FUTURE CITIES CANADA

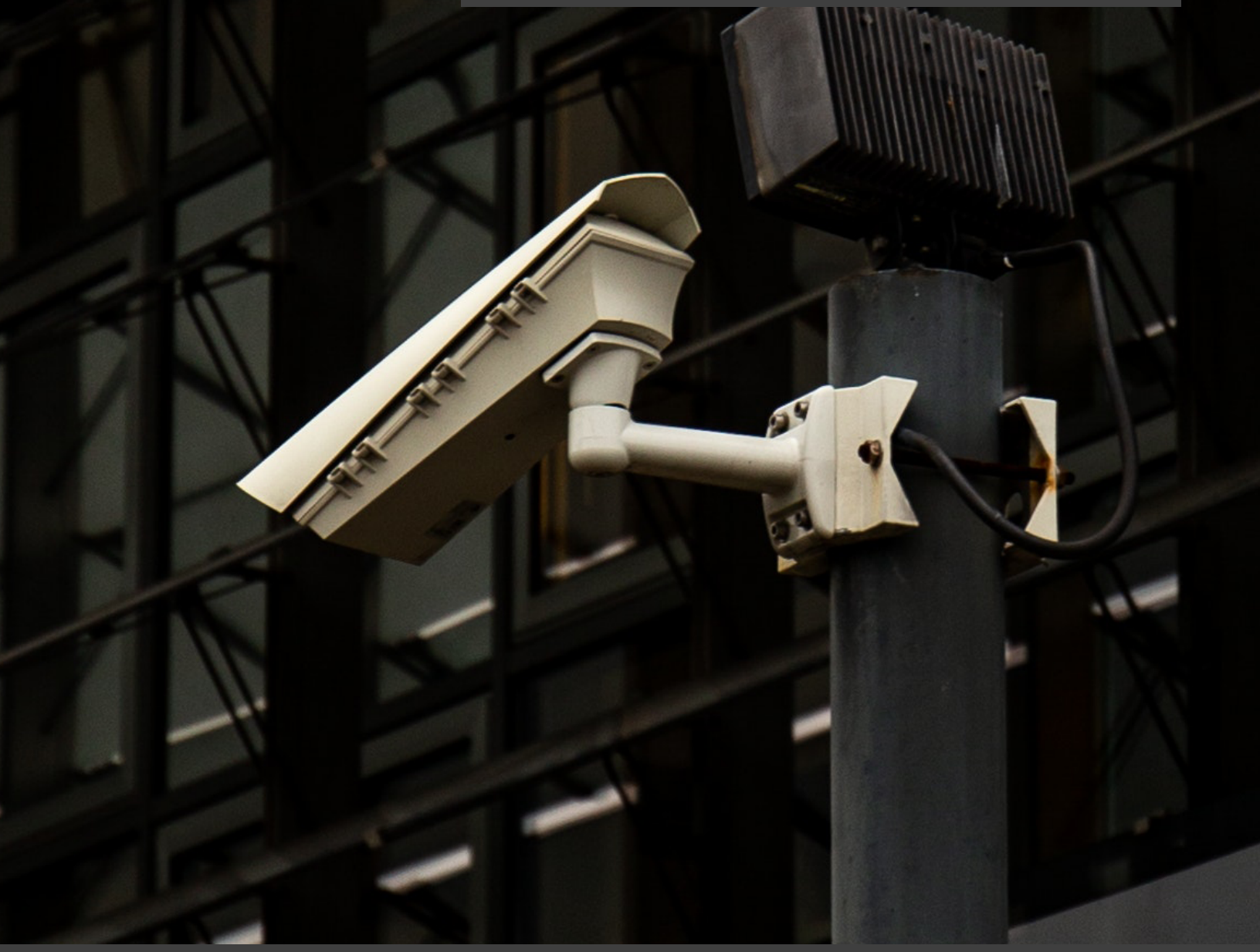
SMART CITIES AND HUMAN RIGHTS

COMMUNITY SOLUTIONS NETWORK RESEARCH BRIEF

JANUARY 2022

ANA QARRI

LEX GILL



Led by: EVERGREEN

Lead technical partner: OpenNorth

With funding provided by: Infrastructure Canada, Canada

Table of Contents

Foreword

by Open North

As communities across the country explore smart city opportunities, there is a pressing need to better understand the risks presented by data and emerging technologies through a lens of Open Smart City principles. This brief is a part of an Open North commissioned series of research papers for policymakers and practitioners, designed to provide insight into how data and technology intersect with the challenges local communities are facing.

An Open Smart Community (OSC) is one where all actors, including residents, collaborate in mobilizing data and technologies to develop their community through fair, ethical, and transparent governance that balances economic development, social progress, and environmental responsibility.[1]

In this brief, the authors outline the risks that smart city technologies pose to human rights as set out in Canadian law. At the fundamental level, local government staff must uphold human rights or otherwise risk legal repercussions and public backlash. In a more proactive framing, this brief explores smart city projects from a different point of view — from the perspective of rights. This brief focuses specifically on the following rights: equality and discrimination; privacy and surveillance; and freedom of expression and association.

Maintaining human rights is central to creating an Open Smart Community and this brief is a resource for local government staff to address the complex challenges that come with implementing data-centric technologies into their programs and operations. Core to an Open Smart Community is residents engaging in policy-making and decision-makers driving outcomes that promote the public good. Maintaining equality, privacy, and freedom of expression are key to ensuring trust between decision-makers and the public, as is hearing the diverse needs of residents. This brief provides information to guide decision-makers to consider a human rights lens to ensure they are creating an environment of trust, engagement, and a better future.

1 Lauriault, T. P., Bloom, R., & Landry, J.-N. (2018). Open Smart Cities Guide V1.0. OpenNorth.

Acknowledgements

The research builds on the Open Smart Cities Guide, which provided the first ever definition of an Open Smart City. It was published in 2018 as a part of a year long collaborative research project led by Open North and funded by Natural Resources Canada's GeoConnections program in 2018. The authors are Dr. Tracey P. Lauriault, Rachel Bloom and Jean-Noé Landry.

These research briefs are produced for the Community Solutions Network, a community-centric platform for communities to connect and build a national centre of excellence in Open Smart Communities. As the project lead, Evergreen is working with lead technical partner Open North and other partners to provide valuable information, learning opportunities, advisory and capacity building services to Canadian communities in key areas of data and technology, helping to improve the lives of residents.

We offer—at no cost to communities—a comprehensive Advisory Service for Canadian communities interested in developing and implementing Open Smart Communities projects. To learn more about the Advisory Service, please visit communitysolutionsnetwork.ca.

A program of Future Cities Canada, the Network receives funding from the Government of Canada. The views expressed in this publication do not necessarily reflect those of the Government of Canada.

Series editors: Nabeel Ahmed, Yasmin Rajabi, and Megan Wylie
Foreword: Megan Wylie
Graphic design: Tatev Yesayan

Introduction

Smart city technologies — when adopted responsibly and democratically — have the potential to improve the urban environment, contribute to public safety, strengthen municipal governance, and enrich residents' quality of life. Yet the application of these technologies has been mired in controversy in recent years. Indeed, there are now countless examples around the world of the ways in which "smart" technologies have contributed to the privatization of public infrastructure, exacerbated systemic discrimination, and threatened individuals' rights and freedoms.[2] How should Canadian municipal leaders account for these risks?

As public authorities in Canada explore proposals to adopt these technologies, leaders must align their vision for open, smart cities with their obligation to respect and promote human rights. This brief, written with both elected and civil servant leaders in mind, offers an introduction to the human rights issues that municipal leaders must consider as they introduce smart technologies in their communities. Although by no means exhaustive, it offers a starting point for understanding three fundamental themes: equality and discrimination, privacy and surveillance, and the rights to freedom of expression and association.

In Canada, these rights are grounded in constitutional law, and in particular the *Canadian Charter of Rights and Freedoms* ("*Charter*"). They are also rooted in international law and human rights instruments, such as the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights*, and the *International Convention on the Elimination of All Forms of Racial Discrimination*. In many cases, federal and provincial human rights statutes (including Quebec's *Charter of Human Rights and Freedoms*), privacy legislation (such as the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*), access-to-information laws, and public sector procurement rules impose additional, specific obligations on municipalities and their private sector partners to respect and protect human rights.

On a practical level, failure to account for human rights can be extremely costly. In Canada, individuals and groups have the right to seek remedies from the courts (and in some cases, before administrative tribunals) in order to prevent, sanction, deter, and claim compensation for the violation of human rights. In certain cases, rights-violating conduct by a municipality can give rise to a claim in damages, whether as an individual claim or in the form of a class action (for example, on behalf of all people who used a certain application, or who live in a neighbourhood impacted by the violation). In addition to monetary damages, residents and public interest organizations can also seek redress in other forms — such as court orders — to end or modify a specific program, or a direct challenge to the constitutionality of a law or policy.

Governments, including municipalities, are required to respect the *Charter* in the course of all of their activities, decisions, and rule-making (including when they enact laws, bylaws, and policies).[3] The *Charter* applies to various public and quasi-public institutions, as well as private municipal partners — from police services to school boards and transit authorities — to the extent that they are carrying out government functions.[4] In other words, the fact that a rights violation is not committed by the government *directly* does not necessarily immunize wrongful actors from *Charter* scrutiny. This principle is particularly important in the smart city arena, where municipalities, police forces, and other institutions routinely seek to partner and collaborate with private firms in order to achieve public sector goals.

2 For example, the controversial Sidewalk Labs (Alphabet) project promoted a vision of Toronto's Waterfront that involved critical infrastructure — from roads and taxation to criminal justice — under the control of private actors. Cardoso, T. & O'Kane, J. (2019, October 30). Sidewalk Labs document reveals company's early vision for data collection, tax powers, criminal justice. *The Globe and Mail*. See also the recent examples cited by Rebecca Williams: Williams, R. (2021, August). ***Whose Streets? Our Streets! (Tech Edition)***. Harvard Belfer Center.

3 *Godbout v. Longueuil (City)*, [1997] 3 SCR 844.

4 See, for example, *Multani v. Commission scolaire Marguerite-Bourgeoys*, 2006 SCC 6; *Greater Vancouver Transportation Authority v. Canadian Federation of Students*, 2009 SCC 31; *Eldridge v. British Columbia (Attorney General)*, [1997] 3 SCR 624.

Recognizing Risks to Human Rights

Right to Equality and Non-Discrimination

In Canada, everyone has the right to the equal protection and equal benefit of the law and to be protected from unlawful discrimination. Section 15 of the federal Charter gives everyone the right to be free from discrimination based on specific protected grounds. Although some of these grounds — such as age, sex, race, religion, and disability — are named explicitly, this list is not exhaustive. Other grounds, such as sexual orientation and citizenship status, have developed through the courts. In Canada, people are also protected by the *Canadian Human Rights Act* and its provincial equivalents. In different provinces, human rights legislation provides additional protection against discrimination based on factors such as whether a person has a criminal record, receives public assistance, or is a parent, as well as characteristics such as gender expression and social condition.[5]

It is essential to understand that discrimination can be both direct and indirect, intentional and unintentional. For example, a bylaw or policy that excludes or disadvantages a group of people differently on the explicit basis of their sex, gender, race, or disability would be an example of direct discrimination.[6] Indirect discrimination, on the other hand, arises in instances where decisions do not explicitly differentiate or exclude residents based on protected characteristics, but when put in practice, the decision or policy has negative effects on or consequences for a specific group of people. This is generally known as adverse impact discrimination.[7] For example, a policy of refusing to hire individuals with gaps in their professional history may amount to adverse impact discrimination on the basis of sex, pregnancy, parental status, or disability in practice. Adverse impact discrimination can also happen at an even larger scale, for example where urban planners make certain municipal services or infrastructure available in some neighbourhoods but not others. In the context of income or race-based discrimination in the deployment of technical infrastructure, this has often been referred to as "digital redlining."[8] Although these kinds of consequences may be unintended, policy-makers and leaders nonetheless have a responsibility to consider them before, during, and after a project. Indeed, regardless of a municipal government's intentions in theory, whenever it discriminates on the basis of a protected ground in *practice*, it faces the risk of a *Charter* breach or other human rights claim.[9]

The right to equality does not mean that everyone must be treated exactly the same.[10] Instead, it requires that the needs, circumstances, and experiences of all residents be considered in decision-making and that the outcomes of policies do not unlawfully exacerbate existing inequalities or create new ones.[11] In order to meaningfully safeguard the right to equality, municipal leaders must therefore pay ongoing attention to the ways in which different groups might experience the effects of new technologies before, during, and after their implementation. These leaders must be particularly attuned to the risk of discriminatory effects where a practice, rule, or technology purports to apply to everyone equally or "randomly," as these circumstances often serve to shield discriminatory exercises

5 *Canadian Human Rights Act*, RSC 1985, c H-6; *Ontario Human Rights Code*, R.S.O. 1990, c. H.19; *Alberta Human Rights Act*, RSA 2000, c A-25.5; *Québec Charter of Human Rights and Freedoms*, CQLR c C-12.

6 For example, direct discrimination would include refusing to hire someone because they are a Black or gay person. The Ontario Human Rights Commission (OHRC), for example, refers to this form of discrimination as direct and intentional: OHRC (2008). *Human rights at work*, III.2 ("What is Discrimination?").

7 See, for example, *Ontario Human Rights Code*, s 11. See also the Supreme Court of Canada's most recent pronouncement on adverse impact discrimination in *Fraser v. Canada (Attorney General)*, 2020 SCC 28.

8 See, for example, National Digital Inclusion Alliance (2017), *AT&T's digital redlining*, a study arguing that AT&T "systemically discriminated against lower-income Cleveland neighborhoods in its deployment of home internet and video technologies" (p. 1).

9 See *Fraser v. Canada (Attorney General)*, 2020 SCC 28 at paragraphs 53, 69. Note that Canadian law recognizes that distinctions based on protected grounds do not always amount to discrimination. Section 15(2) of the *Charter* accounts for ameliorative programs, where laws or government actions differentiate based on protected grounds but do so with the purpose of improving the position of members of that protected group.

10 *Fraser v. Canada (Attorney General)*, at paragraph 40.

11 *Fraser v. Canada (Attorney General)*, at paragraphs 50, 107.

of discretion from legal review. Indeed, in some cases, it may be prudent (or even necessary) for a municipality to proactively collect data[12] about affected communities both *before and after* the adoption of a new technology to ensure that its actions are not inadvertently excluding or harming certain groups or individuals in an unlawful manner.[13]

The risk that smart city technologies will cause discriminatory effects or exacerbate existing forms of inequality are serious, and perhaps most acute in policing and public safety. For example, critics have widely decried the adoption of facial recognition technologies in the smart city context on the basis that these technologies are known to have lower accuracy rates when identifying racialized individuals and can therefore lead to wrongful investigations, detentions, or arrests.[14]

However, smart policing technologies can be discriminatory even when they appear to boast high "accuracy" rates (whether in identifying people or patterns of behaviour) because of the risk that they will contribute to negative feedback loops or "self-fulfilling prophecies" that exacerbate discrimination.[15] There is no serious debate that marginalized, poor, immigrant, and racialized neighbourhoods are disproportionately targeted by law enforcement, and that this reality is reflected in historical policing data. As a result, the use of that historical data to identify crime "hot spots" or a higher concentration of police stops and arrests in a particular neighbourhood will often tell us more about profiling and discriminatory policing practices than about objective measures of community safety. By using this data as a rationale to deploy new policing technologies in these communities, municipalities may exacerbate the risk of unlawful surveillance and police scrutiny without improving public safety. PredPol, a predictive policing tool adopted in Oakland, California, illustrated this form of discrimination when it was discovered that Black people and low-income households were targeted at disproportionately high rates.[16] The installation of CCTV and facial recognition technology in public housing in Tampa and Detroit has raised similar concerns, provoking movements for federal law reform to ban the technology in response.[17]

Discrimination can also take place in other contexts. For example, some municipalities across North America have or are considering partnerships with ride-sharing apps to increase access to transportation.[18] These partnerships promise to improve access to essential services, reduce commuting

12 For example, the OHRC recommends "race-based data collection" as an essential component of strategies that address systemic racial profiling: OHRC (2010), *Policy on eliminating racial profiling in law enforcement* at 37.

13 Information collected for ameliorative purposes, such as to assess discriminatory impacts of new technologies, must nonetheless be collected in line with privacy legislation and any other applicable laws. Decision-makers can, for example, collaborate with their in-house privacy officers or their municipal or provincial Information and Privacy Commissioners to design privacy-respecting strategies for collecting sensitive data regarding protective characteristics such as race, gender, sexuality, religion, etc.

14 A 2019 research study by the U.S. National Institute of Standards and Technology (NIST) found that "contemporary face recognition algorithms exhibit demographic differentials…false positive rates are highest in West and East African and East Asian people." NIST. (2019, December 19). *NIST study evaluates effects of race, age, sex on face recognition software*. In an earlier study examining commercial gender classification systems, A.I. researchers Joy Buolamwini and Timnit Gebru found that "darker-skinned females are the most misclassified group (with error rates of up to 34.7%)." Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1–15.

15 Robertson, Khoo, and Song describe this phenomenon as "feedback loops of injustice" at 105: Robertson, K., Khoo. C., & Song, Y. (2020, September). *To surveil and predict: A human rights analysis of algorithmic policing in canada*. Citizen Lab.

16 *Ibid*., citing Lum, K. & Isaac. W. (2016), To predict and serve? *Significance, 13*(5), 14 at 18.

17 See Williams, Whose Streets? Our Streets (Tech Edition), citing Fadulu, L. (2019, September 24), Facial recognition technology in public housing prompts backlash, *The New York Times*.

18 For examples of collaborations between ridesharing apps and municipalities, see Cmar, W. (2017, February 13), *How cities are integrating rideshare and public transportation*. Ash Center for Democratic Governance and Innovation, Data-Smart City Solutions. For a Canadian example, see Cecco, L. (2019, July 16), The Innisfil experience: The town that replaced public transit with Uber. *The Guardian.*

times, and alleviate some of the pressure faced by public transit systems. However, a deeper look at the experiences of ride-sharing app users reveals the potentially discriminatory impacts of this technology. In particular, several studies have concluded that discrimination against racialized and LGBTQ+ riders is widespread in ride-sharing applications and that drivers are more likely to reject and cancel ride requests from passengers who belong to racial, sexual, or gender minorities.[19] Similar issues have surfaced regarding racism in personalized pricing in ride-sharing apps.[20] Adopting a ride-sharing partnership without putting measures in place to prevent discriminatory passenger selection would thus risk further disadvantaging these groups and embedding those practices in the city's "smart" transit system.

As another example, by building a government technical service in a way that requires residents to own a smartphone, municipalities may indirectly deprive older residents, residents with certain disabilities, or residents from lower socioeconomic backgrounds from the benefits of that service. Similarly, by implementing a smart mechanism that makes entry into certain places or buildings contingent on the possession of a valid government ID or that links benefits to a government-managed digital identity, a municipality may discriminate against those who lack official identification (such as undocumented residents) or exclude those who tend to lack up-to-date documents (often these are groups of people who already experience some form of marginalization, such as people experiencing poverty and homelessness, or students[21]) from municipal services.

As discussed below, in all cases municipal leaders must weigh the importance of the problem they are trying to solve against the risk of unintended consequences.[22] Practices that may seem inefficient or ripe for technological intervention at first glance — from paper tickets, human-staffed service desks, and cash payment systems, to government services provided anonymously — may be providing vital safeguards in practice.

19 Users that exhibit LGBTQ+ support (by having a picture with a rainbow filter, for example) experience higher ride cancellation rates: Mejia, A. J., & Parker, C. (2021), When transparency fails: bias and financial incentives in ridesharing platforms, *Management Science, 67*(1), 166.

20 Pandey, A., & Caliskan, A. (2021, May 19–21). *Disparate impact of artificial intelligence bias in ridehailing economy's price discrimination algorithms* [Paper presentation]. ACM Conference on Artificial Intelligence, Ethics, and Society, virtual event, United States.

21 Elections Canada has documented that, compared to the general population, younger voters consider proof of identity requirements a significant barrier to voting: House of Commons (2016, October 13), Youth voter turnout in Canada, *Research Publication of the Legal and Social Affairs Division*. Laws that require specific forms of identification for voting also have a negative impact on the turnout of minority groups in elections: Hajnal, Z., Lajevardi, N., & Nielson, L. (2017). Voter identification laws and the suppression of minority votes. *The Journal of Politics, 79*(2), 363.

22 For example, the introduction of fraud detection technologies in welfare benefits programs is premised on the (unfounded) assumption that recipient dishonesty is frequent enough to justify government intervention. Evidence from these programs suggests that fraud rates are low to negligible: U.S. studies show that less than 1% of food stamp recipients are ineligible to receive assistance, and approximately 3% of improper unemployment insurance payments are fraudulent. See USDA Food and Nutrition Service (2019, June 27), *What is FNS doing to fight SNAP fraud?*; U.S. Department of Labor (n.d.), *Unemployment insurance improper payment rates*. Nonetheless, the political will to implement fraud detection A.I. is increasing, despite the discriminatory harms these technologies pose to historically disadvantaged communities. In 2020, a Dutch court held that a fraud detection tool used by the Dutch Ministry of Social Affairs and Employment and other agencies violated the human rights of those already living in conditions of poverty and marginalization: Haley, J., & Booth, R. (2020, February 5). Welfare surveillance system violates human rights, Dutch court rules. *The Guardian.*

Right to Privacy and Freedom from Surveillance

It is well established that the adoption of new technologies can threaten individuals' constitutional and statutorily protected privacy rights — but how should municipal leaders think about this issue?

In Canada, individuals have the right to be free of unjustified surveillance and to have their personal information secure and protected from unreasonable forms of state and private sector intrusion alike.

These rights are protected primarily by section 8 of the *Charter* (which prohibits unreasonable searches and seizures) as well as by federal and provincial privacy laws. This means that in addition to the protection from government intrusion or surveillance granted in the constitution, people in Canada are entitled to the protection of their personal data under legislation such as the *Privacy Act* (for the federal government), the *Personal Information Protection and Electronic Documents Act* (for private sector organizations), and human rights legislation such as the Quebec *Charter*, which protects the right to respect for one's private life and the right to non-disclosure of confidential information.

Data protection is a quickly changing area of law,[23] and Canadian privacy obligations will continue to evolve as the country keeps pace with more stringent global regulations, such as the European Union's General Data Protection Regulation.[24] Many smart city technologies, sourced from and operated by private companies, will engage both the private sector's obligations to respect local privacy and data protection laws as well as the local government's legal responsibilities to adopt those technologies lawfully and responsibly.

Although notions such as individual consent are an essential part of privacy law, they are not the full picture. The nature of the privacy rights engaged, the reasonable expectation a person has with regard to their privacy in a particular context, and the degree of legal protection to which that person is entitled are all subject to a contextual analysis. Indeed, the Supreme Court has confirmed that individuals have a right to privacy even in very public places, offering a few examples: "the use of a cell phone to capture upskirt images of women on public transit, the use of a drone to take high-resolution photographs of unsuspecting sunbathers at a public swimming pool, and the surreptitious video recording of a woman breast-feeding in a quiet corner of a coffee shop."[25] This principle is particularly important for municipal leaders to understand: just because an individual is walking the city street or occupying public space, it does not mean that their right to privacy has been waived or extinguished. For people experiencing homelessness — who live a large part of their lives in "public spaces" — the invasion into their privacy is constant and even more damaging.

It is also important to understand that individuals can have a significant and legally protected privacy interest in personal information — such as metadata or a digital identifier such as an IP address — that seems innocuous on its own but which can reveal intimate details when analyzed alongside other sources.[26] Indeed, the location data routinely generated by cell phones is one of the best examples of this problem, because cell phones feature unique mobile identifiers tied to both the device and the subscriber. Knowing that a given mobile device was near a particular cell phone tower on a given day tells you little about either the device or its user in isolation. However, by looking at historical data for all of the cell towers in a given city over time, it is possible to track the movement of a particular device, and as a result, the person to whom it belongs, in extraordinary detail. This kind of location data is extremely rich: it can allow you to link an otherwise anonymous device to a specific person, predict that person's likely future behaviour, determine who else they associate with, and decide what kind of person they are based on the kinds of places they go, from workplaces and homes to protests and places of worship.[27]

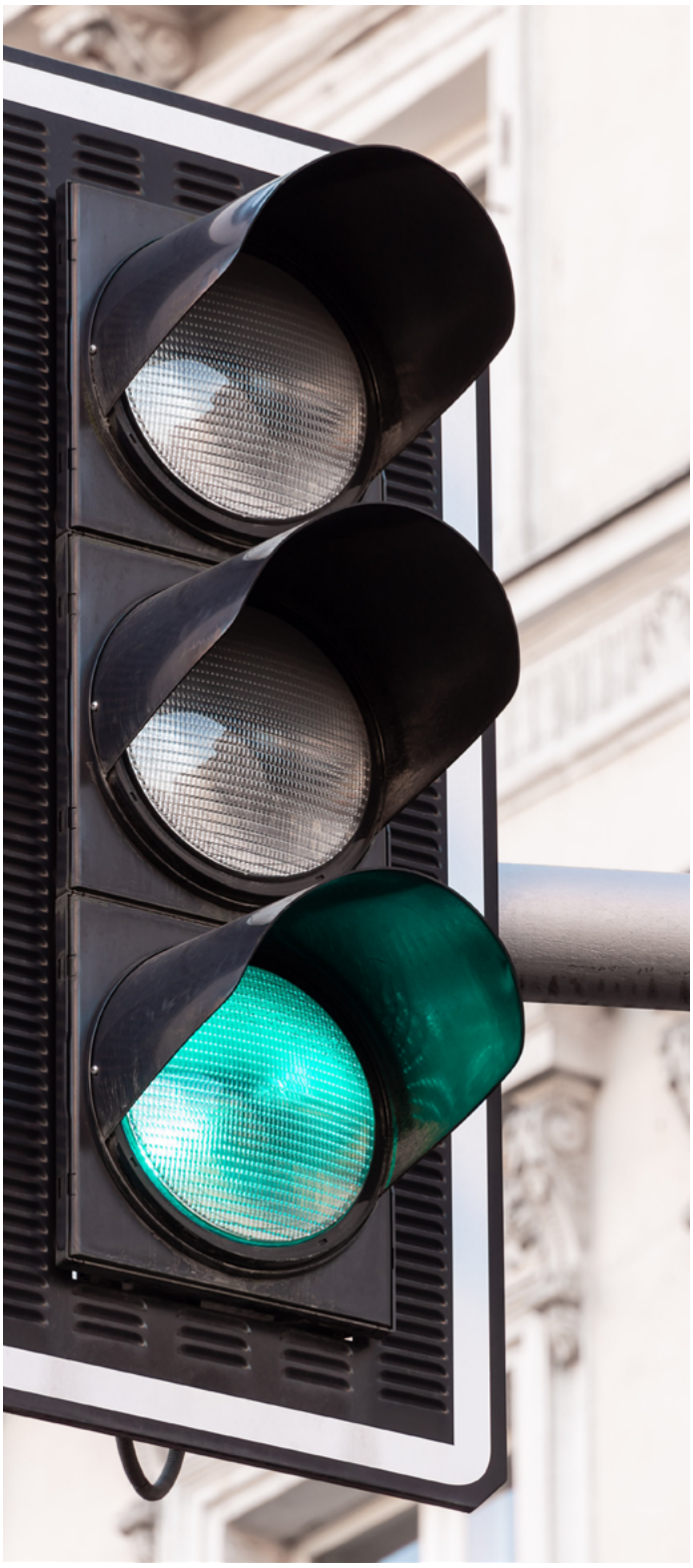
23 The federal government is revamping Canadian private sector legislation through Bill C-11: *Digital Charter Implementation Act*, 2020.

24 General Data Protection Regulation, (EU) 2016/679.

25 *R v Jarvis*, 2019 SCC 10 at paragraph 40.

26 *R v Spencer*, 2014 SCC 43 at paragraphs 27, 63.

27 See, for example, Israel, T., & Parsons, C. (2016, August), *Gone opaque? An analysis of hypothetical IMSI catcher overuse in Canada*. Telecom Transparency Project and Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic.



When cities contract with the private sector to purchase or build smart city technologies, they must reckon with the full scale and intimacy of the information they collect on people and their behavioural patterns, rather than consider these data points in isolation. For example, many municipalities have or are considering products that optimize traffic flow or monitor waste management operations.[28] At first glance, these technologies may not appear like surveillance tools at all: they are powered by smart systems that use sensors to collect data, and that data is simply analyzed to track patterns, understand behaviours, and ultimately to make urban systems more efficient and environmentally friendly. These can be enticing tools for municipalities looking to improve traffic conditions or to make their cities more sustainable. However, combined with other sources of information, law enforcement and private companies can use this data to build intricate profiles of both individuals and communities. These pieces of information can reveal patterns of movement, political or religious affiliations, and even intimate details about activities that take place inside one's home.[29]

Policy-makers must also be aware that law enforcement can request access to the data a municipality and its private sector partners collect, and is increasingly doing so as a matter of routine.[30] For example, Toronto police gained access to smart city data — mobility information from the PRESTO electronic transit pass — through the region's transit agency.[31]

28 See, for example, McKinsey Global Institute (2018, June), *Smart cities: Digital solutions for a more livable future* at 12 (data shows that mobility, security, and utilities management are the leading reasons for the implementation of smart technologies in cities globally). See also the City of Toronto's implementation of Transportation Innovation Zones.

29 Privacy International (2017), *Data is power: Profiling and automated decision-making in GDPR*; Kosinski, M., Stillwell, D., & Graepel, T., (2013), Private traits and attributes are predictable from digital records of human behavior, *PNAS, 110*(15), 5802; Lau, T., (2020, April 1), *Predictive policing explained*, Brennan Centre for Justice.

30 See, for example, Diaz, A. (2020, December 21), *Law enforcement access to smart devices*, Brennan Centre for Justice.

31 Spurr, B. (2017, June 3) Metrolinx has been quietly sharing Presto users' information with police. *The Toronto Star.*

During Black Lives Matter protests in Los Angeles, local police collaborated with Amazon's Ring (a home security camera provider) to gather camera footage directly from residents.[32] Almost any data collected by a municipality or private company can eventually be obtained and used by law enforcement (and in some cases, private litigants) with, and sometimes even without, prior judicial authorization. In practice, this means that regardless of a municipality's intended application or initial purpose for the adoption of smart city technology, the personal data they generate can ultimately be used to monitor, investigate, arrest, and incarcerate residents.

Many Canadian municipalities have also considered implementing forms of surveillance and monitoring technologies with the goal of improving public safety or optimizing urban operations. For example, a combination of CCTVs, police-worn body cameras, and other surveillance tools may be proposed as solutions to prevent crime, improve police accountability, or respond to emergencies. Yet these technologies represent a significant privacy intrusion and have been widely criticized by civil rights lawyers, technologists, and human rights scholars.[33] They deserve careful and rigorous scrutiny — as well as meaningful public consultation and in-depth legal review — prior to adoption.

Indeed, municipal leaders should generally be skeptical of safety-based rationales for the adoption of new smart city technologies, especially when communities that have higher arrest rates or that are perceived as hotspots for "street" level crime are proposed as potential testing grounds. As discussed above, these communities are generally poorer and often home to a high proportion of racialized and migrant residents — in other words, individuals who are already subject to a heightened degree of state scrutiny and overrepresentation in the criminal justice system. In these contexts, privacy invasions and systemic discrimination intersect, contributing to a self-perpetuating cycle that seeks to rationalize greater surveillance and control of marginalized individuals and their communities.[34]

Finally, it is also critical to recognize that certain individuals face more significant consequences than others when the state invades their privacy. For example, smart city technologies that involve certain forms of data collection or surveillance may put undocumented residents at risk of deportation, a particular concern for municipalities that have declared themselves as "sanctuary cities" or which have adopted "access without fear" policies.[35]

Freedom of Expression and Association

Ultimately, the right of city residents to live without undue state scrutiny is not only constitutionally protected, it is an essential characteristic of a city in which every person can express themselves and participate fully in their community. Freedom of expression is a human right, the exercise of which helps give cities their unique character.

Subject only to certain narrow and carefully defined limits, everyone in Canada has the legal right to: express their views freely; associate and gather freely with others; and protest and organize based on their beliefs. These rights are entitled to legal protection under section 2(b) of the *Charter*. Internationally, the obligation to respect freedom of expression is set out in Article 19 of the *Universal Declaration of Human Rights* and reaffirmed in Article 19 of the *International Covenant on Civil and Political Rights*.

32 Biddle, S. (2021, February 16). LAPD sought ring home security video related to Black Lives Matter protests. *The Intercept.*

33 Robertson et al., *To surveil and predict: A human rights analysis of algorithmic policing in Canada*; Williams, *Whose Streets? Our Streets (Tech Edition)*.

34 Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYU Law Review Online, 192.*

35 See Hershkowitz, M., Hudson, G., & Bauder, H. (2020). Rescaling the sanctuary city: Police and non-status migrants in Ontario, Canada *International Migration, 59*(1), 38. To date, these include Toronto, Hamilton, Vancouver, Ajax, Montréal, Edmonton, and London: Mireille Paquet et al., "Sanctuary cities in Canada: Practices, needs and policies" (forthcoming study, research digest published in Spring 2021).

Particularly in larger cities, individuals have come to expect a certain degree of anonymity in public spaces. That anonymity, as with anonymity online, is an essential precondition to the full exercise of one's freedom of expression in a democratic society.[36] Yet as discussed above, smart city technologies often have the capabilities to identify and track people and their behaviours on a large scale. Civil liberties advocates and human rights advocates have therefore raised concerns that the pervasive nature of these technologies can have a chilling effect on residents' freedom of expression.

Indeed, in many cities around the world, law enforcement already uses smart city technologies — such as smart cameras, license plate readers, and drones — to clamp down on lawful protests and to identify participants at those events.[37] Smart city technologies can also impact freedom of expression in subtler ways. Residents use city infrastructure to access all sorts of highly private places and experiences. Someone travelling to an addictions support group, for example, may not want that information to be captured and recorded. Workers attempting to exercise their right to unionize may find gathering without fear of intimidation more difficult when surrounded by technical infrastructure doubling as surveillance tools. There is no doubt that the perception that one is being watched will, at least in some cases, discourage otherwise completely legal behaviour — including participation in political events, religious and democratic gatherings, and artistic expression.[38] In some cases, this chilling effect will discourage already vulnerable individuals from accessing resources they need, such as shelters or local community centres. Municipal leaders must therefore be sensitive not only to the actual information collected about residents, but also to the ways in which monitoring technology can shape and deter lawful and pro-social behaviour.

36 See *R v Spencer*, 2014 SCC 43 at paragraph 43; Frank La Rue (2013), "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," A/HRC/23/40 (17 April 46 2013) at paragraph 23.

37 Mozur, P. (2019, July 26), In Hong Kong protests, faces become weapons, *The New York Times*; Marx, J. (2020, June 29), Police used smart streetlight footage to investigate protesters, *Voice of San Diego*; Metz, C. (2020, December 5), Police drones are starting to think for themselves, *The New York Times*.

38 See, for example, Penney, J. (2016), Chilling effects: Online surveillance and Wikipedia use, *Berkeley Tech Law Journal, 13*(1), 117.

Policy Tools for Human Rights Compliance

Assessment of human rights compliance should take place throughout the lifecycle of smart city technologies: including before technology is built or procured, throughout all stages of the design process, and during and after its implementation. As highlighted in the previous section, the impacts of smart city technologies on human rights may sometimes reveal themselves only following careful analysis of its unintended consequences or once the technology is implemented. Municipalities must be alert and responsive to these possibilities — both in order to protect residents from harm and to protect their institutions from liability.

Public Participation in Smart City Planning

Continuous public participation and expert consultation is essential throughout the choice, design, and implementation stages, wherever smart city technology is involved. Consultation facilitates transparency and responsiveness in public decision-making, and helps to ensure that the community needs or problems that the technological intervention seeks to address are properly defined from the outset. Without meaningful public participation, governments risk allowing private sector companies to dictate the municipal agenda on smart cities. Open North's Open Smart City Guide offers a framework that puts municipal and resident vision ahead of private interests.[39] This framework centres engagement with residents and experts when defining a 'smart city' vision. Among other organizations, Open North provides free educational resources for public engagement, such as the Community Solutions Advisory Service (lms.opennorth.ca), which may assist municipal leaders in problem and need definition.

Procurement Standards

Municipal governments are powerful stakeholders in the smart city technology market and have the potential to influence industry practices. As such, decision-makers should adopt and insist on procurement standards that: (a) benefit their residents and communities; and (b) protect and respect human rights by design.[40]

Private sector actors are often sensitive to questions of intellectual property and trade secrecy, seeking to protect the commercial value of their products. However, corporate secrecy is rarely justifiable in relation to technologies designed for public use and for the public benefit. The harms of private sector secrecy include a lack of control over the long term, increased risk of government and corporate surveillance, and increased risks of security breaches. This kind of secrecy damages public trust in systems that are meant to improve — and not obscure — the workings of urban life.

We note that the concept of an Open Smart City is tightly related to the imperative that municipalities respect and protect human rights because of its emphasis on transparency and accountability. The framework emphasizes the need for technologies that are fit for the purpose and communities they serve, can be repaired, are interoperable, and use open data and software standards.[41]

Municipal leaders should strive to adopt procurement standards that align with and exemplify a respect for human rights, including open systems (including open data), interoperable systems (i.e., a municipality can plug in other technologies alongside the system without permission from

39 Lauriault, T. P., Bloom, R., & Landry, J.-N. (2018). Open Smart Cities Guide. Open North.

40 Penney, J., McKune, S., Gill, L., & Deibert, R. J. (2018, December 20). Advancing human rights by design in the dual-use technology industry. *Journal of International Affairs*.

41 The main components of Open Smart Cities are discussed in Open North's Open Smart Cities Guide (2018) at 6-7.

a corporate partner), and products that guarantee a right to repair (i.e., a municipality can fix, maintain, and update systems freely).[42] These leaders should also seek to adopt procurement standards that increase security and the protection of residents' data; for example, standards that allow the city and its communities to maintain control over the information collected by smart technologies, as well as clearly defined limits or prohibitions on the use, sharing, or sale of data by the private sector partner to third parties.[43]

Impact Assessments

Impact assessments are a well-known tool in the policy and technology space. Most organizations and governments must conduct Privacy Impact Assessments (PIA) as part of their data protection obligations under law. The Global Smart Cities Alliance has also established global PIA standards for smart city technologies.[44] Human Rights Impact Assessments (HRIA) are also used with increasing frequency in development projects in order to measure compliance with a government's human rights obligations.

Throughout the lifecycle of smart city technologies (including after implementation), oversight and transparency measures are essential to ensuring human rights compliance and building public trust. For example, it is essential that residents are provided accessible information about what data is collected, whether about individuals or in aggregate, as well as information about how that data is managed and shared and the purposes for which it is used. Municipalities should also consider proactive transparency measures to report circumstances where law enforcement and other public bodies (such as immigration authorities, intelligence agencies, and private litigants) have sought to access data collected by municipalities and their private sector partners. Finally, in many cases it will be appropriate or even necessary to establish formal oversight bodies for smart city and data governance, a topic on which Open North has published several resources.[45] Such bodies should include public interest technologists, legal experts, and — most importantly — residents, who will be directly impacted by the technologies in question.

For more resources and recommendations on how municipal leaders can think more strategically and responsibly about human rights in the smart city context, the following items may be helpful:

- Rebecca Williams, "Whose Streets? Our Streets! (Tech Edition)," Harvard Kennedy School Belfer Center for Science and International Affairs (2021) (see chapter entitled "10 Calls to Action to Protect & Promote Democracy")
- Immigrant Defence Project & Center for Law, Innovation and Creativity, "Smart-City Digital ID Projects Reinforcing Inequality and Increasing Surveillance through Corporate 'Solutions'" (2021) (see chapter entitled "Best Practices and Policy Recommendations")
- Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" Citizen Lab (2020) (see chapter entitled "Recommendations and Conclusion")
- Open North, Open Smart Cities Guide (2018)
- ACLU Northern California (Chris Conley), "Making Smart Decisions about Smart Cities" (2017)

42 See recommendations 3 and 4 in Open North, Open Smart Cities Guide (2018) at 17.

43 See Open North guides on Open Smart Cities, Open and Ethical Procurement, and Technology Procurement: Shaping Future Public Value. Ferron, P.-A. (2020, December 15). *Open and ethical procurement guide on engaging with the private sector*. Open North. Wylie, B., & Claudel, M. (2021, March 3). *Technology procurement: Shaping future public value*. Open North.

44 Global Smart Cities Alliance. (2020, November). *Privacy impact assessment*.

45 See, for example, ICTC, (2021, October 27), *On a toutes et tous un role à jouer dans la gouvernance des données* [*We all have a role to play in data governance*].