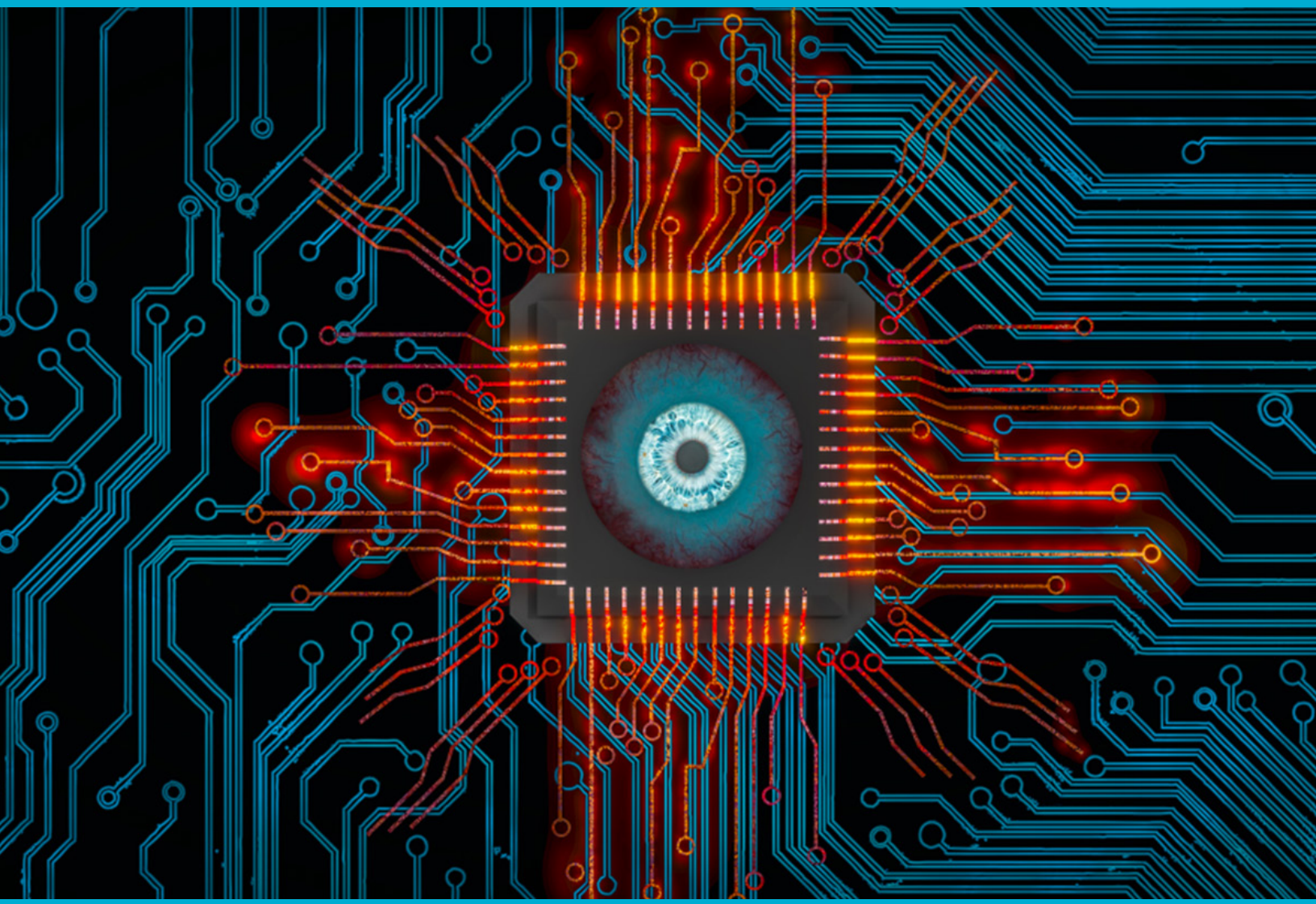
RSC SRC

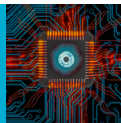
INFOVEILLANCE



RSC WORKING GROUP
2020

Table of Contents

Version française disponible.



Introduction

Infoveillance: Data, Privacy, Equality and Surveillance

David Lyon, Benoît Dupont, Anatoliy Gruzd, and Jane Bailey, with the collaboration of Stephen Wyatt and Monica Heller

Both utopian and dystopian views of digital technologies have long been debated. This set of papers takes up one specific aspect of the sometimes perverse or unexpected consequences of the permeation of such technologies in our everyday lives: what we are calling *Infoveillance*—the integration of information and surveillance technologies.

Smart phones, facial recognition, internet search engines, social media, and self-learning algorithms all provide new opportunities to generate data about our individual daily activities—data that is then used to profile and track us. This phenomenon has come increasingly into the public eye with the COVID-19 pandemic. Five million Canadians have already downloaded *COVID Alert*, the tracking and notification app launched by the federal government, creating heightened tension regarding whether privacy must be traded for safety.

Infoveillance is the subject of increasing discussion among such diverse groups as academics, health professionals, representatives of equality-seeking communities, policymakers, urban planners, and privacy and human rights advocates. This set of papers seeks to explore the significance of this transformative shift, negotiating between the boundless optimism of some and the deep pessimism of others, to consider the path forward for Canadian society.

While we were already increasingly replacing physical offline interactions with virtual online means, whether for work, everyday chats, family get togethers, drinks with friends, entertainment, or shopping, the pandemic has intensified and accelerated this transformative shift. This creates a mountain of data about our interests, our preferences and our habits, and those of everyone with whom we connect. As algorithms analyse this data, they determine other subjects or products that might interest us, thereby nudging us towards certain behaviours—as all who have watched *The Social Dilemma*[1] will appreciate.

This treasure trove of data clearly has huge commercial value and we should not be surprised that new techniques are developed to monetize this information by modifying our behaviour—whether for shopping, eating, voting or visiting. Shoshana Zuboff uses the term *Surveillance Capitalism*[2] to highlight the way that data is a new mode of economic accumulation. Algorithms use this valuable accumulated data to sort us into profiles for marketing and to support corporate and government decision making that directly affects everything from online queries to health care access, employment opportunities, and the justice system. As Safiya Noble makes clear in *Algorithms of Oppression*[3], members of equality-seeking communities are particularly vulnerable to sorting that reflects, perpetuates and reinforces the systemic discrimination that permeates society.

Should we therefore be comforted by the federal government's commitment to enhance our privacy protection? The challenges raised by *Infoveillance* are much greater than simply protecting our personal data but include how even anonymous data is used and by whom. New governance frameworks need to focus on probable futures for collecting, analysing and using information, not just on past and present practices. Developing these frameworks will require creativity in working with all stakeholders, along with

1. *The Social Dilemma* (2020) directed by Jeff Orlowski and released by Netflix
2. *The Age of Surveillance Capitalism* (2019) by Shoshana Zuboff and published by Public Affairs
3. *Algorithms of Oppression* (2018) by Safiya Noble and published by NYU Press

flexibility and accountability to allay Canadians' concerns. It will also require a conceptual shift toward an understanding of privacy as a human right, intimately connected to other rights such as equality.

This multidisciplinary set of essays brings together four experts in various fields, who constituted the RSC's Working Group on Infoveillance (2019-2020), under the auspices of the RSC's Committee on Public Engagement, and with the support of two of the CPE members, Stephen Wyatt and Monica Heller. These essays form a recent RSC sponsored series on *Infoveillance* in *The Conversation*, published at different points in 2020. Together they seek to temper both the optimism and the pessimism, to provide answers for questions, and to pose questions that need to be asked as *Infoveillance* becomes part of the new normal in Canada.

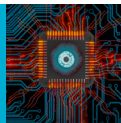
David Lyon, sociologist, Director of the Surveillance Studies Centre at Queens University, developed the concept of surveillance as "social sorting" and directs an international project on "Big Data Surveillance."

Benoît Dupont, criminologist, holds a research chair in cybersecurity at the Université de Montréal and focuses on ways that the proliferation of surveillance technologies affects our society.

Anatoliy Gruzd, information technologist, holds a research chair in social media at Ryerson University and examines the impacts of networks on modern society.

Jane Bailey, a law professor at the University of Ottawa, co-leads The eQuality Project and researches the impact of evolving technology on equality, privacy, and rights, especially for members of equality-seeking communities.

David and Monica are Fellows of the Royal Society of Canada while Anatoliy, Benoît, Jane and Stephen are Members of the College of New Scholars, Artists and Scientists.



Surveillance Beyond Privacy

David Lyon | June 17, 2020

The COVID-19 pandemic is stirring up a surveillance storm, both in terms of the research energy released and of the personal-data-and-public-trust questions thrown up. Researchers rush to develop new forms of public health monitoring and tracking but releasing personal data to private companies and governments carries risks to both personal and collective rights. COVID-19 opens the lid on a much-needed debate.

For example, Google and Apple have offered geolocation data to health authorities, for contact-tracing. And this, with other schemes, is widely debated. The scramble for data 'solutions' is, one hopes, well-meaning, but whether they work or not, they generate risks beyond a narrowly-defined 'privacy.'

Everyone has extensive digital records—on our health, education, employment, police-contact, consumer-behaviour—indeed on our whole life. These are constantly being pulled together in new ways and we can only hope that those handling them respect our 'privacy.' But these data also affect our chances and choices in life, often in critical ways.

Shoshana Zuboff's big book on The Rise of Surveillance Capitalism has been making headlines for its close analysis of just how Google achieves its surveillance, why, and with what consequences. Her thesis is that nothing short of a new mode of economic accumulation has rapidly been emerging ever since internet-based platforms—led by Google—discovered how to monetize the so-called 'data exhaust' exuded by everyday online communications; searches, posts, tweets, texts. The impact—loss of privacy, behavioural modification and the destruction of democracy—is dire.

Whatever one makes of the fine details of Zuboff's work—it is sparking debate!—one cannot miss the cri de coeur and its scathing denunciation of the "radical indifference" of platforms as currently constituted and of their "doctrines of inevitability." But what will it take to persuade us that today's surveillance has become a basic dimension of our societies and that it threatens more than my 'personal privacy'? Undoubtedly, it's complicated, arcane and apparently out-of-control, but those are hardly excuses for complacency. They're reasons for digging into some of the main dimensions of surveillance, prying open black boxes and reasserting human agency.

Four jolts

Let's start by disturbing some common assumptions, that surveillance is about video cameras, state intelligence and policing, that it produces suspects and that it challenges privacy. Google assuredly does 'surveillance,' commonly defined as "any focused, routine, systematic attention to personal details, for the purpose of control, influence or management."

It's not just CCTV cameras, it's smartphones – surveillance is digital, data-driven.

For too long, the stereotypical icon of surveillance is the ubiquitous surveillance camera and this makes sense. The French root of surveillance means to 'watch over' and that's what cameras do. They become increasingly smart, when enhanced by facial recognition technology. Clearview AI, for instance, scrapes

billions of images from platforms such as Facebook or Google and sells their matching services to major police departments in the US—and until recently, in Toronto.

But today, what deserves to be the stereotypical icon is the smartphone. This, above all, connects individuals with corporations that not only collect but analyze, sort, categorize and use the data constantly exuded by that individual. This happens without our say-so, to influence, manage or govern us. Data analysis enables prediction, then 'nudging' of specific population groups to buy, behave or vote in hoped-for ways. The flow of data through personal devices powers surveillance today.

It's not just the state, it's the market – surveillance is for influence, profit-driven

While the state and its agencies do all-too-often overreach themselves through no doubt well-intentioned intelligence and policing strategies, the market, not the state, holds the key cards in the surveillance game. State surveillance still menaces democracy and freedom to differing degrees around the world. Aspects of COVID-19 surveillance may cross that line, too. But the state is no longer alone.

Few noticed in the early C20th that department stores, like Syndicat St Henri in Montreal, kept detailed customer records, giving or withholding credit according to their status. Today our profiles indicate our 'lifetime value' to businesses but they also propel advertising to us, subtly influencing our behaviours and practices, with limited regulation.

A pivotal moment was 9/11 when high-tech companies, craving customers after the dot-com bust, offered their services to government. Such 'public-private' partnerships are commonplace today.

Now, our massively augmented data-profiles indicate our 'lifetime value' to companies. And those data may also be valuable to others, too, such as 'election consultants' – think Aggregate IQ, and Cambridge Analytica.

It's not just suspects, it's everyone – surveillance is for sorting, reputation-driven

'Surveillance' and 'suspects' once belonged neatly together – those thought to be miscreants were watched. What French sociologist Jacques Ellul worried about in 1954 has transpired: the police quest for more and more information makes everyone a suspect. But Ellul never guessed how this could morph into a global network of systems—far beyond policing—in which everyone becomes a target.

But everyone is not targeted in the same way. The systems in question, whether for welfare, commerce or policing, sort populations into categories for different treatment, rather like the emergency room triage. This 'social sorting,' works in marketing to slot people into niches of where you live—find out for yourself by looking it up! Those device-data make up your profile which to companies and others is your reputation. In China today, growing social credit systems are run by government; ours, by companies.

It's not just privacy, it's data justice

Early computerization obliged governments to see that regulation was needed as personal data were collected for more and more purposes. At first the data came from credit cards, driver's licences and social insurance; today it's constant device-use. But privacy regulation alone can't keep pace with today's supersystems for data collection, analysis and use that generate the kind of negative discrimination that demands data justice.

Privacy laws address bodily, spatial and especially informational and communicational privacy and to support the freedoms one expects in a democracy. They have achieved much but we are still left very vulnerable. A radical new direction is needed, prompted by our knowledge of the ways that data analytics, algorithms, Machine Learning and AI are reshaping our social environment. Not just the collection, but

the analysis and uses of the data have to be addressed, invoking new categories such as digital rights and data justice.

Surveillance challenges

Merely scratching the surface of C21st surveillance reveals how vastly things have changed. The landscape of surveillance has shifted tectonically from following suspects, watching workers and classifying consumers to monitoring and tracking everyone—now for public health—on an unprecedented scale. Privacy is undoubtedly a casualty but so also are basic freedoms of democracy, expectations of justice and hopes for social solidarity and public trust. These demand serious attention, not just from policy-makers and politicians, but from computer scientists, software engineers—in fact from everyone who uses a device.

The stakes are high, but the future is not foreclosed.

David Lyon, sociologist, Director of the Surveillance Studies Centre at Queens University, developed the concept of surveillance as "social sorting" and directs an international project on "Big Data Surveillance."

David is a Fellow of the RSC.

COVID-19: The Potential Abuses of Personal Data Surveillance

Benoît Dupont | June 24, 2020

If we are not careful, our right to privacy might well become one of the numerous collateral victims of the COVID-19 pandemic.

To reconquer our temporarily suspended freedom of movement and protect the public against a second wave of infection, we need put in place the basic elements of a dedicated public health monitoring infrastructure.

This infrastructure would include a series of personal data collection devices, such as smart phones, surveillance cameras, connected bracelets, robots and drones. Thanks to innovations made in recent years in the areas of cloud computing, telecommunication networks and artificial intelligence, mountains of data generated by those devices can now be stored for an indefinite period of time. This data can be analysed in real time by the powerful surveillance algorithms executed by tracking and facial recognition application

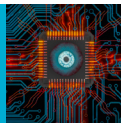
As a criminologist specializing in the study of digital transformation and adaptation of social control mechanisms, I have been studying for several years the new forms of surveillance used by governments and private companies, as well as the forms of resistance that can oppose them.

The temptation of techno-solutionism

The technologies that support this infrastructure are not new, and their implications extend beyond those of those concerning the defense of our right to privacy, as my colleague David Lyon has noted in these pages. Rather, their development has accelerated in recent years, under the pressure of surveillance capitalism, which seeks to translate every human experience into information that can create market value for the companies who own them and know how to generate profit from them.

In the current exceptional situation, where the pandemic has already caused over 350,000 deaths worldwide and where the richest countries' health systems have suffered numerous organizational failures, the use of surveillance as a means to manage this health crisis is quite attractive. Indeed, how can we not succumb to the luring sirens of digital tools that promise to automatize the detection of suspicious cases and to slow down — or even completely stop — the spread of the virus, which would allow us in turn to avoid a total collapse of the economy?

This temptation of "techno-solutionism", which relies on technical solutions to solve even the more complex social problems, carries significant risks. Is the collective fear generated by the ravages of the virus pushing us into an era of total surveillance from which it will be impossible to escape when the crisis is over and which will forever undermine our basic rights?



The ubiquity of health surveillance tools

While we wait for a vaccine to be developed, an increasing number of countries and companies are mobilizing a vast array of surveillance technologies designed to help track infected people and enforce social distancing rules. Such applications are drawing attention from privacy advocates, but they represent only the tip of the iceberg of health surveillance.

Asian countries, which have initially had the best results in containing the virus, have quickly relied on a massive access to the cellphone data of their whole populations: South Korea has put in place a data-sharing system involving 28 organizations, including the three main telecom operators and 22 credit card companies, that can follow the movements of an infected person and their contacts in less than 10 minutes.

People quarantined in Hong Kong are required to wear electronic bracelets connected to their smartphones, which ensures they do not leave their residence and which alerts the police as soon as a suspicious movement is detected. In Singapore, infected people must answer text messages several times a day, which reveals their geographical location.

In China, an application mandatory in over 200 cities and designed by an affiliate of the e-commerce company Alibaba, assigns a colour code (red, yellow or green) to the assumed contagion risk posed by each user based on data relative to their residential address, their life habits, their self-declared symptoms, etc. The data is routinely shared with the police. The speed at which such a technical solution was implemented is a direct result of the systematic citizen tracking and surveillance initiatives taken by the Chinese government as part of its social credit system.

As of mid-May, some 50 tracking applications were available in 30 countries. However, a quarter of those have not yet adopted privacy protection policies and 60% have not implemented specific anonymity protection measures.

In a more radical fashion, Israel mobilized the surveillance capabilities of its internal intelligence service, the Shin Bet, in order to identify those who have been in contact with infected patients. Using GPS data provided by mobile phone operators as part of its counter-terrorism apparatus, the Shin Bet has located approximately 4 000 people which have subsequently tested positive, inaugurating a hybrid form of surveillance combining national security with public health objectives.

A genuine technology arsenal

Companies that want to put their employees back to work and welcome back their clients are also contributing to this "care-veillance" escalation.

Start-ups specializing in artificial intelligence are proposing video-surveillance systems integrating social distancing detectors, which can automatically detect any situation where people come within less than two meters one from the other. Others integrate thermal sensors to their facial recognition technologies to measure continuously, and without physical contact, the body temperature of employees when they move about the premises of the company.

Public and private transportation operators are testing facial recognition devices to check whether their users and drivers are wearing their masks. Manufacturing companies are testing smart watches or badges that can alert users when they are violating social distancing rules and help build employee risk profiles.

Drones and robots finally complete this technology arsenal. Several Italian, Spanish, French and U.S. cities have deployed thermal sensor equipped drones that fly over public spaces to detect people with fever or who might violate confinement rules. Those devices can even interact with people through speakers.

Always up-to-date in the field of surveillance technology, Singapore is experimenting with the use of robot dogs equipped with cameras and speakers to enforce social distancing rules in public parks.

Regulating the creeping implementation of a total surveillance infrastructure

Taken separately, each of these surveillance technologies provides a concrete solution to a new and devastating health threat. Taken as a whole, however, they are tracing the contours of a future world where the ubiquity of benevolent surveillance will infiltrate even the most hidden depths of our behaviours and habits.

It is also likely that this care-veillance will contribute to perpetuate numerous forms of discrimination, with its use of risk profiles, the criteria of which will remain opaque. This will certainly accentuate the vulnerability of the most marginalized groups of our society.

Far from being a plot implemented by dark forces, the convergence of increasingly invasive surveillance technologies is rather a reflection of our insatiable thirst for security and our blind trust in the power of technology to reduce uncertainty.

But this scenario is not an inevitable fate and our assessment of the situation should not leave us paralysed and helpless, quite the contrary. In view of the real risk of seeing this surveillance infrastructure strengthen its hold well beyond this pandemic situation, it has become urgent to debate and get mobilized in order to establish transparent and stringent rules that would limit the risks it imposes on our individual liberties and our social cohesion.

Benoît Dupont, criminologist, holds a research chair in cybersecurity at the Université de Montréal and focuses on ways that the proliferation of surveillance technologies affects our society.

Benoît is a Member of the RSC College.

Canada's Out-of-Date Online Privacy Rules Aren't Protecting You

Anatoliy Gruzd | August 19, 2020

With so many of us stuck at home due to the pandemic, people have been spending a lot more time online in general and on social media in particular. This is not surprising, considering that 99 per cent of Canadian households have access to broadband internet and 94 per cent of online Canadian adults have an account on at least one social media platform, making Canada one of the most connected countries in the world.

However, as we increasingly rely on these platforms to connect us and mediate our relationships, we are also creating more data about our interests and habits. This treasure trove of data about us and the people in our network is being used by a wide variety of stakeholders, including social media platforms and many third parties.

Increasing discomfort

In this context, it is not surprising that social media users are becoming increasingly uncomfortable with how much data is being collected about them and how it is being used. For example, in our survey of 1,500 Canadians, 65 to 66 per cent of respondents said they are uncomfortable with marketers, government, financial institutions and political parties accessing information about them or posted by them on social media.

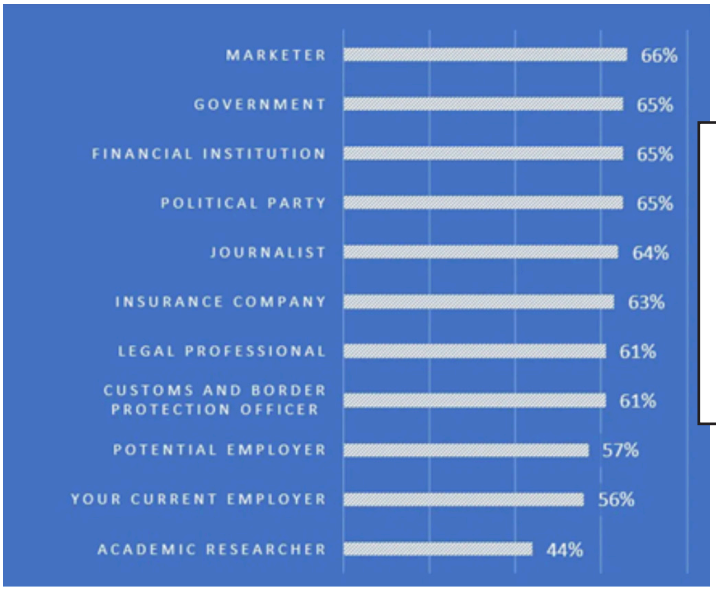


Figure 1. The percentage of 1,500 respondents who are uncomfortable with third parties accessing publicly available social media data posted by or about them.

(Ryerson University Social Media Lab's Social Media Privacy in Canada Report, 2018), Author provided

This lack of comfort is one of the signals telling us that Canadians' online data are not adequately protected under the current Personal Information Protection and Electronic Documents Act (PIPEDA).

PIPEDA is 20 years old, and bringing it in line with the principles set forth in Canada's new Digital Charter is one of the stated priorities for this government. However, the process has been delayed first by the federal election and now by the pandemic. The pandemic itself has also escalated the development and deployment of emerging data-greedy digital tools and techniques such as contact tracing and facial recognition, making a revamp of PIPEDA more critical than ever.

A new privacy and data protection regulation should also account for emerging technologies and their applications that will drive our digital economy in a near future.

Lessons from elsewhere

When the European Union enacted the General Data Protection Regulation (GDPR) in 2018, it found itself in conflict with a whole class of emerging technologies that are based on blockchains. Blockchain is the same technology used to create Bitcoin, but it is not limited to just cryptocurrencies. It also powers social media sites like Steemit, Minds and Memo, which give users more control over their personal data.

The decentralized nature of these blockchain-based sites makes it challenging to comply with GDPR, which assumes that there is a single data controller (either a person or legal entity) that collects personal data from individuals and is responsible for protecting such data. In peer-to-peer blockchain networks, the ledger that stores all data is distributed across multiple nodes and is not controlled by a single entity.

In effect, this constitutes "joint controllership," which is challenging to apply and interpret within the GDPR framework. The decentralized design also conflicts with GDPR's principle of data minimization, requiring data controllers to minimize the amount and types of data collected and stored about individuals.

Another design feature of blockchains to protect data from modification or deletion contradicts the "right to be forgotten" provision of GDPR, which assigns people the right to request deletion of their personal data "without undue delay."

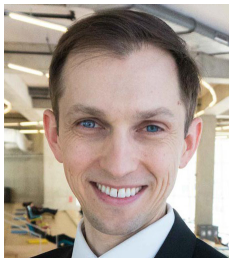
Future protections

Current regulations will need new guidelines that address decentralized, user-driven data collectives like blockchain-based social media sites. But even though these efforts are still underway in the EU, here in Canada there are a couple of lessons we can learn from this example.

First, it is crucial to make sure that updating PIPEDA does not only focus on today's technologies but also what is on the horizon. This is because emerging technologies such as blockchains are changing the power dynamics between data controllers and subjects by creating new ways for user data to be created, collected, accessed and shared.

The second lesson is that ensuring flexibility and accountability to allay Canadians' concerns about the ways that personal data is used will require creativity in working with all stakeholders, including users, governments, platform providers, data brokers, data-driven industries, app developers, researchers, civil society groups and others.

Doing so will allow Canada to foster the next wave of digital innovation while still protecting and empowering Canadians' data rights.



Anatoliy Gruzd, information technologist, holds a research chair in social media at Ryerson University and examines the impacts of networks on modern society.

Anatoliy is a Member of the RSC College.

AI Technologies—Like Police Facial Recognition—Discriminate Against People of Colour

Jane Bailey, Jacquelyn Burkell and Valerie Steeves | September 2, 2020

Detroit police wrongfully arrested Robert Julian-Borchak Williams in January 2020 for a shoplifting incident that had taken place two years earlier. Even though Williams had nothing to do with the incident, facial recognition technology used by Michigan State Police "matched" his face with a grainy image obtained from an in-store surveillance video showing another African American man taking US$3,800 worth of watches.

Two weeks later, the case was dismissed at the prosecution's request. However, relying on the faulty match, police had already handcuffed and arrested Williams in front of his family, forced him to provide a mug shot, fingerprints and a sample of his DNA, interrogated him and imprisoned him overnight.

Experts suggest that Williams is not alone, and that others have been subjected to similar injustices. The ongoing controversy about police use of Clearview AI certainly underscores the privacy risks posed by facial recognition technology. But it's important to realize that not all of us bear those risks equally.

Training racist algorithms

Facial recognition technology that is trained on and tuned to Caucasian faces systematically misidentifies and mislabels racialized individuals: numerous studies report that facial recognition technology is "flawed and biased, with significantly higher error rates when used against people of colour" (Burton-Harris and Mayor, June 2020).

This undermines the individuality and humanity of racialized persons who are more likely to be misidentified as criminal. The technology — and the identification errors it makes — reflects and further entrenches long-standing social divisions that are deeply entangled with racism, sexism, homophobia, settler-colonialism and other intersecting oppressions.

How technology categorizes users

In his game-changing 1993 book, The Panoptic Sort, scholar Oscar Gandy warned that "complex technology [that] involves the collection, processing and sharing of information about individuals and groups that is generated through their daily lives … is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy." Law enforcement uses it to pluck suspects from the general public, and private organizations use it to determine whether we have access to things like banking and employment.

Gandy prophetically warned that, if left unchecked, this form of "cybernetic triage" would exponentially disadvantage members of equality-seeking communities — for example, groups that are racialized or socio-economically disadvantaged — both in terms of what would be allocated to them and how they might come to understand themselves.

Some 25 years later, we're now living with the panoptic sort on steroids. And examples of its negative effects on equality-seeking communities abound, such as the false identification of Williams.

Pre-existing bias

This sorting using algorithms infiltrates the most fundamental aspects of everyday life, occasioning both direct and structural violence in its wake.

The direct violence experienced by Williams is immediately evident in the events surrounding his arrest and detention, and the individual harms he experienced are obvious and can be traced to the actions of police who chose to rely on the technology's "match" to make an arrest. More insidious is the structural violence perpetrated through facial recognition technology and other digital technologies that rate, match, categorize and sort individuals in ways that magnify pre-existing discriminatory patterns.

Structural violence harms are less obvious and less direct, and cause injury to equality-seeking groups through systematic denial to power, resources and opportunity. Simultaneously, it increases direct risk and harm to individual members of those groups.

Predictive policing uses algorithmic processing of historical data to predict when and where new crimes are likely to occur, assigns police resources accordingly and embeds enhanced police surveillance into communities, usually in lower-income and racialized neighbourhoods. This increases the chances that any criminal activity — including less serious criminal activity that might otherwise prompt no police response — will be detected and punished, ultimately limiting the life chances of the people who live within that environment.

And the evidence of inequities in other sectors continues to mount. Hundreds of students in the United Kingdom protested on Aug. 16 against the disastrous results of Ofqual, a flawed algorithm the U.K. government used to determine which students would qualify for university. In 2019, Facebook's microtargeting ad service helped dozens of public and private sector employers exclude people from receiving job ads on the basis of age and gender. Research conducted by ProPublica has documented race-based price discrimination for online products. And search engines regularly produce racist and sexist results.

These outcomes matter because they perpetuate and deepen pre-existing inequalities based on characteristics like race, gender and age. They also matter because they deeply affect how we come to know ourselves and the world around us, sometimes by pre-selecting the information we receive in ways that reinforce stereotypical perceptions. Even technology companies themselves acknowledge the urgency of stopping algorithms from perpetuating discrimination.

To date the success of ad hoc investigations, conducted by the tech companies themselves, has been inconsistent. Occasionally, corporations involved in producing discriminatory systems withdraw them from the market, such as when Clearview AI announced it would no longer offer facial recognition technology in Canada. But often such decisions result from regulatory scrutiny or public outcry only after members of equality-seeking communities have already been harmed.

It's time to give our regulatory institutions the tools they need to address the problem. Simple privacy protections that hinge on obtaining individual consent to enable data to be captured and repurposed by companies cannot be separated from the discriminatory outcomes of that use. This is especially true in an era when most of us (including technology companies themselves) cannot fully understand what algorithms do or why they produce specific results.

Privacy is a human right

Part of the solution entails breaking down the current regulatory silos that treat privacy and human rights as separate issues. Relying on a consent-based data protection model flies in the face of the basic principle that privacy and equality are both human rights that cannot be contracted away.

Even Canada's Digital Charter — the federal government's latest attempt to respond to the shortcomings of the current state of the digital environment — maintains these conceptual distinctions. It treats hate and extremism, control and consent, and strong democracy as separate categories.

To address algorithmic discrimination, we must recognize and frame both privacy and equality as human rights. And we must create an infrastructure that is equally attentive to and expert in both. Without such efforts, the glossy sheen of math and science will continue to camouflage AI's discriminatory biases, and travesties such as that inflicted on Williams can be expected to multiply.

Jane Bailey, a law professor at the University of Ottawa, co-leads The eQuality Project and researches the impact of evolving technology on equality, privacy, and rights, especially for members of equality-seeking communities.

Jane is a Member of the RSC College.

Jacquelyn Burkell, a faculty member in Information and Media Studies at Western University, studies the social impact of technology, with a focus on privacy, access to information, and technology in the justice context.

Valerie Steeves is a Full Professor in the Department of Criminology at the University of Ottawa, co-leads the The eQuality Project and researches young people's experiences of privacy and equality in networked spaces.

The Royal Society of Canada
282 Somerset Street West
Ottawa, Ontario K2P 0J6
www.rsc-src.ca
613-991-6990

La Société royale du Canada
282, rue Somerset ouest
Ottawa (Ontario) K2P 0J6
www.rsc-src.ca
613-991-6990