Advancing a Cybersecure Canada

Introducing the Cybersecure Policy Exchange

July 2020

Charles Finlay | Karim Bardeesy | Yvonne Su

cybersecure policy exchange

Powered by RBC

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is a new initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation.

Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Ryerson University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.

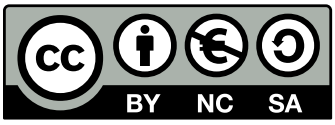
Ryerson Leadership Lab

The Ryerson Leadership Lab is an action-oriented think tank at Ryerson University that develops leaders and solutions to make progress on our most pressing civic challenges. Through research and policy activation, leadership development, and civic convening, the Leadership Lab is building a new generation of skilled and adaptive leaders, at all ages and stages, to build a more trustworthy, inclusive society.

This initiative is made possible by the generous contributions of **Royal Bank of Canada**, which enable our team to independently investigate pressing public policy issues related to cybersecurity and digital privacy. We are committed to publishing objective findings and ensuring transparency by declaring the sponsors of our work.

How to Cite this Report
Finlay, C., Bardeesy, K. & Su, Y. (2020, July 9).
Advancing a Cybersecure Canada: Introducing the Cybersecure Policy Exchange.
Retrieved from: https://www.cybersecurepolicy.ca/agenda

350 Victoria St, Toronto, ON M5B 2K3



Contributors
Sam Andrey, Director of Policy & Research, Ryerson Leadership Lab
Karim Bardeesy, Executive Director, Ryerson Leadership Lab
Sumit Bhatia, Director of Communications and Knowledge Mobilization, Rogers Cybersecure Catalyst
Zaynab Choudhry, Design Lead
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Braelyn Guppy, Marketing and Communications Lead, Ryerson Leadership Lab
Mohammed (Joe) Masoodi, Policy Analyst, Ryerson Leadership Lab
Jon Medow, Principal, Medow Consulting Inc.
Kate Pundyk, Policy and Research Assistant, Ryerson Leadership Lab
Oliver Sheldrick, Senior Research Associate, Medow Consulting Inc.
Yvonne Su, Policy Lead, Ryerson Leadership Lab

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange
For more information, visit: https://www.cybersecurepolicy.ca/

Executive Summary

Canadians are facing unprecedented attacks on their digital security and privacy, and new threats continue to emerge. Our new research finds that a **majority (57%) of Canadians report being the victim of a cybercrime.**

As the technological landscape is rapidly changing, there is an urgent need to address the security and privacy risks and vulnerabilities facing Canadians online. To do so, our governments, our public and private institutions, and all Canadians, must demonstrate leadership, to ensure that we create and implement balanced public policy that will drive innovation while responsibly protecting Canadians.

That's why we launched the **Cybersecure Policy Exchange (CPX).** The goal of CPX is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation.

We are launching our CPX agenda with this report, which includes the results of a representative survey of 2,000 Canadians conducted in mid-May 2020. The survey sought to understand Canadians' experiences, choices and priorities toward their cybersecurity and digital privacy. In this report, we share some of our findings on three high-impact technologies that will be the immediate focus of the CPX agenda:

Social Media Platforms: What policy changes are needed to ensure that social media platforms uphold the privacy and security standards that Canadian citizens and businesses expect?

- Just **15% of Canadians trust Facebook** to keep their data secure.

Internet of Things (IoT): How should government and industry share responsibility to ensure the safety and security of all Canadians and Canadian businesses using physical devices connected to the Internet?

- **68% of Canadians have at least one smart device** in their home.

Biometrics: How can policy change protect the privacy and security of Canadians in the deployment of biometric technologies, like facial recognition?

- **41% of Canadians are uncomfortable with being captured by camera-enabled doorbells** like Amazon's Ring, with 15% supporting a ban on these products.

Cybersecurity and digital privacy are not just technical matters that should only concern experts. They must be matters of vital importance to all Canadians. We look forward to advancing a cybersecure Canada together.

Intent of this Report

Cybersecurity and digital privacy are some of the most pressing challenges facing our modern world.

In this report, we lay out our immediate areas of focus for the new Cybersecure Policy Exchange (CPX); explain what these technologies are; share our most up-to-date understanding of the challenges that each presents to Canadians; and share new research on Canadians' use of, and attitudes toward, these technologies.

This report marks the launch of our plans to actively support and convene public engagement and policy development through research and close engagement with government, academia, industry and civic institutions on each of these urgent challenges.

Introduction

Canadians are experiencing unprecedented challenges facing their digital security and privacy, and new threats continue to emerge.

As we increasingly live our lives online, cybersecurity and digital privacy — ensuring the confidentiality and integrity of our information and information systems — have emerged as key challenges of our time.

From cybercriminals, to insider threats to nation-states, the volume and sophistication of actors attempting to exploit vulnerabilities to gain or disrupt access to our digital systems is growing. Our increasing reliance on networked technologies is accelerating this trend. More social media platforms, smart devices and biometric technologies are emerging. The COVID-19 pandemic has moved so much of daily life online, from birthday parties to the monitoring of key systems.

These challenges impact the most intimate details of our personal, financial and work lives that are captured online, including our ideas, our photos and our identities. They also influence our democracy and our most complex systems — infrastructure, health care and education — and how governments, citizens and businesses engage with each other. More access points, increased connectivity, and therefore more opportunities for threats to target weak spots.

Cybersecurity impacts the everyday lives of Canadians — in fact, **a majority (57%) of Canadians report having been the victim of a cybercrime.** This is a significant increase from 2017 when 36% of Canadians reported being the target of a cybercrime attempt.[1] Moreover, internet users around the world are reporting greater levels of concern about their online privacy than they were a year ago.[2]

Canadians' Self-Reported Cybercrime Experiences

As we have witnessed with the COVID-19 pandemic, shocks to our public health and economy, and the resulting policy changes, also have profound implications for our digital security and privacy — whether it be the security of the video conferencing services we now rely on, or the privacy implications of technologies aimed at tracking the spread of the virus.

Cybersecurity and digital privacy are matters of vital importance to all Canadians, as their impacts are felt at individual and collective levels.

Together, we can create and implement balanced public policy in cybersecurity and digital privacy that will drive innovation while protecting Canadian society.

That's why we launched the Cybersecure Policy Exchange.

Areas of Focus

The Cybersecure Policy Exchange will:

- **Engage** Canadians through webinars, public workshops, roundtables and other events; and
- Actively support **policy development** through research and close engagement with government, academia, industry and civic institutions.

In this paper, we highlight three high-impact technologies that need specific attention from policy-makers, industry, public sector institutions, civil society and the public. Each has its own set of features that attract attention from those who threaten the security and privacy of Canadians online.

In our work throughout the coming year, we will put forward public policy research, approaches and recommendations that relate to these three technologies:

1. **Social Media Platforms:** Online platforms that enable users to connect and share user-generated content.

2. **The Internet of Things:** Physical networked devices connected to the Internet, from consumer electronics to larger industrial and infrastructure applications.

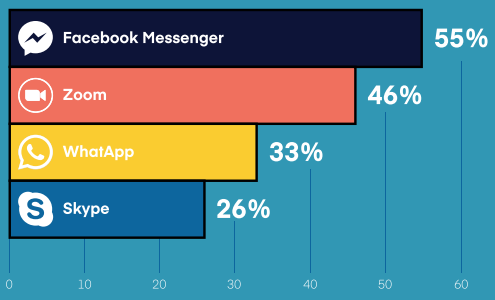
3. **Biometrics:** Technologies that measure and analyze a person's physical or behavioural attributes to recognize or confirm identities, such as facial recognition.

Canadians More Connected Than Ever During COVID-19

Amidst physical distancing, Canadians are using online technologies in record numbers — from banking, to video calls, to doctor's appointments.[3,4] When asked which activities they have done online during the first two months of physical distancing, Canadians said:

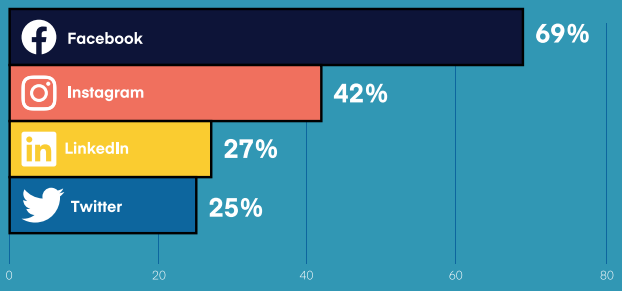
87% Online Banking

79% Online Messaging or Video Calls



77% Online Shopping

76% Social Media



74% Online News

19% Online Health Care

Considerable attention has been paid to the merits of "technology-specific" or "technology-neutral" approaches to public policy governance and regulation.[5] Most notable privacy laws, including Canada's, aim to be technology-neutral and principles-based, a feature that some highlight as a strength to maintain relevance through waves of technological change.[6] But many of these laws, which were drafted in the 1990s and early 2000s, are now often insufficient in the face of new technologies to guard the public interest.[7]

There are good reasons to start with some commonly-used and high-impact technologies when it comes to public policy related to cybersecurity and digital security. Each of the three areas we have chosen focuses on a different set of relationships and therefore a different set of public policy challenges and potential solutions.

For social media, it is the relationships among people – and sometimes institutions – that are mediated by the technology.

Security and Data Governance in Canada

Data are the currency that underpin the technologies discussed in this paper. Whether it is the social media links you click on, the voice commands on your smart devices, or the scan of your fingerprints at the airport, data about us are collected, processed and shared at almost every minute of the day. Because of this, all of CPX's work will have to consider questions about the security and privacy of the data governance regulations that facilitate responsible adoption of new technologies. These include, but are not limited to: retention, minimization, security, storage, purpose, limitation and accountability.[8]

Data governance in Canada is currently outlined in two key federal pieces of legislation: the *Personal Information Protection and Electronic Documents Act* (*PIPEDA,* 2007) for commercial activity and the *Privacy Act* (1983) for federal government agencies. Each governs how organizations collect, use and disclose personal information, providing individuals the rights to access and correct their personal information, to ensure it remains secure and only used for the reasons for which they provide informed consent. The Office of the Privacy Commissioner of Canada (OPC) is responsible for investigating complaints that infringe either Act, though does not have direct enforcement tools; the OPC is able to provide recommendations or apply to the Federal Court to seek compliance orders.

Equally important legislation exists in each province and territory, governing provincial agencies, municipalities, personal health information and some elements of the private sector.[9] Digital technologies can also be regulated under consumer protection legislation, such as if they pose unreasonable hazards to human health and safety.

Given the rapid development of new technologies and their subsequent increased privacy risks in the 21st century, the federal government began a consultation in 2018 to amend Canada's legislation to bring it inline with global best practices.[10, 11] Canada also released its Digital Charter in 2019, presenting 10 principles to "help guide the federal government's work to help address challenges and leverage Canada's unique talents and strengths in order to harness the power of digital and data transformation."[12] The principles included:

- **Safety and Security:** Canadians will be able to rely on the integrity, authenticity and security of the services they use and should feel safe online.
- **Control and Consent:** Canadians will have control over what data they are sharing, who is using their personal data and for what purposes, and know that their privacy is protected.
- **Strong Democracy:** The Government of Canada will defend freedom of expression and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institutions.

The Internet of Things governs the relationship between and among devices, with a wide range of end users. Biometrics are primarily used to facilitate relationships between people and their institutions and devices, often for reasons of identification and authentication.

We will seek to advance public policy solutions to the privacy and security challenges of each of these technologies, while also understanding and explaining their common elements of public policy — where we discover them, in the ways they relate to other horizontal technologies such as machine learning and AI,[13] and where they are already known to exist (for example, in relation to any proposed amendments to Canadian privacy legislation). Moreover, we will work to help Canadians understand their rights and responsibilities as they relate to these technologies, based on a value system with a single, clarion call — **the responsible governance of technology to protect Canadians' security and privacy.**

We will also seek to better understand and propose solutions for the privacy and security implications of these technologies across the variety of circumstances facing differently-situated Canadians. One example is the unequal access to digital services across lines of income, race, geography and age.[14] The digital divide is an example of the deep challenges experienced by many Canadians, exacerbated by the current COVID-19 pandemic; short-cuts to reduce the impact of this divide, like the provision of less expensive and less secure devices or the use of free software applications, can put the security and privacy of some Canadians at greater risk.[15]

Our work will be guided by these core principles:

- Responsible technology governance is a key to Canadians' cybersecurity and digital privacy.
- Complex technology challenges call for original insights and innovative policy solutions.
- Canadians' opinions matter, and must inform every discussion of technology policy.
- Cybersecurity needs to explained and made relevant to Canadians, and cannot be relegated to language and concepts accessible only to experts.
- Canadian institutions matter, and must evolve to meet new cybersecurity and digital privacy risks to maintain the public trust.
- Harms, inequities and injustices arising from the unequal use or application of technology must be confronted, wherever they exist or could arise.

"Regulating technology companies in the name of protecting individuals' privacy and security will mean that we slow down innovation and hurt our economy."

52% Canadians disagree

17% Canadians agree

Key Concepts

Cybersecurity is the preservation — through policy, technology, and education — of the availability, confidentiality and integrity of information and its underlying infrastructure.[16]

Digital privacy is being free from unauthorized access, surveillance or interference to your information that is collected or processed by technology.

Digital **privacy** and **security** are distinct but interrelated concepts. They perhaps can best be understood through a metaphor: if you picture your online presence as a home, your privacy would be the curtains on your windows, and security is represented by the locks on your doors. Open curtains can tempt onlookers to try and enter. Locks can help prevent them from doing so. Neither closed curtains nor locked doors prevent entry alone, but they support one another to keep a home safe.

Standards are established rules or technical requirements for technology, distinct from laws and regulations, that can support interoperability, compatibility and safety.

Platform, action and **network** are three factors that combine to determine cybersecurity and digital privacy implications of online activity.

- **Platform** refers to where an action is taking place. This includes different websites or apps, as well as the underlying operating systems of devices, for example iOS or Android.
- **Action** means what you are doing, for example: sending a message, posting a photo, sending money or entering a password.
- **Network** refers to how the device is connected to the internet, for example public Wi-Fi, private Wi-Fi or a cellular data plan.

Every online activity combines platform, action and network; and each unique combination of these factors carries distinct cybersecurity and digital privacy implications.

Social Media Platforms

Social media platforms have opened up new ways for us to connect, share and learn, but they have also introduced new cybersecurity and digital privacy challenges.

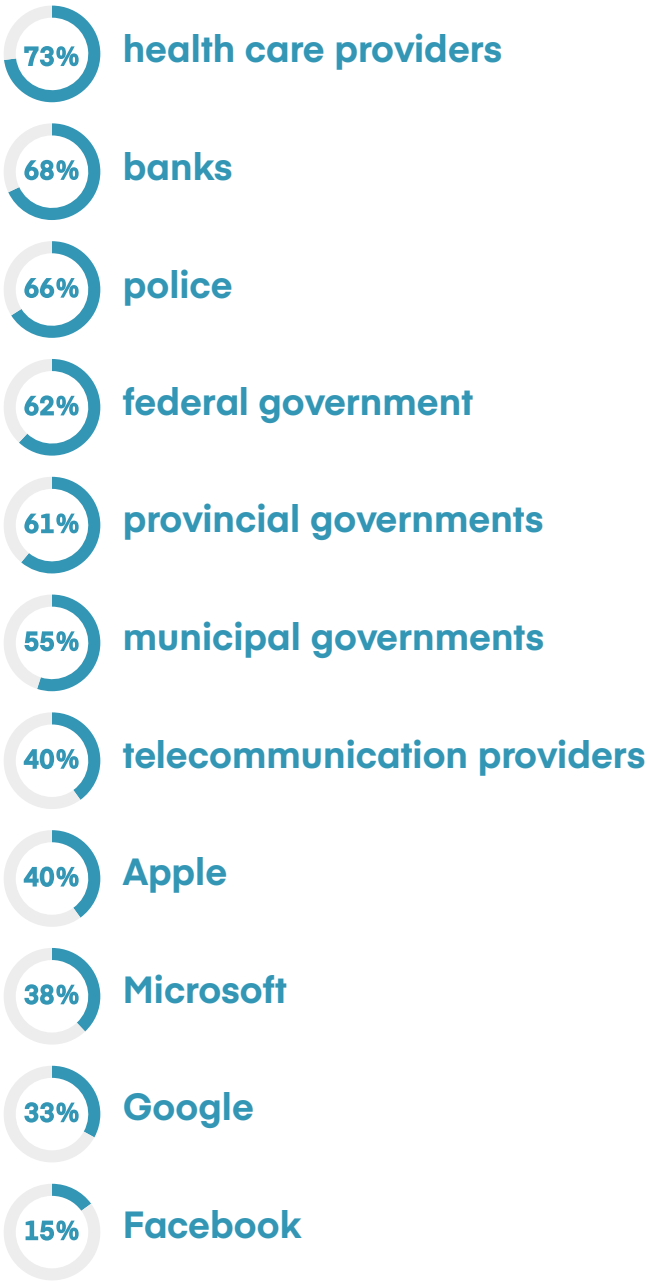
Perhaps most famously, the Cambridge Analytica scandal highlighted how the data sharing and collection techniques of social media platforms can lead to deeply troubling outcomes. While Cambridge Analytica was not a "hack" in the conventional sense, it was a failure of data governance that led to the unauthorized release of 50 million people's personal information provided to Facebook.[17]

Amidst this and other scandals, trust in many of the largest social media platforms has been eroding in recent years.[18] Our survey reveals that trust in major institutions, such as governments, banks and health care providers, to keep Canadians' personal data secure is relatively strong, while Facebook had the trust of less than one in six Canadians.

Cybercriminals are increasingly focusing their resources on social media platforms, as these data-rich environments represent a significant "bang for the buck" in terms of time and resources. Reported crimes involving social media have more than quadrupled in the last five years in both the U.S. and UK,[19] and a 2019 report found that over half of all social media log-in traffic was illegitimate.[20]

There are numerous forms of criminal behaviour conducted through these platforms, ranging from fraud, identity theft, exploitation, harassment, hate speech, gender-based violence, election interference, and incitement to violence and terrorism.

Canadians' Trust to Keep Personal Data Secure



The need for better policy to ensure the security and privacy of social media users has been one of the most prominent discussions in technology policy over the last few years.[21] For example, there has been a long and heated debate in several countries, including

in Canada,[22] over the encryption of private messages on social media platforms. U.S. authorities are seeking legislation to require companies such as Apple, Google and Facebook to use encryption standards that allow access to private messages for law enforcement.[23] The debate between federal authorities and Silicon Valley continued recently, when President Trump signed an executive order in May 2020 calling for limits to the current legal liability protections that social media companies have for the content that they host.[24]

In a 2019 white paper, the Canadian government raised questions about how privacy regulation should better incorporate concerns about social media platforms, such as requirements for the de-indexing of information (similar to the EU's Right to be Forgotten), but relatively little movement toward a clear policy or legislative approach has taken shape to date.[25] The issues are complicated by the presence of firms with global operations and a lack of international governance regimes for the platforms.[26]

What We Plan to Answer: What policy changes are needed to ensure that social media platforms uphold the privacy and security standards that Canadian citizens and businesses expect?

Zoom-Bombing: The new threat during COVID-19

The rapid move to online learning and remote work have contributed to a surge in video conferencing, in particular through the platform Zoom.[27] And with it has come a new phenomenon known as "Zoom-bombing" where video conferences are interrupted by uninvited guests or hackers who yell profanities or display inappropriate or offensive images.[28]

Zoom-bombing became such a widespread issue that the FBI deemed the act a form of cybercrime that should be reported to law enforcement agencies. A study by Ryerson University's Infoscape Research Lab found that a significant percentage of Zoom-bombings contain racist, misogynistic, homophobic and other objectionable content — often directed toward female teachers using the platform.[29]

And it's not just Zoom. Other video conferencing platforms are also vulnerable to attacks, including Google Classroom and Skype.[30, 31] In the U.S., the FBI is warning that public schools relying on remote learning during the pandemic should expect a surge in cyberattacks, due to increased reliance on technology and limited resources to protect sensitive student data.[32] The rapid adoption of video conferencing during the pandemic has had companies and institutions scrambling to make their systems more secure. In any online environment that scales up quickly, fixes do not always keep pace with the new threats.

Internet of Things

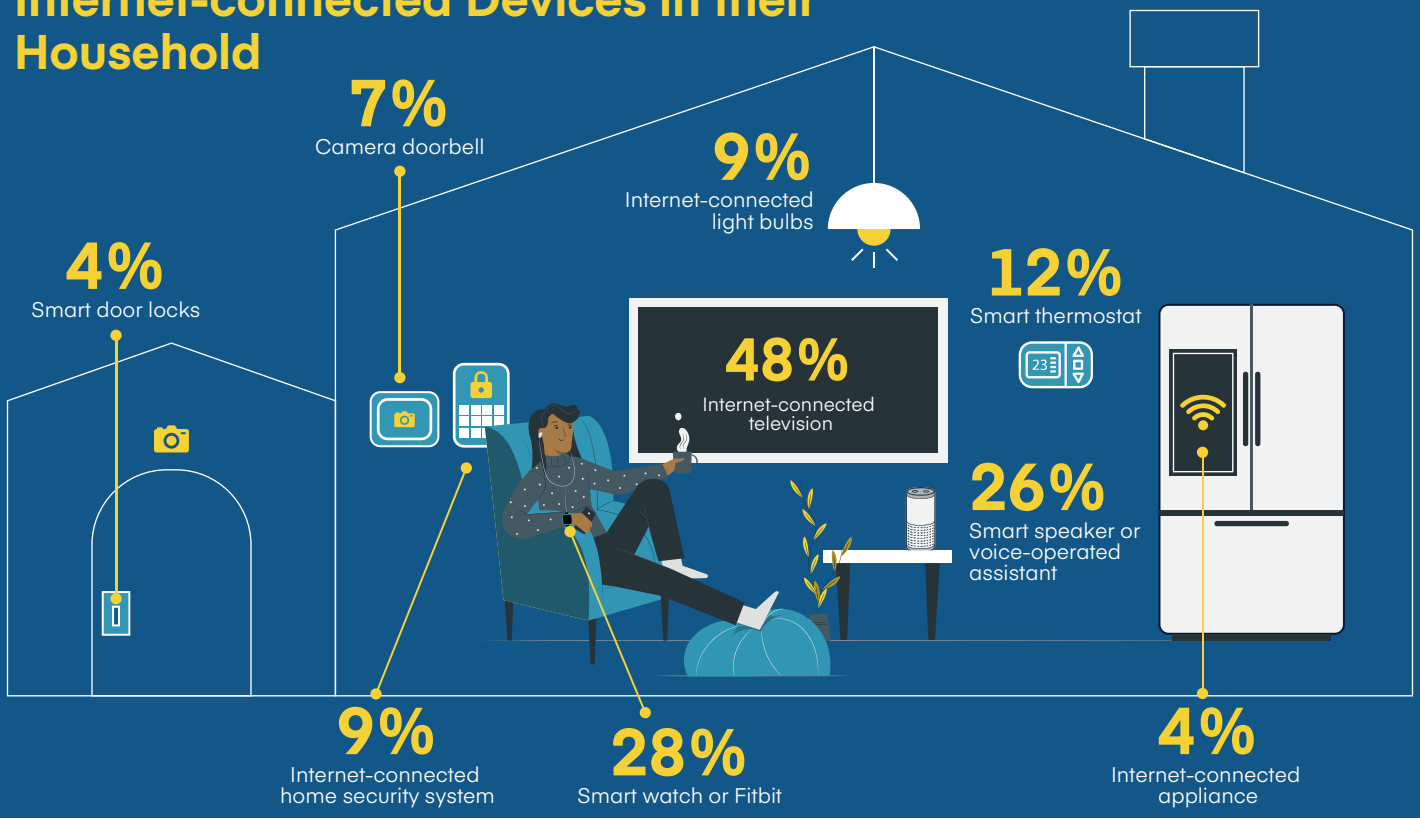
The proliferation of the Internet of Things (IoT) is increasingly blurring the line between threats in the online and offline worlds. As more connected devices enter our homes, neighbourhoods — and even our bodies — cybersecurity risks take on even greater importance.

With multiple IoT devices often centrally connected through our mobile phones, consumers and businesses may unknowingly increase vulnerabilities to their entire network. Between 2015 and 2018, the number of IoT devices more than doubled globally from 3.8 billion to 8.3 billion, and is forecast to reach 21.3 billion by 2025.[33]

Canada is not exempt from this trend. Our survey found that **68% of Canadians have at least one IoT device in their home**, 38% have at least two devices and 20% have three or more. Nearly half of Canadians have an internet-connected television and 26% have a smart speaker or voice-operated assistant. This is also an area where the digital divide comes into stark relief — 51% of Canadian households with incomes under $50,000 have at least one IoT device, compared to 82% for those with incomes of $100,000 or more (see Table 6).

We can loosely categorize IoT-related cybersecurity into the macro and the micro. The macro category captures the risks and

Proportion of Canadians with these Internet-connected Devices in their Household



Cyber Vulnerabilities for Racialized Communities

In the study of CPX's three areas of focus, each area presents unique challenges for racialized Canadians, particularly Black and Indigenous communities. This is an under-researched area in Canada that we hope to collaborate with others to address; Ruha Benjamin at Princeton University describes this phenomenon as "'the New Jim Code': the employment of new technologies that reflect and reproduce existing inequities but that are promoted and perceived as more objective or progressive than the discriminatory systems of a previous era."[34]

Social media algorithms can reinforce existing biases such that they fuel extremist sentiments, particularly against racialized or religious communities. The resulting information silos can then be infiltrated by nefarious actors, as illustrated through the Russian information operations targeting the Black Lives Matter movement in 2016.[35] However, extremist sentiments that are fueled online can also translate into hate crimes in the physical world, as evidenced by violent attacks such as the Québec City mosque shooting in 2017.[36]

This paper highlights the **Internet of Things** technology, the Amazon Ring doorbell, that can be used to flag suspicious activity on neighbourhood doorsteps. This pairing of IoT with cameras that collect biometric data enables devices to profile people based on an algorithmic threat assessment. A review of Ring's technology and the Neighbors app found that its algorithm most often flagged people of colour as being suspicious.[37]

Biometrics are particularly prone to bias. A U.S. study reviewed 189 facial recognition algorithms from 99 developers and found that almost all were more likely to inaccurately flag (present a "false positive" for a negative characteristic) non-white faces.[38] Inaccurate flags from biased algorithms can affect everything from finding a job or renting an apartment, to accessing financial services such as insurance.

vulnerabilities of large-scale infrastructure systems that are networked and utilize sensor inputs for their operations. This includes the management of sensor data from complex devices in areas such as health care, energy systems and so-called "smart city" technologies that include traffic measurement, waste and water management, and streetlights.[39]

A recent and dramatic example of the risk facing these systems was the WannaCry ransomware cyberattack that affected the UK's National Health Service (NHS) in 2017.

The attack shut down thousands of computers with demands for ransom payments, but also attacked IoT medical devices such as devices used for MRIs. The Department of Health estimated the attack cost the NHS £92M and led to the cancellation of 19,000 medical appointments.[40]

Ransomware and phishing schemes are just the most observable threats. Institutions in Canada, especially provincial and municipal orders of government and public sector organizations that run crucial systems that Canadians rely on, have systems that are highly exposed.[41]

The micro category represents the more direct networked interactions consumers make with purchased or installed devices; this covers smart home technologies, such as digital locks, virtual assistant speakers, fitness trackers and connected toys.

The diverse and widespread nature of IoT devices creates entirely new categories of cybersecurity risks that can have more direct physical impacts than ever before.[42] In our survey, **just 26% of those with a voice-operated assistant said they have restricted the information it can access through its settings.** With the pace and low cost of producing these devices, there can also be little incentive for manufacturers to update their security firmware for these products.

Another crucial issue with smart homes is that, when more devices are added to a network, it becomes more likely that a device with a security flaw may be exploited as an entry point to access all the connected devices within our homes. While laptops or mobile phones may be relatively more secure, the same security standards may not be present in smart light bulbs (which can cost as little as $10). For example, in 2017, hackers accessed the entire database of a casino through an unsecure IoT fish tank thermostat that was connected to their network.[43]

With networking capabilities being built into everything from glucose sensors embedded in the skin of a diabetes patient, through to voice-powered microwaves and critical national energy infrastructure, IoT devices are becoming key battlegrounds for the future of our cybersecurity and have received insufficient policy attention.[44, 45, 46] The federal government released The Internet of Things Toolkit for Small and Medium Businesses in 2017, but proactive policy and regulation for manufacturers and institutions producing and managing IoT devices have not been forthcoming.

What We Plan to Answer: How should government and industry share responsibility to ensure the safety and security of all Canadians and Canadian businesses using IoT devices?

Biometrics

Few emerging areas of technology have proven more controversial than biometrics, which includes a range of devices, techniques and systems that allow machines to recognize individuals or confirm their identities. These technologies are able to measure and analyze, for example, facial features, fingerprints, iris scans, gait, voice-prints and DNA. Some of the key concerns with these new technologies are that, unlike passwords or identification numbers that can be changed, biometrics data in the wrong hands can mean that people will never be anonymous again[47] or worse, stolen biometric identities can be easily misused.[48]

In recent years, facial recognition technologies have been controversially deployed in quasi-public venues, including Madison Square Gardens and Walmart.[49] In this example, "semi-camouflaged cameras can determine not only your age and gender but your mood, cueing up tailored advertisements within seconds".[50] Cadillac Fairview has done the same in shopping malls in Canada,[51] only halting its practices after a 2018 Office of the Privacy Commissioner investigation was launched.[52]

Most recently, Canadians have learned that police forces and private businesses have been using Clearview AI's facial recognition technology to identify suspects and persons of interest without warrants, crossmatching photos on a database that scrapes images from social media platforms, such as Facebook, Twitter and Instagram without users' consent.[53] Adding to the concern are reports that Clearview AI has already experienced a data breach.[54]

After privacy commissioners across Canada launched investigations into whether or not the company is complying with Canadian privacy law, the company announced it is exiting the Canadian market.[55]

Facial recognition technology is not only the reserve of large corporations and institutions. With products such as the Amazon Ring video doorbell, individuals are now recording each other in greater numbers. These doorbells already allow users in the U.S. to upload videos of activity they deem to be suspicious to a publicly-accessible "Neighbors" app, which is accessed by over 1,000 police forces through a partnership launched in 2018.[56] Amazon has confirmed that it intends to integrate facial recognition technologies into Ring, allowing for automatic notification to homeowners of "suspicious" activity which users could then upload to police.[57]

Canadians appear to be divided on the use of camera-enabled doorbells, with 49% believing that it is an individual's rights to own and operate these cameras, and a total of 41% of Canadians uncomfortable with being captured on them. But overall, only 15% of Canadians are supportive of an outright ban on products that can capture private video of people without their consent.

Canadian opinions on camera-enabled doorbells

49% believe that it is an individual's rights to own these

26% are uncomfortable with being captured on them

15% are supportive of an outright ban on products that can capture private video of people without their consent

Biometrics During a Pandemic — Is Workplace Surveillance the New Norm?

Amidst COVID-19, biometric technology is being used by employers to monitor their employees at home. Canadian laws do not prohibit remote monitoring of employees so long as they are informed.[58] With many people working from home, a suite of companies is providing software tools to help employers manage the productivity of their employees, including monitoring biometrics such as facial expressions and body language, alongside other data, including keystrokes, mouse activity and GPS location.[59]

The risks and harms associated with these technologies are significant, with the consequences of misidentification potentially dire for individuals, for instance in a law enforcement context. This is compounded by the fact that some facial recognition models have been demonstrated to be less accurate in the identification of individuals with darker skin, adding to existing issues around bias in policing and their use of technologies to disproportionately surveil vulnerable members of society, including the marginalized, communities of colour and the poor.[60, 61]

In the face of mounting concerns, there have been calls for a moratorium on facial recognition technology until greater regulatory controls are in place — from groups ranging from the Digital Justice Lab to the Toronto Region Board of Trade.[62, 63]

Biometrics During a Pandemic — Facial Recognition to Track COVID-19

One example of how COVID-19 is posing challenges to cybersecurity, privacy and inequality is the issue of contact tracing apps. In our new report, *The Race to Trace: Security and Privacy of COVID-19 Contact Tracing Apps*, we make five critical recommendations to evaluate new contact tracing apps.

A more controversial use of biometrics that has proliferated during COVID-19 is the use of facial recognition technologies to enforce public health rules. China, India, Poland and Russia have all used facial recognition technologies to assist them with enforcing rules during the pandemic, such as self-isolation and mask-wearing.[64, 65] Despite facial recognition's struggle with identifying people with masked faces, China has been able to develop technology linked to temperature sensors that identifies individuals with a 95% accuracy rate even when wearing masks.[66] In Central Asia, there are concerns that the increased reorientation of surveillance systems in their smart cities toward facial recognition to fight the pandemic will heighten privacy and human rights concerns.[67]

Amidst recent protests against police brutality and anti-Black racism initiated by the death of George Floyd in Minnesota, technology giants such as Amazon, IBM and Microsoft have each announced that they will not be selling their facial recognition technology to police forces until greater protections are in place.[68, 69, 70]

This decision to pause some sales of facial recognition technology could be seen as an important opportunity for policy discussions on what measures are needed to ensure that the development of these technologies is ethical and responsible. The need to appropriately engage in policy-making regarding the unique risks and vulnerabilities of biometric technology is imperative for the responsible governance of this technology.

This is an area of quickly emerging and soon-to-be-ubiquitous technologies — technologies backed by substantial investments, and powered by large data sets and machine learning. There is an urgent need to create all-encompassing regulatory regimes, fit for the purpose of protecting the security and privacy of Canadians.

What We Plan to Answer: How can policy change protect the privacy and security of Canadians in the deployment of biometric technologies?

Conclusion

With the proliferation of smart devices, our extensive reliance on social media for communication, and the threats that facial recognition pose to our society and democracy, it is clear that the responsible governance of technology to protect Canadians' security and privacy online is becoming even more complex and important.

Together, we can create and implement balanced public policy in cybersecurity and digital privacy that will drive innovation while protecting Canadian society.

As we investigate these key issues in 2020 and beyond, we want you to join us, both in learning more and in thinking about what policy solutions could look like. We have much more engagement and policy development to come. Specifically, we plan to collectively address some of the major questions facing Canadians using three high-impact technologies:

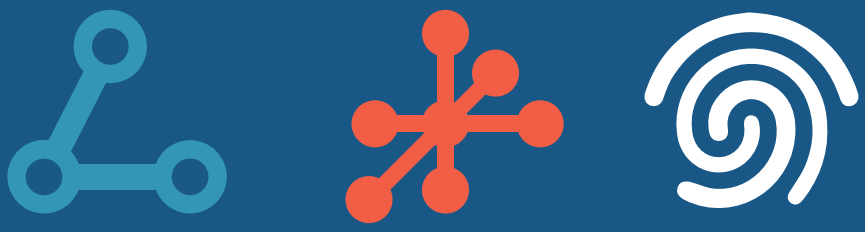
Social Media Platforms: What policy changes are needed to ensure that social media platforms uphold the privacy and security standards that Canadian citizens and businesses expect?

The Internet of Things: How should government and industry share responsibility to ensure the safety and security of all Canadians and Canadian businesses using IoT devices?

Biometrics: How can policy change protect the privacy and security of Canadians in the deployment of biometric technologies?

We will actively support and convene public engagement and policy development through research and close engagement with government, academia, industry and civic institutions on all of these urgent challenges.

We look forward to advancing a cybersecure Canada together.



About the Authors

Charles Finlay is the executive director of Rogers Cybersecure Catalyst, Ryerson University's centre for collaboration and innovation in cybersecurity. Charles brings extensive experience in public administration, law and finance to this role. Most recently, Charles served as chief of staff and director of policy for the Ontario Minister of Economic Development and Growth, where he worked closely with private sector and government leaders to develop and implement the province's strategy to make Ontario a global leader in technology innovation and commercialization. Prior to joining government, Charles was senior legal counsel at BMO Capital Markets, practiced law at Torys LLP, worked as a technology researcher at Forrester Research, and was a freelance business journalist for *The Globe and Mail* and *Canadian Business Magazine*.

Karim Bardeesy is the Co-Founder and Executive Director of the Ryerson Leadership Lab. Karim is a public service leader who has worked in progressively senior roles in public policy, politics, journalism and academia in Toronto and the United States since 2001. Karim was previously Deputy Principal Secretary for the Premier of Ontario, the Honourable Kathleen Wynne, and served as Executive Director of Policy for Premiers Wynne and Dalton McGuinty. He has worked as a journalist, an editorial writer at *The Globe and Mail*, and as an editorial assistant at *Slate* magazine. Karim holds a Master in Public Policy from Harvard's John F. Kennedy School of Government.

Yvonne Su is an Assistant Professor in the Department of Equity Studies at York University. She is a political scientist, researcher and educator with a passion for policy development, research and public engagement on topics of democracy. Yvonne served as the Policy Lead of the Cybersecure Policy Exchange. Yvonne holds a PhD in Political Science and International Development from the University of Guelph and a Masters from the University of Oxford.

Methodology

This report was informed by:

- a literature review;
- a series of interviews with Canadian cybersecurity, privacy and technology experts;
- a series of six weekly video townhalls on the cybersecurity and digital privacy challenges facing Canadians during COVID-19, conducted from April 7 to May 19, 2020, featuring 18 experts and over 1,500 attendees; and
- a representative survey of 2,000 Canadians.

In this introductory paper, we share our first wave of analysis on new data from this survey, with more data and analysis from the survey to be included in our forthcoming work.

This anonymous survey was conducted online by Pollara Strategic Insights with 2,000 Canadian residents aged 18 and older from May 14 to 22, 2020. A random sample of Canadian residents who have opted in to the AskingCanadians panel were invited to complete the voluntary survey.

As a guideline, a probability sample of this size would yield results accurate to ± 2 percentage points, 19 times out of 20 (95%). Totals may not sum or add to 100 due to rounding.

The data were weighted by region, gender and age, based on the most recent Canadian census figures to ensure that the sample matched Canada's population.

Table 1: Rates of Cybercrime

"Have you ever...? (Select all that apply)"

	Total	Income							Visible Minority		
		Under $20,000	$20,000 - Less than $30,000	$30,000 - Less than $50,000	$50,000 - Less than $80,000	$80,000 - Less than $100,000	$100,000 -Less than $150,000	$150,000 or More	Visible Minority	Not a Visible Minority	DK/Unsure
All Respondents	2,000	82	118	264	363	279	409	279	378	1562	60
Weighted Respondents	2,000	79*	116	263	357	282	410	287	398	1542	61*
...been a victim of phishing (obtained your personal or financial information using a deceptive e-mail or website)	252	10	16	40	40	30	53	39	68	175	9
	13%	12%	14%	15%	11%	11%	13%	13%	17%	11%	14%
...had an online account hacked	439	13	28	67	83	50	91	73	107	317	15
	22%	16%	24%	25%	23%	18%	22%	25%	27%	21%	25%
...unintentionally installed/downloaded a computer virus or malware	628	18	35	99	107	79	148	96	132	483	14
	31%	23%	30%	38%	30%	28%	36%	34%	33%	31%	23%
...unintentionally installed/downloaded ransomware (software that threatened to destroy your files, expose your personal information or report you to authorities if you did not pay)	168	3	7	31	30	21	31	25	45	117	6
	8%	4%	6%	12%	8%	7%	8%	9%	11%	8%	10%
...experienced a data breach of any kind that exposed your personal information	558	14	28	56	92	75	131	103	121	428	9
	28%	18%	24%	21%	26%	27%	32%	36%	30%	28%	15%
Selected at least one of above	57%	48%	54%	60%	57%	53%	62%	64%	61%	57%	42%
Not sure/don't know	292	22	23	36	53	41	53	24	63	208	21
	15%	28%	20%	14%	15%	14%	13%	8%	16%	13%	35%
None of the above	562	19	30	68	100	93	105	79	91	457	14
	28%	24%	26%	26%	28%	33%	26%	27%	23%	30%	23%

Table 2: Use of Online Activities

"Which of the following activities have you done on the internet during the past two (2) months? (Select all that apply)"

	Total	Age					Gender		
		18-29	30-39	40-49	50-59	60+	Female	Male	Other/Did not say
All Respondents	2,000	405	344	321	369	561	1014	978	8
Weighted Respondents	2,000	380	351	334	371	564	1025	968	8**
Online banking	1,750	347	325	293	317	468	890	853	7
	87%	91%	93%	88%	85%	83%	87%	88%	87%
Online messaging or video calls	1,589	321	309	264	278	417	826	756	6
	79%	85%	88%	79%	75%	74%	81%	78%	75%
Facebook Messenger	1,102	259	219	166	181	276	610	488	3
	55%	68%	62%	50%	49%	49%	60%	50%	38%
Zoom	920	208	201	151	156	204	488	426	6
	46%	55%	57%	45%	42%	36%	48%	44%	75%
WhatsApp	650	159	181	114	98	98	312	333	5
	33%	42%	52%	34%	26%	17%	30%	34%	63%
Skype	528	108	117	85	95	123	229	296	3
	26%	28%	33%	25%	26%	22%	22%	31%	38%
Online shopping	1,536	306	290	269	288	383	771	757	7
	77%	81%	82%	80%	78%	68%	75%	78%	87%
Social media	1,530	337	296	259	275	362	806	719	5
	76%	89%	84%	78%	74%	64%	79%	74%	62%
Facebook	1,381	299	265	236	245	336	742	636	3
	69%	79%	75%	71%	66%	60%	72%	66%	38%
Instagram	836	273	210	140	104	108	475	357	3
	42%	72%	60%	42%	28%	19%	46%	37%	38%
LinkedIn	542	142	114	100	102	85	231	308	3
	27%	37%	32%	30%	27%	15%	23%	32%	38%
Twitter	500	132	105	88	86	89	213	286	1
	25%	35%	30%	26%	23%	16%	21%	30%	13%
Online traditional media (e.g., newspaper websites, TV news)	1,481	275	266	246	278	416	734	740	7
	74%	72%	76%	74%	75%	74%	72%	76%	87%
Online health care (e.g., virtual appointment with a doctor or therapist)	373	69	76	65	65	99	182	187	4
	19%	18%	22%	19%	17%	18%	18%	19%	50%
None of the above	75	9	11	15	14	26	42	34	0
	4%	2%	3%	5%	4%	5%	4%	3%	-

Table 3: Perspectives on Regulating Technology Companies

"To what extent do you agree with the following statement: 'Regulating technology companies in the name of protecting individuals' privacy and security will mean that we slow down innovation and hurt our economy'?"

	Total	Age					Gender		
		18-29	30-39	40-49	50-59	60+	Female	Male	Other/Did not say
All Respondents (Half Sample)	1,000	199	172	161	171	297	502	494	4
Weighted Respondents	1,002	188	173	172	172	298	508	490	4**
Totally Agree	36	13	7	3	10	4	19	17	1
	4%	7%	4%	2%	6%	1%	4%	3%	25%
Somewhat Agree	130	35	22	14	22	37	48	82	0
	13%	19%	13%	8%	13%	12%	9%	17%	-
Neither Agree nor Disagree	243	35	39	43	41	85	119	123	1
	24%	18%	23%	25%	24%	29%	23%	25%	25%
Somewhat Disagree	240	53	47	41	36	64	129	111	0
	24%	28%	27%	24%	21%	22%	25%	23%	-
Totally Disagree	284	43	43	58	53	87	147	135	2
	28%	23%	25%	34%	31%	29%	29%	28%	50%
Not sure/don't know	68	10	14	13	10	21	47	21	0
	7%	5%	8%	8%	6%	7%	9%	4%	-

Table 4: Perspectives on Ring Doorbells

"Home security cameras, for example the Ring doorbell, provides the convenience of being able to see who's at your door with your phone, or check on deliveries. However, some are concerned about the privacy implications. Which of the following statements best captures your views?"

	Total	Region					
		BC	AB	MK/SB	ON	QC	ATL
All Respondents	2,000	269	264	201	669	397	200
Weighted Respondents	2,000	272	227	130	766	468	138
I don't mind my neighbours having personal cameras facing out to my street and being captured briefly. It's their right to do so.	987	149	126	73	404	164	72
	49%	55%	55%	56%	53%	35%	52%
I am uncomfortable being captured on video by people I don't know, but I don't think there's anything that should be done about it.	512	75	60	31	189	126	32
	26%	27%	26%	24%	25%	27%	23%
I don't think that it should be allowed to capture private video of people without their consent, and these products should be banned.	295	17	20	11	97	135	15
	15%	6%	9%	8%	13%	29%	11%
Don't know/not sure	207	32	21	15	77	43	18
	10%	12%	9%	12%	10%	9%	13%

Table 5: Trust in Organizations to Keep Personal Data Secure

"Below is a list of organizations that often handle data about Canadians. How much do you trust these organizations to keep your personal data secure? Rate on a scale of 0 to 10, with 0 being 'Do not trust at all' and 10 being 'Completely trust.'"

	All Respondents	Sum of 0 to 3	Sum of 4 to 6	Sum of 7 to 10
Health care providers (e.g., hospitals, doctors)	2,000	142	396	1,462
	100%	7%	20%	73%
Banks	2,000	172	464	1,364
	100%	9%	23%	68%
Police	2,000	225	454	1,321
	100%	11%	23%	66%
The federal government	2,000	254	501	1,245
	100%	13%	25%	62%
Your provincial government	2,000	229	549	1,222
	100%	11%	27%	61%
Your municipal government	2,000	247	645	1,108
	100%	12%	32%	55%
Telecommunication providers	2,000	434	773	793
	100%	22%	39%	40%
Apple	2,000	474	720	806
	100%	24%	36%	40%
Microsoft	2,000	457	773	770
	100%	23%	39%	38%
Google	2,000	575	758	667
	100%	29%	38%	33%
Facebook	2,000	988	702	310
	100%	49%	35%	15%

Table 6: Canadians' IoT Device Ownership

"Beyond your smartphone, computer or tablet, which of the following internet-connected devices do you have in your household? (Select all that apply)"

	Total	Income						
		Under $20,000	$20,000 - Less - than $30,000	$30,000 Less - than $50,000	$50,000 Less than $80,000	$80,000 Less than $100,000	$100,000 -Less than $150,000	$150,000 or More
All Respondents	2,000	82	118	264	363	279	409	279
Weighted Respondents	2,000	79*	116	263	357	282	410	287
Internet-connected television	952	22	43	95	163	126	235	184
	48%	28%	37%	36%	46%	45%	57%	64%
Smart watch/fitbit that you wear	569	11	23	49	101	66	144	125
	28%	15%	20%	19%	28%	23%	35%	44%
Smart speaker/voice-operated assistant (e.g., Amazon Alexa, Google Hub/Nest Hub, Apple HomePod)	516	21	17	38	84	78	137	96
	26%	26%	15%	15%	23%	28%	33%	34%
Smart thermostat (e.g., Nest, Ecobee)	245	4	13	30	28	80	69	4
	12%	3%	5%	8%	10%	19%	24%	3%
Internet-connected home security system (e.g., Bell/Rogers Smart Home, Nest Secure)	189	7	1	11	26	25	59	46
	9%	9%	1%	4%	7%	9%	14%	16%
Internet-connected light bulbs (e.g., Philips Hue)	173	5	7	9	23	24	48	43
	9%	6%	6%	4%	6%	8%	12%	15%
Camera doorbell (e.g., Ring)	146	2	4	11	23	14	44	36
	7%	3%	4%	4%	6%	5%	11%	13%
Smart door lock (e.g., Lockley, August)	79	3	2	5	8	10	22	27
	4%	4%	2%	2%	2%	3%	5%	10%
Internet-connected appliance (e.g., fridge, dishwasher, oven, microwave, coffee maker)	77	1	2	6	14	11	22	12
	4%	2%	2%	2%	4%	4%	5%	4%
At least one of above	68%	49%	53%	51%	68%	67%	82%	83%
At least two of above	38%	23%	23%	22%	35%	37%	53%	57%
At least three of above	20%	14%	10%	10%	18%	16%	30%	39%
None of the above	636	40	55	128	114	92	72	49
	32%	51%	47%	49%	32%	33%	18%	17%

* small base

**very small base; ineligible for significance testing

References

[1]Accenture. (2017, November 6). Concern about Cybercrime is Limiting Canadians' Use of Online Services, Accenture Survey finds. Retrieved from: https://www.accenture.com/ca-en/company-news-release-canada-cybercrime-survey-2017

[2]Centre for International Governance Innovation. (2019, June 11). 2019 CIGI-Ipsos Global Survey on Internet Security and Trust. Retrieved from: https://www.cigionline.org/internet-survey-2019

[3]OECD (2020, May 04). Tackling Covid-19: Keeping the Internet up and running in times of crisis. Retrieved from: https://read.oecd-ilibrary.org/view/?ref=130_130768-5vgoglwswy

[4]Sandvine (2020, May). The Global Internet Phenomena Report Covid-19 Spotlight. Retrieved from: https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID%20Internet%20Phenomena%20Report%2020200507.pdf

[5]Koops, B.J. (2006). Should ICT Regulation Be Technology-Neutral? *Starting Points for ICT Regulation*. (Ed. B.J. Koops, M. Lips, C. Prins & M. Schellekens). T.M.C. Asser Press. Retrieved from: https://ssrn.com/abstract=918746

[6]Innovation, Science and Economic Development Canada. (2019, May 21). Strengthening Privacy for the Digital Age. Government of Canada. Retrieved from: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

[7]Birnhack, M. (2013). Reverse Engineering Information Privacy Law. *Yale Journal of Law and Technology,* 15(3). Retrieved from: https://digitalcommons.law.yale.edu/yjolt/vol15/iss1/3

[8]Broadly outlined in Europe's *General Data Protection Regulation* (GDPR), Article 5.

[9]https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-3

[10]Innovation, Science and Economic Development Canada (2019)

[11]Department of Justice. (2020, June 5). Modernizing Canada's Privacy Act. Government of Canada. Retrieved from: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html

[12]Innovation, Science and Economic Development Canada. (2019, May 21). Canada's Digital Charter: Trust in a digital world. Government of Canada. Retrieved from: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

[13]Villeneuve, S., Barron, B. & Boskovic, G. (2019, May). Rebooting Regulation: Exploring the Future of AI Policy in Canada. *CIFAR and Brookfield Institute for Innovation + Entrepreneurship.* Retrieved https://www.cifar.ca/docs/default-source/ai-reports/rebooting-regulation-exploring-the-future-of-ai-policy-in-canada.pdf?sfvrsn=616c04f3_8

[14]Canadian Radio-television and Telecommunications Commission. (2020, January). Communications Monitoring Report 2019. Retrieved from: https://crtc.gc.ca/eng/publications/reports/policymonitoring/2019/index.htm

[15]Fraser, D.C. (2020, June 11). Rural Communities feel social impact of COVID. *The Western Producer.* Retrieved from: https://www.producer.com/2020/06/rural-communities-feel-social-impact-of-covid/

[16]Porteous, H. (2018). Cybersecurity Technical and Policy Challenges. *Library of Parliament.* Retrieved from: https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201805E

[17]Berghel, H. (2018). Malice Domestic: The Cambridge Analytica Dystopia. *Computer* 51(5), 84-89. Retrieved from: https://doi.ieeecomputersociety.org/10.1109/MC.2018.2381135

[18]Edelman. (2020). *Edelman Trust Barometer 2020.* Retrieved from: https://www.edelman.com/sites/g/files/aatuss191/files/2020-01/2020%20Edelman%20Trust%20Barometer%20Executive%20Summary_Single%20Spread%20without%20Crops.pdf

[19]McGuire. M. (2019). Social Media Platforms and The Cybercrime Economy. *Bromium*. Retrieved from: https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

[20]Arkose Labs. (2019). *Fraud & Abuse Report Q3 2019*. Retrieved from: https://na-ab31.marketo.com/rs/465-HCZ-671/images/2019%20Q3%20Fraud%20Report.pdf

[21]Seamans, R. & Bytes, W. (2019, June 12). A Primer on Regulating Big Tech. *Forbes.* Retrieved from: https://www.forbes.com/sites/washingtonbytes/2019/06/12/a-primer-on-regulating-big-tech/#48242422fd73

[22]Parsons, C. (2019, August). Canada's New and Irresponsible Encryption Policy. *The Citizen Lab*. Retrieved from: https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/

[23]Kaste, M. (2020, February 21). Trump Administration Targets Your 'Warrant-Proof' Encrypted Messages. *NPR.* Retrieved from: https://www.npr.org/2020/02/21/805032627/trump-administration-targets-your-warrant-proof-encrypted-messages

[24]Spangler, T. (2020, May 28). Trump Signs Executive Order Targeting Twitter, Facebook That Legal Experts Say Is Likely Unconstitutional. *Variety.* Retrieved from: https://variety.com/2020/digital/news/trump-executive-order-targets-twitter-facebook-1234619250/

[25]Innovation, Science and Economic Development Canada. (2019, May 21). Proposals to modernize the *Personal Information Protection and Electronic Documents Act*. Government of Canada. Retrieved from: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

[26]Owen, T., Docquir, P.F., Donovan, J. Etlinger, S., Fay, R., Girard, M., Gorwa, R., Kimmelman, G., Kate Klonick, K., McDonald, S., Nyabola, N., Penney, J.W., Perset, K., West, J., Winickoff, D., Wyckoff, A., Pickard, V., Tambini, T., & Tworek, H., (2019, October 29). Models for Platform Governance. Centre for International Governance Innovation. Retrieved from: https://www.cigionline.org/publications/models-platform-governance

[27]Neate, R. (2020, March 31). Zoom booms as demand for video-conferencing tech grows. *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2020/mar/31/zoom-booms-as-demand-for-video-conferencing-tech-grows-in-coronavirus-outbreak

[28]Lorenz, T., & Alba, D. (2020, April 7). 'Zoombombing' Becomes a Dangerous Organized Effort. *The New York Times*. Retrieved from: https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html

[29]Elmer, G., Burton, A. G., & Neville, S. J. (2020, June 9). Zoom-bombings disrupt online events with racist and misogynist attacks. *The Conversation*. Retrieved from: https://theconversation.com/zoom-bombings-disrupt-online-events-with-racist-and-misogynist-attacks-138389

[30]Check Point. (2020, March 30). COVID-19 Impact: Cyber Criminals Target Zoom Domains. Retrieved from: https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/

[31]Palmer. D. (2016, February 8). T9000 malware records Skype calls, screenshots, and text messages to steal data. *ZDNet*. Retrieved from: https://www.zdnet.com/article/t9000-malware-records-skype-calls-screenshots-and-text-messages-to-steal-data/

[32]Starks, T. (2020, June 24). FBI alerts on ransomware threat to schools. *Politico*. Retrieved June 24, 2020, from https://www.politico.com/newsletters/morning-cybersecurity/2020/06/24/fbi-alerts-on-ransomware-threat-to-schools-788762

[33]Lueth, K.L. (2018, August 8). State of the IoT 2018: Number of IoT devices now at 7B – Market Accelerating. *IoT Analytics*. Retrived from: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[34]Benjamin, R. (2019). Race after technology: Abolitionist tools for the new Jim code. Cambridge: Polity.

[35]Arif, A., Stewart, L. G., & Starbird, K. (2018). Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse. In Proceedings of the ACM on Human-Computer Interaction, 2(20). Retrieved from: https://doi.org/10.1145/3274289

[36]Bliuc, A., Jakubowicz, A., & Dunn, K. (2019). This is how racism is being spread across the internet. *World Economic Forum*. Retrieved from: https://www.weforum.org/agenda/2019/02/racism-in-a-networked-world-how-groups-and-individuals-spread-racist-hate-online

[37]Haskins, C. (2019, February 7). Amazon's Home Security Company Is Turning Everyone Into Cops. *Vice*. Retrieved from: https://www.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops

[38]Grother, P., Ngan, M. & Hanaoka, K. (2019, December). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. *National Institute of Standards and Technology*. NISTIR 8280. Retrieved from: https://doi.org/10.6028/NIST.IR.8280

[39]Public Safety Canada. (2018). National Cybersecurity Strategy. Government of Canada. Retrieved from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

[40]Ghafur, S., Kristensen, S., Honeyford, K. et al. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine* 2, 98. https://doi.org/10.1038/s41746-019-0161-6

[41]Rider, D. (2019, August 8). Ontario cities ask feds, province for help repelling ransomware attacks. *Toronto Star*. Retrieved from: https://www.thestar.com/news/gta/2019/08/07/ontario-cities-ask-feds-province-for-help-repelling-ransomware-attacks.html

[42]Canadian Centre for Cybersecurity. (2018). An Introduction to the Cyber Threat Environment. Retrieved from: https://www.cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf

[43]Williams-Grut, Oscar. (2018, April 18). Hackers once stole a casino's highroller database through a thermometer in the lobby fish tank. *Business Insider*. Retrieved from: https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4

[44]National Institutes of Health. (2020). Continuous Glucose Monitoring. Retrieved from: https://www.niddk.nih.gov/health-information/diabetes/overview/managing-diabetes/continuous-glucose-monitoring

[45]Perez, S. (2018, November 14). We tried Amazon's bizarre Alexa microwave and weren't convinced. *TechCrunch*. Retrieved from: https://techcrunch.com/2018/11/14/we-were-promised-flying-cars-we-got-alexa-microwaves/

[46]Li, B., Lu, R., Xiao, G., Bao, H., & Ghorbani, A.A. (2019). Towards insider threats detection in smart grid communication systems. *IET Communications*, 13(12), 1728-1736. Retrieved from: https://doi.org/10.1049/iet-com.2018.5736

[47]Thomas, E. (2019, September 19). New Surveillance Tech Means You'll Never Be Anonymous Again. *Wired*. Retrieved from: https://www.wired.co.uk/article/surveillance-technology-biometrics

[48]Pandya, J. (2019, March 9). Hacking Our Identity: The Emerging Threats From Biometric Technology. *Forbes*. Retrived from: https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/#d33161556823

[49]Draper, K. (2018, March 13). Madison Square Garden Has Used Face Scanning Technology on Customers. *New York Times*. Retrieved from: https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html

[50]Gillespie, E. (2019, February 23). Are you being scanned? How facial recognition technology follows you, even as you shop. *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop

[51]Hutchins, A. (2018, November 1). Your mall is watching you. *Macleans*. Retrieved from: https://www.macleans.ca/economy/business/your-mall-is-watching-you/

[52]Office of the Privacy Commissioner of Canada. (2018, August 3). Privacy Commissioner launches investigation into Cadillac Fairview over use of facial recognition technology in malls. Retrieved from: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_180803/

[53]Allen, K., Gillis W., & Boutilier, A. (2020, February 27). Facial Recognition App Clearview AI has been used far more widely in Canada than previously known. *Toronto Star.* Retrieved from: https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html

[54]Ng, A. (2020, February 26). Clearview AI's entire client list stolen in data breach. *CNET.* Retrieved from: https://www.cnet.com/news/clearview-ai-had-entire-client-list-stolen-in-data-breach/

[55]Office of the Privacy Commissioner of Canada. (2020, July 6). Clearview AI ceases offering its facial recognition technology in Canada [Press Release]. Retrieved from: https://priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/

[56]Ng, A. (2020, June 17). Amazon owes answers on facial recognition moratorium, lawmaker says. *CNET.* Retrieved from: https://www.cnet.com/news/amazon-owes-answers-on-facial-recognition-moratorium-lawmaker-says/

[57]Associated Press. (2019, November 19). Amazon has considered facial recognition in its Ring doorbells. *MarketWatch*. Retrieved from: https://www.marketwatch.com/story/amazon-has-considered-facial-recognition-in-its-ring-doorbells-2019-11-19

[58]Buckner, D. (2020, May 14). No slacking allowed: Companies keep careful eye on work-from-home productivity during COVID-19. *CBC News*. Retrieved from: https://www.cbc.ca/news/business/working-from-home-employer-monitoring-1.5561969

[59]Bednar, V. (2020, May 19). #11 Technology to positively stalk employees. *Regs to Riches*. Retrieved from: https://regstoriches.substack.com/p/11?token=eyJ1c2VyX2lkIjo3OTQwMzY4LCJwb3N0X2lkIjo0NTU1MDEsIl8iOiIzU000ZiIsImlhdCI6MTU5MDEwMTUwOSwiZXhwIjoxNTkwMTA1MTA5LCJpc3MiOiJwdWItMzI1MDMiLCJzdWIiOiJwb3N0LXJlYWN0aW9uIn0.fLoFp6qPfiu-Pv2A4IhP7MVIvqQKWEOUSZok1zsroIk

[60]Goode, L. (2018, February 11). Facial Recognition software is biased towards white men, researcher find. *The Verge*. Retrieved from: https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-e rror

[61]Ferguson, A.G. (2020, June 12) High-tech surveillance amplifies police bias overreach. *The Conversation*. Retrieved from: https://theconversation.com/high-tech-surveillance-amplifies-police-bias-and-overreach-140225.

[62]Owen, T. & Ahmed, N. (2020, February 14). Let's Face the Facts: To Ensure Our Digital Rights, We Must Hit Pause on Facial Recognition Technology. *The Globe and Mail.* Retrieved from: https://www.theglobeandmail.com/opinion/article-lets-face-the-facts-to-ensure-our-digital-rights-we-must-hit-pause/

[63]Goldsmith, T. (2019, October 1). We need to regulate facial recognition technology. *Policy Options*. Retrieved from: https://policyoptions.irpp.org/magazines/october-2019/we-need-to-regulate-facial-recognition-technology/

[64]Colaner, S. (2020, May 18). The technologies the world is using to track coronavirus — and people. *VentureBeat*. Retrieved from: https://venturebeat.com/2020/05/18/the-technologies-the-world-is-using-to-track-coronavirus-and-people/

[65]Bedi, A. (2020, June 2). Geo-mapping, CCTV cameras, AI — how Telangna Police is using tech to enforce Covid safety. *The Print.* https://theprint.in/india/geo-mapping-cctv-cameras-ai-how-telangana-police-is-using-tech-to-enforce-covid-safety/433856/

[66]Garcia, R. (2020, June 10). How are governments and corporations leveraging personal data in our current crisis? *Forbes*. Retrieved from: https://www.forbes.com/sites/forbestechcouncil/2020/06/10/how-are-governments-and-corporations-leveraging-personal-data-in-our-current-crisis/#756d264817b6

[67]Putz, C. (2020, May 13). Technology and policing a pandemic in Central Asia. *The Diplomat*. Retrieved from: https://thediplomat.com/2020/05/technology-and-policing-a-pandemic-in-central-asia/

[68]Heilweil, R. (2020, June 11). Big tech companies back away from selling facial recognition to police. That's progress. *Vox*. Retrieved from: https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police?fbclid=IwAR1LzbVRkVX04jKz0FRiVNYudcDVeole4yqtasJKZnXwVsF_Bw1Hfix4vyU

[69]Greene, J. (2020, June 11). Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. *Washington Post*. Retrieved from: https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/

[70]Heilweil, R. (2020, June 10). Why it matters that IBM is getting out of the facial recognition business. *Vox*. Retrieved from: https://www.vox.com/recode/2020/6/10/21285658/ibm-facial-recognition-technology-bias-business


cybersecure
policy
exchange
Powered by
RBC