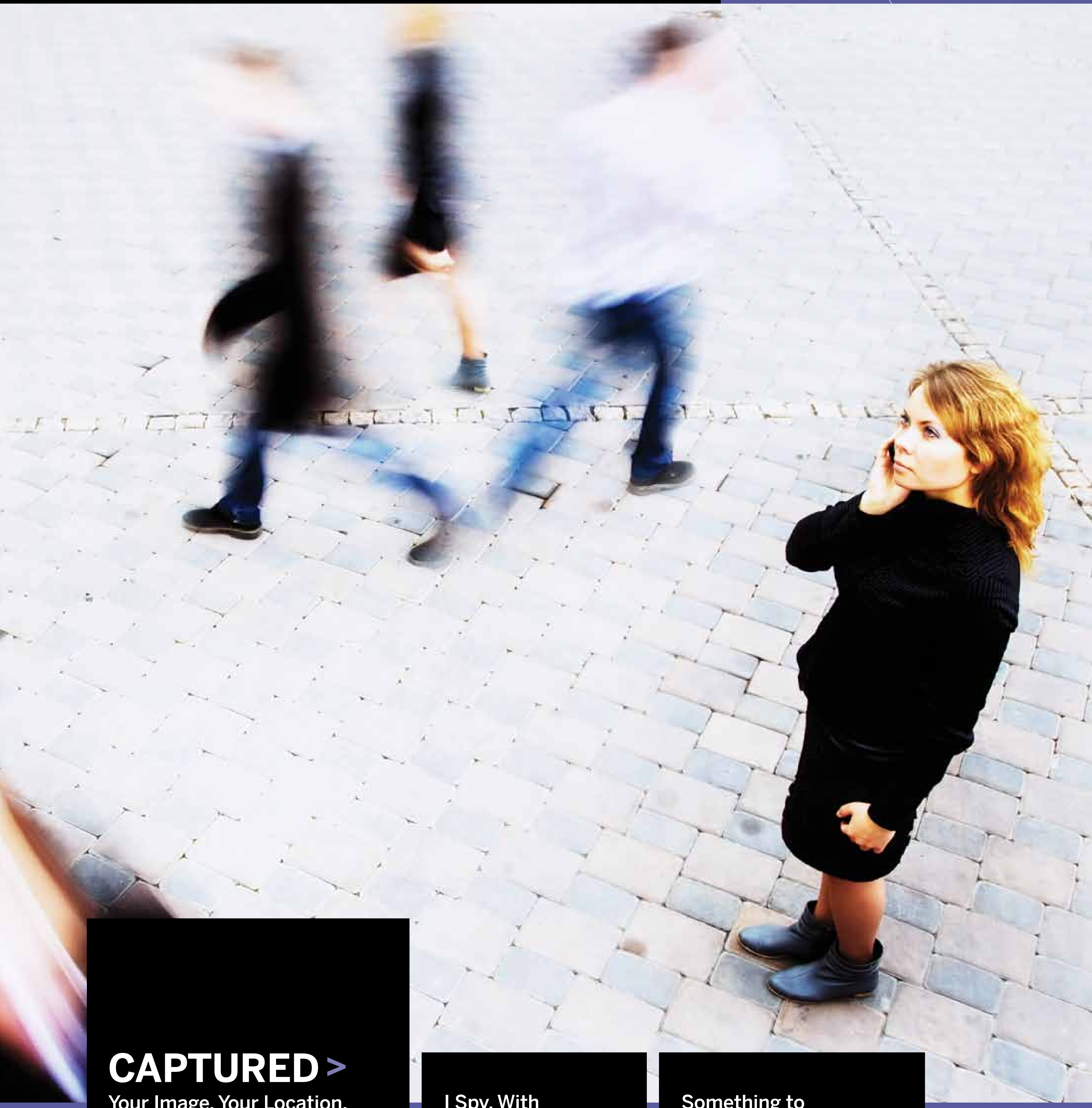
Office of the
Privacy Commissioner
of Canada

REAL RESULTS

PROTECTING PRIVACY RIGHTS
THROUGH INNOVATIVE RESEARCH



CAPTURED >

Your Image, Your Location, Your Personal Data

How can you protect your privacy in the digital age?

I Spy, With My Little Eye

A new study reveals parents are routinely snooping on their kids' online activities. Good parenting, or going too far?

Something to Watch Over Us

As more and more surveillance cameras are installed across Canada, a Queen's University research team is busy 'watching the watchers.'

Contents

Cat. No. IP51-5/2013E-PDF
ISSN 2291-5028

From tapping our smart phones to transfer funds, to swiping an access card to gain entry to our office, technology is seamlessly and ubiquitously woven into our everyday tasks.

And for these technological advances to make our lives a little easier, they create and have access to large amounts of data about ourselves—our contacts, our habits, our likes and dislikes.

How is our information being used to guide decisions about ourselves and the world around us? Do we know how to better protect our privacy in the modern world? What impact does technology have on our privacy?

REAL RESULTS

The Office of the Privacy Commissioner's Contributions Program funds independent cutting-edge privacy research and outreach projects aimed at generating new ideas, approaches and information about privacy in Canada. These projects not only advance the collective knowledge on issues related to privacy and surveillance, but also provide real, tangible research results that Canadians can use to make smart decisions about privacy in their own lives.

The projects highlighted here represent a sample of the innovative and socially relevant independent research the Office of the Privacy Commissioner of Canada has supported through its Contributions Program since 2004.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

The mission of the Office of the Privacy Commissioner of Canada (OPC) is to protect and promote the privacy rights of Canadians. Under its mandate, the OPC oversees compliance with both the *Privacy Act*, which applies to the federal public sector, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's 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 OPC funds research that falls under PIPEDA.

Office of the
Privacy Commissioner
of Canada

STOLEN IDENTITIES, STOLEN LIVES

After hearing too many "tragic" stories, Darrell Evans decided to take action against identity theft—the "perfect non-violent, yet highly lucrative crime"

WHO

Darrell Evans and colleagues at the BC Freedom of Information and Privacy Association (FIPA)

KEY PRIVACY ISSUE

Identity theft is one the fastest growing and most serious non-violent crimes in North America. Victims face devastating consequences—ranging from drained finances and poor credit ratings to lost property titles and false criminal records. More often than not, they must fend for themselves as they navigate a quagmire of redress options.

RESEARCH FOCUS

With support from the OPC Contribution Program, FIPA conducted an in-depth study on the problem of identity theft primarily in Canada, including legal issues and protection offered by the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The report offered a series of recommendations to improve protection against identity theft in Canada.

RESEARCH RESULTS

The report has become required reading for anyone specifically concerned with corporate obligations to prevent identity theft or seeking to understand how PIPEDA can be used to protect consumer interests, including filing a complaint under PIPEDA. More recently, it led to the creation of the Canadian Identity Theft Support Centre, a national Canadian charitable organization focused on supporting victims and potential victims of identity fraud and identity theft.

Although the BC Freedom of Information and Privacy Association, known as FIPA, was originally created to research issues and propose legislation to protect freedom of information (FOI) and privacy rights in Canada, executive director Darrell Evans was appalled by the disturbing phone calls he began to receive from people with eerily similar stories.

"People would call us whose lives were spiraling out of control because their personal information had somehow been compromised," recalls Evans, who retired last year after twenty-two years as Director of FIPA.

What Is Identity Theft?

"Identity theft" happens when an impostor uses someone else's personal information without their knowledge or consent in order to commit fraud. Cases range from forging personal cheques and stealing credit card numbers, to elaborate scams where fraudsters adopt another person's identity to steal assets and access available credit—bank accounts, credit card accounts, and even property deeds.

When a person acquires and collects someone else's personal information for fraudulent purposes, they've committed a serious crime. On January 8, 2010, Bill S-4 (An act to amend the Criminal Code in respect of Identity Theft and Related Misconduct) became law, making it illegal to possess another person's identity information for criminal purposes.

> "These were tragic cases where people had lost their jobs, had their reputations ruined, or faced extreme financial hardship."

"These were tragic cases where people had lost their jobs, had their reputations ruined, or faced extreme financial hardship. Many were caught up in a 'Kafkaesque' nightmare that seemed almost impossible to correct."

Complaints ranged from what Evans describes as "abuse of personal information," including the inclusion of false or out-of-date information about individuals in government and corporate records, improper sharing of confidential psychiatric, medical and financial information, unverified "facts" given to government officials by malicious neighbours, and outright theft of personal information.

Evans listened with horror as complainants described being wrongfully arrested, losing their jobs or government benefits, having to fight years of unfair treatment by government officials or being permanently stigmatized for something they didn't do.

Evans also began hearing about increasing incidents of identity theft. After their personal information was stolen, many victims would discover their bank accounts had been drained, their credit accounts had been run up for purchases they hadn't made, and, in a few cases, big mortgages had been taken out on their homes.

VICTIMS TRAPPED BY "WEB OF FALSEHOODS"

"The few government and private-sector programs available offered general information and a way to report theft and abuse of personal information," recalls Evans, "but nowhere near the kind of personal assistance victims needed to begin unraveling the complex web of falsehoods in which they were trapped."

Evans felt compelled to take action.

"Our idea was to make a case for comprehensive reform of the legislative gaps that contributed to the growth of identity theft and other abuses of privacy, plus a practical program, or even a legal clinic, that could take cases and guide people through the complex steps to correct their information and repair their identity."

But first, Evans and his colleagues at FIPA decided they had some serious digging to do—to find out more about existing individual rights under current law, policy, standards and management practices.

Supported by funding from the Office of the Privacy Commissioner of Canada's Contributions Program, FIPA conducted an in-depth study on identity theft. "PIPEDA and Identity Theft: Solutions for Protecting Canadians" provides a comprehensive assessment of the scope of the problem in Canada.

THE "PERFECT NON-VIOLENT, YET HIGHLY LUCRATIVE CRIME"

The report also details methods of identity theft, legal issues in prosecution, legal responses in the U.S., and the protection offered by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in Canada. The report concludes with a series of recommendations to improve protection against identity theft in Canada.

Describing identity theft as the "perfect non-violent, yet highly lucrative crime," the document struck a chord.

After their personal information was stolen, many victims would discover… in a few cases, big mortgages had been taken out on their homes.

"It proved to be the most popular resource on the FIPA website—by far," Evans notes.

It also became the launching pad for a FIPA-organized conference, "Privacy and ID Theft," co-sponsored by the OPC. At the conference, the idea for creating a resource centre for helping victims of identity theft began to take practical shape.

Following the conference, Evans and his colleagues at FIPA successfully applied for a grant from the Department of Justice Victims' Fund to develop a feasibility study and business plan for the establishment of a full-service victim support centre, education program and research body.

HELPING VICTIMS

Officially launched in 2012, the Canadian Identity Theft Support Centre is a national Canadian charitable organization focused on supporting victims and potential victims of identity fraud and identity theft. The Centre is looking to secure sustainable funding in order to remain operational.

"Poor privacy practices and widespread disrespect for people's personal information are ongoing issues," says Evans. "The problem of identity theft and abuse of personal information continues to grow."

The Canadian Identity Theft Support Centre, for its part, is certainly doing what it can to help victims take control back—over their personal information and their lives.

OPC RESOURCES

Identity Theft Checklist:
http://www.priv.gc.ca/resource/fs-fi/id/checklist_e.asp

Identity Theft and Fraud online resources:
http://www.priv.gc.ca/resource/topic-sujet/itf-vif/index_e.asp

Are You a Victim?

When someone else uses your name, your Social Insurance Number (SIN), your credit card number, or any other type of personal information without your knowledge—you may have become a victim of identity theft.

Has your identity been stolen? Here's what to watch out for:

> You find out that someone has applied for a credit account using your name and address, without your knowledge and consent.

> You receive phone calls or letters declaring you have been approved or denied for a credit account that you never applied for.

> Credit card statements or other bills begin arriving for unfamiliar accounts.

> Your credit card statements are no longer being mailed to you, along with other statements and bills.

> You receive a phone call from a collection agency for a defaulted account in your name that you never opened.

Victim's Toolkit

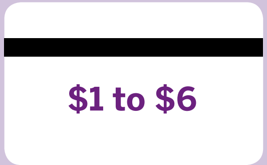
The Canadian Identity Theft Centre has created an extensive toolkit to help Canadians with the problems associated with the ever-expanding and overwhelming problem of identity theft. The toolkit can be downloaded from the Centre's website:

http://idtheftsupportcentre.org/

Identity Theft by the Numbers

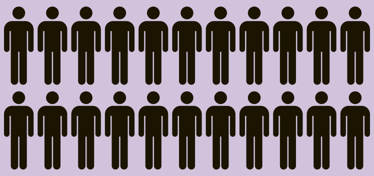
Because it's an underreported crime, accurate and up-to-date statistics about identity theft are hard to find. Crimes range in severity and type, and it can take years for someone to realize they've been victimized. But even the few statistics available point to a growing crime that forces helpless victims to spend an inordinate amount of time and money seeking redress.

Estimated cost of an individual's credit card information on the black market



"The-Cyber-Crime Black Market,"
Panda Security, 2010

Number of Canadians who reported being victims of identity theft in 2011



22,000

Canadian Anti-Fraud Centre

Amount of money reported lost by Canadians due to identity theft in 2011

$13 million

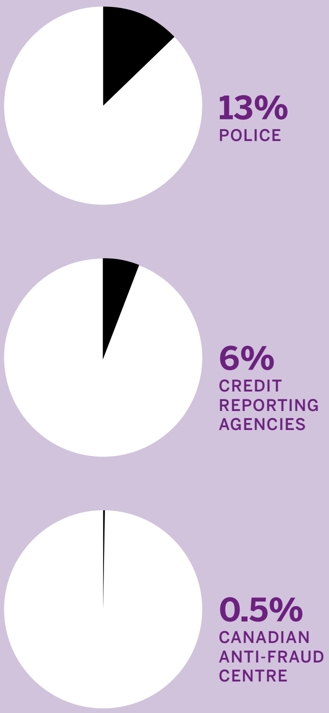
Canadian Anti-Fraud Centre

Estimated combined cost of identity theft every year to consumers, banks, credit card firms, stores and other businesses in North America

$2.5 billion

Canadian Council of Better Business Bureaus

Estimated percentage of identity theft cases reported



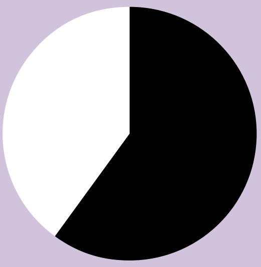
McMaster eBusiness Learning Centre, 2008

Number of Canadians who have already been the victims of identify theft

1 in 6

OPC nationwide public opinion
survey released in 2010

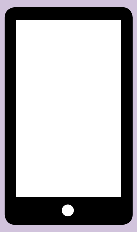
Percentage of survey respondents who felt their personal information is at greater risk than it was 10 years ago



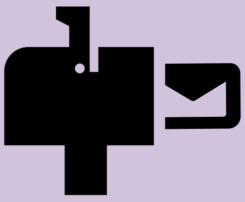
60%

OPC nationwide public opinion
survey released in 2010

Estimated percentage of credit card scams that happen over the phone versus theft from a mailbox



10%



7%

McMaster eBusiness Learning Centre, 2008

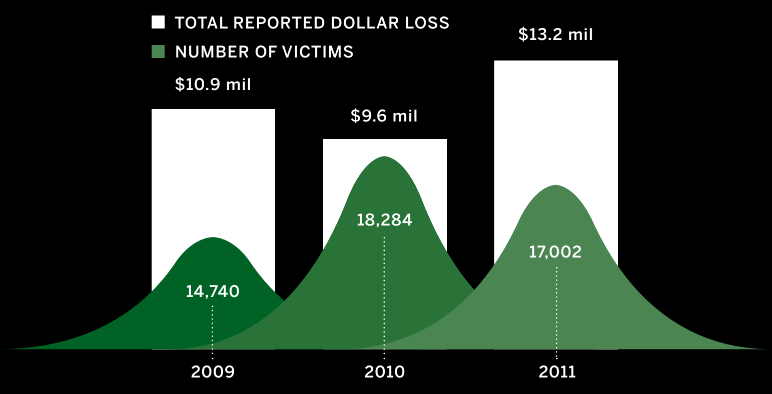
An Underreported Crime

According to the Canadian Anti-Fraud Centre's (CFAC) latest statistics, the number of Canadian identity fraud victims decreased in 2011, but the total reported dollar loss increased.

Originally known as PhoneBusters, the CAFC is a combined effort of the RCMP, the Ontario Provincial Police (OPP) and the federal Competition Bureau. Since its inception in 1993, the CAFC has grown to become Canada's one-stop-shop for fraud reporting.

However, according to the McMaster eBusiness Learning Centre, very few cases of identity fraud are ever reported to the police (13%), credit reporting agencies (6%) or the CAFC (0.5%). Yet, even at these low numbers, the CAFC reported more than 22,000 cases of ID theft in Canada in 2011.

Total Reported Dollar Loss by Canadian Identity Fraud Victims, 2009–2011



Canadian Anti-Fraud Centre

THE "SPY" WHO LOVES ME

Canadian parents routinely invade their kids' online privacy. Is this just good parenting, or has this new culture of hyper-vigilance gone too far?

When MediaSmarts first started exploring parental attitudes towards their children's Internet use, parents were brimming with enthusiasm and optimism.

"Back in 2000, the web represented a brave new future," recalls Jane Tallim, MediaSmarts' Co-Executive Director. "Parents thought it would help their kids get ahead in a knowledge economy."

For their part, kids said the Internet was a place where they could have privacy from their parents to explore their interests and socialize anonymously.

"They thought of it as a place that was theirs," Tallim notes.

FROM OPTIMISM TO FRUSTRATION

By 2005, when the Ottawa-based organization released the second phase of "Young Canadians in a Wired World," the tone had changed considerably.

"Parents reported being frustrated with the reality of having to manage their kids' use of technology," explains Tallim. "They complained their kids were wasting too much time online with instant messaging and video games. They reported having to constantly negotiate their child's computer use. It had become a negative part of family dynamics."

Fast-forward to 2011, with social media now in the mix, and the latest cohort of parents interviewed by MediaSmarts researchers were now reporting downright fear. The positive outlook of parents interviewed a decade ago had been supplanted by a culture of paranoia and hyper-surveillance.

"Today's parents are way beyond frustration," notes Tallim, who worked with lead researcher Valerie Steeves of the University of Ottawa for the third and latest phase of the research project, funded by the OPC. "They're having to contend with multiple messages in the media and from schools that their children are vulnerable to online predation and cyberbullying. They're dealing with the notion that the technology presents a danger to their children."

"LOSS OF CONTROL" BREEDS FEAR AND VIGILANCE

Ever-fearful, parents had unwittingly become spies in their own homes.

"They insist on being 'friended' by their children on Facebook, or they urge other relatives to spy on their kids' online usage and report back to them," says Tallim. "They secretly lurk on their kids' social media pages, check their child's browser history, and snoop text messages and email."

Meanwhile, tweens and teens interviewed as part of the research project begrudgingly reported that constant

LEARN MORE

View the reports:
http://mediasmarts.ca/sites/default/files/pdfs/publication-report/full/YCWWIII-Teachers-Perspectives.pdf

http://mediasmarts.ca/sites/default/files/pdfs/publication-report/full/YCWWIII-youth-parents.pdf

Visit the MediaSmarts website:
www.mediasmarts.ca

surveillance by parents and schools had become the “price of admission” for them to use the Internet and social media.

So, what has driven parents to become secret commandos in a new culture of Internet surveillance?

“As the technology evolved—and kids started having multiple points of entry to the Internet and social media—parents started feeling a loss of control,” explains Tallim. “It was no longer about restricting access to a single desktop computer in the living room. It was smart phones, tablets, gaming devices and consoles. Parents are finding this overwhelming.”

But, is it really so bad for parents to be vigilant? After all, doesn’t every responsible parent want to protect their children from potential harm, such as cyberbullying?

Protecting kids from harm is not the same as protecting them from risk, notes Tallim.

“Yes, [cyberbullying] happens, and needs to be addressed, but kids are far more resilient than we give them credit for.”

RETHINKING THE ROLE OF MONITORING

In spite of parental fears, kids largely self-regulated their

WHO

Jane Tallim, Co-Executive Director of MediaSmarts

KEY PRIVACY ISSUE

The Internet has become a fact of life for young Canadians. But so too have cyberbullying and increased surveillance of kids’ online activities by parents and schools alike. Can parents and teachers help kids develop good habits and stay safe in their online interactions, or are they too busy clamping down on online access?

RESEARCH FOCUS

To gain a better understanding of how young Canadians are using and benefiting from the Internet, Tallim and colleagues from MediaSmarts as well as the University of Ottawa conducted focus groups with teens and tweens, parents, and teachers. Funded under the OPC Contributions Program, the research constitutes Phase III of “Young Canadians in a Wired World,” the most comprehensive investigation into the role of the Internet in the lives of Canadian children and teens. Focus group findings are also providing the basis for a national survey of roughly 12,000 teens and tweens.

RESEARCH RESULTS

The resulting report reveals the “lived experiences of Canadian youth,” who are far more resilient than parents and school administrations believe. The report identifies best practices for teachers that can contribute to learning in today’s networked schools, and how parents can help young people gain the digital literacy skills they need to successfully navigate the online world. “Young Canadians in a Wired World” has proved to be a watershed in understanding how Canadian youth use the Internet, and is relied on and widely cited by researchers and government agencies.

Students “Uncritical” about Online Info, Say Teachers

For the first time since MediaSmarts launched their “Young Canadians in a Wired World” research project in 2000, teachers were surveyed about the role digital technology played in their lives and professional practice.

According to “Teachers’ Perspectives,” “Few professions in our society have been as affected by the advent of digital technologies as teaching: from cell phones in classrooms, to the use of Wikipedia and other online resources in coursework, to the push to integrate information and communications technology (ICT) across different subject areas, every aspect of teachers’ professional lives has changed.”

One surprising finding is that students’ Internet abilities are often greatly overestimated. According to a high school teacher from the Atlantic region, “I don’t think students are all that Internet-savvy. I think they limit themselves to very few tools on the Internet and they don’t think it’s as expansive as it could be. They’re locked into using it in particular ways and don’t think outside the box ... I’m always surprised at the lack of knowledge that students have about how to search and navigate online.”

Many teachers also expressed concern about how uncritical students are about the information they find online.

An elementary teacher from the North described an in-class research project in which grade five students exploring the Sasquatch myth “were taken in by a website that had been intended as an obvious and humorous hoax.”

But the issue most often mentioned by teachers? Many reported being unable to make full use of digital media in their classroom practice due to being unable to access services such as Twitter, Skype and YouTube. Access was typically restricted by their school administration or board policy.

– Adapted from “Young Canadians in a Wired World, Phase III: Teachers’ Perspectives”

own behaviours to avoid and manage cyberbullying, and sought parental guidance when needed. Teens and tweens interviewed for this third phase of the project describe strict online codes of behaviour, and equally strict consequences for betraying those codes.

“Ironically, youth told us that cyberbullying was easier to deal with than offline meanness because the bully left a digital trail,” comments Tallim. “Kids felt okay about challenging the bullies and holding them to account, and their friends could back them up online.”

“We need to rethink the role of monitoring, and foster the trust and communication between adults and kids that is essential in helping kids engage critically with online relationships and content,” Tallim urges, adding, “There is tremendous rhetoric surrounding kids and the Internet. We want to ensure that policy and educational responses are grounded in the lived experiences of Canadian youth. These responses should resonate with youth and equip them to deal with the networked aspects of their lives.”

Ultimately, Tallim believes a culture of surveillance and fear—“life in a fishbowl”—undermines children’s ability to become digitally literate, which she defines as having “critical thinking skills and qualities of good citizenship.” As she astutely reminds us, “you don’t have to invade your kids’ privacy, to protect your kids’ privacy.”

WHAT DO YOU THINK?

As kids learn to accept constant surveillance online—“life in a fishbowl”—will they be able to develop the digital literacy skills necessary to navigate their online worlds?

OPC RESOURCES

“Social Smarts” graphic novel: http://www.youthprivacy.ca/en/gn_intro.html

Surveillance Technologies and Children: http://www.priv.gc.ca/information/research-recherche/2012/opc_201210_e.asp

Life in a Fishbowl

How Kids, Parents and Teachers View Online Privacy

Teens and Tweens	Their Parents	Their Teachers
“Parents have good intentions, but they annoy us.”	“I monitor everything, down to her cell, down to everything.”	“We take the phone away and they get it right back. What have we [accomplished]?”
“My mom keeps on telling me, ‘You’re on Facebook! Get off! Do your homework!’ And I’m like... de-friend.”	“She’s been very open with me with everything because I told her the minute it’s not open, or she lies, or I find out through any of my [spies], it’s all gone.”	“School policies around technologies are very frustrating to me... One of the biggest benefits of having the Internet in our classrooms... is being able to connect with others in a real-time situation, but in fact we can’t use Skype.”
“Yes, it’s my father’s greatest concern, so he has to have my passwords for everything I do. He’s afraid of cyberbullying, so he has to have them at all times.”	“I have nieces, [who]... will write to her, or even call me and say, ‘uh, tell her to change... her wall, her status, or whatever,’ so that’s good.”	“... unfortunately, [students] have to be given the opportunity to make bad choices as often as good choices... And they need adults to be the saving, caring allies... to help them... learn from their mistakes.”

SAY CHEESE: FRAMING YOUR DIGITAL PORTRAIT

A teen's online behaviour can follow them everywhere they go

Revealing photos. Sensitive information. Compromising situations. Teens and tweens seem to be living recklessly online. And despite being aware of the risks, they continue to post risky—and risqué—content.

To help teens and tweens safeguard their privacy—and by extension, their 'digital' reputation—a new educational kit was created to foster sound practices for posting pictures and disclosing personal information online.

Produced by *L'Association sur l'accès et la protection de l'information* (AAPI) and funded by the OPC's Contributions Program, the kit provides junior high school teachers with interactive materials to springboard discussions about online privacy and personal information protection.

"Because of our professional and personal experience, our members are aware of the implications of new technologies, such as social media, on privacy," explains Danielle Corriveau, Chairwoman of the Board of the AAPI, a professional association with more than 500 members, mostly privacy officers. "We also realize that there is an inherent paradox between a teen's desire to communicate and the need to protect their privacy."

When the AAPI decided to create the kit, they didn't follow a top-down approach. Spearheading the project was a group of young people, who were guided by a team of experts: an educational consultant, a lawyer who could explain privacy rights, a youth blogger, a graphic designer who designed the kit's characters or 'avatars,' and the AAPI's general manager, Linda Girard, who directed the project.

"The youngsters were able to comment on all aspects, like the activities and the avatars, to make sure the kit would resonate with them," says Corriveau.

The kit has already been widely distributed in the Quebec secondary school system—40 out of 72 school boards have requested copies to date. The AAPI intends to develop a bilingual version of the kit, for distribution across Canada.

For more resources, advice and tips, or to order "Educational Kit for Developing Sound Practices for Posting Pictures and Personal Information on the Net," visit the AAPI's website (www.aapi.qc.ca) or call (418) 624-9285.

LEARN MORE

French (http://aapi.qc.ca/troussepedagogique/)

OPC RESOURCES

What can YOU do to protect your online rep? (video): www.youthprivacy.ca/en/video_index.html

EXPOSED

As big data becomes more available, and analytics become cheaper, could so-called “de-identified” health information be pieced back together for all to see?

WHO

Dr. Khaled El Emam, Associate Professor in the Faculty of Medicine, Canada Research Chair in Electronic Health Information at the University of Ottawa, and Senior Investigator at the Children's Hospital of Eastern Ontario Research Institute (CHEO)

KEY PRIVACY ISSUE

Personal health information is increasingly disclosed for research, public health, policy, and commercial purposes. In our new era of Electronic Medical Records, collecting and sharing information is easier than ever. So how can we minimize security breaches and avoid revealing—accidentally or not—an individual's sensitive information?

RESEARCH FOCUS

With funding from the OPC Contribution Program, Dr. El Emam and colleagues conducted a series of studies to determine how anonymized or "de-identified" personal data can be re-identified. The goal was to develop principles, metrics and methods for minimizing the probability of re-identifying individuals in publicly disclosed files.

RESEARCH RESULTS

Study results were published in an influential report, "Pan-Canadian De-Identification Guidelines for Personal Health Information," which later became the basis for a practical how-to manual on de-identifying public data sets for privacy officers, policy makers, lawyers and other data custodians involved in sharing and releasing public data.

The manual proved so popular, it grew into a 400-page book—*Guide to the De-Identification of Personal Health Information*—scheduled for release in May 2013 and published by CRC Press, a division of Taylor & Francis. Dr. El Emam has also developed the material into a companion series of training modules now being offered in cities across North America.

The report also led to the launch of a private spin-off company, Privacy Analytics, which develops specialized software to help government, health care providers and commercial enterprises minimize the probability that anonymous personal data can be re-identified at a later date.

It's a dramatic story that's been retold so many times, it's become part of computer science lore.

In 1997, Harvard computer scientist Latanya Sweeney famously identified the medical records of Massachusetts Governor William Weld by linking de-identified, patient-specific medical data to a public voter register.

In the process, she also demonstrated that roughly 87% of the U.S. population could be uniquely identified with just three items: date of birth, gender, and zip code.

The revelation caused shock waves across North America, which led to important changes in de-identification practices and regulation in the U.S. and in Canada, including new provisions in the U.S. Health Insurance Portability and Accountability Act (HIPAA).

Data is anonymized or "de-identified" when it's stripped of information so that the data subject cannot be identified. For example, in health research, data is stripped of elements that could identify the individual patient or research participant.

The benefits of data sharing can be significant. Data is an important resource in a variety of key health areas, including health program and service delivery, health system and clinical program management, public health monitoring and research.

Yet, despite better laws and practices to protect the privacy of individuals, fears continue to arise about the possibility that personal health data can be "attacked," and therefore re-identified, by intrepid computer scientists, emboldened hackers or self-serving commercial interests.

LEARN MORE

Read a summary of the report: (http://www.ehealthinformation.ca/ap0/book.asp)

FEAR OF EXPOSURE TRIGGERS BEHAVIOUR CHANGES IN PATIENTS

According to Dr. Khaled El Emam, Associate Professor in the University of Ottawa's Faculty of Medicine, alarming media reports of data breaches and increasing pressure to share personal information should concern all Canadians.

"If people worry about how their personal health information is being used, they begin to mistrust their health professionals and the health care system," notes El Emam. "We know that patients change their behaviour—they will lie to doctors or pay cash for private services. They will start to self-treat and self-medicate to avoid certain information being added to their medical files. It undermines public trust."

DATA BREACHES ARE ALSO COSTLY AND TIME-CONSUMING TO REPAIR

"Organizations are required by law to notify all individuals affected," says El Emam. "The total cost can be in the millions. In the U.S., penalties can be imposed and potential litigation costs are high. These breaches can irrevocably damage the reputation of the organizations responsible."

However, El Emam cautions that many of the risks of de-identification have been "over-dramatized" in the media. The untold story is the absence of proper safeguards that should have been built in, but were typically not.

MANY DATA BREACHES REVEAL STANDARDS NOT FOLLOWED

"There have been some successful attacks," states El Emam, "but if you look at recent ones closely, those responsible for de-identifying the data didn't follow current standards. It's like cooking your food improperly, getting sick, and then blaming the food. It's how you cooked the food that caused the problem. In many of these cases, either the data custodians didn't know enough about existing [de-identification] standards, or they didn't follow them carefully enough."

To address this growing gap in the knowledge and application of standards, El Emam conducted a research project, with funding from the OPC's Contributions Program, to figure out to what extent "de-identified" data can be re-identified.

Along with colleagues at the Children's Hospital of Eastern Ontario (CHEO) Research Institute, and with Research Ethics Board approval, he set out to reverse de-identified data, and assess existing flaws in security protocols.

"The idea was to understand how re-identification happens and what the risks of successful re-identification are. With that knowledge, we were able to develop more effective techniques for de-identification."

The resulting report, "Pan-Canadian De-Identification Guidelines for Personal Health Information," details the principles, metrics and methods that can be used to manage the privacy risks associated with disclosing data. These guidelines, if followed properly, can maintain low probability of re-identifying individuals in publicly disclosed files, minimizing the probability of inadvertently disclosing sensitive individual information.

CLOSING THE STANDARDS GAP TO PREVENT IMPROPER DATA DISCLOSURE

The report became the basis of a practical how-to manual on de-identifying public data sets. The manual is aimed at privacy officers, policy makers, lawyers and other data custodians involved in sharing and releasing public data.

"Motivated Nosy Neighbour" Can Access Personal Health Information

Armed with just basic background information, could a highly motivated intruder access your personal health data?

Yes, argues Dr. Khaled El Emam, if the data is not properly de-identified before being disclosed to other parties.

Over the past several years, El Emam has used various datasets to re-identify information with a relatively high degree of certainty.

In one well-known example, as part of an ethics board-approved research project, El Emam and colleagues scrutinized prescription records from the Children's Hospital of Eastern Ontario (CHEO) to evaluate the re-identification risk of a dataset requested by a commercial data broker.

The data broker was planning to undertake a benchmarking project – comparing various indicators in hospital datasets – along with providing analytic services for prescribing practices and dosages. CHEO was interested in participating in the project, as long as privacy risks were properly managed. So before disclosing any data, CHEO asked El Emam to concretely assess what those privacy risks were.

Using six months of data from CHEO, El Emam's research team created the same record layout used by one of Canada's commercial data brokers. According to their findings, published in the journal *IEEE Security and Privacy*, 99.6 percent of the data were unique, including age, gender, FSA*, and admission and discharge dates – potentially compromising patient privacy.

According to the journal article, "...a patient's nosy neighbour who is determined to find out information about the patient's health status, for example, would have sufficient background information to identify the unique prescription record and determine the drugs prescribed to the patient as well as the patient's diagnosis."

The team then took the extra step of asking colleagues who worked outside the hospital if they happened to know of any patient admitted during the same six-month period.

It turns out that one colleague was aware of a neighbor's child being admitted with a serious infection during the time period in question. The colleague knew the child's gender, age range, and FSA. A database search using these criteria produced a single record that matched, which was later confirmed to be the patient.

"This is a concrete example of how a neighbour or other motivated individual could use background knowledge about a patient, match it against variables in the prescription record to successfully re-identify the patient, and obtain sensitive health information about him or her," states the article.

Thanks to El Emam's work, CHEO changed the data before release so it was "defensibly de-identified", and added extra requirements for security and privacy audits, averting the risk of possible re-identification of patient data.

Editor's Note: All re-identified datasets mentioned in this story were kept confidential, and the research project was ethics-board approved.

Source: El Emam, K. and Kosseim, P. "Privacy Interests in Prescription Data, Part 2, Patient Privacy", *IEEE Security and Privacy.*

* FSA stands for "Forward Sortation Area", which is the first three digits of a postal code.

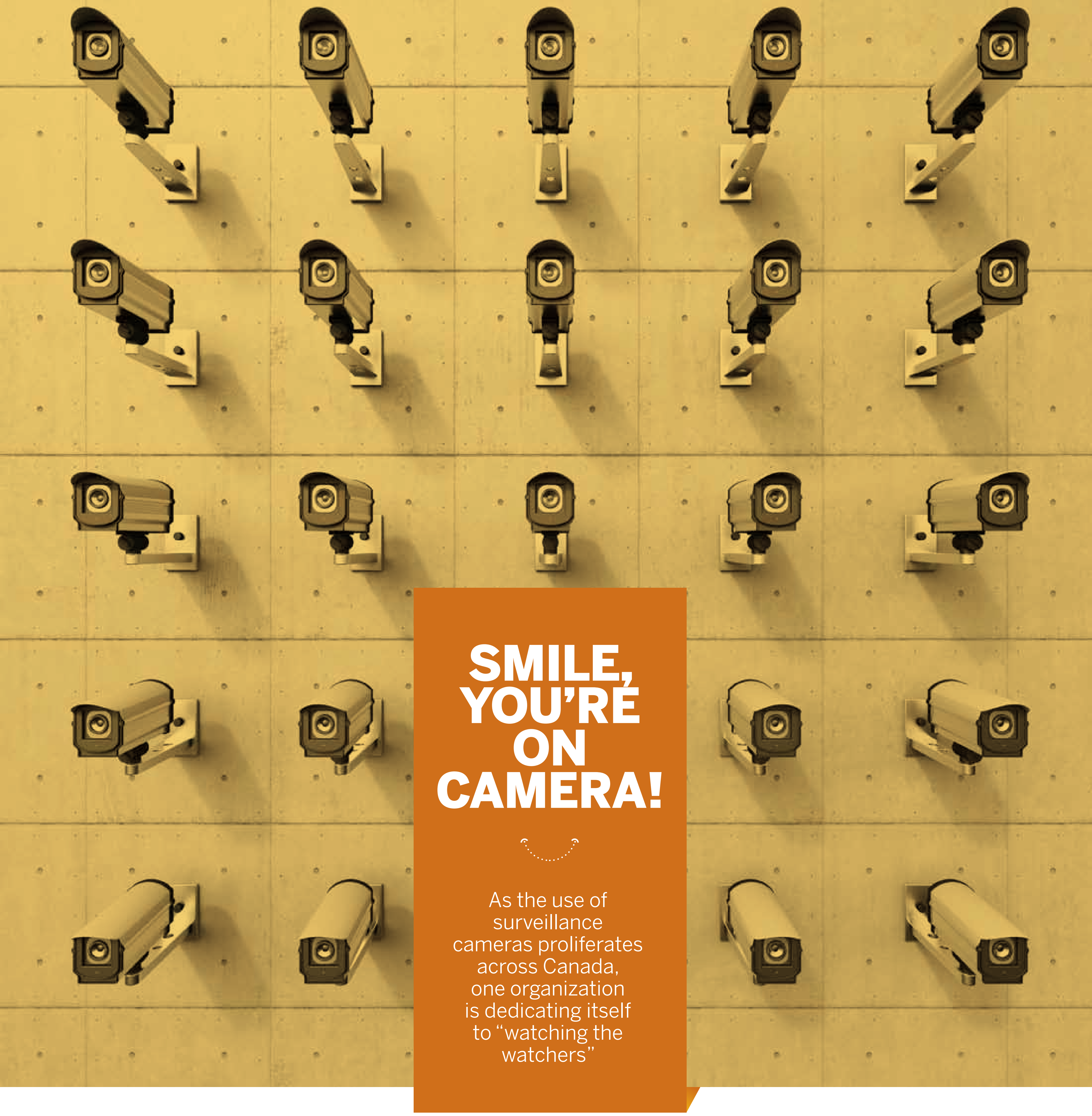
> "Our objective is to give data custodians the tools to make decisions about the best way to disclose data, but also ensure that the privacy of individuals is protected."

"Our objective is to give data custodians the tools to make decisions about the best way to disclose this data, but also ensure that the privacy of individuals is protected," explains El Emam.

The manual proved so popular, it grew into a 400-page book, *Guide to the De-Identification of Personal Health Information*, scheduled for release in May 2013. Dr. El Emam has now developed the material into a companion series of training modules being offered across North America. To reach a large audience in a short period of time, the course will be delivered in partnership with other local and global professional services firms.

This original empirical research also lead El Emam and colleagues to develop a spin-off company—Privacy Analytics—whose software provides integrated masking and de-identification capability.

"It's the only integrated masking and de-identification tool on the market today, and the only tool that incorporates a risk-based approach. Our clients use this tool to mask and de-identify data before they disclose it for secondary purposes," he says.



SMILE, YOU'RE ON CAMERA!

As the use of surveillance cameras proliferates across Canada, one organization is dedicating itself to "watching the watchers"

You wake up a little later than usual, so you skip making your morning coffee and rush straight to your car, parked in its usual spot in your condo's underground lot. >

WHO

David Lyon, Director of the Surveillance Studies Centre and co-leader of the Surveillance Camera Awareness Network (SCAN) at Queen's University

KEY PRIVACY ISSUE

Camera surveillance is a rapidly growing phenomenon in Canada. Every single day, our images are captured multiple times. Have we consented to having our image captured, and what are the unintended social effects?

RESEARCH FOCUS

Lyon led the first systematic survey of camera surveillance in the Canadian context. Aimed at both the public and policy-makers, the OPC-funded report delves into Canadian attitudes towards camera surveillance, and raises a number of key privacy issues.

RESEARCH RESULTS

Issues raised by the report became hot topics at a two-day workshop hosted by SCAN to discuss camera surveillance in Canada. The report and workshop grew into a new book on camera surveillance, *Eyes Everywhere: The Global Growth of Camera Surveillance*, edited by Lyon, along with Aaron Doyle and Randy Lippert. Seed funding provided by the OPC supported the research report and workshop, which was also used as a launch pad for the Surveillance Studies Centre (SSC), a leading global hub for research on expanding surveillance practices.

“Does this type of surveillance comply with privacy guidelines?… Whose images are being captured by these cameras?”

En route, you decide you to do a quick coffee run. You spot an ATM next to the café, and decide to make a quick withdrawal.

Back in the car, you’re a bit distracted by a coffee spill on your lap, so you unintentionally run a yellow light. You get through the intersection safely, but decide to keep your eyes on the road as you pull into the employee parking lot. You walk briskly through the atrium, jump on an elevator, and arrive at your cubicle.

Just another ordinary day in the life of an ordinary Canadian?

But, wait, did you remember to smile each time your image was captured by a closed-circuit television (CCTV) camera? In your parking lot, at the ATM, above the traffic lights, and in your office?

NUMBER OF CAMERAS INCREASING

Every single day, our images are captured multiple times, mostly without our awareness or consent.

Camera surveillance is a rapidly growing phenomenon in Canada. No longer just whirring away in banks, airports, and military installations, CCTVs are being installed by a host of public agencies, private companies and, increasingly, public-private interests—at intersections, building entrances and shopping centres, in parking lots, transit systems, taxis, and elevators … and the list goes on.

The cost of installing and monitoring CCTVs is typically rationalized by a desire to protect property and deter crime.

However, according to David Lyon, Director of the Surveillance Studies Centre and co-leader of the Surveillance Camera Awareness Network (SCAN) at Queen’s University, little convincing research evidence exists to show that camera surveillance actually helps deter, respond to, and investigate crime—but compelling evidence exists to show such surveillance often invades the privacy of ordinary citizens and puts marginalized groups at more risk.

“In the past decade, there has been a steady increase in the use of cameras in public places in Canada, especially in urban settings,” says Lyon. “Our adoption rate has been slower than in the UK, U.S. and China, and we’re more cautious about new surveillance technology and practices, but the number of cameras has grown dramatically since the seventies when they were first introduced.”

And long gone are the shaky, grainy black-and-white images popularized on TV crime shows. Today’s CCTVs are typically high-resolution and have the ability to tilt, pan a room and zoom in.

NO “SILVER BULLET” FOR PREVENTING CRIME

The proliferation of high-tech surveillance cameras is raising serious privacy questions, argues Lyon.

“Does this type of surveillance comply with privacy guidelines?” he asks. “Do these cameras carry appropriate signage to inform citizens? Is there consent involved? Whose images are being captured by these cameras?”

With research funding from the OPC’s Contributions Program, SCAN published “A Report on Camera Surveillance in Canada,” the first systematic survey of the Canadian context.

While the report acknowledges some camera surveillance “may be warranted,” it warned Canadians about the risks of seeing cameras as a “silver bullet.”

“Our research found that criminals were not deterred, but simply moved to other geographic areas. So crime was not prevented, it was displaced,” says Lyon.

Researchers also found that when camera operators are involved, they tend to pay more attention to members of minority groups, and “other perceived ‘undesirables,’ to ensure the ‘right’ sort of people use certain spaces.”

COMING TO GRIPS WITH “EYES EVERYWHERE”

These issues became hot topics at a two-day workshop hosted by SCAN to build on the report and further explore camera surveillance in Canada.

“We brought together a group of informed people to have an evidence-based discussion and come to grips with key trends across Canada and in other countries. A big point of debate was the disconnect between the evidence that camera surveillance prevents crime—which is minimal—and the growth in cameras for the ostensible use of preventing crime.”

Workshop presentations later became the basis for a well-received book on camera surveillance, *Eyes Everywhere: The Global Growth of Camera Surveillance*, edited by Lyon along with Aaron Doyle and Randy Lippert. It is the first international perspective on the development of camera surveillance. Although it has a special focus on Canada, the UK and the U.S., it also explores the situation in Brazil, China, Japan, Mexico, South Africa and Turkey.

SCAN also used the research workshop to launch the Surveillance Studies Centre (SCC). The mission of the new Centre is to advance the field of surveillance studies, with a focus that goes well beyond camera surveillance.

“We were among the first to do work on location-based and mobile surveillance technologies, such as smart phones and automated license recognition [a study also funded by the OPC]. We’re also looking at new border controls, the rapid growth of surveillance drones in Canada, social media, and ‘dataveillance’ methods.”

“We cover the whole range,” says Lyon, “and the range keeps getting broader.”

LEARN MORE

Read the reports:
http://www.sscqueens.org/sites/default/files/SCAN_Report_Phase1_Final_Jan_30_2009.pdf

http://www.sscqueens.org/sites/default/files/SCAN_Report_Phase2_Dec_18_2009.pdf

See the workshop program:
http://www.sscqueens.org/projects/scan_workshop

DID YOU KNOW?

‘Dataveillance’ is a relatively recent term for surveillance methods that monitor data trails created by credit card purchases, mobile phone calls, and Internet and social media usage.

A Bad Sign

CCTV Signage in Four Canadian Cities

Canadian privacy guidelines and policies typically suggest the use of signage to achieve informed consent of the public in situations of overt camera surveillance.

But in a case study of four Ontario cities, the OPC-supported SCAN report found that even when signage was used to notify those who could fall under the camera's gaze, which was rare, it did not fulfill basic requirements:

> notices indicating how the public could access more information (through freedom of information requests, telephone numbers, web sites) were rarely posted or poorly executed

> the location of camera surveillance signage was often already within the gaze of the camera's surveillance

> actual usage often did not match publicly-stated purposes by the authority or organization implementing the surveillance

> references to the applicable legal authority was often unclear or obscure

> no accommodation was made for persons with visual disabilities or literacy difficulties

Adapted from "A Report on Camera Surveillance in Canada," Surveillance Camera Awareness Network (SCAN), Queen's University

WHAT DO YOU THINK?

When it comes to camera surveillance, some say, "if you're not doing anything wrong, you don't have anything to worry about." Are they right?

OPC RESOURCES

Guidelines for Overt Video Surveillance in the Private Sector: http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.asp

Guidance on Covert Video Surveillance in the Private Sector: http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.asp

OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities: http://www.priv.gc.ca/information/guide/vs_060301_e.asp

Workshop on Privacy, Security and the 2010 Olympics: http://www.priv.gc.ca/information/pub/ol_20090202_e.asp

WHO
Drs. Bartha Knoppers and Denise Avard, Department of Genomics and Policy, McGill University

KEY PRIVACY ISSUE
Parents can authorize the submission and storage of their child's tissue samples and related data in paediatric biobanks—for research purposes. Given these children haven't reached the age of consent, how can parents, researchers, and Research Ethic Boards ensure that a child's sensitive genetic information will be not be improperly used or disclosed—in the short term, and also down the road?

RESEARCH FOCUS
With funding from the OPC's Contributions Program, the research team undertook an extensive analysis of privacy and confidentiality in paediatric biobanks from an operational, legal and ethical perspective.

RESEARCH RESULTS
The research resulted in the development of guidelines for paediatric biobanks and their handling of personal information. The project leader also created an easy-to-read pamphlet outlining findings, which has been distributed to Research Ethics Boards and paediatric researchers, and at various public venues across the country.

FLESH AND BLOOD

It's challenging enough to protect the genetic information of adults who consent to having their biological samples stored in biobanks, and who can make decisions for themselves. But how do you protect the genetic information of children whose parents have authorized their tissue donation?

Because biobanks can store massive amounts of biological samples and related health and demographic data—often over a long period of time—they've become an important resource for researchers. But when it comes to protecting the privacy of paediatric research participants, existing legal and ethical guidance is unclear—leaving researchers and Research Ethics Boards to resolve privacy dilemmas in a bit of a vacuum.

Parents can authorize a child's participation in research, but because children have not yet reached the age of consent, are they properly protected from the risk of unauthorized use or disclosure?

Canadian lawyer and McGill professor Bartha Knoppers has spent decades examining the legal and ethical aspects of genetics, genomics and biotechnology.

In her role as Director of McGill's Centre of Genomics and Policy (CGP), she led a comprehensive analysis of privacy and confidentiality in paediatric biobanks to help researchers and Research Ethics Boards navigate the choppy waters surrounding paediatric privacy.

Q What is a "biobank"?
Canada is taking quite a lead in the biobanks area. They're not just 'big fridges,' as some people think. They're collections of biological samples with accompanying data, including medical, biographical and socio-demographic data. Ultimately, they're a resource for studying different chronic diseases such as cancer, diabetes and hypertension; different health processes over time such as aging; or different environmental impacts on populations.

Many of these studies are longitudinal, so researchers may be looking at differences in results over time. For example, you might have a long-term cohort followed for over 20 years, with samples and other testing being requested every five years or so to assess changes.

Why bother to have specialized paediatric biobanks? Aren't samples and data similar for children and adults?
Apart from the fact that they come from children, the samples and data are similar. However, because they

LEARN MORE

Consent, Privacy and Research Biobanks Policy Brief (co-sponsored by Genome Canada and the Office of the Privacy Commissioner of Canada): http://www.genomecanada.ca/medias/pdf/en/GPS-Policy-Directions-Brief.pdf

involve children, who are more vulnerable than adults, they receive a lot more scrutiny than other biobanks.

More 'partners' are involved: there's a tri-partite relationship between parents, who are presumed to have the best interests of their children in mind; paediatricians, who take an active role in advocating for the health of children; and research ethics committees, who see themselves as protectors of children.

Paediatric biobanks are also much less common than typical biobanks because we don't include children in research as often as we include adults.

Is it a good thing that paediatric biobanks are much less common?
I don't think it's necessarily a good thing. Only paediatric research can give us answers to paediatric diseases. If we don't include more children in research, we're in effect orphaning them from the possibility of future treatments for diseases that may be unique to them.

Given they involve children, do paediatric biobanks have to follow special rules?
There are unique limitations involved. For example, you have to be studying something that either has a direct or indirect benefit to children of the same age and condition. So you might have a disease biobank focused on certain childhood cancers or allergies.

It's also possible to use paediatric biobanks to track the normal health and development of children over time. However, these are not widely accepted. This is a shame because understanding normal development in children can be as important as understanding childhood diseases, perhaps not for immediate generations, but for future generations.

Are there other limitations?
With children, we're also much more cautious about predictive genetic testing—cases where researchers may identify a disease or condition which could manifest itself when the child becomes an adult.

This is coming up more and more with whole genome sequencing—researchers are looking for one thing, but they happen upon an incidental finding that could impact future health care decisions.

These sorts of findings raise tricky questions. The information could potentially be of benefit to the child, but we give the child's parents the choice as to whether they want to receive this type of information or not.

Is it fair for parents to decide *not* to receive their child's incidental results?
The difficulty is that I'm not sure parents should be exercising the "right not to know" under certain circumstances. Certainly, we shouldn't burden children with adverse research results or risk information prior to adulthood when nothing can be done. But if researchers find something medically significant that can be treated or prevented during childhood, shouldn't the child have the right to that treatment?

Is "re-consenting" an option—getting consent from children when they become adults able to express their own wish to know or not know?
Re-consenting is theoretically one solution. But in reality, it's either impossible or impractical, except for longitudinal studies where re-contact is normal.

Many researchers are only being funded for three to six years, so that would create an obligation for these researchers to follow these children even when their projects are complete. Of course, children move around, and it can be hard to track them until they reach the age of majority.

The title of your research project is "Privacy in Canadian Paediatric Biobanks: A Changing Landscape." What's changing?
We're at a crossroads, so it's difficult to tell. For upcoming generations, genomics information will likely be normalized, almost like the weather. This next generation will probably openly discuss if they're at risk for a disease or they're a faster metabolizer. They may not share the same privacy concerns we have today. So, is our current caution surrounding genetic privacy in the best interests of upcoming generations, or will upcoming generations look back upon our current caution as extremely paternalistic?

Knoppers and her team analyzed three key privacy concerns related to the use of paediatric biobanks in Canada:

Personal Information
The term "personal information" is often very broadly defined and may include health-related information generally as well as information related to human biological materials.

Consent
It is well accepted that obtaining the informed consent of individuals is necessary in research involving human subjects. Given that children do not have the legal capacity to consent to their own inclusion in research, parental consent is needed. Certain privacy statutes explicitly recognize the role of parents or other legally recognized guardians of minors exercising rights regarding the minor's personal information.

Research
Recognizing that re-consenting may sometimes be impossible in a research context, privacy legislation often contains a waiver by a Research Ethics Committee that allows researchers access to personal information absent consent of the individual to whom the information relates.

From "Privacy in Canadian Paediatric Biobanks: A Changing Landscape"

PINT-SIZED

GAME CHANGERS

What happens when a group of 8- to 10-year-olds are brought together to help create a privacy game?

They exceed expectations.

What’s the first thing to avoid when you’re working with children to build a game that teaches privacy literacy?

WHO

Kate Raynes-Goldie and David Fono, co-founders of Atmosphere Industries, a non-profit game design organization based in Canada and Australia, along with a team of Canadian children aged 8 to 10: Chris, Jordan, Kiri, Mary, Mitchell, Peter and Tinson.

KEY PRIVACY ISSUE

Kids are often warned about online “stranger danger,” but they don’t usually get the chance to practice “privacy literacy” skills—like how to assess which individuals or companies they should share their information with, and how to think critically about the potential consequences of those choices.

PROJECT FOCUS

With OPC funding, the team worked with a group of kids to identify learning goals to help develop privacy literacy, and create a game that teaches online privacy literacy skills in an entertaining way.

RESULTS

An “augmented” board game (iPad + board game hybrid) was created to help kids develop autonomous privacy decision-making skills. The “Watchers” can be downloaded for free, or purchased as a “manufactured” board game, together with a companion web app that guides game play as the story unfolds. A companion research report provides an overview of what the children/co-creators already knew about privacy, and what they felt was important to teach other children. The game’s creators also outline how to support children as co-designers in the game development process.

“Don’t use the word ‘privacy,’” laughs Kate Raynes-Goldie, co-founder of Atmosphere Industries, an award-winning, non-profit game design organization based in Canada and Australia.

“For kids, the term ‘privacy’ is a loaded, but vague, term,” she explains. “I think privacy is vague for everyone, but when kids hear the term, they tend to associate it with being talked down to about the dangers of the Internet by people who, in the kids’ opinion, don’t necessarily know what they’re talking about.”

What’s the second thing?

“Don’t underestimate what kids can bring to the process,” says Raynes-Goldie, who is also a researcher and educator focused on games and social media. “Get them directly involved in creating the game.”

Funded by the OPC’s Contributions Program, the “Gaming Privacy” project team followed an innovative approach—they collaborated with children not only to produce the game, but also to identify its learning goals.

Instead of developing the game in a vacuum, and then throwing it over the ‘playground fence’ to see how kids respond, the team worked with kids from the get-go.

“This would seem obvious, but people might be surprised by how rarely organizations involve kids in developing games that target younger age groups, even educational games,” comments Raynes-Goldie.

“It could be because there are more obstacles involved,” she speculates. “Parents have to get involved to provide consent, and because we were also conducting a research project, as well as developing a game, we had to get research ethics board approval for collaborating with the kids.”

So, why go to all that trouble?

“Kids are so savvy, it’s worth it. Plus, what they have to offer really resonates with other kids,” she says.

Raynes-Goldie and her colleagues at Atmosphere did not teach kids how to memorize ways of avoiding “stranger danger.” Instead, they wanted to help kids develop critical thinking and autonomous privacy decision-making skills for themselves.

“The ‘stranger-danger’ myth has mostly been debunked,” says Raynes-Goldie. “The risks of online predation, although of concern, are actually very small—and most kids are very aware of these risks. The reality is that kids are in more danger of having their personal information compromised online.”

Players can practice figuring out which individuals or companies they should share their information with, as well as thinking critically about the potential consequences of those choices.

“Given the rhetoric around kids and their irresponsible use of the Internet, people might be surprised by how knowledgeable they are about companies’ online marketing practices,” says Raynes-Goldie.

Many of the children commented that service terms were too long and complicated, and that they weren’t meant to be read and understood, but only to protect the company.

“The kids seemed to be able to distinguish between what they called ‘greedy’ companies, which commodified them for marketing or advertising purposes, and more trustworthy ones,” notes Raynes-Goldie.

After the kids collaborated with the project team to identify key privacy issues and learning goals, the production process began. The kids were trained in game development, came up with ideas for settings and scenarios, and helped create the game’s characters—giving them names like “Petor the Puffball,” “Zombo the Milkzombie” and “Kara the Alphawolf.” A professional artist rendered their original character drawings.

“That’s when the kids became our clients. We would show them concepts based on their ideas, and they gave us direction and feedback,” explains Raynes-Goldie, who notes the project team collaborated with the EDGE Lab at Ryerson University to produce the video game.

In May 2012,“The Watchers” was released as an “augmented” board game (iPad + board game hybrid) that can be downloaded for free, or purchased as a “manufactured” board game. A companion web app guides game play as the story unfolds.

“Kids are definitely frustrated with the ‘stranger danger’ narrative. They’re more interested in what companies are doing online, and how that could affect them,” states Raynes-Goldie, adding, “The online landscape is evolving. We need to help kids problem-solve, but we need to give them more credit for being able to contribute to the problem-solving.”

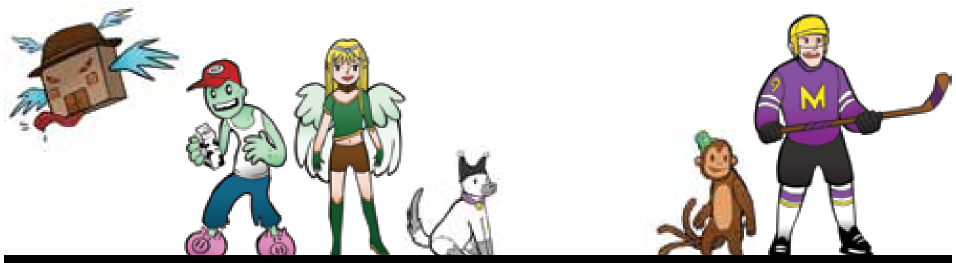
OPC RESOURCES

“Gaming consoles and personal information: Playing with privacy” report:
http://www.priv.gc.ca/information/pub/gd_gc_201211_e.asp

LEARN MORE

Find out more:
www.atmosphereindustries.com

Download the game:
watchersgame.com



Get the Privacy Game!

“The Watchers” takes place in an inter-dimensional town called Union City. Tasked with protecting the city is a secret arm’s-length government agency, made up of the top agents from each dimension. The team must investigate a number of mysterious events surrounding the town’s hat-based augmented reality network, known as Hatnet. Through these investigations, players learn a number of real-world privacy concepts, as well as developing their critical thinking and risk assessment skills. While they learn a great deal about privacy, they never have to even utter the word!

Since 2004, the Office of the Privacy Commissioner of Canada (OPC) has advanced privacy knowledge and outreach through its Contributions Program—considered one of the foremost existing privacy research programs.

The Contributions Program is open to all non-profit institutions interested in generating new ideas, knowledge, and practical approaches to help organizations or individuals make informed decisions about protecting personal information. All proposals submitted are evaluated on the basis of merit through an internal and external peer-review process.

For more information on how to apply, contact:

contrib@priv.gc.ca
Tel: 1-800-282-1376
TTY/TDD: (613) 992-9190

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

Office of the
Privacy Commissioner
of Canada