10110
11001 BIG DATA
01101 SURVEILLANCE

SURVEILLANCE
STUDIES CENTRE

Queen's
UNIVERSITY

BEYOND BIG DATA SURVEILLANCE

Freedom and Fairness

A Report for all Canadian citizens

May 18, 2022

CONTENTS

ACKNOWLEDGEMENTS

This report is authored by David Lyon. BDS team members and others researched and wrote the articles and books over the seven-year project, and partners contributed extensively to the research. The publications were read and synthesized by Sachil Singh, whose survey paper was used to structure and inform the report, that also benefitted from core Executive team comments–from Kirstie Ball, Colin Bennett, Stéphane Leman-Langlois, David Murakami Wood, and Valerie Steeves–plus Mark Andrejevic, Adrian Kelly, Sachil Singh and Emily Smith. The BDS project gratefully acknowledges the Partnership Grant funding from the Social Sciences and Humanities Research Council of Canada. Many thanks to all.

EXECUTIVE SUMMARY

Introduction

Surveillance is growing rapidly around the world, especially during the COVID-19 pandemic. Canada provides clear examples, such as police access to public health data and the use of Telus data for public health analysis. Not only citizen privacy, but freedom and fairness are at stake.

The Big Data Surveillance research team examined Big Data in security, marketing and governance. We see surveillance as finding out about people's lives so that they can better be managed or influenced. This happens in national security intelligence and policing; in marketing, whether analyzing consumer preferences or wooing voters to a political party; or in governance, such as in so-called smart cities, like Toronto's aborted "Sidewalks Labs" project, and smart devices and tools like Alexa. Our everyday lives are increasingly digital, with effects both good and bad.

Persistent problems identified by the research:

- **Lopsided information:** Citizens and consumers have little idea of what data is collected about them, let alone the consequences of being visible, while corporations and government departments amass huge amounts of data on Canadians, often using it in unspecified ways.

- **Tangled surveillance:** In pre-digital times, surveillance was much simpler. Today, it is knotty, both organizationally and technically. Few understand data analysis, and the legal requirements are opaque, often failing to speak to the specifics of surveillance. The pandemic contributes to further intricacy.

- **Inadequate instruments:** Changes in technology and practice appear far faster than any regulations to rein them in. Social media, platform companies and the pocket smart phone meet few rules or resistance that would help to shape technology more appropriately.

- **Exposed groups:** Not everyone is affected the same way; some groups, such as women, Black people and Indigenous groups are particularly vulnerable to today's surveillance. Their situation may worsen, especially during a crisis such as the pandemic.

> *“Our post-pandemic world demands thoughtful and decisive action to assess and confront the emerging world of surveillance, which is everywhere and often discriminatory”*

Challenges before us include the following:

- **Public-private partnerships:** These blur lines between government and corporation; the COVID-Alert app is an example. Such surveillance links once-separate spheres, demanding policy responses that relate to both together.

- **Surveillance capitalism:** This sucks up everyday data, selling it for corporate profit. The data may be recycled for other uses including government and policing. It calls for both improved user–awareness and new modes of limiting surveillance.

- **Techno-solutionism:** As with 9/ll, the pandemic prompts rushed tech “solutions” to show that government is doing something, and companies offer what they claim are up-to-date digital tools for the task.

- **Social sorting:** Surveillance not only “sees” people but also *sorts* people into categories for different treatment. This risks negative discrimination and injustice, especially for those already vulnerable. Knowing about and addressing these problems is vital.

Where from here? Recommendations:

- **Persist with privacy; add data justice.** While privacy protection is good, it is not enough for today’s digital society. The social harms of today’s surveillance highlight the need for new digital rights and data justice. Surveillance does not just collect personal data but also analyses it using algorithms, and uses it for many purposes.

- **Increase collaboration:** The need for active collaboration between researchers–in social and computing sciences–regulators, and civil society is underscored by the urgency created by rapid and often unchecked surveillance developments in digital society. Indeed, involving all citizens and consumers is a priority.

- **Enable public and popular awareness:** Big Data Surveillance touches everyone in Canada’s diverse society today. Raising awareness of what is happening, and how everyday choices and chances are affected is crucial. Accurate, accessible and popular information, in written, video, podcast–any relevant format, is essential.

Conclusion:

Our post-pandemic world demands thoughtful and decisive action to assess and confront the emerging world of surveillance, which is everywhere and often discriminatory. The issues deserve to be front-and-centre of educating everyone for everything from safe smartphone use to responsible computing systems. We need innovative modes of assessing and regulating digital developments. A freer and fairer society is a more humanly habitable world.

BEYOND BIG DATA SURVEILLANCE: Freedom and Fairness

Surveillance has rapidly become a central feature of contemporary everyday life in the twenty-first century. Its powerful presence is palpable in every organization of whatever kind, from policing and security to the minute monitoring of workers and from public health scans to the pervasive profiling by platform companies. Surveillance today relies on the digital infrastructure that has enabled large-scale, fast, distributed computer systems of every stripe, and on the active participation of millions who, wittingly or not, contribute to its growth.

State and corporate surveillance of citizens and consumers is constantly expanding in Canada and around the world. The COVID-19 Pandemic prompted further growth. Alongside authorized tracking of personal data for epidemiological purposes, Ontario polices forces engaged in searches of COVID-19 health databases, relating to active cases,[1] for several months–until the civil liberties whistle was blown–in 2020. People being tested for COVID had no idea that their data was available to police, or the purpose for which it was being used. Taken for granted freedoms were jeopardized.

On a federal level, it was revealed in 2021 that the telecom Telus sold mobile location data, connecting cell phones to active COVID cases, to the Public Health Agency of Canada, to trace the path of the COVID-19 virus and to check whether lockdown was observed.[2] Although the data was anonymized, such data can be re-identified. But beyond privacy and transparency questions, such population level surveillance leads to people not only being made visible, but being represented and treated in specific ways. This can lead to more discrimination against certain vulnerable groups, so fairness is a further issue.

Only a few years ago, the buzzword was Big Data; today the talk is of Artificial Intelligence (AI) and Machine Learning (ML) and their relation to "smart" technologies and the Internet of Things. Such shifts only partially reflect real changes; after all, AI still requires massive quantities of data. Research on these is thus increasingly urgent, both for grasping the realities of a digital society and for responding with appropriate strategies to ensure that both human freedom and social fairness are fostered. Classic concerns for privacy and liberty are now matched by and linked with the equally pressing priority of data rights and data justice as goals for both governments and businesses.

Research on Big Data Surveillance

In 2016 The Surveillance Studies Centre (SSC) at Queen's University launched a 5-year SSHRC-funded project on Big Data Surveillance (BDS) that focused research on three areas: security, marketing and governance. The variety of contexts begs the question: Is surveillance the best concept to grasp these various practices? In our view, surveillance today is best understood in a broad sense: any systematic, routine and focused attention to personal details for management, control, protection and influence. Each area may be considered a key locus for the exploitation of Big Data, which is the large-scale collection, aggregation, analysis and use of data by and about people, things and the interactions between them, in order to generate otherwise inaccessible predictions and insights.

Critical developments were explored in the BDS research, such as post-Snowden changes in intelligence–plus policing–services,[3] the use of Big Data in political elections in the wake of Cambridge Analytica,[4] the rapidly-growing business and marketing uses of data analytics,[5] and the explosion of platform companies, 'smart cities,' and 'smart' surveillance in general.[6] In each case the question was, how is Big Data implicated and what might this mean for public policy, especially privacy, data protection and beyond? This question is vital in a time when everyday data acquisition, analysis and use has grown to become basic to all organizations, whether commercial, governmental or whatever.

Big Data's reach has expanded enormously in recent years, and thus there is constant–sometimes turbulent–change, but the common issues in each area are these: On the one hand, questions about what rights may be impugned by increased surveillance: privacy, self-determination and a right "to be forgotten." And on the other, the ethical, discriminatory, and justice issues that together comprise "social sorting." Automated classification and categorization of different groups produces uneven and sometimes clearly unfair outcomes. Added to which, power clearly resides with those with the sophisticated equipment needed for accumulating, storing and making sense of the data.

When the global COVID-19 pandemic broke out, team members turned their attention to how Big Data is implicated in coping with a public health crisis. Because of the already existing interest in and government-corporate enthusiasm for exploiting Big Data, the challenges from some hasty and tech solutionist pandemic responses sharpened the research. Pandemic delays in research offered an opportunity to extend BDS research into public health surveillance.[7]

A careful, cumulative, and comprehensive survey of our work[8] shows that our research on Big Data Surveillance demonstrates the growing dominance of digitalization on everyday citizens' lives and the resultant troves of data-generated insights. The overlapping complexity of issues in each stream also became more evident. The main themes arising from our research are identified as *lopsided information*, especially affecting voters; *tangled surveillance*–it is complex and understood by fewer people, citizens and operators; *inadequate instruments* and the lack of transparency; and *exposed groups*; more vulnerable to manipulation.

In what follows, these main themes are explored further, before highlighting the main challenges and proposing appropriate ways forward.

PERSISTENT PROBLEMS

This section of the report examines "persistent problems" with surveillance and data, as revealed by our research. Of course, no problems in this field are simply "new." Most are old problems in a new guise, but they are urgent today for two reasons: their effects are felt more intensely by populations that were previously less affected, and old measures do not adequately address them. In earlier days, for instance after World War II, surveillance issues revolved mainly around paper documents, along with telephone communication and the use of film cameras. Computing was in its infancy and had not yet been combined with communication technologies. Today's digital technologies make for unprecedented changes in the surveillance world, enabling ubiquitous, 24/7 surveillance across every governmental, administrative and commercial field. This affects everyday life in profound ways, sometimes for good. But its negative consequences are felt more deeply by those who are already disadvantaged.

Lopsided Information

Asymmetrical or "lopsided" information occurs for example when citizens or consumers are not aware of how their data is processed by government departments or by large corporations. Simply put, large organizations have collected huge amounts of information on ordinary citizens, consumers, workers, students, children and so on. And the growing data processing capacities of such large and powerful bodies increasingly give them a vast advantage.

In Canada, as in other democratic countries, security agencies–such as the Communications Security Establishment (CSE)–and the police are ultimately accountable to the citizens that they are mandated to protect. Research on such agencies is notoriously difficult. For example, in order to simply discover how and in what ways Big Data is used by the CSE, Access to Information requests have to be made.[9] When citizens are in the dark about such agencies, they clearly suffer from the consequences of lopsided information. Citizens would benefit from much more transparency, because they lack information to hold agencies democratically accountable for their actions. Citizens deserve reassurance that they are not under needless or illegal surveillance.

Lopsided information may also be clearly seen in the Cambridge Analytica scandal in which psychographic profiles were built from data extracted from Facebook and combined with large-scale voter datasets to try to influence citizens during elections. Those citizens had no idea that the Facebook-based "personality quiz" they agreed to would be used in this way, so they were doubly disadvantaged by the lopsided information involved.[10]

Another example of lopsided information in marketing is the techniques used to make young people more transparent to companies. The talking "Hello Barbie" doll, for instance, holds "conversations" with children using algorithms "crafted to encourage particular kinds of consumption."[11] Children cannot be expected to have "adult" knowledge and expectations when exposed to online communications, which makes their vulnerability to messages and manipulation even greater. As Val Steeves observes, this transparency of children "tips the power scales in favour of the company."[12]

At the height of the pandemic, too, ordinary citizens had no means of knowing how their health data was being used: What were Ontario police doing with COVID-19 contact tracing data?[13] Thousands of unauthorized searches were made through the COVID-19 "first responder" portal, using postcodes to find active cases. Neither was much public attention paid to the targeting of ordinary homes by commercial entities, when the domestic space was conscripted for employment, entertainment, schooling and shopping. Yet in this way the lopsidedness of information was ratcheted up even further during the pandemic.[14]

BDS research was also used as background information to create the short film series *Screening Surveillance*, using near-future fiction to highlight contemporary surveillance issues. The short film *Blaxites* demonstrates this lopsidedness dramatically. It follows an anxious student, who agrees to wear an electronic wristband, provided by her doctor, to monitor her activities. It shows how the interaction between medical databases may render certain patients more vulnerable, disadvantaging them in unexpected ways.[15]

Tangled Surveillance

"Tangled" surveillance happens when surveillance goes far beyond simple observation or monitoring to become twisted, matted, complicated, and confused or in other words, complex. The growing complexity of surveillance practices is a second key factor. Its outcome is that fewer and fewer people understand surveillance, which also increases its lopsidedness. Today's surveillance is troublingly tangled. The complexity affects not only those on the "receiving end" of surveillance (users, citizens), but also those agencies doing the surveillance.

Security analysts are increasingly called upon to be data scientists. Equally, marketers also struggle to keep up with the data analysis leaders. At the same time, the legal requirements are often opaque, having been created and augmented in an unsystematic fashion, often long before today's complexity developed. Few government departments such as CSE, RCMP and CSIS or marketers in new fields seem actively to seek assurances that their data activities are appropriate.

As Sachil Singh observes, "Some of the main concerns with this approach are that the purpose of technological implementation is unrefined, the methods of implementation are unclear, and the intended outcomes are unknown."[16] Many note the discrepancy between the new compulsion to adopt data-driven practices on one hand, and the legal provisions on the other.[17] Some researchers suggest that the increase in manipulative marketing could be related to the struggle for influence in a data-driven context. If so, then consumer empowerment will continue to suffer.[18]

Artificial Intelligence does often spell the displacement of the human worker, which has led to calls for more algorithmic transparency, and broader ethical guidelines, especially as machines increasingly program each other. But few, even among computer scientists, have worked out what such transparency might entail. Proposals include the assurance that there is still a "human in the loop." However, various agencies, including police departments, continue to press for the use of more data analytics, despite having questionable capacities for using them in police intelligence work.[19] And within the Canadian CSE, there is little sign that using the new data-driven methods is matched by a sense of the obligations that go with them–for public accountability and a reform of their culture of secrecy.[20]

In another area, in the early days of the pandemic, the creation of new integrated public health databases in Ontario was achieved in rushed fashion with inadequate consultation and in a non-transparent manner. Changing details of both FIPPA and PHIPA[21] occurred rapidly and within an omnibus bill. Yet the changes were undoubtedly tangled. As Teresa Scassa notes, these changes "would be difficult for the lay person to understand or contextualize without assistance; some are frankly almost impenetrable."[22]

Inadequate Instruments

The rapidity of changes in surveillance, as dependence on increasingly abstract technologies continues, means that the regulations and laws governing surveillance are less and less directly relevant to current conditions. Shifts to Big Data, AI, Machine Learning and the consequent "smartness"–for instance, your car collects data on your driving habits and may even track your eyes to see if they're on the road[23]–of so many dimensions of everyday life were not anticipated by those making many of the existing laws to restrict inappropriate or excessive surveillance. These instruments are frequently not suited for today's conditions. They are inadequate.

Thus, law, regulation, and transparency are not changing in line with the actual changes in data practices that occur with great rapidity. Neither the democratic balance of power between state and citizen, or the relatively level playing field assumed by many consumers regarding companies, can easily be maintained in today's data-climate. The social contract between state and citizens–and now, perhaps, between companies and consumers–if it ever truly existed, is under overwhelming pressure.[24] The blurring of public and private, for instance, has intensified–and is further exacerbated by pandemic prompts to further data analysis.

For instance, during the pandemic, commercially gleaned data was used for Public Health tracking of the virus. As noted in the introduction, the telecom company, Telus, sold location data of 33 million Canadians to the Public Health Authority of Canada (PHAC). In February 2022, The House of Commons ETHI Committee held hearings to discover more about how this occurred, who authorized it, or exactly how the data was used–let alone whether the grounds for its legality were ever tested. After indicating several inappropriate aspects of what occurred, the Privacy Commissioner concluded that both federal privacy laws should be "updated concurrently" in order to recognize the significance of today's extensive interactions between public and private sector data.[25]

When it comes to platform companies such as Facebook, a key problem is their notorious agility in evading legal restraint and their simultaneous weak transparency.[26] Facebook insists that it owns user data and at the same time it operates as a monopoly. The available instruments for curbing platform power are generally quite inadequate. While the data-handling and privacy aspects should properly be the purview of the Privacy Commissioner, the monopoly aspects should be examined by the Commissioner of Competition and the possibilities for making social media a public utility, a matter for the Canadian Radio-Television and Telecommunications Commission (CRTC).[27]

The main problem is that legislation and regulation, established in good faith to cope with surveillance situations, often arising decades ago, cannot keep up with the changes occurring in Big Data Surveillance and its current expansions through AI and "smart" technologies. Not least among these is determining what now counts as "personal information," a question returned to below.

Despite the delays in developing new and up-to-date privacy and data protection law, the constant barrage of new legislation allowing more and more surveillance makes it difficult to evaluate the efficiency of advocacy groups, but also makes it all the more urgent.[28]

A subsidiary problem is that transparency of surveillors–though not in itself the "solution"–is at a very low ebb. Demands for transparency need to be translated for data-driven times, while remembering that the *purpose of transparency* is always to achieve the *accountability* of those pursuing data-driven and smart surveillance.

Exposed Groups

While the previous three "persistent problems" affect everyone in society, they do not affect everyone to the same extent or in the same way. Some groups are more exposed to surveillance than others and such social vulnerability may be seen in each of the previously discussed problems. Surveillance becomes increasingly intimate, rendering its targets more at risk of manipulation.

One group clearly at risk of disproportionate surveillance is Indigenous peoples, especially when they exert their right to protest.[29] Both individual leaders and communities and movements are under extra scrutiny. Cindy Blackstock, for instance, Gitskan activist for child welfare and McGill professor, was monitored by Indigenous and Northern Affairs and the Department of Justice between 2009 and 2011. Protest against pipelines or forest destruction is met with intensive police surveillance on the pretext of "threats to national security," which resonates with settler colonial assumptions about land ownership.[30]

Urban policing also shows that Black people in Canadian cities are subjected to higher levels of surveillance than others.[31] Much less dramatically but no less seriously, Black women also experience negative surveillance in health-care and related areas–which includes under-representation due to "data gaps" as well.[32] Inequalities and inequities in health surveillance can also disadvantage women in Canada long term, across the lifespan.[33]

Social vulnerability increases as manipulation-through-intimate-surveillance expands. This theme straddles the previous three and affects citizens, consumers, employees, and many other categories. Few can keep up with the speed and magnitude of changes in data analysis and use, which means less protection, especially for the most vulnerable. Consent has become an intractable issue. Platforms become more predatory. Racialized and socio-economically disadvantaged people are worst affected, both pre-and especially post-pandemic.

THE CHALLENGES BEFORE US

Public-private partnerships

The implications of corporate-government collaboration in the production and use of surveillance are huge and mushrooming. They have a long history in areas from security and policing to industrial relations and military development and marketing, as shown in Kirstie Ball and Laureen Snider's collection on *The Surveillance-Industrial Complex*.[34] The rapid rise of public-private partnerships (P3s), encouraged by neoliberalism, from the 1990s, also involved surveillance, for example in the development of CCTV in the UK, followed by the US and Canada.

The collaboration of state and commerce in matters of surveillance has been increasingly evident since the start of this century, and became strikingly visible after 9/11. The expansion of social media offered access to new kinds of user-generated data that were quickly sought for surveillance by national security agencies and police forces, a public-private relationship that continues to flourish. The COVID-19 pandemic has accentuated this in a number of ways worldwide, as seen for example in digital contact-tracing and vaccination certificate systems.

As governments come to rely on data-intensive forms of management, data storage and processing is often offloaded onto private companies, with the result that government departments become beholden to such companies, whose commercial imperatives may be in tension with public responsibility and democratic accountability.

The upshot of the surveillance-industrial complex in Canada is that relationships between state and corporation are deeper and more taken-for-granted than ever.[35] Realism about this is essential if progress is to be made in regulating and reining-in unnecessary, excessive and illegal surveillance. This means that any program for reducing surveillance has to involve both government *and* commerce, as well as independent research institutions and other relevant agencies and networks in civil society.

Surveillance capitalism

The rise of surveillance capitalism is critical to our understanding of key surveillance issues today. Surveillance capitalism is the commodification of everyday personal data for corporate profit. But consumer complicity continues to play an important part. Surveillance capitalism depends on the willing participation of its users. The positive aspect of this is that its effects could be mitigated by informed and active users.

Power is a crucial issue here. As Jim Balsillie argues, structural power imbalances are exacerbated by surveillance capitalism. The scale and efficiency of data analysis, especially using AI and algorithmic decision-making exposes citizens and consumers not only to identification, but also to power relations in which influencing behaviour is at the core.[36] This has been recognized by Daniel Therrien, the federal Privacy Commissioner, who in his 2021 Annual Report also warns of the "growing power of tech giants Google and Facebook, which seem to know more about us than we know about ourselves."[37]

Public awareness of surveillance capitalism was boosted tremendously by the publication of Shoshana Zuboff's book in 2019 but popular awareness of its meaning for everyday lives is still low (even if you have watched the *Social Dilemma*[38] documentary). The key problem remains the apparent advantages for convenience and comfort of using digital machines and devices for communication, commerce, education, health-care and so on. These maintain the attractiveness of the media while distracting from its socially-negative effects.

Techno-solutionism

The marketing of ML and AI, not to mention data itself, may be thought of as techno-solutions. Techno-solutionism[39] is often present as a theme in public-private partnerships, where tech companies lobby governments for business, and governments adopt technologies to indicate that they are "doing something" about social and political problems. Perhaps the Ontario Chamber of Commerce ironically entitled their report In Data We Trust,[40] which sounds techno-solutionist, because they clearly wish to alert members to the need for privacy and the strengthening of data-related law.

Techno-solutionism received a great boost after 9/11, as ailing technology corporations competed for government contracts, and an even larger impetus during the global COVID-19 pandemic. The associated haste with which such "solutions" were sought, led in each case to the adoption of systems and practices that were insufficiently tested, approved, or democratically debated. Matters such as democratic procedures or human rights are thus sidelined, especially where surveillance–often associated with power and control–is concerned.

However, techno-solutionism is not an appropriate way forward. Evidence from policing and security agencies and also, now, from the experience of the pandemic, strongly suggests that such rushed and over-eager surveillance responses simply may not work as originally imagined. It is not at all clear, for example, that the GAEN COVID-Alert App used in Canada achieved any of its touted aims in reducing the spread of the virus.[41] And of course, techno-solutionism is evident in many other areas than digital contact tracing and also, in many other countries around the world.[42]

The pandemic has perpetuated and made more urgent many of these questions. But at the same time, techno-solutionism–the belief that in a health-related, social and political "crisis," public bodies should turn first to technological remedies–and the haste with which many data-based innovations were made has pushed many such questions into the background. During the pandemic, not only have certain marginalized groups been worst affected, but also their condition has in some cases been exacerbated by the proffered "solutions."

Social Sorting

Social sorting is a feature of surveillance that cuts across all the streams–and themes–of the research. As Singh notes, citing the Stream 3 report, "Central to all these cases are the ethical, discriminatory and justice dangers of social sorting."[43] Recall that Stream 3 concerns issues of marketing as surveillance, in which, classically, dividing consumers into groups through ongoing classification is the mechanism for targeted advertising. This practice has become far more sophisticated since Oscar Gandy first demonstrated its contribution to the creation and perpetuation of inequality in his pioneering *The Panoptic Sort*.[44]

> *“privacy laws can no longer be depended on as the sole mode of managing technological change as data practices proliferate. New data-governance models are required that combine technical issues with broader questions of how the social sorting that perpetuates inequalities and injustices can be curtailed by data rights and data justice”*

Indeed, it is striking to consider the massive changes that have occurred in less than a generation. Gandy now speaks not only of technologies for consumer sorting and inequality, but also of the transformations of capitalism that accompany them. Quantities of data gathered, processed and distributed have become astronomical, and they are now used not only by corporations but by government agencies, and public-private partnerships. Not only this, autonomous devices have unprecedented power, based on advanced Artificial Intelligence and Machine Learning. Each enhances the sorting and discriminatory features of surveillance.

These developments in sophistication and power may readily be seen in other areas that are frequently built on practices that first were used in marketing. In the post-9/11 context, a strikingly similar logic lies behind airport screening, which also depends on coded categories for sorting between passengers. If personal data is extracted, combined and extrapolated to create profiles of potential consumers, a similar logic allows data to be processed to identify and isolate groups and persons as potential terrorists.[45] As the research on BDS shows, such practices are reproduced and intensified–for instance, as Stéphane Leman-Langlois shows, using neural technologies–in today’s security intelligence.[46]

Beyond this, the sorting processes are also highly visible in the ways that features of marketing and security surveillance reappear in the realm of governance. Smart cities, for example, are touted as the attractive-sounding wave of future urban living and organization. The ambiguities of contemporary surveillance are seen here once again. Who would not want greener cities, with smart transit, fast internet and climate-controlled buildings? But the same smartness makes it a “data-driven ubiquitous surveillance society,” notes David Murakami Wood.[47]

The very notion of consent is eliminated in a context where–like the now defunct plans for the Sidewalk Lab smart city in Toronto–sensors and cameras constantly collect data in every conceivable context. And the kinds of inequality and injustice currently plaguing today’s cities are reproduced in a data-dependent environment–where the modes of data-use are scarcely questioned. These practices are technologically upgraded forms of social sorting, in a milieu where public participation in decision-making is minimized.

What this means, among other things, is that privacy laws can no longer be depended on as the sole mode of managing technological change as data practices proliferate. New data-governance models are required that combine technical issues with broader questions of how the social sorting that perpetuates inequalities and injustices can be curtailed by data rights and data justice. Surveillance capitalism–or “platform capitalism”–must be met with coherent limits so that harms related to privacy and to social disadvantage can be addressed. Consumer data can actually lead to higher prices and more limited choices for Canadians. Pursuing *consumer welfare* should be the goal if truly fair competition is sought.[48]

WHERE FROM HERE?

The Persistent Problems that we have identified as urgent matters for public attention are *Lopsided Information*, *Tangled Surveillance*, *Inadequate Instruments* and *Exposed Groups*. These must be considered in the context of the major challenges of *Public-Private Partnerships*, *Surveillance Capitalism*, *Techno-Solutionism* and *Social Sorting*. For ongoing research, all these themes make more urgent the need for multi-disciplinary investigation, but also for expanding the field of concern and vastly increasing public education.

What our research shows, strikingly, is that the growth of Big Data Surveillance–along with algorithmic analysis, augmented by Artificial Intelligence and Machine Learning–touches every area of life, for the entire population. Our overall recommendation is that this be recognized and built on, through extensive cooperation with other players–in research, education, commerce and different layers of government, regulatory and civil society groups, in a multi-sectoral fashion. Moreover, certain areas demand priority attention, given current demographics and the rapid expansion of data analytics in Canada. The priority areas include ageing, geography, health and race.[49]

A FINAL THREE RECOMMENDATIONS FOLLOW:

Persist with 'privacy,' add data justice

A key recommendation of this project is that privacy protection, important though it is, should be seen as part of a much larger set of requirements for responding appropriately to the growth of surveillance in digital societies. Privacy legislation relates especially to problems of inappropriate data handling and to the personal control of personal information. It is primarily a matter between individuals and organizations. However, the social value of privacy as a human right requires broader protections that go beyond data protection.

As Lisa Austin and David Lie insist, referring to the Sidewalk Labs situation, "collecting data in smart environments is not easily modelled on the intentional sharing of personal information with an organization providing you with a product or services. Instead, it involves opaque collection of information that may or may not be about people and may or may not be identifiable."[50]

Despite this "opaqueness" of data handling, certain all-too-identifiable harms are generated, several of which are discussed above. "Chilling effects," for instance, were once considered too vague to warrant legal action. However, Jonathan Penney demonstrates how surveillance chills internet searches. Users became more cautious about using certain potentially suspect words, indicating that post-9/11 security surveillance had tangible chilling effects.[51] This falls outside of familiar "privacy" concerns but is no less a real "harm" created by surveillance.

Today we need to consider further harms, especially in smart environments, where, for example, behaviour is modified. As Mark Burdon and Tegan Cohen say, discussing Google Home, harms include "…the ability to harness, direct, and provide 'frequency' to flows of sensor data to achieve continual behavioural modification and shape social norms about the purposes and benefits of such modification."[52] This is not only social sorting but also social shaping. What Shoshana Zuboff sees at the individual level is also a profoundly social and political matter.

Following from the recognition of social surveillance harms, we should develop new ways of framing responses, including "data rights" (or "digital rights"). For Bianca Wylie, this is "a range of protections regarding access to the internet, privacy, transparency regarding how data is used, control over how data is used, democratic participation in municipal technology decisions and more."[53] Beyond this, more broadly, is "data justice," which speaks to the way that surveillance makes visible, identifies, represents and treats given populations unevenly, due, for example, to biased algorithms.[54]

These concepts also have to be mobilized in relation to more than one area, connecting privacy concerns with competition, for one example, and revising both Canadian federal privacy laws together. Each of these examples is discussed earlier. Beyond these, intellectual property questions are raised, as well as the need to develop ethical guidelines for appropriate computing.

Increase collaboration

A second recommendation is that collaborative research in this area be strengthened. The Big Data Surveillance research program offered many opportunities for increased collaboration, both within and beyond Canada. We are pleased that the SSHRC has supported our work, over many years, and also that of other colleagues in many disciplines.

The beauty of this particular relationship is that it requires researchers to be actively involved with partners, in our case connecting social/data science researchers with both regulatory and civil society groups, particularly ones dedicated to data justice and data rights.

When researchers get the opportunity to collaborate with others who are approaching the same issues from a different–*practitioner*–angle, the benefits are two-way. Our partners can take advantage of the research they need but have no time or budget for, while researchers have access to those who are very directly involved and whose everyday lives are affected by the issues that are being researched. For all of us, this has been a boon, in nearly two decades of researching surveillance and privacy issues in Canada.

However, such opportunities should not be taken for granted. This report also recommends that such multidisciplinary and collaborative partnerships should not only be maintained but also expanded. In areas relating to our digital society in particular–for which surveillance studies is centrally vital–this is something that should be basic. The rapidity, ubiquity and consequentiality of changes in this sector are so huge and all-encompassing that they call for continuing and expanded research relationships such as the one that this project has enjoyed since 2015.

Enable public and popular awareness

A third and final recommendation is that the matters discussed here in an academic and policy-related format are urgently translated into the vernacular, using online tools as well as time-honoured face-to-face learning practices. These research findings are not for only academic interest, or even solely for the benefit of our partners. It is vital that they inform Canadian society at many levels. Creative means of dissemination are sought, which may be done with various kinds of partners, beyond the regulatory and civil society partners with whom we already work.

> *“Surveillance is now a major public issue that demands attention on many levels. Privacy is still important, but today’s surveillance also calls for serious attention to new harms that it causes, new dimensions of social life in which it is implicated–making visible, identifying, representing and treating people in new ways, requiring not only data rights but data justice as a goal, and finally, data as public infrastructure that demands fresh approaches in order not only to minimize harms but to enable human flourishing in a digital era.”*

For instance, in public education, our project has also made several short films–under *‘Screening Surveillance’*–to illustrate the issues, especially intended for younger people. They are available on YouTube and have also been shown at festivals and in educational contexts–with language subtitles–around the world.

As we observed earlier, informed and active online participants are vital to the health of the internet and of the digital world generally. The social and political benefits of the digital realm will not be fully realized without significant changes, including in the awareness, knowledgeability and commitment of its participants, of all ages and in all regions of Canada.

CONCLUSION

We are in a moment of opportunity as the pandemic becomes less severe and as we learn to live with it. Many have spoken in “apocalyptic” terms about the pandemic, stressing its disastrous effects. But “apocalypse” in its Greek origin speaks not only of catastrophe but also of unveiling, laying bare. And the pandemic has laid bare–has revealed even more–the rapid rate of growth of new forms of surveillance–data-driven, smart, and evolving in ways that go far beyond the capabilities of privacy and data protection to ensure that surveillance is used only for positive purposes. Surveillance is now a major public issue that demands attention on many levels. Privacy is still important, but today’s surveillance also calls for serious attention to *new harms* that it causes, *new dimensions* of social life in which it is implicated–making visible, identifying, representing and treating people in new ways, requiring not only *data rights* but *data justice* as a goal, and finally, *data as public infrastructure* that demands fresh approaches in order not only to minimize harms but to enable *human flourishing* in a digital era.

Endnotes

[1] The CBC reported that some police searches were unrelated to active calls, suggesting that fishing expeditions were occurring, at: https://www.cbc.ca/news/canada/toronto/covid-police-database-1.5745481

[2] Swikar Oli. 2021. “Canada’s public health agency admits it tracked 33 million mobile devices during lockdown,” *National Post*, December 24, at: https://nationalpost.com/news/canada/canadas-public-health-agency-admits-it-tracked-33-million-mobile-devices-during-lockdown/

[3] David Lyon and David Murakami Wood (eds.) 2020. *Big Data Surveillance and Security Intelligence*, UBC Press.

[4] Colin Bennett and David Lyon. 2019. special issue on “Data-Driven Elections” in *Internet Policy Review* 8 (4).

[5] Kirstie Ball and William Webster. 2020. special issue on “Big Data and Surveillance: Hype, Commercial Logics and New Intimate Spheres” *Big Data & Society* 7 (1).

[6] Valerie Steeves and David Murakami Wood. 2021. special issue on “Smart Surveillance” in *Surveillance & Society*, 19 (2).

[7] For example, Mark Andrejevic and Zala Volcic. 2021. “Pandemic lessons: Total surveillance and the post-trust society,” *The Political Economy of Communication* 9 (1); Kirstie Ball. 2021. *Electronic Monitoring and Surveillance in the Workplace* (discusses specific COVID-19 developments) European Union JRC Publications Repository; Stéphane Leman Langlois. 2022. cited in Raphaël Pirro, “Données géographique: la pertinence du programme L’ASPC remise en question” *Le Journal de Montréal*, 21 janvier; David Lyon. 2022. *Pandemic Surveillance*, Cambridge: Polity Press; David Murakami Wood, in Yann Sweeney. 2020. “Tracking the debate on COVID-19 surveillance tools” *Nature Machine Intelligence*, 2, 301-304; Valerie Steeves, Val Michaelson and Robert Porter. 2021. “For teenagers, the internet helps during lockdowns, but it’s no substitute for the outside world,” *The Conversation*, May 18.

[8] Sachil Singh, 2021. Big Data Surveillance: Collated Research Findings. Report on BDS Research, September-April.

[9] See Scott Thompson and David Lyon. 2021, ‘Pixies, Pop-out Intelligence and Sandbox Play’, in Lyon and Murakami Wood (eds.) *Big Data Surveillance and Security Intelligence: The Canadian Case*, UBC Press.

[10] See Bennett and Lyon. 2019.

[11] Valerie Steeves. 2020. “A dialogic analysis of Barbie’s ‘conversations’ with children.” *Big Data & Society*, Jan-Jun 1-12.

[12] Steeves. 2020: 10.

[13] See https://www.policingthepandemic.ca/

[14] David Lyon. 2022. *Pandemic Surveillance*, Polity Press, chapter 4.

[15] *Blaxites* in the Screening Surveillance series, at: www.screeningsurveillance.ca.

[16] Sachil Singh. 2021. Report on BDS Research, see footnote 8.

[17] Kirstie Ball and William Webster. 2020. ‘Big Data and Surveillance: Hype, Commercial Logics and New Intimate Spheres’, *Big Data & Society*, January-June: 1-5.

[18] Aron Darmody and Detlev Zwick. 2020. “Manipulate to empower: Hyper-relevance and the contradictions of marketing in the Age of Surveillance Capitalism.” *Big Data & Society*, Jan-Jun: 1-12.

[19] Craig Forcese. 2020. ‘Bill C-59 and the Judicialization of Intelligence Collection’, in Lyon and Murakami Wood (eds.) *Big Data Surveillance and Security Intelligence: The Canadian Case*, UBC Press.

[20] Andrew Clement. 2020. ‘Limits to Secrecy: What Are the Communications Security Establishments’s (CSE) Capabilities for Interception Canadians’ Internet Communications’, in Lyon and Murakami Wood (eds.) *Big Data Surveillance and Security Intelligence: The Canadian Case*, UBC Press.

[21] FIPPA: Freedom of Information and Protection of Privacy Act; PHIPA: Personal Health Information Protection Act.

[22] Teresa Scassa. 2020. “Interesting amendments to Ontario’s health data and public sector privacy laws buried in omnibus bill.” March 30, at: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=323:interesting-amendments-to-ontarios-health-data-and-public-sector-privacy-laws-buried-in-omnibus-bill&Itemid=80.

[23] Matt Bubbers. 2020. “What kind of data is my new car collecting about me? Nearly everything it can, apparently.” *The Globe and Mail*, January 15, at: https://www.theglobeandmail.com/drive/technology/article-what-kind-of-data-is-my-new-car-collecting-about-me-nearly-everything

[24] See e.g. Robert Pallitto. 2020. *Bargaining with the Machine: Surveillance, and the Social Contract.* Lawrence: UP of Kansas.

[25] OPC Appearance before ETHI, February 7, 2022, at: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_20220207/ Researchers David Lyon and David Murakami Wood also gave evidence at EHTI, the Canadian House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[26] BDS Team members have been involved in the Digital Charter Implementation Act (Bill C-11).

[27] Andrew Clement and David Lyon. 2018. “Facebook: A mass media micro-surveillance monopoly,” *The Globe and Mail*, April 23, at: https://www.theglobeandmail.com/opinion/article-facebook-a-mass-media-micro-surveillance-monopoly/

[28] Tim McSorley and Anne Guertin. 2020. ‘Confronting Big Data: Popular Resistance to Government Surveillance in Canada since 2001’, in Lyon and Murakami Wood (eds.) *Big Data Surveillance and Security Intelligence: The Canadian Case*, UBC Press.

[29] Lex Gill and Cara Zwibel. 2017. “Why does Canada spy on its own indigenous communities?” *Open Democracy*, December 6.

[30] Andrew Crosby and Jeff Monaghan. 2018. *Policing Indigenous Movements: Dissent and the Security State*, Black Point NS: Fernwood.

[31] Steven Hayle, Scot Wortley and Julian Tanner. 2016. “Race, street life, and policing: Implications for racial profiling.” *Canadian Journal of Criminology and Criminal Justice*, 58(3): 322-353.

[32] David Williams and Ronald Wyatt. 2015. “Racial bias in health care and health: challenges and opportunities.” *Jama*. Aug 11, 314(6): 555-6.

[33] Stephanie Austin, Sari Tudiver, Miga Chultem and Mireille Kantiebo. 2007.“Gender-based analysis, women’s health surveillance and women’s health indicators–working together to promote equity in health in Canada,” *International Journal of Public Health*, 52: S41-S48.

[34] Kirstie Ball and Laureen Snider (eds). 2013. *The Surveillance-Industrial Complex: A Political Economy of Surveillance*, London: Routledge.

[35] David Lyon. 2018. *“State and surveillance”* CIGI Online, at: https://www.cigionline.org/articles/state-and-surveillance/

[36] Jim Balsillie. 2021. “Liberal privacy bill fails to curtail surveillance economy or protect Canadians.” *National Post*, March 15, at: https://nationalpost.com/opinion/jim-balsillie-liberal-privacy-bill-fails-to-curtail-surveillance-economy-or-protect-canadians

[37] Daniel Therrien, OPC Report Annual. 2021. cited by Jim Bronskill, Canadian Press/CBC December, at: https://www.cbc.ca/news/politics/privacy-commissioner-report-daniel-therrien-1.6279665

[38] *Social Dilemma*, a documentary from Netflix, 2020, at: https://www.thesocialdilemma.com/

[39] Evgeny Mozorov. 2014. *To Save Everything: Click Here*, New York: Public Affairs.

[40] OCC. 2020. *In Data We Trust*, at: https://occ.ca/wp-content/uploads/OCC-DataReport.pdf

[41] CBC. 2022. “Where did things go wrong with Canada’s COVID Alert app?” February 09, at: https://www.cbc.ca/radio/costofliving/from-boycott-to-bust-we-talk-spotify-and-neil-young-and-take-a-look-at-covid-alert-app-1.6339708/where-did-things-go-wrong-with-canada-s-covid-alert-app-1.6342632

[42] See e.g. Rob Kitchin. 2020. “Civil liberties or public health or civil liberties and public health: Using surveillance technologies to tackle the spread of COVID-19” *Space & Polity*, May, at: https://kitchin.org/wp-content/uploads/2021/01/SP-2020-civil-liberties-and-public-health.pdf

[43] See Kirstie Ball, and William Webster. 2018. ‘Workshop Report: New Lines of (In)Sight: Big Data Surveillance and the Analytically Driven Organization’, at: https://www.sscqueens.org/sites/sscqueens.org/files/bds-crisp_report_stream_two_2018_0.pdf, p.l.

[44] Oscar Gandy. 1993. *The Panoptic Sort: A Political Economy of Personal Information*, New York: Oxford, 2021 (updated edition of the 1993 book from Westview Press).

[45] David Lyon. 2006. “Airport screening, surveillance and social sorting: Canadian responses to 9/11 in context,” *Canadian Journal of Criminology and Criminal Justice*, 48 (3): 397-411.

[46] Stéphane Leman-Langlois. 2020. “Big Data Against Terrorism” in Lyon and Murakami Wood (eds.) Big Data Surveillance and Security Intelligence: The Canadian Case, UBC Press.

[47] https://www.queensu.ca/research/features/smart-cities-city-future

[48] Ana Qarr. 2022. “Canada must reform competition and privacy law together to protect consumers” *Policy Options/ Options Politique*, February 28.

[49] See the report on BDS by Sachil Singh, 2021, see footnote 8.

[50] Lisa Austin and David Lie. 2021. “Data trusts and the governance of smart environments: Lessons from the failure of Sidewalk Labs’ Urban Data Trusts,” *Surveillance & Society*, 19(2): 255-261.

[51] Jonathan Penney. 2021. “Understanding chilling effects” *Minnesota Law Review*, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855619/

[52] Mark Burdon and Tegan Cohen. 2021. “Modulation harms and the Google Home” *Surveillance & Society*, 19(2): 154-167.

[53] Bianca Wylie. 2019.“Why we need data rights: everything about us should not be for sale,” *CIGI online*, January 30, at: https://www.cigionline.org/articles/why-we-need-data-rights-not-everything-about-us-should-be-sale/

[54] See Linnet Taylor. 2017. “What is data justice? The case for connecting digital rights and freedoms globally,” *Big Data & Society* November 2017, at: https://journals.sagepub.com/doi/10.1177/2053951717736335 and Lina Dencik, Arne Hintz, Joanna Redden and Emiliano Treré. 2019. “Exploring data justice: Conceptions, applications and directions,” *Information, Communication & Society*, May, at: https://www.tandfonline.com/doi/full/10.1080/1369118X.2019.1606268 The call for data justice also raises questions of what social-political arrangements for the ownership and control of data-intensive surveillance systems are compatible with democratic politics and the safeguarding of civic and human rights.

10110
11001 BIG DATA
01101 SURVEILLANCE

SURVEILLANCE
STUDIES CENTRE

Queen's
UNIVERSITY

UNIVERSITÉ
LAVAL

uOttawa

University
of Victoria

University of
St Andrews

The
Office of the Privacy
Commissioner of Canada

Office of the
Information &
Privacy Commissioner
for British Columbia
Protecting privacy. Promoting transparency.

International Civil Liberties
Monitoring Group

CRISP
CENTRE FOR RESEARCH INTO INFORMATION,
SURVEILLANCE & PRIVACY

BC
CLA
BRITISH COLUMBIA
CIVIL LIBERTIES
ASSOCIATION