO, 2022). The bid makes the technological parallels between smart city devices and policing devices unmistakably apparent. It calls for "investments in smart public safety technology and infrastructure" (Thunder Bay, 2018) in which

- "smart poles will serve as connected safety stations and include intelligent surveillance cameras to record and analyze imagery in real time (and) send alerts based on suspected activities";
- "cognitive-based analytic systems (smart with prescriptive analytics) will analyze streaming data and issue alerts to appropriate response teams to action alerts (e.g. based on crowd size and activities). The system can detect violence or intoxicated citizens"; and
- "video Surveillance with Smart Camera and outdoor occupancy sensors (LoRa sensors) will be used to analyze and track people (without compromising privacy) quickly with the use of facial recognition and motion signature (gates). Location application overlay of movement and association (attestation) can be determined to narrow the search radius for missing people."

Although ultimately unsuccessful, this bid for federal funding is a carbon copy of existing real-time operations centres in police services in major urban centres across Canada and the United States. This surveillance-based digital transformation paradigm is only facing partial, piecemeal resistance when isolated technologies are criticized and ruled on in court. However, what can be criticized and ruled on in court is primarily a product of what the public can uncover, and law enforcement in particular has engaged in extremely secretive behaviour around digital data technologies. As a number of researchers in Canada have attested to (Linder, 2021; Monaghan, 2017), police secrecy impedes democratic oversight and discussion of the validity of these technologies and so critically undermines their

What can be criticized and ruled on in court is primarily a product of what the public can uncover, and law enforcement in particular has engaged in extremely secretive behaviour around digital data technologies.

legitimacy. Robertson et al. (2020) argue that "the absence of complete information poses a significant challenge in determining the extent to which existing or potential uses of algorithmic policing technologies may violate police agencies' constitutional and human rights obligations or may raise other legal concerns" (p. 150). This opacity and ambiguity was a key motivation behind this project, and also a central finding. However, before moving to that discussion a more granular look at how the courts have tackled the issue is necessary.

What does the data governance literature contribute to this issue?

As we have argued so far, rapid digital technological change has been frequently catastrophically undemocratic and exploitative, and one vector – although by no means the only vector – through which this has occurred is via the direct and indirect violation of privacy and the resultant intersectional risks to human rights and freedoms. The sometimes subtle, sometimes blatant violations of these rights has led to a wide-ranging collapse in public trust in private and public usage of digital technologies (Bannerman & Orasch, 2019). We argue in this section that data governance is evolving into a crucial tool with which to redesign how data and technology are used in society and rebuild that trust.

Discourse and practice around data governance has evolved considerably over the last decade, moving from a predominately corporate concept to an explicitly politicized socioeconomic framework for shifting power, benefit, and responsibility in a rapidly digitizing society. There are several aspects to this change, however the most relevant to this report are data governance's promises to restore trust in digital systems through accountability, transparency, and inclusivity-enhancing measures. Although still undergoing rapid evolution, several such data governance measures are developing to achieve these goals by transforming how the public is involved in decision making across the data and technology lifecycle and how privacy and risk are assessed on collective and systemic levels as well as individual.

The concept of data governance derives originally from the private sector and was advanced throughout corporate industry as a framework through which to maximize the value that could be derived from the data a company held. Numerous handbooks and manuals, most notably the '*Data Management Body of Knowledge*' but many more besides, attest to this governance treatment of data as a resource to be effectively managed and leveraged for profitable gain. However, with the rise of the 'smart city' as outlined above, so too the idea of data governance entered into the sphere of municipal governance. Given the marked neoliberal, private sector-driven structure of early 'smart city' projects (Cardullo, Di Feliciantonio, & Kitchin, 2019; Mattern, 2021; Mosco, 2019; Valverde & Flynn, 2020) this crossover is unsurprising, particularly in the wake of decades

of New Public Management transformation. In this discourse, cities were exhorted to understand the multivalent, pluripotent value of data: to realize its multiple uses and values, and to best effect such realization through comprehensive and rigorous data governance (Abraham, Schneider, & vom Brocke, 2019; König, 2021).

As the field of smart city development has matured, however, there have been movements to shift away from private sector- and user-centric paradigms into more ecosystemic conceptions of cities as networks with highly heterogeneous stakeholders, communities, interests, and incentives. "Data governance," as Franke and Gailhofer put it (2021, p. 5), "in turn, decides what data may be collected and used, by whom, in what way, and for which purpose, including, e.g., rights to access and/or use data as well as rules to manage and control the quality and completeness of data." In this change, so too the concept of data governance has expanded. As we saw in the previous sections, thinking about data became more than thinking about data as a singular resource and instead involved considering it as an environment, or a "datasphere" (Davies, 2022). As Choenni et al. write, "Given, on the one hand, the importance of data sharing in a smart city and, on the other hand, the increased complexity involved with data sharing among (many) stakeholders, we argue the need for establishing appropriate data ecosystems" (Choenni, Bargh, Busker, & Netten, 2022, p. 32). This paradigm treats "data as being more than just about data" but instead as being constitutive as well as reflective of society's structure (Linder, 2023). Data, as Kitchin has argued, is not given in the world but rather constructed by the systems people have put in place – in which case data governance is a crucial mechanism involved in that construction. Whether concerning data collection, quality, sharing, management, sale, visualization, or destruction, these are all data governance issues and are fundamental in the central sense to the structure of our society. Data governance therefore concerns itself with society as a system.

This change in thinking places greater emphasis on three key components, and in so doing crucially re-orients the purpose and goal of data governance: participation, value, and risk. As Franke and Gailhofer's definition above demonstrates, the first change that comes through clearly in their definition is the centralization of the 'who' of decision making as prior to the 'what' of the decision. If data governance is fundamental to the structure of society, it behooves a democracy to be inclusive in the structure of decision making. In combination with the realization that there are multiple types and perhaps contradictory interests in value creation with data, we've seen the wild proliferation of thinking and experimentation with different data governance models, like data trusts, commons, collaboratives, cooperatives, and other stewardship models. To appropriate a phrase: data is too important to be left to the managers – the public must be brought in.

The issue of broader participation and value is crucial, but less immediately relevant to this particular project. On the issue of intersectional privacy risk and governance, the change in thinking about data governance has also placed greater

emphasis in the literature on thinking more expansively about risks, and the need for more participatory democratic involvement. In the corporate approaches risk is treated mainly from a compliance perspective, and data governance tools were concerned with issues like cybersecurity or adherence to privacy legislation. In Canada, the collapse of the Sidewalk Labs smart city project in Toronto had, to a large degree, to do with the mismatch in existing data governance thinking around issues of risk, privacy, and who got to have a say in what data was shared with whom, for which purpose, and how the risks around that were analyzed and mitigated (Lorinc, 2022; O'Kane, 2022; Valverde & Flynn, 2020). Indeed, Scassa, writing about the abortive attempts to develop new data governance models towards the end of the Sidewalk Labs project, says "in some cases, the nature and/or volume of the data to be collected, the obvious demand for access to the data, the individual or group interests in the data, or the need for compromise between public and private sector partners, may call out for the creation of a new data governance framework to facilitate data sharing according to articulated values" (2020b, p. 46). In response, municipal data governance in Canada is trending towards more "openness and collaboration" (Chen, 2023, p. 105), and some of the larger cities like Toronto and Montreal have begun developing digital charters on data governance to emphasize risk assessment and community engagement, e.g. the City of Toronto's Digital Infrastructure Strategic Framework.

Choenni et al (2022, p. 41) have conducted a recent assessment of identified changes to data governance as a result of the kinds of privacy issues we identified in the previous section. It is worth quoting them at length here. They recommend a framework that

- is attuned to identifying and mitigating privacy risks, rather than making a dichotomy between personal and non-personal data, or between private and public spheres,
- provides a new approach to notice and choice, with an emphasis on enhancing user awareness and understanding rather than presenting corporate disclaimers of liability,
- allocates responsibility according to data usage and the risks inflicted to data subjects, rather than making a formal dichotomy between data controllers and data processors,
- makes a sensible balance between data retention needs and individuals' right to be forgotten; and
- governs cross border data transfers based on accountability and ongoing responsibility, rather than creating arbitrary barriers and requiring bureaucratic form fillings.

The first and second point have been treated as particularly important, and Choenni et al. (p. 41) themselves complete their assessment with "In summary, there is a need for alternative types of agreement such as the formation of multistakeholder bodies and mechanisms to help privacy governance." The last few years have shown considerable innovation in thought, and slowly even in deed,

in this area. The growing realization that there are risks to autonomy, dignity, self-determination, free speech, etc. – rights that are safeguarded at least in party by privacy rights – that function on the collective or group level, or further up the value chain, and thus are not countered by regulations centered on personally identifiable information, has led to growing calls to incorporate public engagement in privacy and risk assessment.

This expansion of data governance thinking to actively include public participation has been most notable in the subsection that concerns itself with the governance of artificial intelligence and big data technologies. Indeed, Solano et al., writing about AI data governance for the European Union (Solano, de Souza, Martin, & Taylor, 2022, p. 4), argue that given the rapid changes to the way data is being collected and used, and thus the unknowability of emergent risks, structural involvement of public participation, particularly of marginalized and impacted communities, is essential. The growing literature on algorithmic impact assessments (Moss, Watkins, Singh, Elish, & Metcalf, 2021; Reisman, Schultz, Crawford, & Whittaker, 2018) emphasizes the criticality of community involvement in the assessment of intersectional risks, but also warns that it is a potentially very broad term that can be understood differently by different stakeholders and end up obfuscating more than it clarifies. As such, it is crucial, as OpenNorth has argued extensively (Linder, 2023), to ensure that public engagement is transparently and accountably determined within a data governance framework, while also ensuring it is flexible enough to adapt to the issue under consideration.

While, as many researchers continue to point out, the field of data governance research and development continues to change rapidly, what this outline shows is that data governance is expanding its remit to cover a much broader digital ecosystem. This expansion is driven, in part, by concerns about privacy risks that are not easily grasped within more established privacy protection regulations: group privacy, social harms, risk from upstream applications of aggregated or de-identified data, algorithmic bias, and as yet unknown emergent risks. While data governance is not on its own a solution, nor is it yet even clear what exact structures it should take on, it is rapidly becoming a key tool in the toolbox for municipalities. Recommendations like clear and accountable mechanisms for public engagement, transparent decision making across the data lifecycle, risk analysis beyond PII, and alternative data stewardship models are all charting new paradigms for intersectionality-aware data governance.

Yet despite this advance, and the extant debate about policing and data, this data governance literature looks exclusively at cities in general and higher levels of government, or at private corporations. The discourse has not yet expanded sufficiently to explicitly consider an organization like law enforcement, even though it is a significant and unique actor in the digital data ecosystem. The next section takes a step in that direction by delineating our empirical findings on the state of governance of data sharing between law enforcement and cities.

RESEARCH FINDINGS

Law Enforcement and Local Government

As noted in the methodological section, we conducted interviews with 27 individuals across five municipal or regional police services and 10 municipal or regional governments. Due to the high level of resistance we encountered to being interviewed on this topic, our results cannot be said to represent the actual frequency or distribution of these "states of data sharing and governance." However, as the following sections will show, these 'states' were acknowledged in the interviews with sufficient regularity that they can be considered common enough to warrant serious consideration.

While the interviews covered many different aspects of data sharing and governance, we have chosen to focus on four areas: what respondents acknowledged knowing of the current state of data sharing; how the current state of data sharing governance was articulated; whether any privacy or impact assessment was undertaken that went beyond PII; and whether participants thought that any change to data sharing and data governance was necessary. Careful content coding of the interviews revealed a number of types for each of the four focus areas. The following sections are organized by areas and types, rather than by interviewees, institutions, or case studies. This has the effect that interviewees will be mentioned multiple times across the section, which in turn allows us to highlight patterns as well as inconsistencies and tensions.

The state of data sharing between Law Enforcement Agencies and other municipal agencies

The first and primary line of questioning across all interviews was about the amount of data sharing that occurred between municipal or regional government and the respective law enforcement agencies. This was met with a wide range of responses, with interviewees differing on how much they concretely knew was being shared and how much they suspected was being shared, but about which they didn't have concrete knowledge. This is a crucial differentiation, as can be seen throughout the following sections, because it underscores the dominant outcome of this research that there is frequently little oversight over how much data is being shared, how it is shared, and with whom.

#1 Type: There is not a lot.

One common initial response was that they didn't think there was a lot of data sharing happening. What exactly constitutes 'a lot' was hard to pin down and

undoubtedly differed across respondents' subjective assessments. However the exact responses are illuminating. As a director of information and technology (IT) services at an Ontarian police service said "So, I will say there's a lot of intersections. But I think, also, surprisingly, there's very little data interchange between the entities" and "so, as far as data interchange, there's not a lot that I know of." Another director of IT in a major Albertan police service said "police have done an absolutely terrible job in terms of sharing data across the organization or across the country."

Municipal employees leading the smart city division of a city in the Greater Toronto Area (GTA) echoed this statement, saying that they shared traffic data around accidents and other incidents, but were not aware of anything else. This assessment, that maybe there was some sharing of traffic data, but not much beyond that, was reiterated by another chief digital officer of a major Ontarian city. They went on to say, "but otherwise, from a city data perspective, or things like that, there's nothing that I've come across in my time here. Or no, there's no data sharing agreements in place, either" and "from a data sharing perspective, really, I'm not aware of any instances where data has been shared."

Prima facie, it would seem that a significant percentage of the institutions we interviewed did not think that there was much, if any, data sharing happening between law enforcement and local government. However, the respondents above as well as others frequently qualified this initial response with statements that while they did not know exactly what or how much was being shared, they thought that there probably was data sharing happening, but that it was not sufficiently registered or governed for them to know about it, or that it occurred on an unofficial level and did not feature as a data sharing 'agreement.'

#2 Type: We do not know.

One of the directors of law enforcement IT cited aboves continued by saying: "We have…a lack of formal governance policy or formal data-sharing policy. I guarantee you that there are other places that have shared data, either with or without an MOU (memorandum of understanding) that I may not be aware of. So there… there may be ones in addition to that, but I just don't know where they are." This kind of qualification after stating that there was not, to their knowledge, much data sharing happening, was a common trend throughout the interviewees' statements.

A member of an Ontarian police service board said that data sharing was an operational issue, and thus not within the purview of the board, and "as far as operations are concerned, I am not aware of any direct data sharing." A senior employee of a real-time operations center (RTOC) in the GTA, spoke at length about the real-time operations center's data sharing with other law enforcement agencies as well as its ongoing efforts to expand direct access to municipal as well as private CCTV networks (e.g. in malls, schools, campuses, etc.) – but went

on say that "indirectly, some of our our people within here have relationships with others at post cities where they may exchange information, but I don't know that any of that is done on a formal level" and "in terms of anything else, I don't I don't really know how that's done."

These kinds of responses cast a different light upon the statements that only limited data sharing is occurring. This is not to imply that they are incorrect, but rather that the very terminology involved is misleading. What, exactly, do all parties understand by 'data sharing'? What does it mean when heads of information technology (IT) departments or operational managers of data heavy units like a RTOC say they "do not know" of any data sharing? These are not intended to be rhetorical or facetious questions, but rather to highlight the startling ambiguity we encountered when asking what we had thought were simple questions about how much data is shared, how, and by whom.

#3 Type: Yes, there is data sharing.

As frequently as we were told that there is not any data sharing and that there might be but the amount is unknown, we were also unambiguously told that there was – although this was sometimes by the same people who told us that there was not or that they did not know.

The two most common areas of data sharing mentioned were traffic incidents (near ubiquitous across respondents) and social service and health data. For example,an IT director at an Alberta police service, despite stating above that sharing was inadequate and the data quality bad, said "we do…we share a lot of data with the city. So…particularly…a really good example is our traffic data," and also, "We're trying to get our health care system kind of plugged into that whole concept of policing." Two major GTA police service IT directors also spoke of the importance, and difficulty, of sharing health data for social services, whether with regards to opioid crisis calls for service, or for mental health calls. The Albertan IT director went on to add that "we also work closely with, you know, with bylaws, some of the social disorder sort of data, as well. Right. So we've got, we've got friends, you know, there's maybe a certain supermarket down in [City X] that's attracting a lot of social disorder. And there's a homeless camp setting up here. So we work closely with some of our homeless support agencies and things like that. So we were sharing that data back and forth."

One of the Ontarian IT directors said that they had "only shared data with one entity, and it was through a formal MOU." This entity was a public safety organization running a risk terrain modelling (RTM) project. RTM is a significant, big data–driven, predictive policing technology that seeks to leverage data collection and sharing from numerous sources across a city to predict what elements in a city's infrastructure (hedges, lights, proximity to bars and liquor stores, etc.) are criminogenic (Robertson et al., 2020). However, an MOU is not a formal data-sharing agreement and the data governance of Peel Police's MOU remains unclear.

The RTOC with which we spoke continues to actively seek data-sharing agreements with CCTV networks belonging to cities as well as malls, gas station chains, corner store chains, schools, and campuses. SImilarly, the ambiguity and its potential causes came to the fore with another GTA police service after we spoke with their board. After saying that data sharing was an operational matter and they weren't aware of it, the service's two senior IT directors said independently of each other that there was extensive data sharing occurring as a matter of policy between numerous organizations, including the city's traffic department and various social services agencies. These inherent contradictions highlight a lack of standardized language and understanding and thus comprehensive oversight over what data is shared. Based on the numerous interviews undertaken for this research, it appears that the ambiguity is not a result of disingenuity but rather, a result of a lack of common language and policy around data governance.

A different Albertan city also reported wide-ranging data-sharing projects, going back many years. Beyond the usual cases of traffic data sharing, they also mentioned another risk terrain modelling project, as well as another that also involves sharing data between law enforcement and various agencies of the city. The city's IT director spoke not only of the many data-sharing projects, but also of their data and technological details as well as the data governance frameworks that were in place to govern them. In this case, the existing data governance frameworks appeared to be considerably more developed than others – but actual comparison is made impossible by a lack of comprehensive data.

Finally, one trend that emerged across a number of different interviews was the subtle yet noticeable tendency to raise open data portals when asked about data sharing, for example from one GTA police service IT director: "because of external pressure, we developed an open data policy and put data that we thought we could put on, on our website, basically." As our interview sample is not representative it is not possible to know whether this trend is reflective of a concerted phenomenon; but even as a set of isolated incidences, or as a reaction to an interpretation of 'data sharing' that focuses more on a general, public, transparency-driven notion of the concept, it is noteworthy. Six other cities and law enforcement agencies all referenced their open data portals as examples of what they considered to be data sharing between law enforcement and local government.

Interestingly, in some cases, open data portals were described as replacements for specific data-sharing agreements. A couple of participants said that this replacement had come to the detriment of their projects, as the quality of the data – particularly the rate at which it was updated – declined, causing projects to be shuttered or drastically redesigned. Across the mentions of open data portals as a kind of or substitute for data sharing was the implication that this was a simpler, low-cost way of going some way to fulfilling requests for data without the difficulty of working through purpose-driven data-sharing agreements. It is to these agreements that we now turn.

The state of governance of data sharing

The second set of questions asked about the data governance frameworks and policies in place to govern how data was shared. Here we received a similarly divergent range of responses, which again is probably just as reflective of the lack of standardized language and understanding around thinking about data governance as it is about the state of actual data governance.

#1 Type: We lack a formal and comprehensive policy.

To revisit the issue of open data portals as a form of data sharing between law enforcement and municipalities again, a number of those who brought this up referred to the act of designating data as acceptable to be 'open' as sufficient in terms of governance. That is, any data that can be designated as open – sometimes explicitly on the basis of freedom of information legislation, sometimes implicitly – is shareable with any entity, obviating the need for any further governance considerations. In some cases it was implied that this solution was chosen in lieu of a more complex, differential data-sharing governance framework. For example, an IT director of a police service in southern Ontario spoke of open data as their data sharing: "How we share information between our organization… between us and the region – we haven't had those discussions. And maybe we should, right…but how do we share data…we have never sat down and talked about it." This point was echoed by an IT director in the GTA, saying "I'm relatively certain that there are some people who…some smart people in our organization who connect to the open data portals and get data from…. I don't know that it's done in any kind of coordinated way. It's, you know, people taking the initiative to go. But I would say that we don't have a – to the best of my knowledge, we don't have a policy around that."

In line with the comments above about open data governance, participants also said that in general there were no frameworks that comprehensively cover all data sharing. The IT director quoted directly above said, "We have lacked, still do lack formal governance policy or formal data sharing policy. I guarantee you that there are other places that have shared data, either with or without an MOU that I may not be aware of." And serendipitously speaking directly to that, the senior RTOC employee of the same law enforcement agency said "Indirectly, some of our people within here have relationships with others at cities where they may exchange information, but I don't know that any of that is done on a formal level, right?"

However, confusingly, that police service also contradicted that statement – and most other respondents also indicated that they do at least have data sharing agreements, if not overarching governance frameworks that guide sharing policy as a whole. These we have sorted into the following two types.

#2 Type: There are policies of sorts.

A number of respondents said they had standardized procedures in place to govern data-sharing requests and agreements. The RTOC, for example, stated "Now, all of that access is governed not only through the MOU, but through the (information and) privacy commissioner (IPC) as well." From our conversations it was clear that the police service had clear, IPC-approved MOUs with the public and private owners of the CCTV networks they could access via the RTOC. They were also clear that the data sharing they conducted with the risk terrain modelling project was also governed by an MOU. It seems from this clarity that sizable, significant, ongoing projects were covered by MOUs, but there is also a lot more informal data sharing. It was unclear from the responses we got whether this informal sharing was in contravention of a policy or is an area that is uncovered by policy.

This was made even less clear by the IT director of that police service saying, "We don't just turn over data to anyone who asks. If somebody is asking they should there should be a formal agreement between us and the requesting agency." However, an MOU is not a formal agreement in the sense that it is not a legally binding agreement. A data-sharing agreement, such as the kind required by several cities to share their CCTV networks with law enforcement, is a legally binding agreement. According to one of these cities, MOUs are insufficient in this age of valuable and risky data, and shifting to legally enforceable data sharing agreements is a key component of their nascent Data Sharing Initiative and is considered by them to be a best practice that other public institutions should adopt.

Indeed, MOUs were cited by many other interviewees as the frameworks by which data sharing agreements were governed. Another GTA police service IT director said that data sharing between the service and social services, traffic, and community housing was governed by MOU. Interestingly, when asked how these kinds of data-sharing agreements were governed, under what kind of policy, another IT director of the same service said "So those would be going through the board and will be made public at some point." This directly contradicts what a member of that board had said, that the governance of data sharing was an operational matter and thus not under the purview of the board. This may reflect the long-standing disagreement over the proper remit of a police service board vis-a-vis the police service (Roach, 2022, p. 13), or may reflect further conceptual ambiguity around MOUs vs. legally binding data-sharing agreements. Either way, it is indicative of the lack of comprehensive understanding and coverage of 'big data'-adequate governance. Finally, one of the Albertan cities also said they used MOUs with their police service for all data sharing projects, including the risk terrain modelling project — until they were cut off and the MOU was replaced by the police service's open data portal.

It was not clear from the responses we got what exact data governance measures were included in the MOUs, but one mechanism that was brought up frequently

was PIAs. PIAs will be discussed further in the following section on intersectional impact analysis, but in terms of data governance our conversation with a Nova Scotian city is instructive. Their IT director said that while an MOU with the police service was not necessary as they are not a distinct entity like many others are, all data collection projects had to undertake PIAs as mandated by Freedom of Information legislation. However, it was under the authority of each business unit's executive director to decide whether or not to do such projects, and the police service was known to take a considerably less stringent view on their necessity, which might lead to the collection of data that other business units would not have authorized. Here, too, we see an example in which individual data projects are de jure covered, but de facto as a whole the system is less than comprehensive due to an insufficient overarching data governance framework.

The state of intersectional risk assessment in the governance

As the conversation with Halifax shows, our questions about governance frameworks quickly lead to conversations about privacy and other impact assessments they conduct as a part of data governance. Here, too, we received a range of different responses detailing the degree to which interviewees did or didn't assess privacy or other impacts when engaging in data sharing. While also not necessarily representative of the situation across Canada in proportion, the types of responses we received do indicate different levels of understanding of the importance of assessing privacy risk to individuals. As we discussed in the literature review section, privacy understood as the PII of an individual is the dominant paradigm for assessing this kind of risk, but not the only one – and there is a growing realization that 'big data' and 'AI' technologies necessitate a more expansive conceptualization of privacy risk. This section provides an outline of some of the different ways in which privacy risks are being thought about with regards to data sharing between law enforcement and local government.

#1 Type: Personally identifiable information.

As is to be expected, there was fairly widespread reference to freedom of information law, and claiming on that basis that as long as data wasn't personally identifiable information there was no issue in sharing it. To that end, a number of data-sharing projects like the Risk Terrain Modeling projects claim to only share de-identified and minimize information. In the case of one city this was data points on incident, location, and date. In the case of CCTV data sharing, their MOUs with the camera owners have requirements about footage retention time for live access. Past that time, a production order is required to access the data. Some referenced PIAs as tools to ensure that PII had been correctly determined, as what constitutes PII is not necessarily immediately clear, and PIAs are supposed to generate the kind of contextual analysis to make that determination. Several said they conduct PIAs for all data sharing projects.

However, as the research on the real-world effectiveness of PIAs shows (R. Bayley et al., 2007; R. M. Bayley & Bennett, 2012), their proper application is patchy, as is borne out by several interviewees. Some also said that while they only provide de-identified incident data along three data points (location, date, incident type) they made that assessment to use these particular data points without conducting a PIA. The following quote from a GTA police service IT director once again underscores the kind of patchwork ambiguity around data governance we encountered:

> *"In the case of (RTM project), we made sure all the information was anonymized. So we didn't provide any personal descriptors. I think we provided a lat / long. I'm sure we provided an age and a sex, and then the type of incident. So in that case, I don't think we did a PIA.... But whenever we are standing up a new system, we do a privacy impact assessment. And in order to recognize the – what we need to do to keep the data safe still, in some aspects? Yes, we do. Absolutely. Not usually not in the context of data sharing, because again, we're – as a police agency, we tend not to share a great deal. Yeah."*

This quote shows how crucial comprehensive data governance, and a broad understanding of the language around it, is to properly governing the rapidly emerging data ecosystem. It's no secret that PIAs are only as effective as their implementation and continued oversight (R. M. Bayley & Bennett, 2012; Bennett & Bayley, 2016; Bennett & Raab, 2018) and need to be embedded in an ecosystemic governance framework and practice to fulfill their intended role.

#2 Type: Beyond anonymization

Most interviewees either avoided responding to the question about intersectional or group/collective risks, or did so within the frame of PII. This is again likely primarily a result of a lack of awareness of this kind of privacy risk thinking, not an attempt at evasion or obfuscation.

Speaking of their open data portal as a data sharing project, a GTA police service IT director said that in the assessment of what data could be safely considered 'open' was an analysis of whether the data could differentially stigmatize certain groups. They said this assessment was undertaken together with public stakeholder groups to provide sufficient perspective on the issue. They were unable to provide details about how this stakeholder engagement is organized and to what degree it is standardized policy, but it would represent an example of privacy impact assessment that goes beyond the consideration of PII to include issues of intersectional group privacy.

Another strong example of assessing intersectional privacy risk is demonstrated by one of the Albertan cities we interviewed. For all their projects, but most notably with regards to their RTM, they claim to undertake a gender-based analysis plus (GBA+) analysis: "We also do what we call a gender based analysis assessment

as well. Just sort of looking at okay, so in looking at anticipating the impacts of this project, are we, you know, potentially doing any harm to vulnerable populations?" What, exactly, the assessments for the GBA+ tool are wasn't clear from the responses we got, but we were told that it wasn't just a box-checking exercise exercise. Staff had received GBA+ training, and for each project they were required to articulate how they had undertaken the assessment and what conclusions they had drawn. The city's in-house data ethics specialist explained that GBA+ had been brought into the city from the federal government's GBA+ policy (W. and G. E. Canada, 2021), and they were in the process of maturing their usage of it. While staff were required to take extensive training there wasn't yet sufficient experience in using it, and it is still very much an internal consideration process and lacked more fulsome public stakeholder engagement.

GBA+ was also deployed within a broader approach towards risk and impact assessment. Their data science manager said, "So, there's three things that we look at in projects. It's just part of our intake process. One is privacy. So we have the office of the city clerk here in the city. So you know, if a project requires one, we go through a privacy impact assessment. So privacy is one. So that tells us what we can and cannot do. Data ethics is a second, which – that tells us what we should and should not do. And then the last one is gender based analysis, GBA plus."

While the exact steps and procedures involved in this assessment did not come through in the interview, their manager did provide insight into the results with regards to intersectional privacy and risk assessment on their RTM project:

> *"This is an approach that is meant to democratize insight that would normally be only held by enforcement bodies to social service agencies. So that's one way that serves GBA plus. And even to get a bit more granular in the way that it serves GBA pluses from the principles of data minimization. So there's no personal personally identifiable information included in the application. The entire model is based on three data fields. So the time of a locate, and sorry, the time of an incident, the location of the incident and the incident type. So there's no offender data in there."*

In this response we can see an approach to data, data sharing, and data usage that considers intersectionality far beyond the narrow understanding of individual privacy risk. This approach includes a consideration of risk to groups as well as how they may also be better served as well as just protected: "We're doing community safety prediction; but then thinking, you know, on a community safety continuum, who is the most appropriate person to respond, like, all the way from, you know, social services to law enforcement." Such an approach is far more commensurate with the growing awareness that it is not enough to mitigate privacy risks, but it is also incumbent upon service providers to ensure that other risks, like the inequitable distribution of benefits, is also considered.

However, the city's approach was in the minority, and a number of participants were clear that they needed better policies and frameworks to adequately tackle the growing data ecosystem. We turn now to those calls.

What needs to change?

In keeping with our overarching assessment of the heterogeneity and ambiguity in the governance of data sharing between local government and law enforcement, the responses to the questions about what needs to be changed to improve the current situation and/or prepare for the future also diverged wildly.

One IT director of a police service in Ontario said, as we noted earlier, "We have lacked, still do lack, a formal governance policy or formal data sharing policy. I guarantee you that there are other places that have shared data, either with or without an MOU that I may not be aware of." They continued to say, "I think that there has to be some kind of parameters and formality" and "so I think someone needs to kind of put a framework in front of them (the police) of, this is how you do x so that we can follow it, because otherwise, we will find the path of least resistance." According to them, while there may be in some instances some policies that cover data sharing, they are frequently inadequate and do not provide comprehensive coverage, especially when seen in the light of the digitalization still to come. However, they think that although some police services are beginning to develop their own policies (e.g. the Toronto Police Service's new AI policy), what is needed is standardized policy implemented on the provincial level to better ensure safe sharing between organizations and between provinces.

An IT director at an Albertan police service noted that another aspect of this issue is that of data quality: "Police have done an absolutely terrible job, in terms of sharing data across the organization or across the country"; "The data quality in policing is just terribly poor, which has caused agencies to say, oh, honestly, I don't want to share it." Many stressed the growing importance of data sharing with other service delivery organizations, like social service, health care, housing, emergency response, etc., but then bemoaned the difficulties in getting data shared in the timely and effective manner. They continued with, "Yes. And which we could use some help with, for sure. It's like, there's nothing legislated across Canada, or even provincially, for that matter, to say, hey, you need to standardize these fields. Like, something is something as good as that would, would really help drive it forward. So every agency kind of does their own thing, you know."

A similar concern was expressed by an police service IT director in southern Ontario on the subject of Next Generation 911. The NG911 system represents a paradigmatic example of the intersection of digital transformation of law enforcement and local government: it involved a full systems change from the analogue 911/e911 systems to a fully digital emergency call and response management system that would be capable of collecting and sharing far more data than just a call.

The NG911 system would enable and maybe even require inter-provincial sharing of potentially very high-risk data like health data, emergency incident data, offender data, and live footage data – but without data governance standardization this would be very difficult to do adequately. In addition to this instance, NG911 was brought up (without prompting on our side) as a looming and problematic area around data sharing by nearly half of our interviewees. Local governments and law enforcement have been mandated to switch over to NG911 by 2025, and according to our respondents very few are on track to do so with adequate levels of governance.

Looking forward to even the near future, a GTA IT director said that far better ecosystemic data governance was necessary to handle even the upcoming plans for the Community Safety and Well-Being Plans the province of Ontario and others were developing. The plans are intended to coordinate emergency and social services across the area, but currently lacks sufficient data governance systems to ensure its proper functioning. Looking further, as the Toronto Police Service's work on their AI policy has shown, agencies across the country still have a lot of governance development work ahead of them to properly cover more disruptive technologies coming down the pipeline.

Specific ideas for data governance improvement are disparate and contested. A member of a GTA police services board, for example, said that the board's recent AI policy alone was not enough to cover the upcoming changes. On the topic of the governance of data sharing specifically, he brought up the idea of a registry of data sharing, akin to the idea of an AI registry that is rapidly becoming standard practice – but declined to say whether he thought it was necessary or not. That service's IT director, however, emphatically thought a data sharing registry was a good data governance policy innovation. However, many other participants saw the need for improvements in general but were unclear about what exactly those should be and who should implement them.

It is into this ambiguous need and vacuum of solutions that we introduce the results of our two expert workshops on digital technologies, data governance, and policing in the next section.

Expert Workshops

As we have shown, the results of our interview-based research were confused, ambivalent, ambiguous, highly heterogeneous, and as such difficult to interpret. We had noted across our interviews that interviewees could not speak to the situations in other police services or local governments. There was a distinct lack of comparative or country-wide knowledge – itself indicative of a problem, particularly when considering the inherently multi-stakeholder nature of data sharing – and as a result we decided to host two workshops with experts in this field to try and add another layer of information collection and analysis to our research.

The workshops had slightly different foci and somewhat different participants to elicit a more fulsome collection of opinions and data. The first focused on the police use of data and digital technology broadly, with exploratory questions about the digital and democratic governance thereof. The second was more narrowly focused on the intersectional risk issues of data usage and sharing in law enforcement. Participating in one or both of the workshops were Brenda McPhail, Renee Sieber, Merlin Chatwin, Teresa Scassa, Vivek Krishnamurthy, Thomas Linder, Christopher Parsons, Cristiano Therrien, Jonathan Obar, Bianca Wylie, Daniel Konikof, Alex Luscombe, Ushnish Sengupta, Alok Mukherjee, Meghan McDermott, and Jamie Duncan. In this section we summarize the workshops' findings, before putting them into conversation with the interviews in the final conclusion. The workshops produced five key assessments of the current issues around law enforcement's use and sharing of data and data-driven technologies, and from them four recommendations for improving the situation.

Law enforcement is unlike other government agencies

A central question underlying this research project was whether law enforcement needs to be treated differently than other governmental organizations and whether data sharing with law enforcement or law enforcement's acquisition and usage of data and data-driven technologies is inherently riskier than with other institutions. Participants in both workshops agreed this was the case, arguing that the combination of police discretion and the legal mandate for the use of violence on its own would justify the assertion. However, the police also have a well-established history and present of systemic discrimination against minority and marginalized groups like women, trans people, queer people, people experiencing homelessness, people of colour, Indigenous people, people experiencing mental health issues, and environmental or left-wing activists. Understood, further, in combination with the current deployment of law enforcement to manage a whole range of social issues far beyond crime, the mixture of state-sanctioned violence with systemic discrimination dramatically exacerbates the intersectionality aspect of privacy risk posed by the access to and use of data about such groups.

Brenda McPhail is worth quoting at length here: "More broadly, are there unique risks of sharing data with law enforcement? Of course, because law enforcement is a body that is granted significant discretion in our society to take actions that have enormous consequences for individuals in their lives. So, it would almost be better to say, what are the unique risks rather than are there [such risks]? The unique risks come with the power asymmetry between law enforcement and individuals, and the impacts that law enforcement activities have on individuals lives, exacerbated, in the intersectional way of speaking, by what we know about the ways that systemic discrimination is embedded in policing processes and policies and behaviors.... Intersectionality absolutely provides, I wouldn't say just a useful lens, I would say a necessary lens."

This sentiment was echoed by the participants in the two workshops and became a key perspective for interpreting the ambiguity in data-sharing practices and governance presented by the interview participants. When looking at an absence of governance for sharing data with an institution whose actions have disproportionately negative consequences for particular community groups, the urgency to address the insufficient guardrails increases.

Governing personally identifiable information is insufficient

As already detailed in a previous section, the arguments around what does and does not constitute PII have been argued for years. The workshop experts agreed that this was a serious issue as PII fundamentally delineates in Canadian law the difference between data that should be considered for risk and data that is without risk. Yet, the fraught nature of this conceptual dichotomization is only going to be exacerbated by emerging technologies. Big data and algorithmic analytics have for a while now enabled the use of anonymous data to identify and dramatically influence groups of people – yet this data is not protected under PII, even though such techniques clearly impact privacy as understood as a right to autonomy.

In addition, on both an individual and a group privacy level, the more recent advent of generative AI as a technique for processing big data, and the synthetic data it outputs, raises even more complex questions around the training data used in such systems and the status of the synthetic outputs produced. Does synthetic data constitute an opinion? Is it PII? What mechanisms under privacy legislation does a resident have to access that data, to access the techniques by which it was produced? These unanswered questions led to the next issues around access, consent, and oversight (Scassa, 2022).

Consent is not required, and access is broken

Canadian privacy legislation, whether for the public or private sector, primarily uses either principles of Consent or Access (or both) as mechanisms with which the collection and usage of data can be made transparent and accountable. Law enforcement does not require consent for data collected for the purpose of fulfilling its mandated roles, so access is the sole mechanism of oversight and redress. However, workshop experts pointed out at length that access is frequently difficult, even impossible, for a number of reasons. As Vivek Krishnamurthy put it:

> *"The idea that a person might contact Facebook or Rogers to get their information, imagine having to do the same thing with the police. Talk about intimidating. So in a scenario like this, I think one of the concerns for members of marginalized and vulnerable communities in particular, is that when you don't have a system in place that's very transparent, the likelihood that the things that are afforded in the law, the opportunity to engage in choice protections, control over your data, auditing your data, are increasingly less likely to happen, especially*

in contexts where individuals are likely to be intimidated or feel threatened. So it doesn't align with information protections that are fundamental to things like privacy law, notice, consent, and choice – these being some of the most fundamental components of protection that exist."

Access, too, hinges upon PII. Thus when PII fails to cover data that potentially is biased or causing discrimination, there is no mechanism for residents to assess it. Further, as Vivek Krishnamurthy pointed out, these people are frequently ones who have already experienced intersectional discrimination in a wide variety of ways – and so attempting to gain access to law enforcement data, an organization well known to them as the state-sanctioned violence wielding agency with a long history of discrimination, is even further deterred. Without consent or access, particularly for those most in need of it, what remains of democratic oversight and accountability?

Democratic oversight is inadequate

Out of a broader conversation around data and technology procurement and usage in law enforcement there came a number of crucial points about inadequate oversight.

Police boards, as the de jure civilian oversight body, were widely assessed as not having enough insight into the technologies the police services were procuring and the data they were using. Experts stated that the boards frequently were either not made aware of new data and technologies, did not have enough time and expertise to properly assess them, or were kept in the dark about techniques and uses by claiming they were 'operational' and thus outside of the board's remit. However, the structure and practice of boards needed to go further to ensure more intersectionally representative engagement with and effective feedback on issues of data and technology.

Indeed, the experts underscored the lack of meaningful public engagement on issues of data and technology. While recent efforts by the Toronto Police Service around AI and race-based data were lauded as good starts, broadly speaking the practice is rare, and when it is carried out it occurs in the form of 'consultations' with little clear impact or intentional consideration of intersectionally marginalized groups. Particularly around issues of algorithmic impact assessment, the need to include diverse voices from a range of impacted groups is unambiguous. Further to that point, many experts argued that, particularly in the case of technologies that learn and adapt over time, regular audits from a publicly accountable and transparent third party are essential and by now well-established best practice.

Finally, existing policy and its adherence were generally as well as specifically criticized as falling short and exacerbating potential intersectional privacy risks. Key points raised on this topic were of PIAs as being only partially deployed and

with little subsequent oversight, of the lack of order-making powers for privacy commissioners, the carve outs for law enforcement in privacy legislation, the broad scope of data that can be collected without consent under the operational mandate of law enforcement, and the lack of clarity about data re-use for a different purpose. This ambiguous and ambivalent policy landscape was a clear theme throughout, and led to the last theme of the subsequent section.

Policy fragmented and outdated, policy development is siloed and ungoverned

The inadequacy of policy's functioning was a point of sustained critique throughout the workshops. Several experts stated that existing policy as it pertains to data collection, sharing, and overall governance in law enforcement is currently fragmented and partially contradictory, leading to tensions and ambivalences with regards to correct operating procedure. "Competencies," as Christopher Parsons put it, "can be very divergent" between larger and smaller municipalities and law enforcement agencies. "And over time, (this divergence) expands through a form of policy enabled function creep" in which real procedures shift slowly away from original policy, frequently as a result of technological change, and further undermines attempts to assert homogenous and reliable policy adherence across the organization.

Such difficulties in implementing policy are simultaneously difficulties in developing policy. As Parsons went on to say, "you have this sort of divergent policy process where you have stuff in the ground that bubbles up that may be less refined, to be generous, and stuff from the bigger places that sort of percolates down," and "you do see a lot of like informal knowledge sharing that takes place in the situations. And that's where I think you see a lot of the policy development that's going on, often at middle-level staff discussions." Several experts went on to point out that while a few larger agencies, like the Toronto Police Service, do have some capacity to innovate in this sphere, many do not. As a result, policy development and diffusion amongst smaller law enforcement agencies can be an ad hoc process of unstructured connections and influence in which smaller agencies talk amongst each other and adopt witnessed practices without sure guidance as to their adequacy. This situation is made all the more likely on the kinds of issues of technological change currently underway with the digital transformation of services and operating processes as well as the influx of new technologies that ambiguously exceed the existing governance protocols.

In addition, several experts contended that this situation is further exacerbated by the lack of official support for, and regulatory options for, policy experimentation in this area. These are genuinely difficult things to regulate, and law enforcement agencies do not have the opportunity to develop, test, iterate, and innovate on policy. This is a product of established policy development procedures and norms

that cannot contend with current modes of technological change – but also of the unnecessary secrecy within which so much technological adoption and usage in law enforcement is shrouded.

Conclusions

At first blush our interviews appeared to have uncovered more confusion than clarity, more ambiguity, contradiction, and heterogeneity than a clear landscape of even policy differentiation, let alone policy coherence. However, as we considered these findings we realized that this muddle is an important insight that requires timely and intentional action. The fact that some interviewees in positions of significant seniority and responsibility for information and communications technology and data policy knew exactly how the data sharing was being governed, while many did not or provided contradictory or unclear responses, is an important research outcome. This led us to the first two conclusions:

1. The actual amount of ongoing data sharing is not well known in terms of metrics nor well understood conceptually, but
   a. many saw it as very important to the functioning of government services, and
   b. most agreed that it is set to rise precipitously in the near future.
2. Yet, on an institution-wide level data-sharing governance is something that is frequently not considered important enough to warrant standardization or strong oversight.

A quote from a law enforcement IT officer makes this tension between the perceived need for more digital data technology to improve service delivery and the growing public awareness of the risks and distrust in how they are governed (emphasis ours):

> *"So, generally, and strategically, where I'm trying to drive us is to say, we should use technology wherever possible to catch what technology can catch. So, think of red light cameras. People making right turns on the fly through reds, which happens a lot. But it is very detectable, machine detectable kind of situation. And we police are getting more expensive, like actual having officers gets more and more expensive every year. So having officers do that work does not make sense. And we're issuing fewer and fewer traffic tickets, because we've got other pressures in the city. And as a consequence, we need to look at, at doing more machine learning and machine vision, and automation and digital in that space.* ***But because there's a lack of trust in policing, in police agencies, then it's best if that's done not in police, and the investment is not going to police. So the defund the police argument is not made.****"*

This quote gets to the heart of the issue, and it was echoed by many of the experts across the two workshops we conducted. There are significant privacy

and intersectional risk issues with these data-driven and digital technologies, and the scale of their usage is growing while the awareness of these issues both within and without policing climbs too. The lack of clarity and coherent, open public discussion is driving tensions between criticism, secrecy, and the need for responsible policy reform – including potential innovations in data and technology governance in which technological capacities are better circumscribed and apportioned to the most appropriate governmental agencies. However, in subsequent questions we probed further, looking at how what was said about its governance was articulated, we drew further conclusions:

3. What governance does exist is frequently ad hoc on a project-by-project basis. There may be a template for an MOU or a legally binding data sharing agreement, but rarely an overarching policy.
4. In terms of privacy risk assessment, there is little awareness of or consideration for going beyond the measures prescribed by FIPPA around PII and successfully conducting a PIA.
5. Amongst the minority of respondents who did recognize the salience of comprehensive governance and/or of risks posed by data sharing beyond those covered by individualistic conceptions of privacy, there was a concomitant appreciation for the need for improved data governance and risk assessment policy.
6. However, very few were able to articulate suggestions for what that policy might contain.

Indeed, another quote simultaneously describes the extensive imbrication of municipal services, public safety needs, and law enforcement as well as the complications of governing sensitive data flows amongst them: "But we don't do projects for (law enforcement), like they have their own, they've got their own crew. We do, however, have enforcement related teams here in the city. So we have, like, corporate security, and you know, a peace officer, team, etc, etc. So, you know our projects, we're always looking at points of overlap, and you know, where teams can be, we have this interesting vantage point where everybody comes to us for stuff, but they sometimes don't talk to each other."

Important collaboration between government services is still deeply siloed and fragmented, and our findings show that there exists a wide, and quite ambiguous range of approaches to governing data sharing – one that practitioners themselves clearly state needs comprehensive reform to meet the needs of growing digital interconnection. Here, too, the expert workshops concurred: the current state of both existing policy and the processes by which policy innovation occurs needs improvement to reach the needs for responsible governance in these times of rapid technological change. Interrelated issues around PII, risk assessment, data governance of sharing processes need more considerate attention, particularly given the inherently more intersectionally dangerous practice of policing.

Across the interviews and the workshops a few examples of intersectional risk-aware practices were raised. Projects in which policy development occurred with the public and the transparent input of relevant marginalized voices as supported by frameworks like GBA+. However, these instances remain few and far between – and while they show a potential path forward, even when they occurred there was room for improvement. Both in the expert workshops and in the interviews GBA+ was repeatedly brought up as an example of a framework for intersectional (privacy) risk assessment that exists in theory, but in practice is rarely well implemented. As Chris Parsons said, "gender-based analysis is really, really, really important. And frankly, I'm very disappointed in the government and its failure to generally instrument (it). One of the challenges is that gender-based analysis is pushed down from relatively higher levels of government, but it is not accompanied by a governance framework that is then meaningful or can be instrumented by the parties who are doing it."

What this report has brought to light is that there is growing concern across the board about the intersectional privacy risks of law enforcement data sharing and usage, yet this concern is very unevenly distributed, rarely present in existing governance tools, and almost entirely undiscussed in the policy development processes. There are tools in existence and in development that would help conceptualize and operationalize these considerations, but without better governance that gives regulatory power to these tools their use remains sporadic or incomplete. A much more comprehensive, transparent. and societally and democratically inclusive conversation is necessary to ensure that this situation does not deteriorate, resulting in further erosion in public trust in good governance. In this current situation of intersecting crises in the legitimacy of law enforcement, this is an opportunity to develop significant new approaches to data, privacy, and the risks they entail, particularly to the most vulnerable. It is into this regulatory space and this rapidly growing need for significant innovation that we wish to insert this report, so that it may serve as a springboard for discussion and new development.

NEXT STEPS

This research project was most notable for the lack of concrete data governance examples or conversations with regards to data sharing between law enforcement and municipal authorities. Our conclusions were drawn as much from what was not said as from what was said. Paired with the expression of disproportionate risk that many communities face from law enforcement practices, we recommend that a working group be established to explore the development of a comprehensive, ecosystemic data governance framework in the space between law enforcement and municipal authorities.

Data sharing is far too ubiquitous, incentivized, and complex in the social, economic, and technological web of a digitized society, to be left to be (un)governed in silos. The solutions to this challenge have only just begun to be debated (Ada Lovelace Institute, 2022; "Disrupting Data Governance," 2023; Linder, 2023). As a result of these conclusions, we recommend a working group with experts from academia, civil liberties organizations, local government, law enforcement, and representatives from a comprehensive range of social groups. The goal is to begin mapping out what a better governance of law enforcement data sharing would encompass, how to take the growing issue of intersectional risk into account, and how to start developing strategies for implementing reforms.

In the original conceptualization of this project, we hypothesized that law enforcement's access to private data would play a significant role in our analysis. To familiarize ourselves with the legal structure that the police operate within, we conducted an extensive legal analysis of law enforcement's legal access to privately held urban data. While the empirical data of our research led the paper in a different direction, the analysis is appended in Appendix A and serves as a first step in such a follow-up project.

We are still in the infancy of data sharing between different public entities, and although the technical systems are rapidly growing in complexity we possess the capacity to develop policy to steer this development into formations that benefit society and avoid risk. This report lays out an initial situation for the working group to react to and build upon. The working group and subsequent knowledge mobilization could build on this momentum and bring us all that bit closer to a more open, democratic, and responsible digital governance. In addition, in the course of conducting the interviews and the expert workshops we encountered numerous individual and organizations across law enforcement, local government, and civil society, who expressed strong interest in continuing this work with us.

This research in combination with the extensive resonance and support it encountered represents an ongoing opportunity for the Office of the Privacy Commissioner to continue funding research and policy development in this space.

BIBLIOGRAPHY

Abdelaal, N., & Andrey, S. (2022). *Overcoming Digital Divides: What We Heard and Recommendations*. Toronto: Ryerson University. Retrieved from https://www.ryersonleadlab.com/overcoming-digital-divides

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*, 424–438.

Ada Lovelace Institute. (2022). Rethinking data and rebalancing digital power. Retrieved March 9, 2023, from https://www.adalovelaceinstitute.org/project/rethinking-data/

Ajana, B. (2013). *Governing through biometrics: The biopolitics of identity*. Springer.

Anderson, R. (2007). Thematic content analysis (TCA). *Descriptive presentation of qualitative data*, 1–4.

Andrey, S., Masoodi, M. J., Malli, N., & Dorkenoo, S. (2021). *Mapping Toronto's Digital Divide*. Ryerson Leadership Lab and Brookfield Institute for Innovation + Entrepreneurship. Retrieved from https://brookfieldinstitute.ca/wp-content/uploads/TorontoDigitalDivide_Report_Feb2021.pdf

Andreychuck, K. (2019). *Contextual Analysis of Crime in Edmonton, Canada Herman Goldstein Award Submission 2019*. Retrieved from https://popcenter.asu.edu/sites/default/files/19-17_edmonton_ab_contextual_analysis_of_crime.pdf

Artyushina, A. (2020). Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto. *Telematics and Informatics, 55*, 101456.

Artyushina, A., & Wernick, A. (2021, November 8). Smart city in a post-pandemic world: Small-scale, green, and over-policed. *Spacing Toronto*. Retrieved February 9, 2022, from http://spacing.ca/toronto/2021/11/08/smart-city-tech-post-pandemic-small-scale-green-over-policed/

Bannerman, S., & Orasch, A. (2019). *Privacy and Smart Cities: A Canadian Survey* (Report for the Office of the Privacy Commissioner of Canada (OPC)). McMaster University. Retrieved December 9, 2019, from https://smartcityprivacy.ca/wp-content/uploads/2019/01/Bannerman-Orasch-Privacy-and-Smart-Cities-A-Canadian-Survey-v1-2019.pdf

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM, 57*(11), 31–33. ACM New York, NY, USA.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California law review*, 671–732. JSTOR.

Bayley, R., Bennett, C., Charlesworth, A. J., Clarke, R., Warren, A., & Oppenheim, C. (2007). Privacy impact assessments: International study of their application and effects. UK Information Commissioner's Office.

Bayley, R. M., & Bennett, C. J. (2012). Privacy impact assessments in Canada. *Privacy Impact Assessment*, 161–185. Springer.

Beer, D. (2016). *Metric power*. Springer.

Benjamin, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code*. John Wiley & Sons.

Bennett, C. J., & Bayley, R. M. (2016). Privacy protection in the era of 'big data': Regulatory challenges and social assessments. *Exploring the boundaries of big data, 205*. Amsterdam University Press Amsterdam.

Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (2014). *Transparent Lives: Surveillance in Canada*. Athabasca University Press.

Bennett, C. J., & Raab, C. D. (2018). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance, 14*(3), 447–464.

Bradbury, D. (n.d.). De-identify, re-identify: Anonymised data's dirty little secret. Retrieved March 9, 2023, from https://www.theregister.com/2021/09/16/anonymising_data_feature/

Brandusescu, A., Chan, A., Diaz, F., Ferraro, A., Ketchum, A., McKelvey, F., Rhim, J., et al. (2021). *Comments on the Toronto Police Services Board Proposed Policy on AI Technologies—Montréal Society and Artificial Intelligence Collective (MoSAIC)* (SSRN Scholarly Paper No. ID 3987388). Rochester, NY: Social Science Research Network. Retrieved March 22, 2022, from https://papers.ssrn.com/abstract=3987388

Brayne, S. (2017). Big data surveillance: The case of policing. *American sociological review, 82*(5), 977–1008. SAGE Publications Sage CA: Los Angeles, CA.

Brayne, S. (2020). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press, USA.

Brown, D. C., & Toze, S. (2017). Information governance in digitized public administration. *Canadian public administration, 60*(4), 581–604. Wiley Online Library.

Browne, S. (2015). *Dark matters: On the surveillance of blackness.* Duke University Press.

Canada. Department of Justice. (2019, August 20). Modernizing Canada's Privacy Act. Retrieved March 23, 2020, from https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html

Canada, O. of the P. C. of. (2008, August 15). Provincial and territorial privacy laws and oversight. Retrieved March 4, 2023, from https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/

Canada, O. of the P. C. of. (2014, May 15). Summary of privacy laws in Canada. Retrieved March 4, 2023, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15

Canada, P. S. (2018, December 21). Hub Model. Retrieved March 15, 2023, from https://www.publicsafety.gc.ca/cnt/cntrng-crm/crm-prvntn/nvntr/dtls-en.aspx?i=10015

Canada, W. and G. E. (2021, March 31). Gender-based Analysis Plus (GBA Plus). Retrieved March 7, 2023, from https://women-gender-equality.canada.ca/en/gender-based-analysis-plus.html

Cardullo, P., Di Feliciantonio, C., & Kitchin, R. (2019). *The right to the smart city.* Emerald Group Publishing.

CBC News. (2022, June 15). "We do not accept your apology," activist tells Toronto's police chief after race-based data released | CBC News. Retrieved March 14, 2023, from https://www.cbc.ca/news/canada/toronto/toronto-police-race-based-data-use-force-strip-searches-1.6489151

Chen, Q.-S. (2023). *Investigating the current approach to developing data governance in the Canadian smart city* (Master's Thesis). University of Waterloo.

Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, (Preprint), 1–21. IOS Press.

City of Edmonton. (2017). *Gender-Based Analysis Plus (GBA+).* Retrieved from https://webdocs.edmonton.ca/siredocs/published_meetings/120/677815.pdf

Clarke, A. (2020). Data Governance: The Next Frontier of Digital Government Research and Practice. In E. Dubois & F. Martin-Bariteau (Eds.), *Citizenship in a Connected Canada: A Policy and Research Agenda* (pp. 97–118). Ottawa: University of Ottawa Press.

Crawford, K. (2021). *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.

Crump, C. (2016). Surveillance policy making by procurement. *Wash. L. Rev., 91*, 1595. HeinOnline.

Davies, T. (2022). *Data governance and the Datasphere: Literature Review*. Datasphere Initiative. Retrieved from https://www.thedatasphere.org/datasphere-publish/data-governance-and-the-datasphere/

Disrupting Data Governance: A Mozilla Guide for Reshaping the Data Economy. (2023, February 15). *Mozilla Foundation*. Retrieved March 9, 2023, from https://foundation.mozilla.org/en/blog/disrupting-data-governance-a-mozilla-guide-for-reshaping-the-data-economy/

Duncan, J., & Barreto, D. (2022). Policing Canadian Smart Cities. *Changing of the Guards: Private Influences, Privatization, and Criminal Justice in Canada*, 99. UBC Press.

Ericson, R. V., & Haggerty, K. D. (1997). Policing the risk society. University of Toronto Press.

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Publishing Group.

Ferguson, A. G. (2019). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press.

Five Eyes | Privacy International. (n.d.). . Retrieved August 3, 2023, from https://www.privacyinternational.org/learn/five-eyes

Foucault, M. (2019). *Power: The essential works of Michel Foucault 1954-1984*. Penguin UK.

Franke, J., & Gailhofer, P. (2021). Data governance and regulation for sustainable smart cities. *Frontiers in Sustainable Cities*, *3*, 148. Frontiers.

Government of Alberta. (2021). *2021 Minister's Awards for Municipal Excellence.* Retrieved from https://open.alberta.ca/dataset/6b7bfcb4-9c45-4c3c-a4e4-28667affc1ca/resource/ce14e32d-4b22-4cee-84d6-66d9fba9783c/download/ma-ministers-awards-for-municipal-excellence-2021.pdf

Green, B. (2019). *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*. The MIT Press. Retrieved June 30, 2022, from https://direct.mit.edu/books/book/4204/the-smart-enough-cityputting-technology-in-its

Grieman, K. (2019). *Smart City Privacy in Canada* (Report for the Office of the Privacy Commissioner of Canada). Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC). Retrieved from https://smartcityprivacy.ca/wp-content/uploads/2019/03/Greiman-OPC-Report_Final-2019.pdf

Grzanka, P. R. (2018). *Intersectionality: A Foundations and Frontiers Reader*. Routledge.

Joh, E. E. (2019). Policing the smart city. *International Journal of Law in Context, 15*(2), 177–182. Cambridge University Press.

Kitchin, R. (2014a). *The data revolution: Big data, open data, data infrastructures & their consequences.* Los Angeles, California: SAGE Publications.

Kitchin, R. (2014b). The real-time city? Big data and smart urbanism. *GeoJournal, 79*(1), 1–14.

König, P. D. (2021). Citizen-centered data governance in the smart city: From ethics to accountability. *Sustainable Cities and Society, 75*, 103308. Elsevier.

Kwon, J., & Wortley, S. (2022). Policing the police: Public perceptions of civilian oversight in Canada. *Race and Justice, 12*(4), 644–668. SAGE Publications Sage CA: Los Angeles, CA.

Ladak, A. M., Ladak, R., & Ladak, I. (2021). Data Access and Privacy in the Age of Artificial Intelligence.

Lauriault, T. P., McArdle, G., & Kitchin, R. (2018). *Data and the City*. Routledge.

Linder, T. (2021, May). *Intelligence-Captivated Policing: Real-Time Operations Centres and Real-Time Situational Awareness in Canadian Police Services* (PhD Thesis). Queen's University, Kingston, ON. Retrieved from http://hdl.handle.net/1974/28866

Linder, T. (2023, February 16). Data Governance for Equity: Principles-Driven and Structurally Iterative. *Open North*. Retrieved March 9, 2023, from https://opennorth.ca/2023/02/3102/

Lomas, N. (2019, July 24). Researchers spotlight the lie of "anonymous" data. *TechCrunch*. Retrieved March 9, 2023, from https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/

Lorinc, J. (2021, January 5). How exactly are smart cities built? From facial recognition and 5G networks to cheap sensors — these are the essential components. *Thestar.com*. Retrieved March 15, 2023, from https://www.thestar.com/news/atkinsonseries/2021/01/05/how-exactly-are-smart-cities-built-from-facial-recognition-and-5g-networks-to-cheap-sensors-these-are-the-essential-components.html

Lorinc, J. (2022). *Dream States: Smart Cities, Technology, and the Pursuit of Urban Utopias*. Coach House Books.

Mattern, S. (2021). *A city is not a computer: Other urban intelligences*. Places books (1st ed.). Princeton: Princeton University Press.

Mattu, J. L., Julia Angwin,Lauren Kirchner,Surya. (n.d.). How We Analyzed the COMPAS Recidivism Algorithm. *ProPublica*. Retrieved March 7, 2023, from https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Maynard, R. (2017). *Policing Black Lives: State Violence in Canada from Slavery to the Present*. Fernwood Publishing.

McQuade, B. (2015). *Securing the homeland? Inside the world of intelligence fusion*. State University of New York at Binghamton.

Meijer, A. (2018). Datapolis: A Public Governance Perspective on "Smart Cities." *Perspectives on Public Management and Governance, 1*(3), 195–206.

Molnar, P., & Gill, L. (2018). Bots at the gate: A human rights analysis of automated decision-making in Canada's immigration and refugee system. Citizen Lab and International Human Rights Program (Faculty of Law ….

Monaghan, J. (2017). *Security aid: Canada and the development regime of security*. University of Toronto Press.

Mosco, V. (2019). *The Smart City in a Digital World.* Emerald Group.

Moss, E., Watkins, E. A., Singh, R., Elish, M. C., & Metcalf, J. (2021). Assembling accountability: Algorithmic impact assessment for the public interest. *Available at SSRN 3877437*.

Muller, B. J. (2010). *Security, risk and the biometric state: Governing borders and bodies*. Routledge.

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism.* NYU Press.

O'Kane, J. (2022). *Sideways: The City Google Couldn't Buy*. Random House of Canada.

Open North. (n.d.). Open Smart City Principles and Domains.

Palmater, P. (2016). Shining light on the dark places: Addressing police racism and sexualized violence against Indigenous women and girls in the national inquiry. *Canadian Journal of Women and the Law, 28*(2), 253–284. University of Toronto Press.

Privacy International. (2017). What Is Privacy? *Privacy International*. Retrieved March 8, 2023, from http://privacyinternational.org/explainer/56/what-privacy

Rambukkana, N. (2021). *Intersectional Automations: Robotics, AI, Algorithms, and Equity*. Rowman & Littlefield.

Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018). Algorithmic Impact Assessments: A Practical Framework for Public Agency. *AI Now.*

Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYUL Rev. Online, 94*, 15. HeinOnline.

Roach, K. (2022). *Canadian Policing: Why and how it Must Change*. Irwin Law, Incorporated.

Robertson, K., Khoo, C., & Song, Y. (2020). *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada.* Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) and the International Human Rights Program (Faculty of Law, University of Toronto). Retrieved from https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications, 10*(1), 3069.

Roller, M. R. (2019). *A quality approach to qualitative content analysis: Similarities and differences compared to other qualitative methods.* SSOAR-Social Science Open Access Repository.

Rosner, G. (2019). De-Identification as Public Policy. *Journal of Data Protection & Privacy, 3*(3), 1–18.

Safe City Mississauga. (2022). *Safe City Mississauga 2022 Annual Report.* Retrieved August 3, 2023, from https://safecitymississauga.on.ca/reports/2022-annual-report.pdf

Scassa, T. (2020a). A human rights-based approach to data protection in Canada. *Citizenship in a Connected Canada: A Research and Policy Agenda, Ottawa, ON: University of Ottawa Press (2020), Ottawa Faculty of Law Working Paper*, (2020–26).

Scassa, T. (2020b). Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto. *Technology and Regulation, 2020*, 44–56.

Scassa, T. (2022, July 6). Anonymization and De-identification in Bill C-27. Retrieved August 8, 2023, from https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80

Shapiro, A. (2020). *Design, control, predict: Logistical governance in the smart city*. U of Minnesota Press.

Solano, J. L., de Souza, S., Martin, A., & Taylor, L. (2022). Governing data and artificial intelligence for all: Models for sustainable and just data governance. European Parliament.

Stelkia, K. (2020). Police brutality in Canada: A symptom of structural racism and colonial violence. *Yellowhead Institute, 72*.

Taylor, L., Floridi, L., & Van der Sloot, B. (2016). *Group privacy: New challenges of data technologies* (Vol. 126). Springer.

Thunder Bay. (2018). Smart Cities Challenge Application. Retrieved from https://www.thunderbay.ca/en/city-hall/resources/Documents/Grants-Incentives-and-Funding-Programs/Smart-Cities-Challenge-Application.pdf

Toronto, C. of. (2021, February 1). SafeTO: A Community Safety & Well-Being Plan. City of Toronto. *City of Toronto.* Retrieved March 15, 2023, from https://www.toronto.ca/community-people/public-safety-alerts/community-safety-programs/community-safety-well-being-plan/

Tulumello, S., & Iapaolo, F. (2022). Policing the future, disrupting urban policy today. Predictive policing, smart city, and urban policy in Memphis (TN). *Urban Geography, 43*(3), 448–469. Taylor & Francis.

UN Human Rights Council. (2014, June 30). The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. Retrieved from https://undocs.org/A/HRC/27/37

Valverde, M., & Flynn, A. (2020). *Smart Cities in Canada: Digital Dreams, Corporate Designs: Independent experts analyze often-controversial schemes from Nunavut to Montreal to Toronto's failed Sidewalk Labs waterfront scheme.* James Lorimer & Company.

Wilson, D. (2017). Algorithmic patrol: The futures of predictive policing. *Big data, crime and social control* (pp. 108–128). Routledge.

Wilson, D. (2019a). Predictive policing management: A brief history of patrol automation. *New formations, 98*(98), 139–155. Lawrence and Wishart.

Wilson, D. (2019b). Platform policing and the real-time cop. *Surveillance & Society, 17*(1/2), 69–75.

Wortley, S., & Owusu-Bempah, A. (2011). The usual suspects: Police stop and search practices in Canada. *Policing and society, 21*(4), 395–407. Taylor & Francis.

Wortley, S., & Owusu-Bempah, A. (2022). Race, police stops, and perceptions of anti-Black police discrimination in Toronto, Canada over a quarter century. *Policing: An International Journal*, (ahead-of-print). Emerald Publishing Limited.

APPENDIX

Legal Analysis of Canadian Law Enforcement Access to Smart City Data

There is as yet little Canadian case law that speaks directly to these emerging technologies. This is because the law develops slowly and generally only when there is need to act, which is further compounded by a lack of transparency from law enforcement bodies. If police bodies and other law enforcement were more transparent with the investigative techniques they used then they could be discussed openly or have their constitutionality assessed on a regular basis. However, there is very little knowledge on police techniques and they often come to light only in the rare cases where an accused challenges their constitutionality or as a result of a journalistic investigation, e.g. on IMSI catchers (Braga, 2017). The lack of public information severely hinders the development of constitutional privacy jurisprudence. However, there are some cases we can take both as direct examples of law enforcement access to smart city data as well as analogies for how access might occur. As smart city policing develops, police will likely rely on the ambiguity afforded by this legal framework to determine whether they are in fact required to get production orders for smart city related data collection/ requests or whether they can just request this data through voluntary mechanisms and direct communications with the organizations that hold the data. This exploitation of ambiguities and legal loopholes directly contributes to the erosion of trust in the use of these technologies for the common good and in the democratic accountability of the institutions using them.

Tracking Location Data: Possibilities for Law Enforcement

The section below explores the question of cell tower data dumps. Those would fall under the transmission data orders or orders to trace specified communications depending on the technique used by law enforcement. Less well documented, with an absence of clear use cases, is the use of production orders for historical tracking data. However, historical tracking data rely heavily on location information. Location data can be harvested from any sort of device that someone carries with them, not just cell phones that ping into towers. Different types of smart devices could send Bluetooth signals to other devices, connect with satellites, with cloud systems of different companies, etc., and create a detailed trail of location data (discussed more also in the section on geofence warrants).

Production orders for historical tracking data are based on the lower standard for requesting judicial authorization of privacy intrusion: reasonable grounds to suspect. This means that the police do not need to have reasonable grounds to

believe that a crime has been or will be committed, but just to suspect[2] that it might and that the information collected will assist the investigation. This lower standard is attached to this production order because the privacy interest in tracking data is considered to be reduced compared to things like content (photos, messages, etc).

What about real-time (as opposed to historical) tracking data? To engage in real-time tracking of devices, police need to obtain a tracking device warrant which allows them to do things like install, maintain, use, and collect information from a device attached to the suspect's "things" (generally referring to vehicles).[3] Under this framework, police cannot collect real-time tracking data from companies/agencies unless they have some sort of informal relationship with them (which is likely circumscribed by the confidentiality obligations owed by the company to their consumers under PIPEDA or public sector privacy laws). Placing a tracking device on a vehicle functions on the lower standard (reasonable ground to suspect that a crime has been or will be committed). The Supreme Court has recognized a privacy interest in location information (or read more narrowly, information about the movements of a car) in the case R. v. Wise 1992 (Supreme Court) where police installed a tracking device on the suspect's car without warrant.

What kinds of information could police collect with a production order for historical tracking data? Historical tracking data can comprise a great deal of types of information in our already very digital and location-focused world. In *Search and Seizure*, the authors identify the following examples of the possibilities available to law enforcement:[4]

1. **Wi-Fi network locations.** Whenever a user connects to a Wi-Fi network, the user's device is assigned a unique media access control address – with unique MAC addresses you can then find the locations of Wi-Fi networks accessed by that MAC address at relevant times.
2. **Peer-to-peer ridesharing and car sharing companies.** Retain data relating to the historical whereabouts of drivers and passengers. Investigators may sometimes obtain this data from a person's device using an ordinary section 487 warrant authorizing the seizure and examination of the device. If the device is unavailable or the data has been deleted, investigators may also obtain the data from the ride sharing or car sharing company itself. Can compel the company to produce information relating to the person's history of trips as a driver or a passenger.
3. **Residential utilities.** Historical data from smart thermostats or records of hydro consumption or home internet usage to piece together a person's probable presence or absence from the home. As homes increasingly become more automated these will continue to grow.
4. **Credit card usage.** Through financial institutions. Can tell police a lot about where the person has been, when, how often, etc.

(2) Criminal Code (RSC 1985, c C-46), s. 487.017:

"Conditions for making order
(2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that (a) an offence has been or will be committed under this or any other Act of Parliament; and (b) the tracking data is in the person's possession or control and will assist in the investigation of the offence."

(3) Criminal Code (RSC 1985, c C-46), s 492.1: RSC 1985, c C-46 | Criminal Code | CanLII

(4) David Schermbrucker, Randy Schwartz, Mabel Lai, Nader Hasan, *Search and Seizure* (2021, Emond Publishing) at page 184.

Cell Tower Dumps: Developments in Canada

What is colloquially known as a tower dump is legally "an order for production of all records of cellular traffic through a particular cell tower over a specified period of time."[5] In other words, tower dumps are a type of production order to trace communications also known as orders for transmission data (section 487.015 of the Criminal Code). Tower dumps are used by investigators to identify potential suspects, witnesses, or victims by finding all phones active near the scene of crime / interest. According to criminal defense lawyers, police seem to use these techniques in two cases: when police have reason to suspect that two or more crimes have been committed by the same person at different locations/times and when police are investigating a single incident and have reason to believe that an unidentified perpetrator or witnesses used a cellphone at the scene.

(5) David Schermbrucker, Randy Schwartz, Mabel Lai, Nader Hasan, *Search and Seizure* (2021, Emond Publishing) at page 170.

When requesting a tower dump order police cannot get basic subscriber information (that names people/their accounts) but can get phone numbers. If they want basic subscriber information, police have to get authorization for a general production order, which has a higher threshold (because it infringes on privacy more than a specialized tower dump order that might be used to identify potential suspects instead of to identify a specific person of interest).[6]

(6) The standard is "reasonable ground to believe": http://criminalnotebook.ca/index.php/General_Production_Orders

The only public litigation on "tower dumps" is R. v. Rogers Communications Partnership 2016. While these issues may have arisen before, this is the only time a court has considered the legal limits of tower dump production orders. In R. v. Rogers, officers investigating a string of jewelry store robberies obtained tower dumps covering a total of 37 cell towers. They obtained general production orders for the tower dumps and did not limit their request to narrowly defined transmission data. They sought information disclosing all available names, addresses, locations, consumer billing information including bank and credit cards. The private information of all innocent third parties was able to be viewed by the police. The details are described in more details in the case:

> *"In the course of investigating a string of jewelry store robberies, the police obtained production orders requiring the applicant cellular providers to provide cell phone records for all phones activated, transmitting and receiving data through all of the Telus' towers proximate to 21 municipal addresses and 16 identified Rogers' towers. The information required by the production order included names, addresses, billing information and, if the person to whom the communication was addressed was also a customer of the named provider, the same data regarding that customer. Telus estimated it would include the personal information of at least 9,000 customers and Rogers estimated that they would be revealing information regarding about 34,000 subscribers. The production orders did not specify how customer information was to be safeguarded and did not expressly restrict the purposes for which the police could use the information."*

The case makes it clear that these types of production orders have been used en masse historically:

(9) The Telus affidavit indicates that since 2004, it has dealt with thousands of court orders requiring cell records. In 2013 alone, it responded to approximately 2,500 production orders and general warrants. To the knowledge of the Telus deponent, the order that it now challenges is the most extensive to date in terms of the number of cell tower locations, and the length of time periods, for which customer information is required.

(10) The Rogers affidavit indicates that from 1985 to 2014, it has complied with many thousands of court orders requiring the production of cell records. In 2013 alone, it produced 13,800 "files" in response to production orders and search warrants.

The judge found that Canadians have a reasonable expectation of privacy in their cellphone records and therefore, the production order could not be as broad and unrestricted as the police requested. The judge decided that production orders must be designed with the principles of minimal privacy intrusion and incrementalism in mind. He set forth guidelines for police to consider when crafting production orders, including encouraging police to seek reports created by the telecom company summarizing the data and anonymizing it appropriately instead of seeking all the underlying data. It's unclear to what extent they are following these guidelines and how practical they are.[7] Other guidelines included 1) providing context to explain the relevance of the locations, dates, and times being targeted and confirm that the towers for which record are sought service those locations; 2) ensuring that the relevance of all of the data being sought is clearly articulated and if not relevant, omitted from the orders; 3) reviewing the facts of each case and considering whether they have done everything possible to limit the scope; and 4) considering the resources of the company / how manageable the request is.

(7) Search and Seizure book, page 177

It is important to note that these are just guidelines and not necessarily constitutional imperatives. It's not clear how strictly they are being adhered to and whether there are informal channels for collecting communication transmission data (which tower dumps are a type of). No new case law exists on this topic.

Geofence Warrants

There is no case law in Canada on geofence warrants. There have been minor developments in the United States recently. Geofence warrants seek location data that identifies devices used at a precise location or within a certain geographical range. These warrants rely on the detailed location data tracking and retention carried out by technology companies. The data comprises GPS signals, cell phone towers, Wi-Fi devices and Bluetooth connections. The Electronic Frontier

Foundation describes it thus: "Using a single warrant—often called a 'geo-fence' or 'reverse location' warrant—police are able to access location data from dozens to hundreds of devices—devices that are linked to real people, many of whom (and perhaps in some cases all of whom) have no tie to criminal activity and have provided no reason for suspicion. The warrants cover geographic areas ranging from single buildings to multiple blocks, and time periods ranging from a few hours to a week."

The use of geofence warrants in the U.S. has been confirmed by reporting by Wired and New York Times. Similar reporting has not taken place in Canada. However, geofence warrants are similar in structure to tower dumps, in that they rely on a similar structure: identifying all devices present in a specific location. Geofence warrants might fall under a production order for tracking data, rather than a production order for transmission data. The requirements that law enforcement have to meet for both of these types of orders are essentially identical. This means that it is likely the same principles of minimization and incrementalism would apply. However, given that geofence warrants have never been litigated or discussed publicly, it is impossible to know what types of process police follow to obtain geofenced data.

A recent case in the U.S., United States v. Chatrie, found that the use of geofence warrants such as these documented by the above reporting violated U.S. constitutional privacy rights. This follows the findings of other lower courts throughout the United States. This issue has not been heard by an appellate level court, meaning that it is possible that these findings of unconstitutionality may change over time as these matters continue to be litigated at higher level courts. Right now, this means that geofence warrants need to be narrowed in scope and not capture the intimate information of a large number of potentially innocent people. Of course, these issues only rarely come to light, as explained by Memo 1. While judges may be making these findings years after these warrants are issued, in the meantime many individuals are likely getting caught in what can be described as fishing expeditions by police in the hopes of catching someone who was related to a criminal activity.

Confidentiality Obligations to Consumers: What obligations do private companies owe to their consumers when police request disclosure of information?

When police send a company a production order requesting disclosure of data, these companies are obligated to respond since they are court-ordered by judges. As described by Canada's Department of Justice: "The *Personal Information Protection and Electronic Documents Act* allows for the disclosure of personal information without the knowledge and consent of the individual to whom it pertains, as long as that disclosure is requested by a government institution that has identified its lawful authority to obtain such information." In the case of law enforcement, a warrant or production order satisfies the definition of 'lawful authority' for obtaining data.

In addition to having to disclose information where police have lawful authority to request it, companies can also disclose information without the knowledge or consent of the consumer on its own accord.[8] The organization would have to develop its own reasonable grounds to believe that a crime has or will be committed in order to justify disclosure under this part of the private sector privacy law. Presumably, organizations might have their own internal processes to identify such information and to determine when disclosure is necessary. **It would be interesting to understand how much law enforcement has shaped these internal policies, if at all, and whether channels of communication are established between corporate teams and law enforcement liaisons**.

(8) Section 7(2) of PIPEDA: an organization may, without the knowledge or consent of the individual, use personal information only if (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention.

The question of whether police can request subscriber information without an order or warrant from an internet service provider (ISP) was discussed in R. v. Spencer 2014 SCC 43. In that case, the Supreme Court found that when police request information without judicial authorization from an ISP, the contractual terms and the statutory (i.e. PIPEDA) terms between the accused (Spencer) and Shaw (the ISP) weigh in favour of recognizing a reasonable expectation of privacy in subscriber information data. A request by police that an ISP voluntarily submit to sharing this information amounts to a "search" under section 8 of the Canadian Charter. Without prior authorization, this search would be unreasonable and violate the individual's constitutional privacy rights.

In the smart city context, this means that companies could be disclosing data from sensors and smart city tech to police in two ways: voluntarily arising from their own monitoring systems that identify potential criminal activity or they can be forced to disclose through a production order. Whether they can disclose information through a police request (that doesn't come as a search warrant or a production order) will depend on the type of information they are being asked to share. Location data, for example, attracts constitutional protection due to the *R. v. Wise* decision at the Supreme Court, so it is possible to argue that information collected from smart bus/metro passes requires a warrant for some type of metadata protection order. However, not all data requested by police will be the type that attracts constitutional protection.

As this analysis shows, police have numerous methods at their disposal to access a wide range of data from cities. What it also shows is that there are several areas of regulatory ambiguity that have been, and no doubt will continue to be, exploited to increase data access. The categorical distinctions between PII and other data is difficult to ascertain and harder still to currently govern, and much of what might shared "may be de-identified and subjected to a range of aggregation or blurring techniques in terms of individual identity, but still reflects on one level or another the behaviour and activities of those users" (Taylor et al., 2016, p. 12).

The Intersectional Privacy Risks of Data Sharing
Between Law Enforcement and Local Government