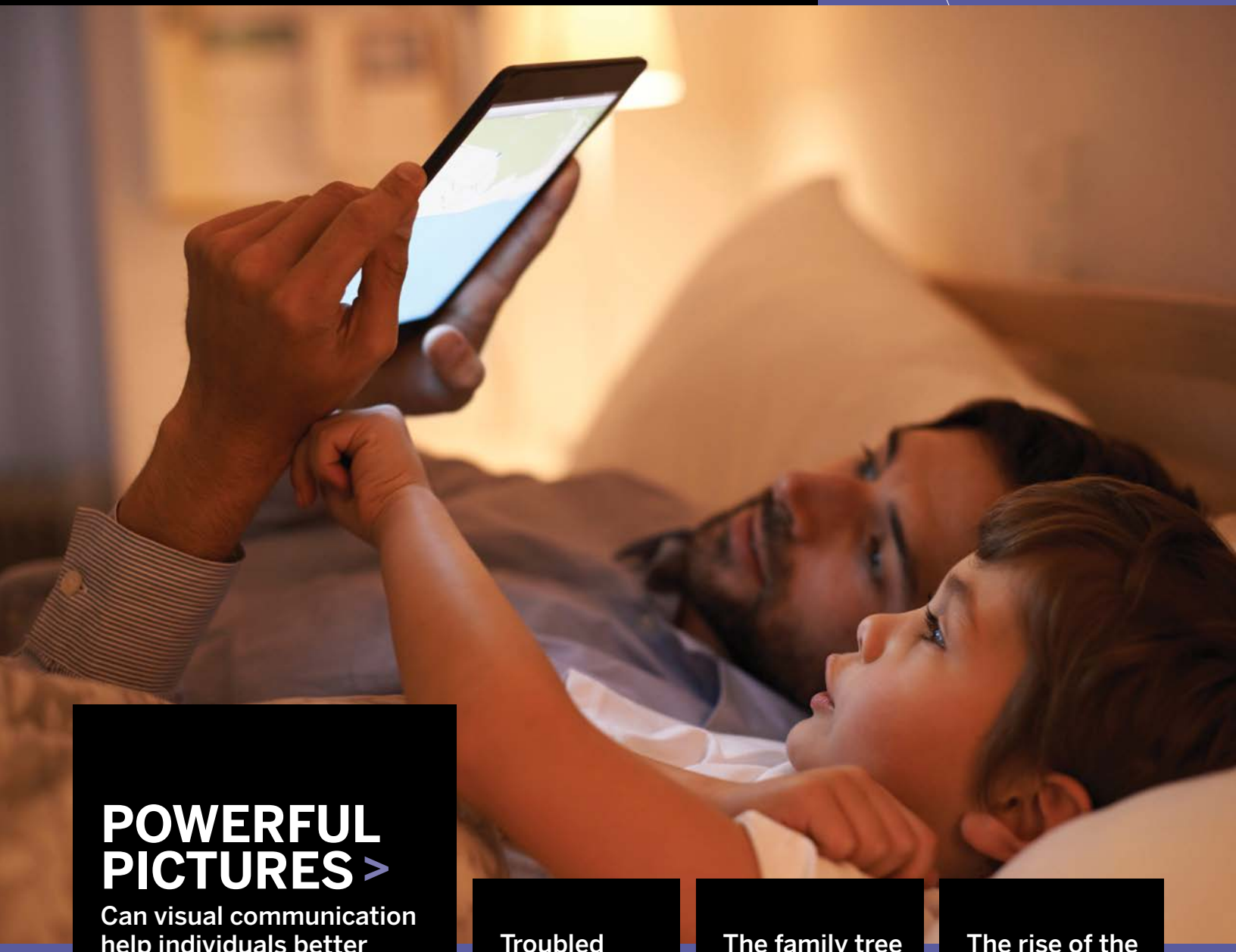
REAL RESULTS

PROTECTING PRIVACY RIGHTS
THROUGH INNOVATIVE RESEARCH

VOL. 2

Office of the
Privacy Commissioner
of Canada



POWERFUL PICTURES >

Can visual communication help individuals better protect their privacy?

Exploring privacy through games, comics and infographics

Troubled by the past

Are background checks revealing more than just criminal convictions?

The family tree goes digital

A new documentary film explores the privacy risks of ancestral searches

The rise of the connected car

Is privacy taking a back seat in Internet-enabled cars?

Contents

The OPC's Contributions Program funds independent privacy research and knowledge translation projects. The opinions expressed by the experts featured in this publication, as well as the projects they discuss, do not necessarily reflect those of the Office of the Privacy Commissioner of Canada.

Cat. No. IP51-5E-PDF
ISSN 2291-5036

INTRODUCTION

The issue of privacy has been intertwined with the Internet ever since our lives moved online. Worries about security breaches, identity theft, and web tracking are nothing new.

As technology marches on, new privacy issues are constantly surfacing. Data moves at lightning speed. Connectivity is being embedded in the "things" all around us—our mobile devices, body sensors, homes, and even our cars. We can store and analyze colossal amounts of "big data."

But at what risk to our privacy?

Genealogical databases now contain billions of online records. This personal information can be aggregated and sold to the highest bidder, and is being entwined with medical records and genetic sequencing data—for purposes as yet mostly unknown.

As we get behind the wheel of Internet-connected cars, our activities can be tracked, monitored and mined—potentially making us unwitting generators of location, demographic and marketing data.

As kids play with more online games and Internet-connected toys, they may not know how to protect their personal privacy and avoid being data mined.

Sometimes our ability to get a job, go on holidays across the border, or volunteer as a coach on our kids' soccer team can be at stake.

Even a slight brush with the law in years past—as a suspect or even as an individual seeking medical assistance—can culminate in non-conviction information, including sensitive mental health data, being kept in police databases and shared indeterminately with potential employers and volunteer managers.

Many online innovations have made our lives easier, more convenient and more enjoyable. Some have even improved our safety. But are we trading away our privacy in exchange for the perks of the digital age?

Where does our data trail lead? Who owns our personal information? And how can we protect it in the digital age?

How can we develop new tools, skills, knowledge and mental models to understand privacy issues and take control of our personal information?

These are complex questions, which researchers from across the country set out to address with funding by the Office of the Privacy Commissioner of Canada.

REAL RESULTS

The Office of the Privacy Commissioner's Contributions Program funds independent research and related knowledge translation initiatives aimed at generating innovative ideas, approaches and information about privacy in Canada. These projects not only advance the collective knowledge on privacy, they provide real, tangible research results that Canadians can use to make smart decisions about privacy protection in their own lives and that organizations can apply in practice to enhance compliance with their privacy obligations.

The projects highlighted here represent a recent sample of the innovative and socially relevant independent research the Office of the Privacy Commissioner of Canada has supported through its Contributions Program.

Along with providing information about the projects themselves, *Real Results* features the commentaries and ideas of the independent researchers behind the projects. While the opinions expressed do not necessarily reflect those of the Office of the Privacy Commissioner of Canada, they offer unique perspectives on the issues and help articulate the practical value of the privacy research we fund.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

The Privacy Commissioner of Canada is mandated by Parliament to protect privacy in Canada. The Commissioner enforces two laws for the protection of personal information: the *Privacy Act*, which applies to the federal public sector; and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal private sector privacy law.

As the public advocate for privacy rights in Canada, the Privacy Commissioner is mandated to raise public awareness and foster understanding of privacy rights through a number of ways, including research. Through its Contributions Program, the Office funds research that falls within the scope of PIPEDA, which sets ground rules for how organizations may collect, use or disclose information about individuals in the course of commercial activities.

POLICE BACKGROUND CHECKS

Are They Revealing Too Much?

You've applied for your dream job, but instead of an employment offer, you receive the dreaded rejection letter.

It's possible you weren't as qualified as the other candidates. But what if you were rejected because of a criminal charge that was dropped two decades ago? Or a long-ago mental health incident in which the police were called?

Having this information disclosed can result in substantial barriers to employment, education and volunteer opportunities, cross-border travel, and some social services.

"It's an unfair practice that could affect thousands of ordinary, innocent people," notes Berger.

MILLIONS OF RECORD CHECKS CONDUCTED EVERY YEAR

Even the CCLA was initially surprised by the scope of the problem. After releasing its first report on the subject in 2012, "Presumption of Guilt? The Disclosure of Non-Conviction Records in Police Background Checks," the organization was contacted by dozens of individuals seriously impacted by the disclosure of non-conviction information.

People are often very surprised to find out what information can be disclosed in a police record or background check.

Most people assume that if they don't have a criminal record—meaning they've never been convicted under the Criminal Code—they'll successfully pass a background check. So why worry?

According to Laura Berger, Acting Program Director of the Canadian Civil Liberties Association (CCLA), prospective employees and trainees could have plenty to worry about when it comes to background checks—whether they know it or not.

"People are often very surprised to find out what information can be disclosed in a police record or background check," explains Berger. "Most people assume that only criminal convictions are included, but virtually any information the police collect and store about an individual can be shared."

Prospective employees and trainees may lose out on a job because of a long list of non-conviction information. What's on the list? Being charged with a crime, but never convicted. Being acquitted of a crime altogether. Being named during a police investigation. Calling 911 for a mental health crisis. And on it goes….

"We thought our report would be popular with law nerds and end up as a reference tool," explains Berger. "But we received a flood of calls and emails from people who were personally affected. We were truly taken aback by how widespread the problem is."

As part of a more recent research project funded by the Office of the Privacy Commissioner's Contributions Program, "Police Background Checks and the Private Sector," the CCLA zeroed in on private organizations, as well as non-profit organizations requesting background checks as part of routine hiring and management practices.

The research found that "police forces across the country are running millions of record checks per year, and are disclosing information that goes far beyond convictions and formal findings of guilt."

'The private sector sees it as a way to mitigate risk," notes Berger. "They're concerned about

protecting their clients and their assets. They may feel pressure to run record checks by their insurance companies, as well as regulatory or contract requirements. But most have not developed any policy guidelines to interpret what is relevant in a person's history, and what is not."

The application of privacy and human rights legislation is another matter. According to the research report, such legislation is inconsistently applied in the employment context. In part, that's because there's a "patchwork of different laws that apply to different pieces," explains Berger.

All Canadian human rights legislation prohibits discrimination based on mental illness, but only some provinces and territories provide human rights protection for individuals with past police contact. In those instances, affected individuals can contact their local human rights commission or a legal clinic that deals with complaints.

CCLA is calling for concrete reforms to increase respect for privacy, human rights and the presumption of innocence. The organization also argues for "reintroducing perspective and balance to the societal use of police record checks."

However, Berger foresees the problem getting much worse before it gets better. "Requests for background or police record checks from

True stories

Countless individuals who have been impacted by the disclosure of non-conviction information shared their stories with the CCLA. Here are just a few excerpts from the research report:

GABRIEL went to the police for advice after he got a text message threatening his life. The police arrested the woman who sent the text message—and the day after she was released on bail, she went to the police and made a series of serious allegations against him. Two days later Gabriel was arrested and charged. Months afterwards all the charges against him were withdrawn—but the police refused to destroy the records.

ROBIN was 18 and pregnant when her male roommates started dealing drugs out of the apartment. She tried to find a new place to live, but before she could move, the police came and charged everyone who lived there with trafficking. The charges against her were withdrawn, but her record has followed her, preventing her from pursuing her career and furthering her education.

LOIS was trying to board a flight to Los Angeles to spend Thanksgiving with family when she was pulled over by American border officials for secondary screening. She was told she was not able to cross over to the United States because Toronto police had attended her home years earlier after a 911 call for medical assistance.

JANE AND JOHN'S DAUGHTER was a straight-A student nearing the end of a nursing program. She had passed multiple background checks while at school. But suddenly one of these checks brought up an incident from years earlier, where the police had taken her to hospital under a mental health act.

CHRIS had been accepted as a volunteer firefighter in his small town and was several months into training when he realized that his vulnerable sector check listed him as the subject of a drug investigation. Chris had never even been questioned by the police, much less charged with any offence. He assumes that his name was entered into police databases because he had a friend who was arrested and charged with drug offences—Chris had met the undercover officer who was investigating his friend, but Chris was never questioned by police or charged with anything.

Visit the CCLA's microsite for more stories and full recordings: www.ccla.org/recordchecks/resources

Sidebar adapted from CCLA content

What is a criminal record?

It seems like a basic question. Unfortunately, Canadian law and police policies do not offer a simple answer. We have outlined three basic categories of police records below.

Information from all of these categories can potentially be disclosed on a police record check—including in the case of people who have never been convicted or found guilty of a crime. What exactly will be disclosed depends on the police service's policies and the level of record check an individual requests.

Please note that this information applies to adult records only—if you think you may have a youth record, you should look for specific information guides on youth records.

Criminal conviction

- Custodial sentence
- Intermittent sentence
- Suspended sentence
- Conditional sentence
- Fine or forfeiture

Non-conviction: Finding of guilt

- Absolute discharge
- Conditional discharge

Non-conviction: No finding of guilt

- Police contact and surveillance
- Mental health apprehension
- Charges withdrawn
- Charges withdrawn—"alternative measures" or diversion
- Acquittal at trial
- Stay of proceedings

Sidebar adapted from CCLA content

OPC RESOURCES

TAKE THE NEXT STEP

Want to know what a police record is? How to try to deal with a non-conviction record? What privacy and human rights laws apply, or best practices for employers?

The CCLA has developed a series of guidelines and information sheets on all these topics. Read more at www.ccla.org/recordchecks/resources.

Canadian organizations are on the rise. More and more organizations are requiring police record checks as part of their basic hiring and management practices."

Such requests are coming not only from employers, but also volunteer managers, educational institutions, licensing bodies and governments.

WHAT YOU DON'T KNOW COULD HURT YOU

Ironically, many people applying for jobs and training positions will never know that a non-conviction record was responsible for their inability to obtain a desired position. That's because they may never be told they were rejected because of non-conviction information disclosed during a routine background check.

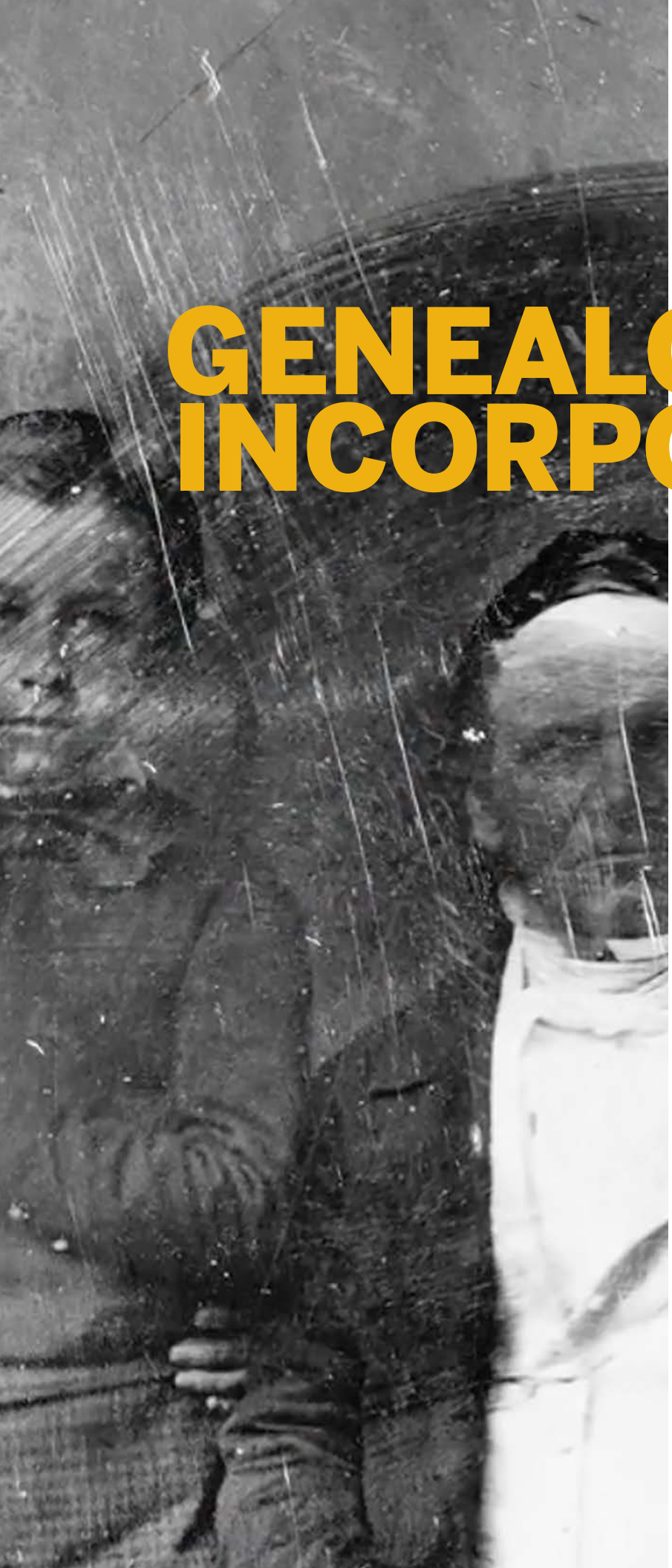
For individuals who have had contact with the law, Berger recommends they request a copy of their criminal record to see what information shows up.

If someone suspects they've been adversely affected, do they have recourse? Where can they turn?

One option is to apply to police services to have certain information "purged" or "supressed," though not all police services have procedures in place to do this. Alternatively, individuals may contact human rights commissions or legal clinics to file a complaint.

The CCLA has developed extensive resources and educational materials to help people understand their rights and what steps can be taken if they've been discriminated against based on non-conviction information. They've also developed best practices for employers in an effort to increase awareness of their legal obligations and curb their appetite for non-relevant information.

"We're tackling this issue from multiple angles," says Berger, "including educating employers so we can push back against their instincts to use background checks as a risk management tool. They're not bulletproof." R



GENEALOGY INCORPORATED

"Who came before us?" Seeking the answer to this question has made genealogy an exceedingly popular pastime in Canada.

Whether it's the discovery of a minor aristocrat, a political reformer, or even a small-time criminal, people are deeply invested in finding out more about the characters who populate their family histories and their countries of origin—if for no other reason than to have a good story to tell. Interest has also been primed by celebrity genealogies revealed on TV shows such as "Who Do You Think You Are?"

Previously a rather painstaking pursuit involving sending letters and making personal visits to archives, courthouses, churches, and libraries to request copies of records and information, genealogical research nowadays has gone viral thanks to the ease of conducting such research on the Internet.

Billions of marriage and death certificates, government census records, ship passenger lists, military histories, city directories, family photos and other data have been uploaded to the Internet by individuals, non-profit organizations, and for-profit genealogical companies. And the rush to digitize ancestral information shows no signs of abating.

But who owns this information? And who will protect it over time?

A documentary about genealogy finds a whole new set of privacy issues arises when personal information is added to online databases and aggregated. *Below*: Director Julia Creet and a series of production stills from the film.

FAMILY SECRET SPARKS DEEPER SEARCH

About a decade ago, spurred on by the desire to uncover a family secret, Julia Creet embarked upon her own ancestral quest. Searching for information about her mother, who had hidden her Jewish identity after surviving the Holocaust, Creet spent years combing through family archives and a trail of documents.

The more she probed, the more she began pondering the business of genealogy itself.

"I started getting the sense that many, many people were doing genealogical research and that there was a whole other context to this enterprise," explains Creet, an Associate Professor of English at Toronto's York University. "I started to wonder: If I'm part of the genealogical 'zeitgeist', are my motivations purely individual or are they being driven by larger forces?"

These nagging questions sparked a deeper investigation into the reasons for genealogy's exponential growth, and eventually inspired Creet to make a documentary film: *Data Mining the Deceased.*

Made with funding support from the Office of the Privacy Commissioner of Canada's Contributions Program, the film documents Creet's quest to unearth the genealogy industry's key players and examine their motivations. Along with thorny questions about racial identity, the film raises concerns about the ownership and privacy of personal data, particularly the merging of genetic and genealogical information.

"I didn't start out looking at privacy issues, but it quickly became apparent that there were tensions even within my own family. Not everyone wants family secrets to become public," explains Creet. "A whole new set of privacy issues arises when personal information is added to online databases and aggregated. When you connect that information to genetic information, what you're giving away is much more valuable than what you're getting in return."

> "Not everyone wants family secrets to become public… A whole new set of privacy issues arises."

ICELAND'S FAMILY TREE

The film initially follows Creet to Iceland, which has the most complete genealogical database in the world. Records have been kept since the ninth century, shortly after the isolated island was settled.

Iceland's situation drew worldwide attention when, starting in the 1990s, private genetics company deCODE sought to link DNA research to Iceland's national health system population resources, with the aim of discovering genetic risk factors for common diseases.

The company also provided funding to accelerate the digitization of Icelanders' genealogical records, and asked for volunteers to donate their DNA. It later received a 12-year licence from the government, along with permission from the country's data protection authority, to access nationalized medical records. Although that access was later revoked after a public outcry, tens of thousands of records had already been transferred to the company.

"Iceland is a canary in a coal mine. When deCODE started braiding genetic information with genealogical information, privacy issues started to surface. Some people started to object to their medical history becoming part of a

privately owned database," states Creet, noting that deCODE has since been sold to US biotech giant Amgen, further complicating issues of data ownership.

"Few people read the fine print," Creet continues, "but when you give your DNA to a private database, they have complete proprietary rights. They can aggregate it, sell it to other companies, and sell it for research—by non-profit institutions or for-profit companies."

BILLIONS OF RECORDS NOW ONLINE

Even when non-profit databases are created by volunteers guided by a religious mission, corporate interests may eventually become involved, as Creet discovered when she began unpacking the relationship between the Mormon Church's free FamilySearch database and ancestry.com, owned by Ancestry, "the world's leading family history brand." The site has two million paying subscribers who can access over 16 billion records.

Mormons believe they should offer baptism to dead relatives. To help members trace their family tree, the Church of Jesus Christ of Latter-day Saints (LDS) has amassed about thirty times the amount of information held by the Library of Congress—and new records are continually being added. FamilySearch now contains an estimated one-quarter of the human race's genealogical information. Using the site's substantial records, the church aims to build a family tree of as many people in the world as possible.

In the film, Creet interviews executives from FamilySearch and co-founders of Ancestry, revealing strategic partnerships between the two. Over the years, numerous LDS databases have been sold to Ancestry. In one recent deal, FamilySearch agreed to release one billion international digitized genealogical records online over five years for Ancestry subscribers.

When Creet broaches the subject of privacy with Ancestry's co-founders, they admit it's "at best a gray area."

"I think there's protection for living people...," states one former Ancestry executive, "I'm not sure there is any movement or any effort to try to protect any records that pertain to people who are no longer living."

Building a family tree using online databases can put your privacy at risk.

Ancestry is now charging users to submit their DNA to "uncover your ethnic mix, discover distant relatives, and find new details about your unique family history with AncestryDNA." The company recently sold access to its DNA database to Calico, a genetic company backed by Google, which intends to examine genetic patterns in people who live long lives.

A CAUTIONARY TALE

"Most people who purchase these services do not read company privacy policies beforehand," Creet says. "Private companies are accumulating vast amounts of vital information. Much of that information is donated by users and then bought and sold. We really have no idea how the information will be used, but it could have implications for insurability and employability. We've all seen how an old Facebook post can come back to haunt you."

Ultimately, Creet's film is a cautionary tale for anybody undertaking genealogical research. Her advice for individuals pursuing their family histories? "If you want to guard your privacy, stay away from online databases. Ask other family members about your shared ancestors. After two or three generations, the stories are mostly fiction anyways." R

Julia Creet can be contacted at creet@yorku.ca.

To inquire about screening Data Mining the Deceased*, please contact the film's distributor at www.vtape.org or info@vtape.org.*

LEARN MORE

View a synopsis of the report and clips from the film: http://past-productions.apps01.yorku.ca/need-to-know/synopsis/

THE CONNECTED CAR

Privacy Risk on Wheels?

Is your car keeping an eye on you? If this sounds like something straight out of a Bond movie, consider that, by 2020, an estimated 90 percent of all new vehicles will have built-in connectivity. >

The "connected" car has in-car Wi-Fi and a built-in 3G modem to provide its own Internet connection. Car manufacturers are now racing to add new features to make their own connected cars stand out from the competition.

The latest in-vehicle telematics systems go beyond simple engine controls and car diagnostics to deliver more responsive navigation and roadside assistance (a vehicle can call 911 the moment an accident happens), consumer-like "infotainment" apps, enhanced voice-activated technology, and many more whiz-bang features.

It's thanks to the Internet of Things, or "IoT," that the car is morphing into a smartphone on wheels. With IoT, everyday objects and devices can be embedded with electronics, software, sensors and network connectivity. Built-in connectivity enables cars to talk to other cars to avoid crashes. It also enables cars to communicate with a nascent Internet-enabled transportation infrastructure to improve safety and combat traffic congestion. These government-run "Intelligent Transportation Systems" (ITS) planned for Canada will eventually connect smart emergency vehicles, trucks, trains, traffic signals, and other devices.

Even now, some connected cars can capture images of their drivers to detect fatigue. Many can report bad driver behaviour, like speeding and hard braking. And most can track a driver's every movement with sophisticated on-board geolocation technology.

CONVENIENT, BUT "CREEPY"?

Undoubtedly, some of these features will benefit drivers by delivering improved safety, efficiency and enjoyment. But when does the convenience factor turn into the "creep factor"? What are drivers signing up for when they get behind the wheel of a connected car?

Such questions preoccupy privacy advocate Philippa Lawson, a lawyer, and a researcher affiliated with the BC Freedom of Information and Privacy Association (FIPA).

Principal researcher of "The Connected Car: Who's in the Driver's Seat?"—a recent report funded by the Office of the Privacy Commissioner of Canada's Contributions Program—Lawson acknowledges that a vehicle's high-tech features can enhance driving experience and improve safety. But she worries about the steep cost to privacy.

"Their car can potentially track where they go, who they're with, how they're driving, and what they're doing while in their cars. When combined, this data can provide a very detailed profile of someone's private life."

The report takes a close look at many connected car features, such as vehicle monitoring devices, voice and video recorders, biometric scanners for driver identification, and geolocation tracking. What do most of these have in common? They can produce a stream of data that can be sent to manufacturers, insurance companies, and marketers—virtually unbeknownst to drivers.

"Connected cars are different from smartphones because they can generate so much data," Lawson explains. "Very few drivers understand the extent to which this data can be of a very personal nature: Their car can potentially track where they go, who they're with, how they're driving, and what they're doing while in their cars. When combined, this data can provide a very detailed profile of someone's private life."

The potential for a loss of privacy, whether by hacking or state monitoring, is enormous, according to Lawson.

"Many of us think of our cars as extensions of our homes," Lawson explains. "Imagine you're at home and your every move is being tracked, images are being captured of your activities, and your conversations are being recorded. And some of this data is being sent to external organizations for unknown purposes without your informed consent. No one would stand for it."

DATA MINING DRIVERS

For Lawson, the ease with which geolocation

Navigating the road ahead

A broad set of recommendations for mitigating privacy risks inherent in new high-tech vehicles

"The Connected Car: Who's in the Driver's Seat?"—a recent report funded by the Office of the Privacy Commissioner of Canada's Contributions Program—sets out the following four recommendations to enhance privacy protections in connected cars:

RECOMMENDATION #1:

Establish data protection regulations for the connected car industry.

Data protection regulations for the automobile industry could be enacted under the regulation-making powers of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and related provincial legislation. Security-related regulations could also be enacted under the federal *Motor Vehicle Safety Act*, alongside the existing Canada Motor Vehicle Safety Standards.

RECOMMENDATION #2:

Develop national data protection standards for usage-based insurance (UBI).

UBI is regulated at the provincial level, and is only just beginning to be offered in Canada. Rather than having each provincial and territorial regulator develop its own set of standards for UBI, a working group should be established with industry stakeholders including the Insurance Bureau of Canada, the Insurance Brokers Association of Canada, insurance companies, provincial associations, provincial regulators, and the federal and provincial privacy commissioners to develop national standards for use by each provincial/territorial regulator.

RECOMMENDATION #3:

Involve privacy experts in the design stage of Intelligent Transportation Systems, including connected vehicle research projects.

This study did not focus on public sector "Connected Vehicle" or V2V initiatives, but there is clearly a need for privacy to be designed into these initiatives. While there appears to be widespread acknowledgement of the need to ensure data privacy in the design of such systems, it is not clear to what extent privacy experts are involved in current research and design initiatives.

RECOMMENDATION #4:

Adopt privacy by design principles and related tools.

It will take time to develop data protection standards for the Connected Car industry and to incorporate them into industry regulations. In the meantime, automakers and other industry players should adopt 'Privacy by Design' principles and tools such as Privacy Impact Assessments to bring themselves into compliance with Canadian data protection law and to prepare themselves for industry-specific regulation.

The following recommendations begin with a list of specific actions that individual organizations should take internally, followed by collaborative actions to develop tools that could be used by all parties to the benefit of the industry and consumers:

- Establish a privacy management program
- Identify and avoid unintended uses
- Be open and transparent
- Respect for user privacy: keep it user-centric
- Work with device manufacturers, OS / platform developers, network providers, application developers, and data processors to integrate controls and data minimization techniques.

and other tracked information can be used for data mining and market research is also worrisome.

Marketers are gleeful not only about directly marketing new apps, rewards and services to drivers, who become unwitting prospects, but increasing brand attachment—with the car conveniently acting as central hub for these activities.

"It can seem really creepy if you drive past a coffee shop and a personalized coupon for the shop's donuts flashes on your car's infotainment screen," notes Lawson. "But the other issue is that your behaviour profile may have been sold to advertisers without your knowledge or consent. Most connected-car drivers would be surprised to find out they're generating marketing data every time they drive."

Assuming that drivers are even aware of the presence of monitoring systems in their cars, can they opt out of the unnecessary collection, use and disclosure of personal information?

"For the most part, it's 'all or nothing'," explains Lawson, "There is no opt-out of non-essential uses, which are common and sometimes open-ended. There is some variation by manufacturers and service providers, and most do let you opt out of receiving marketing messages, but one of our key findings is that if you want the service, you are forced to agree to an often open-ended array of unnecessary collection, use, or disclosure of your personal information."

Becoming an avid reader of privacy agreements is not the answer. In one connected car alone, Lawson identified more than a dozen after-market manufacturers, most with their own heavily legalistic usage agreements. Some don't even bother to provide agreements, presuming consent by the mere fact that a driver has purchased the vehicle and used the feature.

ADOPTING "PRIVACY BY DESIGN"

To remedy privacy concerns, which are not unique to connected cars, one of the report's recommendations is for manufacturers to adopt "privacy by design" principles.

"Manufacturers should involve privacy experts in the design stage of connected cars and Intelligent Transportation Systems, so privacy protections can be built right into systems from day one," argues Lawson.

"Manufacturers should involve privacy experts in the design stage of connected cars and Intelligent Transportation Systems, so privacy protections can be built right into systems from day one."

Along with manufacturers and marketers, the report identifies insurance companies as requiring special oversight. Under usage-based programs, drivers can voluntarily enable their vehicle management systems to send detailed information about their driving behaviour—such as acceleration, braking and speed—to insurance companies.

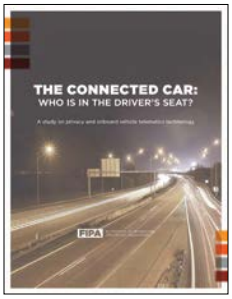
Noting that several insurance brokers in Ontario and Quebec offer reduced rates for drivers who agree to be monitored under these programs, the report foresees a day when insurance companies could make these programs mandatory, so they can keep a watchful eye on a driver's driving behaviours—and make "bad drivers" pay stiffer premiums.

Given the inherent privacy risks sparked by these cars, the report argues that governments must step up to regulate the burgeoning connected car industry. The report calls for standardized regulation on what kind of data can be shared, and Canada-wide data protection standards for usage-based insurance, to guard against undue privacy invasion.

"Market forces will not resolve these mounting privacy issues," states Lawson. "Car manufacturers won't voluntarily self-regulate because consumer demand does not drive privacy the way safety and emissions do. We also cannot rely on self-regulation for behind-the-scenes, personal data gathering. We need concrete hard standards, not meaningless consent mechanisms." R

LEARN MORE

Access the report at:
https://fipa.bc.ca/connected-car/



THE POWER OF VISUAL COMMUNICATION

Exploring privacy through video games, comics and infographics

Sometimes a picture is worth a thousand words—especially when those words are describing highly complex topics like online security, data mining and privacy policies to youth and young adults.

To help young people become more aware of how to protect their privacy in the digital age, two research teams funded by the Office of the Privacy Commissioner's Contributions Program used creative visual methods ranging from video games to comics and infographics.

To help young kids, along with their teachers and parents, become savvier about online privacy issues,

VISUALIZING PRIVACY

MediaSmarts—a Canadian not-for-profit charitable organization for digital and media literacy—created a game called "Privacy Pirates." As they play the game on a desktop computer, iPad, or smartphone, children assemble a map leading to a pirate treasure. Why pirate treasure? The researchers designed the game to help kids understand they have something valuable—personal information or a "treasure"—which others may want.

Meanwhile, another research team at Carleton University employed visual techniques to help young adults improve their "mental models" of online security and privacy. The team used infographics and interactive comics with relatable characters to explain threats like malware and geo-tagging. These entertaining materials were then put to the test to see if they helped users take more security measures.

TWO TEAMS ARE BETTER THAN ONE

After learning about each other on the Office of the Privacy Commissioner of Canada's website, the two research groups discovered mutual interests and are now collaborating on a number of projects. Students working on the Carleton project bring experience in graphic design, computer science, and human-computer interaction, which nicely complements MediaSmarts' expertise in educational development.

MediaSmarts will be integrating cybersecurity comics developed at Carleton into a digital literacy framework the organization is launching, with the aim of extending the framework's reach into more age groups.

Students at Carleton are now involved in a 'reboot' of one of MediaSmarts' older games. Together, the two groups are completely revamping the game, including adding new lessons in cybersecurity, an updated storyline and visual design, and scenarios and outcomes that mirror kids' daily lives.

Through the OPC Contributions Program, the two research teams have discovered exciting synergies and are leveraging their resources and capacity to further advance privacy protection for Canadian youth.

HELPING KIDS PROTECT THEIR PRIVACY ONLINE? THERE'S AN APP FOR THAT!

Kids' online play is being monitored, tracked, and mined for commercial purposes. Now there's a game to help kids understand their privacy rights.

It's a marketer's dream-come-true.

A young boy visits a popular kid-friendly website, and is asked to share some personal information to register. To access premium content, he's asked to disclose a little more personal information. A contest suddenly pops up on the screen. The price of getting a chance to win? Sharing a few more personal tidbits about himself and his friends.

He hasn't even played the game yet, and his privacy may already be at risk. But the worst may be yet to come.

Mitigating Kids' Privacy Risks: Tips and Tricks

It's next to impossible to keep kids away from online games and connected toys. But there are ways to help them safely navigate online to mitigate privacy risks.

"The idea we always try to get across to kids is the permanence and replicability of online information. Once something is online, it can live online forever," says Matthew Johnson, Director of Education at MediaSmarts, a Canadian not-for-profit charitable organization for digital and media literacy.

"Our ultimate goal is to teach general skills, rather than just how to set your privacy settings on Facebook this month. Online sites are always changing, so it's knowing the general principles that will help protect you over time."

HERE ARE SOME TIPS FROM MEDIASMARTS:

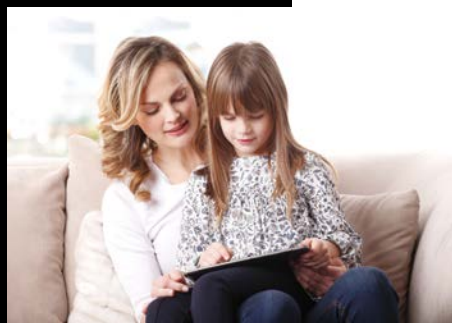
> Give out as little information as possible. If asked to register with websites to play games, win prizes, engage in chat or join clubs, consider using an alias.

> When registering for an online game, only answer mandatory questions, which will be marked in some way, such as by a different text colour or by an asterisk. Leave the other ones blank. Beware of innocent-sounding questions asking about favourite colour or cereal—it's not immediately obvious but these are being asked to build a demographic profile.

> Delete or limit the installation of cookies, which can track activity every time a website is visited. These files can be used by marketers to create customer profiles and deliver customized information to young visitors.

> Beware of the integration of apps, games and websites with social media sites like Facebook. Kids might end up sharing more information than they realize this way.

> Limit Wi-Fi access so toys can't be connected to the Internet.



As he chooses characters, makes choices, and chats with other players, data about his preferences, behaviours, and conversation topics can now stream directly into the hands of marketing teams.

The data can be aggregated, scanned, and sorted into demographic and behavioural profiles. These profiles can be sold to advertisers, who create online ads targeting kids who share similar demographics and behaviours.

It's a potential gold mine for marketers and advertisers, but is it potentially harmful for kids?

"The ultimate goal for advertisers is finding better ways of targeting their products to people," says Matthew Johnson, Director of Education at MediaSmarts, "but many parents will be surprised that these companies are essentially 'watching' their kids online. While they may not be collecting individualized information, we know that they build profiles that can be provided to advertisers."

The Canadian not-for-profit charitable organization for digital and media literacy has been closely monitoring the phenomena of using kids for data mining.

"Our research has shown that youth like the idea of targeted ads, but they don't like the idea of marketers collecting data about them and watching them online," says Johnson.

"What's also of concern is that children and their parents are not typically very knowledgeable about privacy laws and their rights," adds Johnson. "They don't typically know how these commercial companies will protect and use their information."

WHO'S READING THE FINE PRINT?

Johnson points to Hello Barbie as one example. The Wi-Fi-connected doll uses a technology called "interactive voice response" to "chat" with children. At the mere push of a button on the doll, these recorded conversations are uploaded to servers operated by ToyTalk, Mattel's partner.

The fine print discloses that ToyTalk can use the recorded conversations for "data analysis purposes" and share them with "vendors, consultants, and other service providers."

"Mattel is upfront about the fact that they're collecting information," notes Johnson, "but nobody knows what they're going to do with that data."

LEARN MORE

Access the game and related information at: http://mediasmarts.ca/game/privacy-pirates-interactive-unit-online-privacy-ages-7-9

OPC RESOURCES

Youth privacy web page: www.priv.gc.ca/youth-jeunes/index_e.asp

SHIVER-ME-TIMBERS: PIRATE GAME HELPS KIDS PROTECT PRIVACY

To help kids, along with their parents and teachers, become savvier about these issues, MediaSmarts created an online game in 2011 called "Privacy Pirates" with funding support from the Office of the Privacy Commissioner of Canada's Contributions Program.

Originally created for playing on a desktop computer, the game is now available as a downloadable app for tablets and smartphones.

Designed for children aged seven to nine—the average age MediaSmarts research found that kids are starting to use digital devices unsupervised for the first time—the game comes with an intro tutorial on the concept of online privacy. The intro helps kids tell the difference between what's appropriate to disclose and what should be kept private—and how this can change depending on the situation.

In the game, children assemble a map leading to a pirate treasure. "We created the game to show them that information that may not seem valuable to them is often still valuable to somebody, and that it's worth protecting. Pirates are always looking for something valuable."

Along the way, players are asked questions about privacy and personal information on the Internet. Rather than teach general principles, the game takes kids through specific scenarios and actual situations where they encounter privacy challenges. Correct choices are rewarded with an additional piece of the map.

"We spent a lot of time looking at best practices for teaching young kids," explains Johnson. "Research shows that kids this age don't learn from what they did wrong. So we try to focus on what they do right. The game is very forgiving—there are ample opportunities to retry questions to get the right answer."

Both the intro and game sections provide access to a 'mentor' character who gives advice if requested, mimicking the key skill of asking a trusted adult for help whenever a child is uncertain about the right choice.

"Our goal is to give kids a sense of empowerment, so they can take control of their online experiences," says Johnson.

THE BIGGEST CYBER SECURITY THREAT YOUNG ADULTS FACE: THEMSELVES

Most young adults "live" online—whether they're using social media sites, online shopping, online banking, or emailing.

And while most know that these activities put them at increased risk of identity theft or unauthorized access to their private information, many fail to take the necessary security precautions to protect their personal information.

What gives?

According to Sonia Chiasson, an Assistant Professor at Carleton University's School of Computer Science, "Most security advice is

LEARN MORE

Check out the project's comics and infographics at www.versipass.com/edusec. (Note that Flash is required to view the comics.)

OPC RESOURCES

Graphic novel for youth—Social Smarts: Privacy, the Internet and You: www.priv.gc.ca/youth-jeunes/fs-fi/res/gn_index_e.asp

given as a list of do's and don'ts without any real explanation of how these actually help improve security. This quickly becomes unmanageable when you've got up to 15 of these lists of rules to follow. There's no way anyone can remember all of them, and there's no real incentive to do so."

With financial support from the Office of the Privacy Commissioner of Canada, Chiasson researched the use of "visualization" to improve young adults' (aged roughly between 18 and 25) mental models of online security and privacy, to enable them to better protect their personal information.

Her team designed infographics and interactive comics about malware and antivirus software, and mobile privacy and geo-tagging. Using these materials, the team conducted studies to see if visuals were effective in helping participants change their behaviour.

Q Why did you see a need to improve young adults' "mental models" of online security and privacy?

While conducting user studies in the past, we noticed that most people had misconceptions about computer security. We thought if we could help people—notably young adults—better understand how these attacks work and why certain protective actions help, they might be more likely to comply.

Why use infographics and interactive comics?

We felt that they were a better way to get the attention of young adults. They also helped make the subject more approachable and entertaining than the usual written instructions. This was our intuition, and earlier literature suggested it was true for other subjects.

Our studies showed that our participants felt the same way. For example, participants said that the comics were funny and enjoyable, and that the characters were relatable, making it quick and easy to learn the information.

Can you describe the research process?

We iteratively designed the comics and infographics, getting feedback along the way. Then we conducted full user studies to evaluate them.

In the lab, we tested our participants' understanding of the subject before and after reading the infographics or comics to see whether it had improved. A week later, we re-tested their understanding to see if they remembered what they had learned, and asked whether they had made any changes in their real lives as a result.

For the infographics, we also compared against a plain text version of the exact same information, to see whether presenting the information in a visual way was more effective.

Do visuals improve user understanding of online security and privacy?

Participants thought the comics and infographics were an effective method of teaching technical material they would not otherwise be interested in reading. One week after viewing the materials, participants continued to exhibit increased knowledge about the specific security threats and mitigation strategies discussed in the infographics and comics.

Perhaps more importantly, the research demonstrated that the materials had persuaded users to modify their real-life online behaviour towards more secure actions. For instance, users reported they had subsequently updated their antivirus software and were more cautious during online browsing. They had also changed their mobile geolocation settings, were more careful about what they posted online, and had shared lessons learned with family and friends. R

A series of infographics and interactive comics were used by Carleton University Assistant Professor Sonia Chiasson to determine if visualization could improve young adults' mental models of online security and privacy information.

THE OFFICE OF THE PRIVACY COMMISSIONER'S CONTRIBUTIONS PROGRAM

Since 2004, the Office of the Privacy Commissioner of Canada has helped advance privacy research and knowledge translation through its Contributions Program.

Created to support independent, non-profit research on privacy, further privacy policy development, and promote the protection of personal information in Canada, the Contributions Program is considered one of the foremost privacy research funding programs in the world.

The Contributions Program is open to all non-profit institutions interested in generating new ideas, approaches, and knowledge about privacy that organizations can apply to better safeguard personal information and that individual Canadians can use to make more informed decisions about protecting their privacy.

The Office issues an annual call for proposals and, in some years, a special call for knowledge translation projects based on previously completed research.

For more information on the Contributions Program:

contrib@priv.gc.ca
Tel: 1-800-282-1376
TTY/TDD: 819-994-6591

www.priv.gc.ca
Follow us on Twitter: @PrivacyPrivee

Office of the
Privacy Commissioner
of Canada