Submission to the Ontario Ministry of Consumer Affairs on the prospect of introducing legislation to regulate privacy in the private sector

16 October 2020

Privacy and Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440, 10816 Macleod Trail SE, Calgary AB T2J 5N8
Telephone: 877.746.7222
Email: info@pacc-ccap.ca
Website: www.pacc-ccap.ca

About the Privacy and Access Council of Canada

The Privacy and Access Council of Canada is an independent organization that is nongovernmental, nonpartisan, nonprofit, and not funded by government or industry.

Since 2002, the Privacy and Access Council of Canada has taken a leadership role in representing access and privacy professionals from all sectors, and advocating for Canadians who deal with any of our country's dozens of privacy and access laws.

We are the certifying body for Canada's privacy and access practitioners; and our members are in private, non-profit, and public organizations in sectors as diverse as law, technology, academia, health care, law enforcement, and government.

PACC is run by a volunteer Board of Directors, and is dedicated to the ongoing professional development, education, and expanded expertise of people who work in the field of privacy, access, and data protection.

PACC plays a cornerstone role, and has made landmark advances in establishing credible accreditation standards and professional certification of information access and privacy professionals.

As the voice of privacy and access, PACC plays a pivotal role in ensuring the independent autonomy of access and privacy professionals to administer privacy and access legislation, while directly and independently addressing the needs of industry, the public and private sectors.

More information about PACC is available at www.PACC-CCAP.ca

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Contributors

This report was prepared by Sharon Polsky BIS MAPP, with contributions from members of the Privacy and Access Council of Canada and other individuals, organizations, and stakeholders.

The broad perspective of PACC members and stakeholders is particularly relevant to implementing privacy and access-to-information legislation applicable to the private sector, to charitable organizations, and to non-profit entities, since PACC members are access and privacy practitioners — as well as citizens, parents, members of military and law enforcement families, and actively involved in their communities.

PACC members are representative of the larger Canadian context, except that our members' awareness of privacy and access laws, and the real-life application and limits of those laws, is perhaps somewhat greater than among the general population.

Like the Greek princess Cassandra, daughter of the King of Troy, privacy professionals have insight and perspective akin to the gift of prophecy, and share Cassandra's curse when others disregard their warnings.

PACC members understand the complexities and practical aspects of the issues that arise from domestic and international data protection regimes and the technologies, business practices, and governmental policies that affect individuals of every age; and they appreciate the importance and value of effective and enforceable privacy, access, and data protection laws.

We would like to thank the contributors for their insights, input, and collaboration in developing this submission, and appreciate their ongoing commitment to data protection, privacy, and access to information.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

Table of Contents

PIPEDA Potency 1
Is Change Needed 3
Benefits of Effective Regulation 5
Adequacy Status 6
PIPEDA in Practice 7
- Pandemic Privacy Pitfalls 7
- DNA Test Kits 7
- In-Home Entertainment and Digital Assistants 8
- Data Brokers 8
- GPS Trackers 9
- Smart Watches 9
- Tenant Screening 9
- Bluetooth 10
- Fitness Monitors and Interactive Online Health Assessment Tools 11
- Biometrics and Facial Recognition 11
- Video Doorbells 11
- Artificial Intelligence 12
- Employee Monitoring and Applicant Tracking Tools 12
- Collaboration Tools 13
- Data Sovereignty 13
- Connected and Autonomous Vehicles 14

Consent Conundrum 17
- Website Privacy Policies 18
- Reverse Onus 19
- Accountability 20

Recommendations 21
- Clarity 21
- Consent 21
- Intent 21
- Access 21
- Accountability 22
- Access Requests 22
- Frivolous Requests 23
- Enforcement 23
- Breach Notification 23
- Privilege 24

Appendix – Automated Tenant Screening 25
Appendix – Google Privacy Policies 27

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

PIPEDA Potency

The private sector in Ontario has been subject to the federal Personal Information Protection and Electronic Documents Act (PIPEDA) since its enactment — a generation ago, in an era that predates the pervasive use of electronic communications and data storage. As a 'technology neutral' law, PIPEDA could be applied to various technologies; but does not contemplate and is inadequate to respond to, the global exchange, processing, and storage of personal information — whether legitimate, direct, or indirect — that is now commonplace; nor could it anticipate the machinations that industry and governments would undertake to wrest monetary value from information about individuals.

The past twenty years have seen the blurring of lines between state and corporate actors, the consolidation of commercial activity and influence in the hands of a few technology companies, and the privacy-invasive power of data being amassed by industry — revealing a fundamentally flawed consent model supported by PIPEDA's inadequacies.

The law's shortcomings, combined with promises of social and economic benefit to be derived from innovative technology, have been allowed to transcend common sense and manifest in law and public policy intended to, firstly, support the economic interests of the corporate influencers.

But the good intentions and benefits to be enjoyed from innovative technologies can lead to pernicious unintended consequences — that are arising with increasing frequency and impact — as the direct and indirect result of inadequate laws that allow organizations to collect, share, trade and monetize personal information with impunity.

Vendors — that were not elected to represent individuals' views and whose motives are, by definition, biased to favor their own investors' economic benefit — now enjoy the privilege of directing public policy. Companies are at liberty to set the rules of engagement with their customers, users, and competitors — thanks in large part to inadequate privacy laws that have enabled companies to disregard legal and moral obligations to regard individuals' privacy or to provide consumers with any real choice.

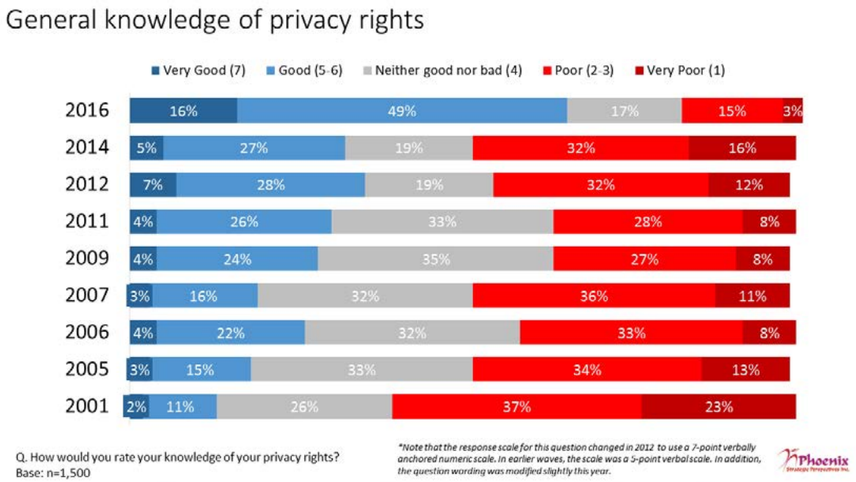
Advanced technologies continue to be deployed in all sectors, but without adequate consultation or unequivocal safeguards to identify and guard against their problematic and privacy-invasive impacts. As a result, many of the benefits from services, technologies, and business models that have come into existence this century have also created novel risks to individuals and to society at large.

At the same time, as business owners worked to keep their businesses afloat in some of the most economically challenging times since the Great Depression, the level of understanding about PIPEDA has been consistently low. Indeed, the most recent Survey of Canadians on Privacy[1] conducted by the Office of the Privacy Commissioner of Canada (OPC) reveals that only 16% rate their knowledge of privacy rights as very good — more than double the number in any previous OPC survey.

Despite this chronic and pervasive ignorance of privacy rights and responsibilities, privacy-invasive technologies and processes have been woven into all aspects of everyday life — with few controls and great latitude, at the peril of individuals' privacy.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector



The vast majority of Canadians — 85% — are concerned about the collection and use of information from their body for non-medical reasons.

More than 75% of Canadians are very concerned about how information about them will be used — whether to determine insurance or health coverage (46%), by marketing companies to analyze their preferences (43%), or about data being used to assess their suitability for a job or promotion (39%).

Canada's obsolete privacy laws whose consent provisions favor corporate interests, combined with foreign data protection regulations and a longstanding dearth of education and awareness about privacy and access rights and responsibilities, obliges lawmakers to respond with thoughtful, effective, and enforceable legislation that will, firstly, provide individuals with genuine control over information about themselves and provide an effective right of access-to-information held by organizations; and will guide, direct, and control the private sector in collecting, using, disclosing, and safeguarding personal information.

PACC looks forward to new legislation to provide Ontarians with a genuine right of access to information and to control privacy of information about themselves.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

Is Change Needed

In the decades since PIPEDA was enacted, sophisticated Internet-based commerce, 'smart' devices, and international data flows have proliferated and revealed the extent of PIPEDA's inadequacies that could not have been anticipated by its authors.

We recognize that privacy laws do not grant an absolute right to privacy; rather, they provide a mechanism that must strike a balance between privacy and a range of competing interests in administrative proceedings[2], in the workplace[3], between privacy protection and information flows[4], and between the interests of the police and the privacy rights of individuals.[5]

History has shown that the necessary balance has been elusive.

From the fundamental failure of the accepted consent model that has facilitated unimaginable and life-altering privacy-invasive impacts, to its usefulness as a mechanism to enable individuals to have control over their personal information, PIPEDA has enabled an economy based largely on the exploitation of information about people.

As the impacts of technological encroachment upon personal privacy have become more apparent, industry has balked at the suggestion that it be required to obtain meaningful and informed consent for the collection, use or disclosure of personal information; that genuine privacy be the default setting for all products and processes; or that they be required to notify affected individuals when information about them is compromised — claiming that such obligations might hamper innovation.

Industry proponents that profit from trafficking personal information point to their voluntary codes of conduct[6] as a sufficient surrogate for regulation. Corporations have worked mightily to convince Canadians that existing privacy legislation, the Charter of Rights and Freedoms, and industry-sponsored voluntary measures are sufficient to safeguard personal privacy, and avoid the subtle distinction that laws can only proscribe and prescribe behaviors.

Corporations insidiously claim that privacy and access laws "protect" information — avoiding the subtle distinction that ***laws do not protect information*** and that privacy legislation merely indicates limits and requirements for how organizations collect, use, and disclose personal information. It is the conduct of people and organizations who comply with effective data protection laws that protect information.

Facilitating the effectiveness of industry's obfuscation efforts is a flawed consent model that has enabled domestic and international organizations to funnel Ontarians' personal information to foreign corporations to be monetized — and improve the economies of those nations.

PIPEDA's woeful inadequacies at providing individuals with genuine control over information about themselves underscores the need for clearly-articulated, unambiguous, and readily enforceable law to be able to rein in the many industries that have been allowed to prosper at the very real cost to individual privacy — often with life-altering impacts.

Submitting to legislative inertia or industry sway would avert any need (and cost) for domestic and foreign organizations to improve their data protection, privacy, and accountability practices.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Indeed, doing nothing is a choice that would signal a short-term preference to protect corporate interests over individual and human rights; and it would further entrench the latitude that businesses now have and exploit — at the expense of individuals' privacy and Ontario's economic future that is already on the brink thanks to COVID and the Schrems II decision.

In the years since PIPEDA's enactment, protection professionals, Commissioners, as well as the Privacy and Access Council of Canada and countless academics, associations, and individuals have recognized and experienced its shortcomings, and have urged successive governments to move beyond promises and platitudes, and finally ensure individuals' privacy and effective access to information that does not provide a shield against organizational accountability.

> *"It's the critics who drive improvement. It's the critics who are the true optimists."*
>
> *Jaron Lanier, Founding father of virtual reality; computer scientist.*

History, commerce, international geopolitical developments, and the sage wisdom of privacy professionals makes it abundantly clear that maintaining the status quo is not a viable option for Ontarians or the province; and hoping that the federal government will substantively strengthen PIPEDA is unlikely in the near term, leaving Ontarians at the mercy of an outdated, ineffective, and inadequate privacy law.

As Julie Brill, Chief Privacy Officer at Microsoft and former Commissioner of the Federal Trade Commission, notes, "businesses have too much leeway on what they can do with the data they collect, and consumers have too little control."[7]

Industry and those who develop physical and digital products available in Canada have never been required to embed strong and reliable privacy protections and data security as part of the design process, or to maintain such protections throughout the entire data lifecycle. And there is no effective independent watchdog to ensure compliance.

That needs to be changed.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

Benefits of Effective Regulation

Since 1999, when Scott McNealy, then CEO of global technology company Sun Microsystems, uttered the oft-quoted quip that "you have zero privacy anyway; get over it," industry proponents have echoed that sentiment to nudge Canadians (and, indeed, much of the world's population) into accepting — as a foregone conclusion — that nobody cares about privacy.

The lack of effective laws and mechanisms to ensure Canadians have genuine control over their information or to protect individuals' privacy has left Canadians with little option but to become resigned to an onslaught of privacy incursions. That resignation is too often characterized as evidence that industry's self-serving truism is valid; leveraged as rationale to further encroach on personal privacy; and interpreted as satisfaction with the current privacy laws.

Nothing could be further from the truth. University of Manchester Professor Carole Goble famously stated that 'Scientists would rather share their toothbrush than their data!' Canadians are equally reticent about sharing their data — when they don't trust what will happen to it.

Daily reports about data breaches, inappropriate use of personal information with significant and long-term impacts on affected individuals, and few, if any, meaningful consequences for offending organizations or impetus for improvement, however, have garnered mounting dissatisfaction among Canadians — with significant economic consequences for local, regional, and national economies.

Ontarians' distrust became evident in their vocal opposition to the Sidewalk Labs-Waterfront Toronto plan[8] to develop a 'smart city' that leveraged technology to have a profound impact on personal privacy. Ontarians' opposition to the prospect of pervasive privacy-invasive technology led to the project being abandoned — forsaking projected economic benefits that included 44,000 direct jobs (and 93,000 total jobs), and $14.2 Billion in annual economic impact by 2040.

More broadly, eliminating the status quo will provide profound economic advantages for Ontario's economic prosperity and Canada's international trade opportunities.

Businesses should have long ago complied with PIPEDA, and many already comply with the U.S. Sarbanes-Oxley Act, the GDPR, and other foreign data protection and accountability laws; so, any operational changes to comply with new Ontario privacy laws should be relatively minor.

> *"Current federal laws are simply not up to protecting our rights in a digital environment. All Canadians deserve strong privacy protections."*[9]
>
> *Daniel Therrien, Privacy Commissioner of Canada*
> *October 8, 2020*

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Adequacy Status

In 2001 (and reaffirmed it in 2006), the EU granted *adequacy status*[10] to Canada, recognizing that PIPEDA offers a level of data protection equivalent to that provided to residents in the EU, where privacy is considered a human right.

By contrast, organizations in the EU wishing to transfer personal information to the US (which has not been granted adequacy status) relied on the Privacy Shield Framework[11], a mechanism in effect since 2015 (when its predecessor Safe Harbor was declared invalid) intended to facilitate the lawful transfer of personal information from the EU to the United States (where privacy is often viewed as an impediment to commerce and innovation).

Canada's adequacy status became tenuous when the GDPR took effect in May of 2018. In June of 2018, the Government of Canada committed to reforming PIPEDA; and when the federal government officially launched the National Digital and Data Consultations, it committed to reforming PIPEDA and "to examine the viability of certain changes to PIPEDA to ensure that it continues to meet its stated purpose of maintaining trust and confidence in the marketplace.[12]" Substantive updates to PIPEDA have not been forthcoming.

More recently, the Court of Justice of the European Union removed all doubt about the validity of transferring personal information from the EU to third countries, including Canada. The decision in the Schrems II matter[13] immediately invalidated Privacy Shield, further threatened Canada's preferred *adequacy status,* and compounded the urgency for Canada to substantively modernize its privacy and access laws lest the legislative inertia results in decisive economic and commercial trade implications that Canada — and Ontario — can hardly afford.

We commend the Ontario Government for moving to fill the longstanding dearth of privacy and access legislation that would apply to the private sector, and to create robust and enforceable legislation that will give Ontarians genuine control over the collection, use, and disclosure of information about themselves, and a genuine right to gain access to information held by private sector organizations.

Strong, clear, and definitive laws will encourage innovation to enable industry to meet its goals while genuinely respecting individuals' privacy; and it will facilitate international commerce and allow Ontario businesses to be the beneficiary of trade fostered by personal information transmitted across borders. That would, in turn, improve Ontario's fortunes and the trust they have in their government and economy, and public sector.

In order for lawmakers to craft legislation that is effective, enforceable and responsive, however, we must look to the past and to other jurisdictions to offer practicable and realistic recommendations for the future.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

PIPEDA in Practice

In the decades since PIPEDA was enacted, sophisticated Internet-based commerce, 'smart' devices, and international data flows have proliferated, with results that could not have been imagined by its authors.

The law's usefulness as a mechanism to enable individuals to have control over their personal information, and some of the consequences of its shortcomings, are described in the following examples.

Pandemic Privacy Pitfalls

As governments around the world, including across Canada, introduced technological contact tracing apps in an effort to slow the spread of the novel coronavirus, without public input or discussion, little mention was made that many 'contact tracing' apps are merely re-branded location-tracking technologies from surveillance or marketing companies.

The COVID crisis has given the technology industry an unparalleled opportunity for innovation and sales. Whether for online communications, online purchasing, or family safety, the increased use of digital tools used to respond to the health crisis has been characterized as a 'demand' for their use, with industry implying that it is merely providing the privacy-invasive surveillance and monitoring systems that individuals are demanding.

That has had an immediate impact on Ontarians' privacy.

DNA Test Kits

In the 1930s, Germany used IBM punch card technology to catalog an entire population. It was rudimentary technology compared to today's computers.

A century later, powerful computers and at-home DNA test kits from companies like 23andMe and Ancestry have enabled people to trace their heritage and piece together family trees.

Canada's Genetic Non-Discrimination Act, SC 2017, c 3[14] "prohibits any person from requiring an individual to undergo a genetic test or disclose the results of a genetic test as a condition of providing goods or services to, entering into or continuing a contract or agreement with, or offering specific conditions in a contract or agreement with, the individual." The Act neither restricts the sale of the kits in Canada, nor requires the analysis and storage of samples, or test results, to remain in Canada. As a result, Canadians' genomes have been collected by foreign companies that are at liberty to sell the results back to Canadian organizations — providing an effective 'end run' around the law.

That needs to be changed.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

In-Home Entertainment and Digital Assistants

It seems a quaint idea from a bygone era that parents would be worried that their children's eyes might be damaged by watching too much TV. Now our TVs watch us and identify who's watching TV.

The longer-term danger is that our children — who now receive a mobile phone for their own use[15] long before they are taught about online safety and risks — are being desensitized to constant surveillance in the form of cars, toys, and devices that are armed with digital sensors, microphones, and speakers.

Voice-controlled in-home devices like Nest (from Google) and Alexa (from Amazon) that routinely listen to conversations — and desensitize children to accept surveillance as the norm — have been joined by Mattel's WIFI enabled Hello Barbie, which monitors what's going on around her. Within months of being introduced into society, more than 1700[16] phrases had been added to Hello Barbie's voice recognition/response system. By listening to children's delightful banter Hello Barbie learns everything it can: their likes and dislikes, their preferences, their family and friends, and the nearby conversations and sounds.

Perhaps parents are reassured by Mattel's Children's Privacy Statement[17] which says the company does not ask "for more personal information than is necessary for a child to participate in an activity" or that Hello Barbie met the kidSAFE Seal[18] Program's minimum standards of online safety and/or privacy.

Does Mattel really need to hear, record, and retain the conversations from a child's bedroom or living room? Do parents realize that inviting Hello Barbie and other digital surveillance devices into their home constitutes consent for unlimited access and use of their children's personal information?

Perhaps parents are reassured by Mattel's assurance that identifiers such as gender, birth month and day are "not personally identifiable"— although those identifiers are sensitive personal information under PIPEDA, the GDPR, and California's Consumer Privacy Act.

Like Cardinal Richelieu said in the 1600s, *give me six lines written by the hand of the most honest of men and I will find in them something with which to hang him*. Five hundred years later, technology now records, videotapes and preserves everything for an unknown length of time, distributes it all to an unknown audience, for unknown purposes, ready to be reused 'for business purposes' that can haunt for a lifetime.

That needs to be changed.

Data Brokers

The collection and trade in personal information spawned a new $200 billion data broker industry.

Data brokers collect everything they can about us including our preferences, associations, opinions, and purchases — and sell it for pennies per life; yet the companies that traffic the minutiae of our lives have no direct relationship with the us, and have no obligation to notify Canadians or regulators about their business practices or data breaches.

The data broker industry remains hidden and unregulated in Canada.

That needs to be changed.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

GPS Trackers

Youngsters are tracked from the moment they step onto a school bus — for safety and peace of mind. GPS trackers embedded in school buses give the location of the bus in real time — and each child who boards the bus must 'tap in' to register their presence, and 'tap out' so their parents, the school board, the bus company, the technology company — and we don't know who else — can know when and where the child stepped off the bus: near home, a friend's house, the local candy shop or, for teenagers, at the pool hall or liquor store.

School districts mandate the use of such devices, leaving parents no option but to consent — or to limit their children's information (and their own) being disclosed with the providers of these GPS peace-of-mind systems. And it's all done based on the parents giving consent — without knowing or being told the behind-the-scenes details.

That needs to be changed.

Smart Watches

The convenience and utility of 'smart' watches is merely a starting point for some products that are sold as an essential tool to improve children's safety and as a way to offer parents peace of mind. Smart watches for children can receive voice calls to parent-approved numbers and send emergency alerts — and some also contain undocumented back doors that make it possible to remotely capture camera snapshots, wiretap voice calls, surreptitiously listen to and transmit sounds, and covertly track locations in real time and transmit the data.[19]

That needs to be changed.

Tenant Screening

Automated background-checking tools — required by an increasing number of landlords across the private and public sectors — use artificial intelligence to screen prospective residential tenants. Promulgated as a way to select reliable tenants and streamline the application process, and for tenants to find accommodations, these tools facilitate a "seamless consent-based exchange of data" that allows landlords to better understand the needs of prospective tenants.

Many of the tools go well beyond conducting credit checks by demanding copies of government-issued photo identification, and requiring information unrelated to tenancy (i.e., commute information, pets' names and weights) and scanning social media accounts that often contain information that is irrelevant to tenancies (and which landlords are prohibited from asking for under human rights and anti-discrimination laws).

Various of these tenant-evaluation services require and capture biometric information, and obtain additional information from "public social media content" and "information accessible via the internet;" and their "privacy" policies indicate that prospective tenants' personal information (which includes information about dependents and children) is shared with Facebook and advertisers, without any way for individuals to opt out of that occurring.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

The algorithms use the gathered information to assign a 'score' that reflects its prediction of how likely a tenant is to cause damage to property, to be late on their rent (including by reason of actual or implied health or wellness issues that might prevent regular work), or to vacate before the lease expiry date; and often evaluate a property's "suitability" for a prospective tenant.

The results from tenant screening tools, combined with the 'feedback' about tenants that is provided by landlords, is useful to streamline the rental application process; and will be useful to predict who is at risk of becoming homeless.[20]

Tenant screening tools also produce tenant rental performance databases that landlords can consult — that serve as a blacklist that can hamper renters' ability to qualify for housing.

Given that most tenant screening tools and the amassed databases are outside of Canada, tenants have little recourse to gain access to or verify correctness of information collected about them; to know how decisions about them are made; or to have incorrect information corrected.

An increasing number of property owners require prospective tenants to apply through screening apps; so, anyone who is unwilling or unable to apply online has no chance of being considered. Simply put, if a person wants to have any chance of living in a chosen residence where the landlord or rental agent uses automated tools, the individual has no option but to consent to use the automated tool, to the collection of whatever information the app requires, and submit to whatever demands are made by the landlord.

That needs to be changed.

Bluetooth

Customers of Canadian icon *Tim Hortons* were surprised to learn the store's apps[21] tracked user location — even when the app was not in use. That is a clear example of how easy it is for companies to circumvent their obligations under PIPEDA.

More fundamentally, "a user can turn Bluetooth off on their smartphone running Google's Android software, and the phone will continue to use Bluetooth to collect location-related data and transmit that data to Google."[22]

That needs to be changed.

Fitness Monitors and Interactive Online Health Assessment Tools

Employers are increasingly coercing employees to give employers and benefits providers full access to the health, location, and physiology information collected by personal fitness monitors — which is outside the scope of health information privacy laws — typically in exchange for a promise of personalized wellness plans.

The promise has already seen employee benefits plans require that employees' family members consent to be monitored, or face the threat of coverage being reduced or rates increased.

That needs to be changed.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

Biometrics and Facial Recognition

As industry has pressed for the adoption of facial recognition technology, its significant privacy and societal dangers have become apparent.

The consequences of systems that generate a 92% false positive rate (which UK police excuse as "no big deal"[23],) and racially biased[24] facial recognition systems can be life-altering[25] .

Sweden[26], France[27], San Francisco[28], and Washington State[29] are among the many jurisdictions that have banned or set moratoria on the use of facial recognition due to significant error rates.[30]

In Canada, however, facial recognition use remains essentially unregulated.

That needs to be changed.

Video Doorbells

Industry and police encourage homeowners to install video doorbells, and to allow police ready access to the video stream. Promoted as valuable tools to improve personal, family, and community safety and provide peace of mind, the devices capture any activity in the doorbell's field of view.

With the increase in online purchasing through COVID-19 lockdowns, and occasional media reports of "porch pirates" stealing packages left on doorsteps, media[31] have eagerly featured rare stories of video doorbell systems that captured various crimes; and that has been exploited as valid reason to encourage the use of digital doorway monitors.

Privacy experts have characterized the devices as an 'unmitigated disaster'[32] for neighborhood and individual privacy, because the devices capture all activity in the doorbell's field of view, and offer no way for anyone to avoid being recorded, whether they are at the doorstep or across the street.

In addition, since many popular 'smart' video doorbell security systems (including Google's Nest,[33] and devices from Tend[34] and Honeywell[35]) integrate facial recognition, the devices provide an ongoing inventory of identifiable faces that is easily correlated to provide detailed information about where individuals go, and how frequently.

Furthermore, "face analysis encompasses a growing range of inference-drawing capacities that extend beyond recognition. This can include attempts to algorithmically infer age, gender, race, health conditions, and behavioral traits based on facial characteristics or impressions"[36] and enable assumptions to be drawn — with no way to dispute the conclusions.

European and American lawmakers[37] have recognized that embedding facial recognition software into video doorbells raises significant privacy and civil liberty implications. The practice remains unregulated in Canada.

That needs to be changed.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Artificial Intelligence

Artificial intelligence is among the most highly-promoted technologies, and in its current state is unfair[38], easily susceptible to attacks[39], and inherently biased[40].

Academics and industry insiders are adamant that artificial intelligence is often biased; and that it can — and always could — be resolved. But without any regulatory requirement to ensure AI is not biased, or to compel designers to allow third parties to scrutinize their AI systems, developers and tech companies have had no reason to create unbiased, ethical products.

Canadians are under the same technological stranglehold as the United States. The majority of technology used by Canadian governments, organizations, and individuals is American; and the data that is collected, generated, processed, and stored through those technology companies typically resides outside of Canada, and beyond Canada's lax privacy laws.

That needs to be changed.

Employee Monitoring and Applicant Tracking Tools

Artificial Intelligence-based recruiting tools are used with increasing frequency to scan[41] various features such as video or voice data of job applicants and their CVs to assess if they are worth hiring.

Although the psychometrics are incorporated into some recruiting tools must meet standards[42] of fairness and quality, psychometricians are permitted to work without supervision in technology environments.

Facebook is among the (mostly American) companies offering workplace collaboration tools that can facilitate communications between workers, managers, and headquarters and help employees feel valued[43] and recognized for their efforts. The platforms offer convenience and confidentiality — as conversations and comments are monitored, analyzed, and assessed to detect emotions, intent, and behavior.

All of these technologies can have entirely legitimate workplace applications, such as to protect against discriminatory conduct; but the practical reality is that they can also be (and are) used to monitor performance, discipline employees for general conduct, and peer into home-offices and collect information to which employers are not entitled.

That needs to be changed.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

Collaboration Tools

The use of virtual platforms offered by commercial enterprises has soared through the pandemic.

What now passes for consent also allows organizations to scour and collect unstructured web content, including online discussions inside enterprises and across the Internet, and turn that into machine-readable data feeds which are sold to other organizations.

The vast majority of popular collaboration platforms are based outside of Canada and are clear that they collect and share the information provided (through registering for the service, through using the service, and from 'other sources') for myriad purposes. The content of many discussions can reveal opinions, health conditions, and other personal information; but with virtually unlimited consent provisions, enable the commercial entity to monetize the information at will.

That needs to be changed.

Data Sovereignty

The advances in electronic information holdings theoretically make possible the increase of direct access to information by individuals. Without an awareness of precisely who is gathering that information, and the specific purposes to which it is and might be put, Canadians cannot make informed decisions or hold organizations accountable. The dilemma of this reality is that it is impossible to ask for or verify the accuracy of information when one is unaware that the information exists, by whom it has been gathered, or to whom it has been or will be transmitted.

The results of a PACC survey about data sovereignty were striking: Fully 85% of respondents recognize that being unable to control data residency invites the prospect that data will be sent to jurisdictions where laws permit or require disclosure, mass interception of communication, and state/corporate access to users' data (precisely the concerns that resulted in the Schrems II decision).

The majority of survey respondents indicated that their ability to conduct comprehensive and meaningful Privacy Impact Assessments will be drastically (30%) or significantly (40%) hampered if data cannot be restricted to Canadian systems.

Fully 85% of respondents note that being unable to control data residency undermines efforts to search for responsive documents, thus making it impossible for their organizations to respond to access requests, or identify parties with whom personal information has been disclosed.

In other words, the uncontrolled cross-border distribution of personal information makes it impossible for private and public sector organizations to comply with current access to information laws.

That needs to be changed.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Connected and Autonomous Vehicles

The Information Highway used to refer to the Internet. With emotionally aware vehicles[44] that scan our eyes, fingerprints, and faces,[45] communicate with other vehicles, with smart street light systems[4647], with smart buildings, smart bicycles, and with the smart phones in our hands, our roadways now *are* the Information Highway.

IBM has cautioned that modern vehicles are datacenters on wheels where up to 80% of innovation is driven by software and may contain as much as 10,000 vulnerabilities.[48]

Like other databases, in-car personal profiles stored in the cloud[49] are an accident waiting to happen — as Ontario improves its infrastructure to benefit from smart auto industry innovations.

As long ago as 2004, the US Department of Transportation acknowledged that connected vehicle technology raises many privacy and liability concerns due to the continuous communication of data between personal vehicles.[50] Other concerns have become apparent.

Long haul truckers' engines are governed, and their travels are monitored. For safety, of course. And that provides peace of mind to their families and employers. It also provides a wealth of information for the truck manufacturers, and others — about which the driver has no say.

Automakers working to improve long-term revenue-generating capacity[51] are increasingly leveraging the information collected and created by vehicles — from such innovations as integrating third-party apps and in-vehicle infotainment systems, and adopting the Android automotive OS, which comes with a plethora of applications. Automakers are working with Google, Apple, Amazon, and Baidu to provide — and be able to capitalize on data derived from — embedded location-based commerce services, in-car media applications, mobile apps, and enterprise services.

Innovative automakers are also working to guarantee revenue streams by moving to subscription-based services that will see annual fees for a wide range of functionality beyond the current fee-based GPS, satellite radio, and roadside assistance. Annual vehicle OS update fees will ensure revenue streams (and allow insurers to decline coverage for failing to update a vehicle's operating system) and enable automakers to follow the example of cellphone makers that stop supporting models after a few years — effectively "bricking" vehicles and forcing people to purchase new versions.

Automotive telematics (already in use in Ontario and elsewhere) that reveal driver behavior are being supplemented with more privacy-invasive video telematics that can have unintended consequences. Integrating 'smart' cameras to provide "actionable" video intelligence — ostensibly as a way to help people improve their driving and reward driver safety —gives "mobile network operators, OEMs, insurers, dealers and service providers the tools to build customer relationships and increase revenue opportunities[52] and provide "driver scores" as well as instant, live, and recorded evidence of driver error that are valuable for employee discipline and to minimize insurance payouts.

When Nissan transmits personal information to other countries[53] that have a patchwork of definitions as to what constitutes 'personal information', PIPEDA's protections are meaningless.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

When Ford Canada's website assures consumers that personal information will be kept according to a retention schedule and then be destroyed[54] — but retention schedules are internal corporate documents that can stipulate that all data will be retained indefinitely — PIPEDA is of no help.

Automakers collect information about us from online, off-line, and third-party sources[55] such as social media. Others have integrated voice-enabled intelligent personal assistants[56] into cars — leaving drivers who want to regain their privacy one option: physically remove the telematics transponder[1] unit from the vehicle — which can "cause unusual conditions in the car."[2]

Drivers might be concerned that their insurance rates could be influenced by questions they the in-vehicle Siri or Alexa digital personal assistant. They might also be concerned that PIPEDA is ineffective to protect them against assumptions made about the people in vehicles that regularly drive to mosques, churches, synagogues, or massage parlors. Or that our vehicles visit the women's shelter, AIDS clinic, or mental health clinic.

Vehicle owners have no way to know which nameless partners,[57] affiliates, and marketers their vehicles have shared personal information with.

What child on the way to hockey practice consents to the vehicle they are riding in collecting their social media conversations and their location?

What civil servant consents to their in-car conversations — about anything from the mundane to fundraising or the next minister's meeting — being analyzed by a nameless partner or affiliate in another country?

And what are we to expect when automakers like the General Motors Family of Companies put the onus squarely on us to obtain consent for all of this from anyone who uses our vehicle?

These are just *some* of the privacy and access issues that needs to be changed — before connected or automated cars become a literal road to hell paved with good intentions.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Consent Conundrum

Underlying the entire problem facing Ontarians who want to control over the information about themselves, and lawmakers contemplating a privacy law applicable to the private sector, is the fundamental matter that the current consent model is fatally flawed — and needs to be changed.

The current consent model is based on the premise that individuals have the ability to exercise control over the collection, use, and disclosure of their personal information whether for commercial interactions online or in person. In reality, however, individuals have remarkably little ability to wrest or exercise control over whether, when, how, and from what sources information about them is collected.

Instead of being able to opt in to grant permission for their information to be collected, or used for specific purposes, as is required under the GDPR, Ontarians are left to accept the terms and policies presented. An all-or-nothing proposition, with little ability to opt for 'nothing', does not provide choice. Indeed, Privacy Commissioners have approved forms of 'consent' that list a range of 'purposes' so broad that nothing except 'unlawful activity' is excluded.

Equifax is a grand example of that. Few people realize that every purchase or transaction having a financial component is, in some way, reported to a credit bureau. And they would be astounded to learn how much other information credit bureaus have amassed about each one of us. Yet we are deemed to have consented to the collection, use and distribution of our most personal information with companies we have never heard of, in places we have never been.

Sensors in the 150-plus computer systems in our cars surreptitiously report readouts back to auto manufacturers or components makers[58] But automakers insist that they only collect personal information with explicit consent.

In addition, the entire discussion about data gathering, analysis and monetization ignores — entirely—the reality that information traverses beyond the protection of domestic privacy laws, and that corporate 'privacy' policies also make clear that information about individuals will be gathered from a range of sources that are entirely unrelated to the immediate transaction or the parties involved in the transaction, and with which that person has no direct relationship.

For instance, Tesla's website cautions that it might use the information collected about individuals "to communicate[3] with you, to provide and improve our products and services, and for other purposes." Unfortunately, the "other purposes" are not specified, so there is no way to know precisely what one is agreeing to when purchasing or driving a Tesla vehicle.

Continuing to allow Canadians' driving habits, associations, geolocation patterns, bodily functions, and behavioral data to be gathered and stored outside of Canada — without adequate and effective safeguards to genuinely protect Canadians' data — puts the entire Canadian driving population, and their human payload, at risk of being little more than marketing fodder for foreign interests.

That needs to be changed.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

The massive stores of data about Canadians — from the mundane to the bizarre and criminal — are being gathered and secreted away by domestic and foreign corporations under the rubric of "informed consent" while, at the same time as the freedoms historically enjoyed by Canadians are being eroded or being bargained away in the name of commerce.

That needs to be changed.

All the data from the vehicles and smart devices that promise to make our lives more convenient is readily available to insurance companies, employers, people and agencies, and an entire world of private surveillance companies who can obtain it because users have unwittingly provided their consent.

That needs to be changed.

PIPEDA does nothing to ensure individuals have — from the outset — any genuine control over their information; nor do they prevent corporations, government, and other organizations from gathering, sharing, and monetizing the digital details of our movements, associations, and preferences.

That needs to be changed.

Website Privacy Policies

The 'privacy' assurances presented as website privacy policies by most organizations are carefully crafted statements that allow an organization to do what it wishes with the information it gathers, while presenting the illusion of care and confidentiality.

Sadly, few people read beyond the first line of 'privacy' policies that optimistically promise "We respect your privacy" or "Your privacy is extremely important to us"[59] to realize that they have little choice but to accept gives organizations authority to do with our information what they wish.

A 2006 survey conducted UC Berkeley survey found that only 1.4 percent of participants read online privacy policies "often and thoroughly."[6]

Findings from a March 2017 survey conducted by the Office of the Privacy Commissioner of Canada (OPC) echo the Berkeley findings, confirming that few read privacy policies — but defend that choice by dealing with reputable companies or companies they trust or with which they are familiar.

When privacy policies are so convoluted and voluminous that even the technology titans (including Mark Zuckerberg) acknowledge that few people read them, the current concept of 'informed consent' is a fantasy.

Google offers a 4227-word long 'privacy policy[60]' (a 29-page PDF) with links to the specific privacy practices of 8 other frequently-used Google products and services "that you may use".
In all, the Google privacy policy is 18,665 words.
Calculating that a single-spaced page of type using 12-point Arial font contains an average of 470 words,
Google's privacy policies are 40 pages long.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Consumers are left to pore over hundreds of lines of confusing language in the privacy policies that are designed to give consumers comfort in knowing the company will safeguard personal information — but the vague language grants carte blanche and results in personal information being collected, used, disclosed, and monetized with impunity — and with no way for individuals to know or control what happens to information about themselves, how it is used, or by whom.

That needs to be changed.

Reverse Onus

Website privacy policies and vendor terms put the onus on consumers to read, understand, and compare current and previous versions. On rare occasion, a statement such as "we've changed how we use your information" is offered, but without any indication of just what was changed, or where the revision is within the text of the document.

According to the CSA Group, however, the fault lies with users: "privacy agreements are designed around consent and control, which puts the responsibility of making choices related to data collection on users who are ill-prepared to make and accept the consequences of their choices"[61]

The CSA Group has proposed a system of graphic icons to improve make privacy policies easier to understand, "improving the accessibility and comprehension of long and complex documents."[62]

Reducing complex contractual and data transfer provisions into simple pictograms to "improve readers' understanding of the content" does nothing at all to "make it easier for consumers to handle their own data" — especially when 'consent' provisions are so vaguely written as to impose an all-or-nothing Faustian bargain that consumers have no choice but to accept.

That needs to be changed.

Accountability

Website privacy policies are internal corporate documents, and are changeable at will. Website privacy policies are carefully crafted statements that give broad, vague statements that present the illusion of care and confidentiality while actually giving the organization almost unlimited license do what it wishes wish with the information collected.

As well, unlike the requirements of Europe's recently-implemented GDPR, Canadian privacy laws do not require any real degree of granularity so there's no way to use many platforms without accepting the terms of service in an all-or-nothing Faustian bargain.

That needs to be changed.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

Recommendations

Clarity

- Draft the legislation to be simple and direct in meaning and application, and to ensure clarity and coordination between access and privacy provisions.

Consent

- Require that organizations be compelled to provide goods and services without being permitted to impose coercive control over individuals to extract consent.
- Require that organizations be required to clearly specify, with precision and granularity, the purposes for which information is sought; and that individuals may elect to provide consent for some, all, or none.
- Require that all non-essential cookies be off by default; that keystroke tracking be prohibited; and that other web-based beacons, trackers and identification tools be prohibited.

Intent

- Require that organizations be compelled to conduct Privacy Impact Assessments for all contemplated and existing projects, programs, processes, services, and equipment to determine whether it can have an impact on personal privacy and, if so, to require the organization mitigate identified risks to privacy prior to implementing/delivering/releasing the product/service.
- Require organizations routinely incorporate the concepts of Privacy by Design and Privacy by Default for all contemplated and existing projects, programs, processes, services, and equipment to determine whether it can have an impact on personal privacy and, if so, to require the organization mitigate identified risks to privacy prior to implementing/delivering/releasing the product/service.

Access

- Require that organizations publish the name, title, email address and mailing address of the individual to whom requests for access to information should be sent. Merely publishing "title and address" enables an institution to simply provide a generic title (i.e., Privacy Officer) and general office address, effectively making it impossible to know whether or by whom an access request is being evaluated. It puts the requestor in the unenviable position of having to await contact or acknowledgment; and if such acknowledgment is not forthcoming, leaves the requestor without any way of contacting a person to be able to obtain clarification about the status of their request.

Accountability

- Require the privacy law and its regulations be subject to mandatory review every five years without exception or extension; and require that the results of the review be acted upon within a defined and brief time (lest the recommendations merely be tabled and the law left to languish, unchanged, until the next five-year review).
- Impose executive accountability (with ensuing and meaningful consequences) for overall organizational effectiveness in achieving privacy, access, and data governance objectives and complying with privacy law.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Access Requests

- Limit the circumstances and opportunities for organizations to claim any exemption from providing access to information.
- Limit the amount of fees that organizations can demand when individuals request access to information about themselves; restrict organizations from delaying or circumventing their obligation to provide meaningful and timely access to information; and make it 100% clear that information provided digitally is free of cost.
- Require that, where information is available digitally, requesters should always be provided with an open format (i.e., machine processable) version if that is what they want; that organizations must make a reasonable effort to convert non-digitally recorded information into an open digital format where the requester wants that; and prohibit organizations from charging a fee for digitizing records.
- Prohibit organizations from requiring requesters to give reasons for why they want information
- Specify what forms of information may and may not be used to verify identities; impose clear and robust data safeguard requirements to ensure organizations adequately protect identity information; and ensure individuals have genuine choice and options to enable them to refuse to allow their identities to be verified in a foreign jurisdiction.
- Ensure that exceptions and exclusions to the right of access are narrowly defined and subject to both a test of actual harm and a mandatory public interest override.

Frivolous Requests

- Require that access requests made to obtain information must be specific to the record being sought and not to a range of information that the requestor thinks might exist.
- Implement an effective deterrent to frivolous requests for information, including a scalable application fee with greater sums applicable to requests for nonspecific information (i.e., fishing expeditions) and for professional requestors including those from or on behalf of members of the media and legal profession.
- Provide a mechanism for organizations to reject frivolous or vexatious access requests; but require that they obtain the IPC's prior approval to reject any access request as frivolous, vexatious, made in bad faith, or otherwise an abuse of the right to make a request for access to records.
- Specify within the legislation (not regulations) the characteristics of a request that would constitute a 'vexatious' request. Defining the test that would have to be met to qualify as a vexatious request would eliminate the potential for improper bias or subjectivity.

Enforcement

- Grant the Information and Privacy Commissioner order-making power to facilitate effective compliance with the legislation; and with the authority and power to enforce such orders. Incorporate into law a range of mechanisms to enable the Commissioner to compel compliance with such orders; and incorporate into law the requirement to adequately fund the Office of the Information and Privacy Commissioner to enable the effective enforcement of orders.

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

Breach Notification

- Require that organizations notify all affected individuals and the Information and Privacy Commissioner within 72 hours of becoming aware of any incident that compromises the integrity, security, privacy or availability of personal information.
- Require that the Information and Privacy Commissioner publish the details of all Privacy Impact Assessments and all data breach notices upon receipt — to enable Ontarians to make informed choices, provide informed consent, and be able to be aware of circumstances worthy of withholding or revoking their consent
- Require that corporate data management practices be audited annually by an impartial third party, and that the results and recommendations of such audits be required to be implemented within six months.

Privilege

PACC acknowledges that solicitor-client privilege is a substantive right, and a cornerstone of the rule of law that has constitutional dimensions. The public's right of access to information also has constitutional dimensions, as the Supreme Court of Canada has affirmed.

The public interest in upholding privilege is vitally important, and so is the public interest in neutral, cost-effective and expert review of privilege claims, to ensure that claims of privilege are properly made.

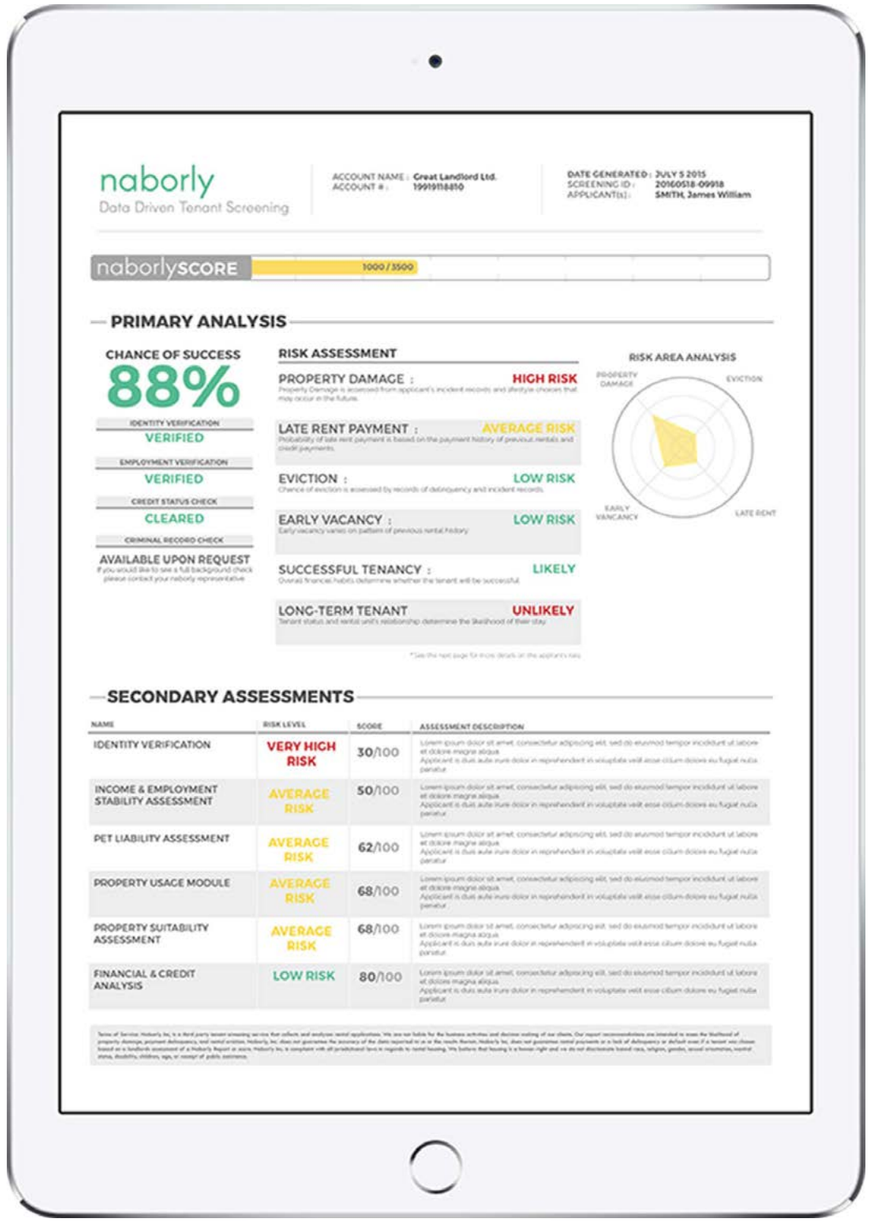
The Supreme Court of Canada has affirmed that Parliament may empower statutory tribunals with the authority to decide constitutional matters.[63] The Court must be understood to have affirmed this when it ruled, in 2016, that a legislature may authorize a statutory tribunal—which the Commissioner effectively is—to compel production of allegedly privileged records.[64] The Court did not suggest that there is any constitutional bar, despite its earlier ruling, against Parliament enacting such a clause (or empowering a tribunal to decide privilege claims). The Court would surely not have let this point pass unmentioned in 2016 had it wished to turn away from its explicit ruling in 2003.

- Clarify that the Information and Privacy Commissioner has full authority to compel and view allegedly privileged records in investigating a complaint that an organization has withheld information on the grounds of privilege.

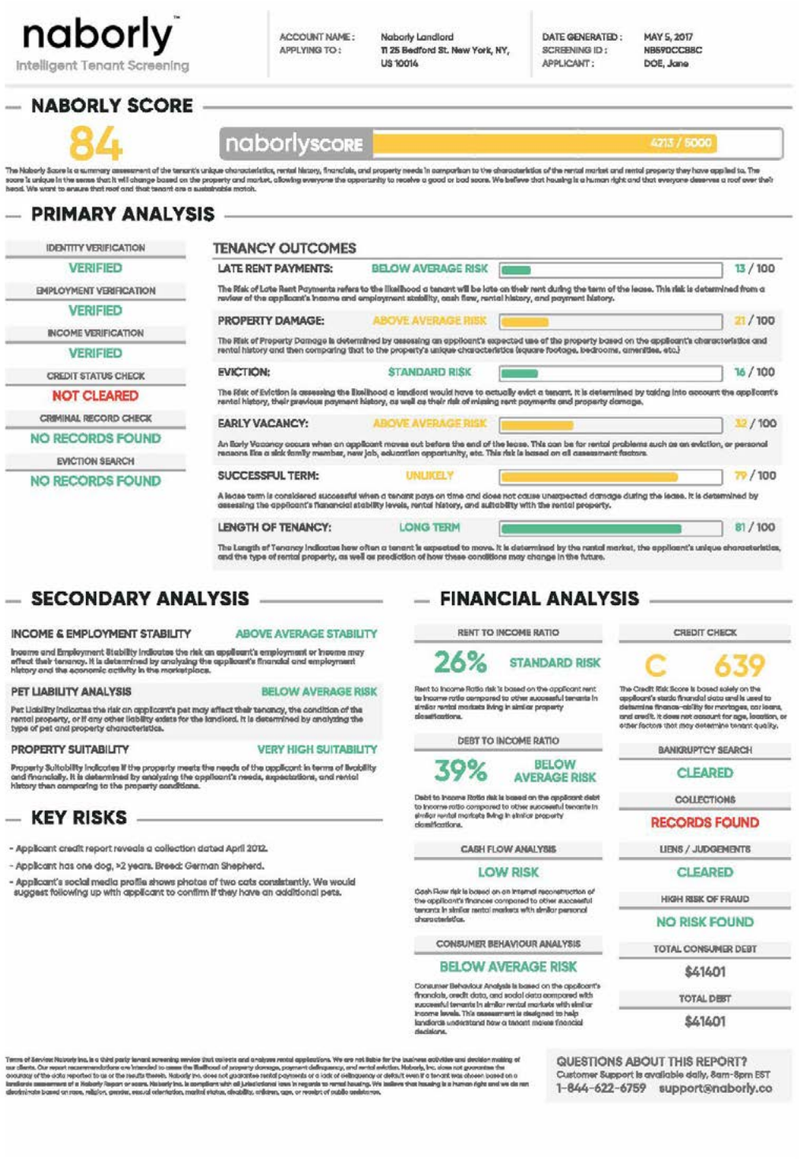
Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Appendix – Automated Tenant Screening



Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222



naborly
Intelligent Tenant Screening

ACCOUNT NAME: Naborly Landlord
APPLYING TO: 11 25 Bedford St. New York, NY, US 10014
DATE GENERATED: MAY 5, 2017
SCREENING ID: NB59DCC88C
APPLICANT: DOE, Jane

NABORLY SCORE

84

naborlyscore 4213 / 5000

The Naborly Score is a summary assessment of the tenant's unique characteristics, rental history, financials, and property needs in comparison to the characteristics of the rental market and rental property they have applied to. The score is unique in the sense that it will change based on the property and market, allowing everyone the opportunity to receive a good or bad score. We believe that housing is a human right and that everyone deserves a roof over their head. We want to ensure that roof and that tenant are a sustainable match.

PRIMARY ANALYSIS

IDENTITY VERIFICATION: VERIFIED
EMPLOYMENT VERIFICATION: VERIFIED
INCOME VERIFICATION: VERIFIED
CREDIT STATUS CHECK: NOT CLEARED
CRIMINAL RECORD CHECK: NO RECORDS FOUND
EVICTION SEARCH: NO RECORDS FOUND

TENANCY OUTCOMES

LATE RENT PAYMENTS: BELOW AVERAGE RISK 13 / 100
The Risk of Late Rent Payments refers to the likelihood a tenant will be late on their rent during the term of the lease. This risk is determined from a review of the applicant's income and employment stability, cash flow, rental history, and payment history.

PROPERTY DAMAGE: ABOVE AVERAGE RISK 21 / 100
The Risk of Property Damage is determined by assessing an applicant's expected use of the property based on the applicant's characteristics and rental history and then comparing that to the property's unique characteristics (square footage, bedrooms, amenities, etc.)

EVICTION: STANDARD RISK 16 / 100
The Risk of Eviction is assessing the likelihood a landlord would have to actually evict a tenant. It is determined by taking into account the applicant's rental history, their previous payment history, as well as their risk of missing rent payments and property damage.

EARLY VACANCY: ABOVE AVERAGE RISK 32 / 100
An Early Vacancy occurs when an applicant moves out before the end of the lease. This can be for rental problems such as an eviction, or personal reasons like a sick family member, new job, education opportunity, etc. This risk is based on all assessment factors.

SUCCESSFUL TERM: UNLIKELY 79 / 100
A lease term is considered successful when a tenant pays on time and does not cause unexpected damage during the lease. It is determined by assessing the applicant's financial stability levels, rental history, and suitability with the rental property.

LENGTH OF TENANCY: LONG TERM 81 / 100
The Length of Tenancy indicates how often a tenant is expected to move. It is determined by the rental market, the applicant's unique characteristics, and the type of rental property, as well as prediction of how these conditions may change in the future.

SECONDARY ANALYSIS

INCOME & EMPLOYMENT STABILITY: ABOVE AVERAGE STABILITY
Income and Employment Stability indicates the risk an applicant's employment or income may affect their tenancy. It is determined by analyzing the applicant's financial and employment history and the economic activity in the marketplace.

PET LIABILITY ANALYSIS: BELOW AVERAGE RISK
Pet Liability indicates the risk an applicant's pet may affect their tenancy, the condition of the rental property, or if any other liability exists for the landlord. It is determined by analyzing the type of pet and property characteristics.

PROPERTY SUITABILITY: VERY HIGH SUITABILITY
Property Suitability indicates if the property meets the needs of the applicant in terms of livability and financially. It is determined by analyzing the applicant's needs, expectations, and rental history then comparing to the property conditions.

KEY RISKS

- Applicant credit report reveals a collection dated April 2012.
- Applicant has one dog, >2 years. Breed: German Shepherd.
- Applicant's social media profile shows photos of two cats consistently. We would suggest following up with applicant to confirm if they have an additional pets.

FINANCIAL ANALYSIS

RENT TO INCOME RATIO
26% STANDARD RISK
Rent to Income Ratio risk is based on the applicant rent to income ratio compared to other successful tenants in similar rental markets living in similar property classifications.

DEBT TO INCOME RATIO
39% BELOW AVERAGE RISK
Debt to Income Ratio risk is based on the applicant debt to income ratio compared to other successful tenants in similar rental markets living in similar property classifications.

CASH FLOW ANALYSIS
LOW RISK
Cash Flow risk is based on an internal reconstruction of the applicant's finances compared to other successful tenants in similar rental markets with similar personal characteristics.

CONSUMER BEHAVIOUR ANALYSIS
BELOW AVERAGE RISK
Consumer Behaviour Analysis is based on the applicant's financials, credit data, and social data compared with successful tenants in similar rental markets with similar income levels. This assessment is designed to help landlords understand how a tenant makes financial decisions.

CREDIT CHECK
C 639
The Credit Risk Score is based solely on the applicant's credit financial data and is used to determine finance-ability for mortgages, car loans, and credit. It does not account for age, location, or other factors that may determine tenant quality.

BANKRUPTCY SEARCH: CLEARED
COLLECTIONS: RECORDS FOUND
LIENS / JUDGEMENTS: CLEARED
HIGH RISK OF FRAUD: NO RISK FOUND
TOTAL CONSUMER DEBT: $41401
TOTAL DEBT: $41401

Terms of Service: Naborly Inc. is a third party tenant screening service that collects and analyzes rental applications. We are not liable for the business activities and decision making of our clients. Our report recommendations are intended to assess the likelihood of property damage, payment delinquency, and rental eviction. Naborly, Inc. does not guarantee the accuracy of the data reported to us or the results thereto. Naborly Inc. does not guarantee rental payments or a lack of delinquency or default; even if a tenant was chosen based on a landlords assessment of a Naborly Report or score. Naborly Inc. is compliant with all jurisdictional laws in regards to rental housing. We believe that housing is a human right and we do not discriminate based on race, religion, gender, sexual orientation, marital status, disability, ethnicity, age, or receipt of public assistance.

QUESTIONS ABOUT THIS REPORT?
Customer Support is available daily, 8am-8pm EST
1-844-622-6759 support@naborly.co

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

Appendix – Google Privacy Policies

Platform	Current Policy Date	Word Count
Google Privacy Policy	September 2020	4227
Google Chrome Privacy Notice[65]	May 20, 2020	4692
Google Play Privacy Policy for Books[66]	October 13, 2011	1180
Google Payments Privacy Notice[67]	28 August 2020	1801
Google Fiber Privacy Notice[68]	2020-09-03	1962
Google G Suite for Education Privacy Notice[69]	Undated	1341
YouTube Kids Privacy Notice[70]	August 7, 2019	1434
Privacy Notice for Google Accounts Managed with Family Link[71]	Undated	2028
		18665

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

Endnotes

1 2016 Survey of Canadians on Privacy. Office of the Privacy Commissioner of Canada https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/#fig1

2 Balancing Transparency, Privacy and Expediency in Administrative Proceedings: Finding the Sweet Spot in a Digital Age. Address by Patricia Kosseim, Senior General Counsel and Director General, Legal Services, Policy, Research and Technology Analysis Branch, Office of the Privacy Commissioner of Canada. June 2016. https://www.priv.gc.ca/en/opc-news/speeches/2016/sp-d_20160204_pk/

3 Finding the right workplace privacy balance. Address by Jennifer Stoddart Privacy Commissioner of Canada. November 2006. https://www.priv.gc.ca/en/opc-news/speeches/2006/sp-d_061130/

4 Balance Between Privacy Protection and Information Flows. Address by Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada. November 2007. https://www.priv.gc.ca/en/opc-news/speeches/2007/sp-d_071126_pk/

5 Striking a balance between privacy and national security - Address by Daniel Therrien
Privacy Commissioner of Canada. June 2016. https://www.priv.gc.ca/en/opc-news/speeches/2016/sp-d_20160608/

6 Voluntary Codes Guide – What is a Voluntary Code? Government of Canada. http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00963.html

7 The Privacy Whisperers. Oct 1, 2020. https://www.marieclaire.com/culture/a33898214/how-companies-are-using-data/

8 https://www.sidewalktoronto.ca/plans/economic-development

9 Remarks by Privacy Commissioner of Canada regarding his 2019-2020 Annual Report to Parliament. https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20201008/

10 2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002

11 https://www.privacyshield.gov/welcome

12 Canada's Digital Charter in Action: A Plan by Canadians, for Canadians. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

13 Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

14 Genetic Non-Discrimination Act, SC 2017, c 3https://laws-lois.justice.gc.ca/eng/acts/G-2.5/FullText.html

15 Use of Mobile phones and tablets is a daily activity among preschoolers. https://natureworldreport.com/2015/11/kids-using-mobile-at-a-much-younger-age-video/

16 http://hellobarbiefaq.mattel.com/wp-content/uploads/2015/11/hellobarbie-lines-v2.pdf

17 Mattel Children's Privacy Statement Updated Dec 20, 2019. https://www.mattel.com/en-us/childrens-privacy-statement

18 kidSAFE Seal Program https://www.kidsafeseal.com/aboutourseals.html

19 Undocumented backdoor that covertly takes snapshots found in kids' smartwatch. https://arstechnica.com/information-technology/2020/10/a-watch-designed-exclusively-for-kids-has-an-undocumented-spying-backdoor

20 Canadian city will now be able to predict who might become homeless using AI technology. Reuters. October 15, 2020. https://www.iol.co.za/technology/software-and-internet/canadian-city-will-now-be-able-to-predict-who-might-become-homeless-using-ai-technology-b875bc31-3f95-4e58-b7f9-d6f604e89bd8

21 Tim Hortons facing class-action lawsuit over app location tracking. 20-06-30. https://www.msn.com/en-ca/money/topstories/tim-hortons-facing-class-action-lawsuit-over-app-location-tracking/ar-BB16axi5

22 Google can still use Bluetooth to track your Android phone when Bluetooth is turned off. https://qz.com/1169760/phone-data/

23 UK police say 92% false positive facial recognition is no big deal. 5/7/2018. https://arstechnica.com/tech-policy/2018/05/uk-police-say-92-percent-false-positive-facial-recognition-is-no-big-deal

24 How is Face Recognition Surveillance Technology Racist? June 16, 2020. https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/

25 Losing Face-How a Facial Recognition Mismatch Can Ruin Your Life. October 13 2016. https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/

26 First GDPR Facial Recognition Fine For Sweden School. Aug 22, 2019. https://ipvm.com/reports/sweden-gdpr

27 France Declares School Facial Recognition Illegal Due to GDPR. October 31, 2019. https://ipvm.com/reports/france-ban

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca

Submission to the Ontario Ministry of Consumer Affairs
on the prospect of introducing legislation to
regulate privacy in the private sector

28 San Francisco bans facial recognition technology. May 14, 2019. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

29 Washington state Senate passes bill to rein in facial recognition. 21 February 2020. https://nakedsecurity.sophos.com/2020/02/21/washington-state-senate-passes-bill-to-rein-in-facial-recognition/

30 Massive errors found in facial recognition tech, especially in case of nonwhites: U.S. study. December 20 2019. https://duckduckgo.com/?q=%22Background+Check+Services%22canada+landlord+tenant&t=ffab&atb=v225-1&ia=web

31 Terrifying abduction footage caught on doorbell camera. https://www.news.com.au/world/north-america/terrifying-abduction-footage-caught-on-doorbell-camera/news-story/d5196537f-5c376acd3316b26e3cbf07d

32 Rise of doorbell cameras an 'unmitigated disaster' for neighbourhood privacy: experts. https://globalnews.ca/news/5658796/amazon-ring-doorbell-camera-privacy-police-surveillance/

33 Nest Hello review: Google's smart facial-recognition video doorbell. https://www.theguardian.com/technology/2018/sep/20/nest-hello-review-google-smart-facial-recognition-video-doorbell

34 https://www.tendinsights.com/products/indoor2

35 https://www.honeywellhome.com/us/en/products/security/doorbells/silver-trim-skybell-video-doorbell-dbcam-trim/

36 FACIAL RECOGNITION: TRANSFORMATION AT OUR BORDERS. CIPPIC. October 2020. https://cippic.ca/uploads/FR_Transforming_Borders.pdf

37 Amazon says it's considered face scanning in Ring doorbells. November 19, 2019. https://www.wpri.com/business-news/amazon-tells-senator-its-considered-face-scanning-doorbells/

38 Toward ethical, transparent and fair AI/ML: a critical reading list for engineers, designers, and policy makers. Jan 27, 2019. https://github.com/rockita/criticalML

39 Breaking things is easy. Dec 16, 2016. http://www.cleverhans.io/security/privacy/ml/2016/12/16/breaking-things-is-easy.html

40 Artificial intelligence is hopelessly biased - and that's how it will stay. May 24, 2020. https://www.techradar.com/news/playing-god-why-artificial-intelligence-is-hopelessly-biased-and-always-will-be

41 AI Is Now Analyzing Candidates' Facial Expressions During Video Job Interviews. https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html

42 Psychometrics are regulated in the United States by the Uniform Guidelines on Employee Selection Procedures (1978) as adopted by the US Equal Employment Opportunity Commission, and professional testing standards (American Educational Research Association, American Psychological Association, & National Council on Measurement in Education, 1999; Society for Industrial and Organizational Psychology, 2018)

43 Facebook study: Frontline workers don't feel valued or empowered. October 15, 2020. https://www.techrepublic.com/article/facebook-study-frontline-workers-dont-feel-valued-or-empowered/

44 Building emotionally aware cars on the path to full autonomy https://venturebeat.com/2017/02/11/building-emotionally-aware-cars-on-the-path-to-full-autonomy/

45 Continental puts face and fingerprint recognition in cars at CES 2017. https://www.cnet.com/roadshow/news/continental-puts-face-and-fingerprint-recognition-in-cars-at-ces-2017/

46 Sternberg Lighting Intellistreets Products. tPLyipKxyMwhttp://www.sternberglighting.com/intellistreets/

47 Intellistreets DHS Smart Street Light System. https://www.youtube.com/watch?v=

48 Iris Recognition as an Emerging Technology for Connected Cars. http://www.iritech.com/blog/iris-connected-car-0317/

49 Facial-recognition technology comes to the car. http://www.autonews.com/article/20170116/OEM06/301169990/facial-recognition-technology-comes-to-the-car

50 ITS JPO Policy and Institutional Issues. https://www.its.dot.gov/factsheets/policy_factsheet.htm

51 Jury Still Out on Automaker Data Deals. October 8, 2020. https://www.tu-auto.com/jury-still-out-on-automaker-data-deals/

52 CalAmp iOn™ Vision is a fully integrated video telematics platform that provides actionable video intelligence to boost driver safety, proactively protect fleets and help mitigate potential legal liabilities stemming from roadway accidents and incidents. https://www.calamp.com/ionsuite/

53 Nissan Canada Privacy Policy. http://www.nissan.ca/en/privacy.html?next=footer.privacy.link#!

54 "We have established retention policies and procedures to ensure that when the retention period expires, your personal information will be removed from our systems and destroyed in a secure manner." http://www.ford.ca/help/privacy/

55 OnStar LLC Privacy Statement for Application Services Last Updated April 1, 2016 https://www.onstar.com/content/dam/onstar-web/temp-footer/Vehcile%20Mobile%20App%203.1.0%20Privacy%20Statement%20US.pdf

56 Can Amazon talk its way into autos? http://www.autonews.com/article/20170624/MOBILITY/170629883/amazon-alexa-auto-industry

57 General Motors Family of Companies privacy statement Last Updated January 1, 2017. https://www.onstar.com/us/en/footer-links/privacy-policy.html "Given the nature of our products

Privacy and Access Council of Canada — Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440 | 10816 Macleod Trail SE |Calgary AB Canada T2J 5N8 | 877.746.PACC | 877.746.7222

and services, there may be times when someone other than you is using one of the products and services we provide to you (for example, you let someone else drive your vehicle). We rely on you to inform such person about this Privacy Statement and the privacy choices you have made."

58 Connected Vehicle Weather Data for Operation of Rural Variable Speed Limit Corridors. http://www.ugpti.org/resources/reports/downloads/mpc15-299.pdf

59 FCA Canada Inc. Privacy Policy. http://www.fcacanada.ca/privacy/privacy_statement.pdf

60 Google Privacy Policy effective September 30, 2020. https://policies.google.com/privacy?hl=en&gl=ca#content

61 Rethinking Privacy Agreements. March 2020. https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Privacy-Agreements.pdf

62 Rethinking Privacy Agreements. https://www.csagroup.org/article/research/rethinking-privacy-agreements/

63 Paul v. British Columbia (Forest Appeals Commission), [2003] 2 SCR 585, 2003 SCC 55 (CanLII). In that case, the Court held that British Columbia could empower a tribunal to adjudicate questions of aboriginal rights, which—unlike solicitor-client privilege—are explicitly protected under section 35 of the Constitution Act, 1982.

64 University of Calgary v. Alberta (Information and Privacy Commissioner), [2016] 2 SCR 555, 2016 SCC 53 (CanLII).

65 https://www.google.com/chrome/privacy/

66 https://books.google.com/googlebooks/privacy.html

67 https://payments.google.com/payments/apis-secure/get_legal_document?ldo=0&ldt=privacynotice

68 https://fiber.google.com/legal/privacy/

69 https://workspace.google.com/terms/education_privacy.html

70 https://kids.youtube.com/t/privacynotice

71 https://families.google.com/familylink/privacy/child-policy/