What's New in Access, Privacy and Health Care

Brian Beamish
Commissioner

Ontario Connections
May 21, 2015

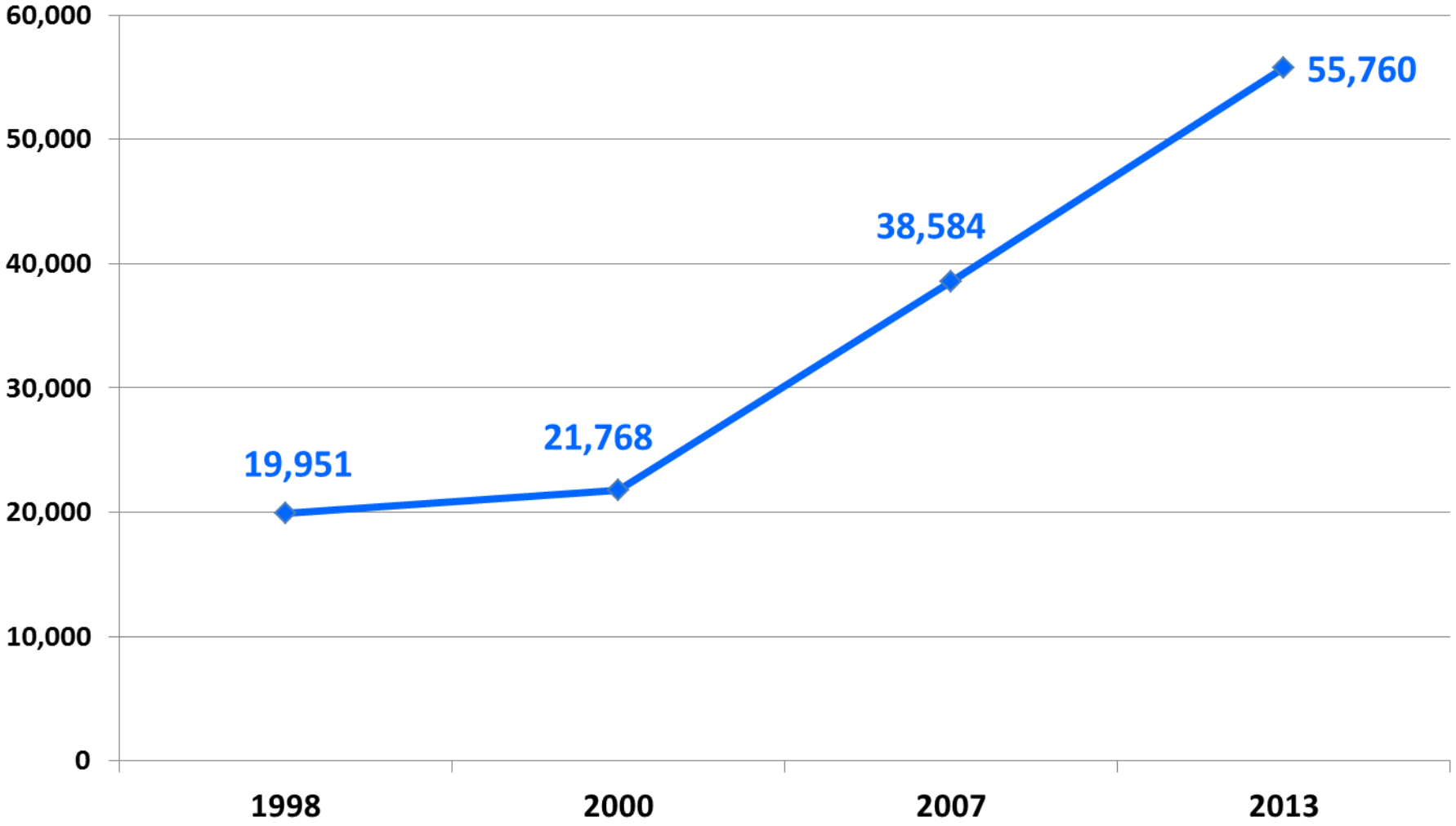
Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

The Three *Acts*

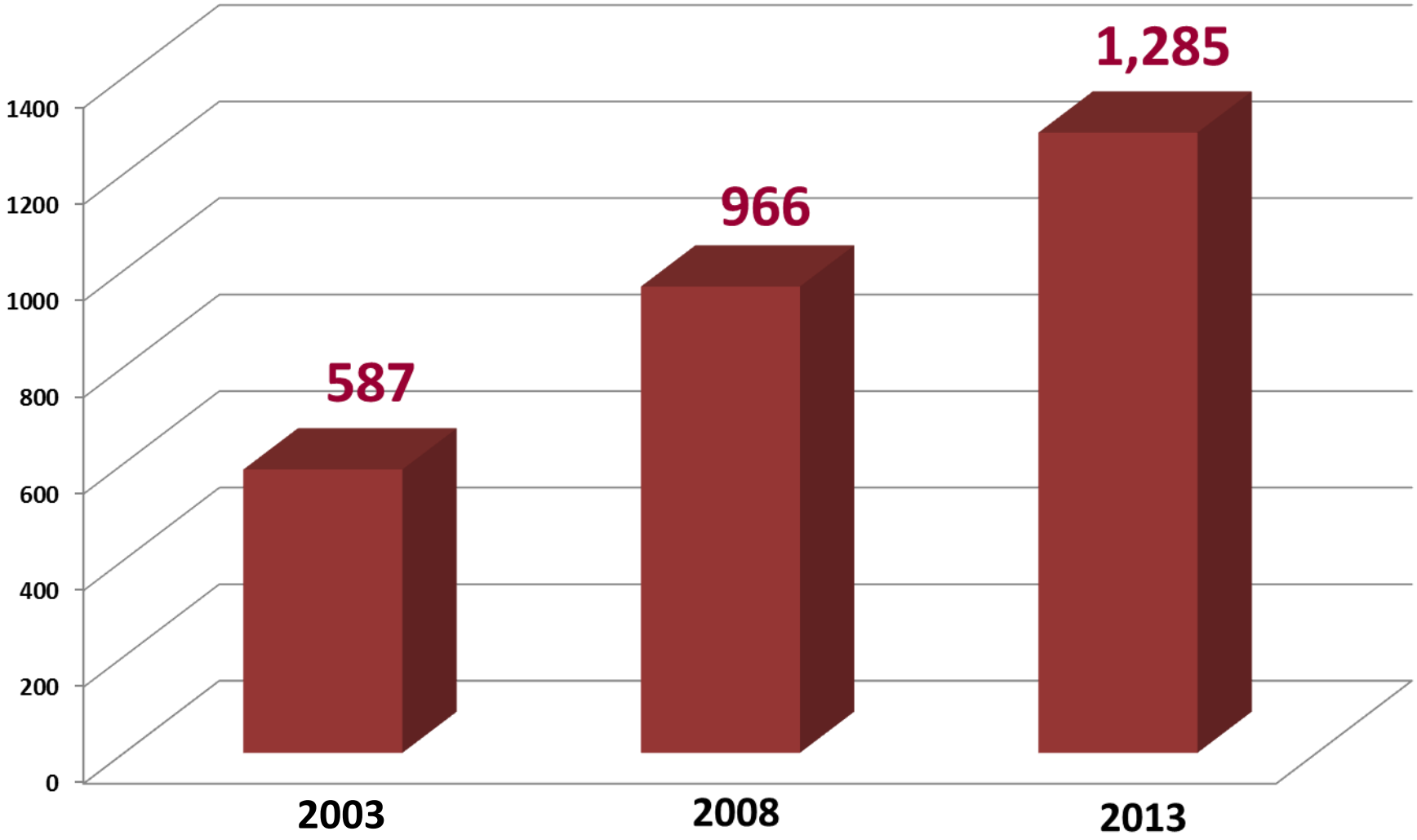
The IPC ensures compliance with:

- *Freedom of Information and Protection of Privacy Act (FIPPA)*
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
- *Personal Health Information Protection Act (PHIPA)*

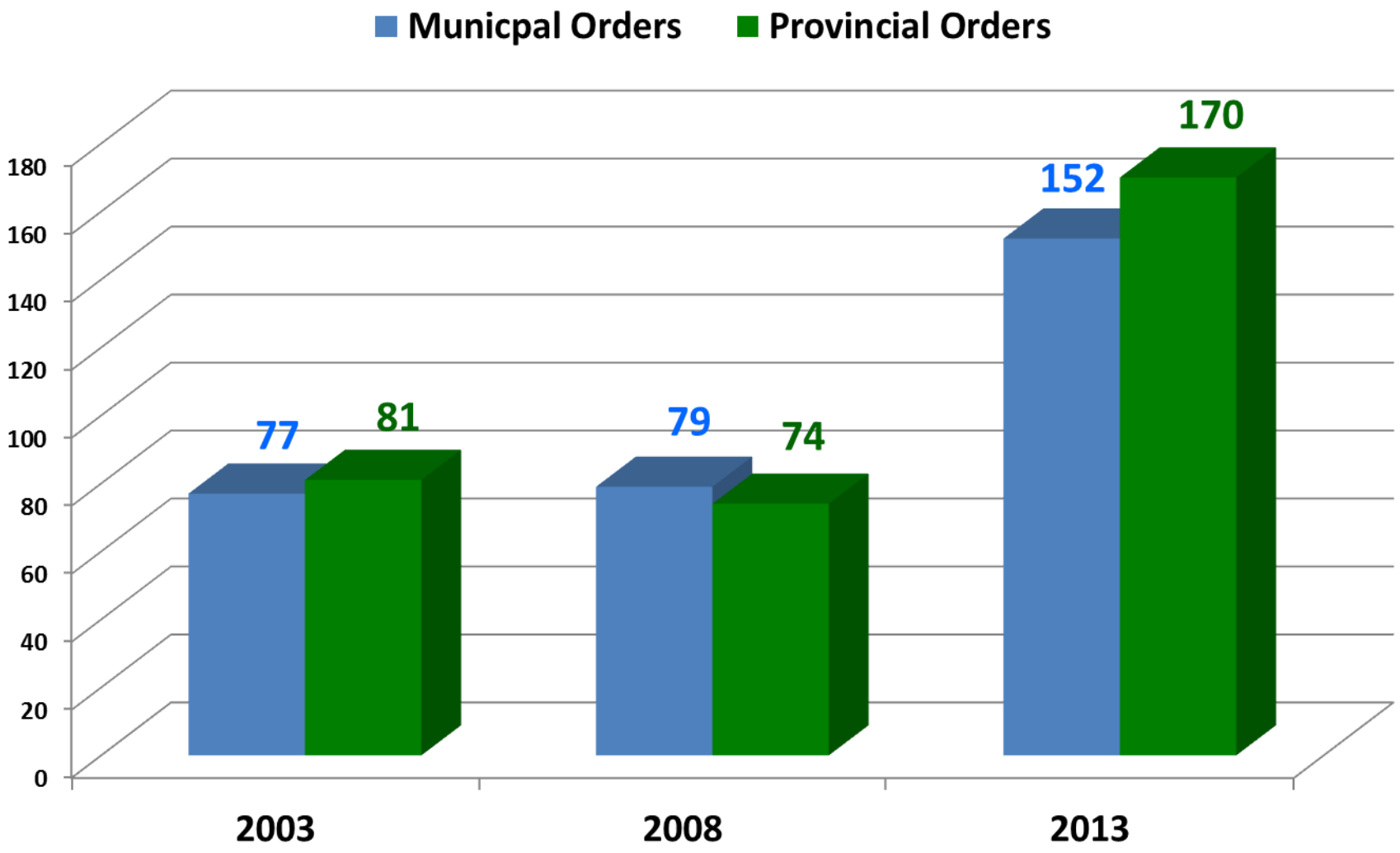
Total Access Requests Per Year



Total Appeals Received Per Year

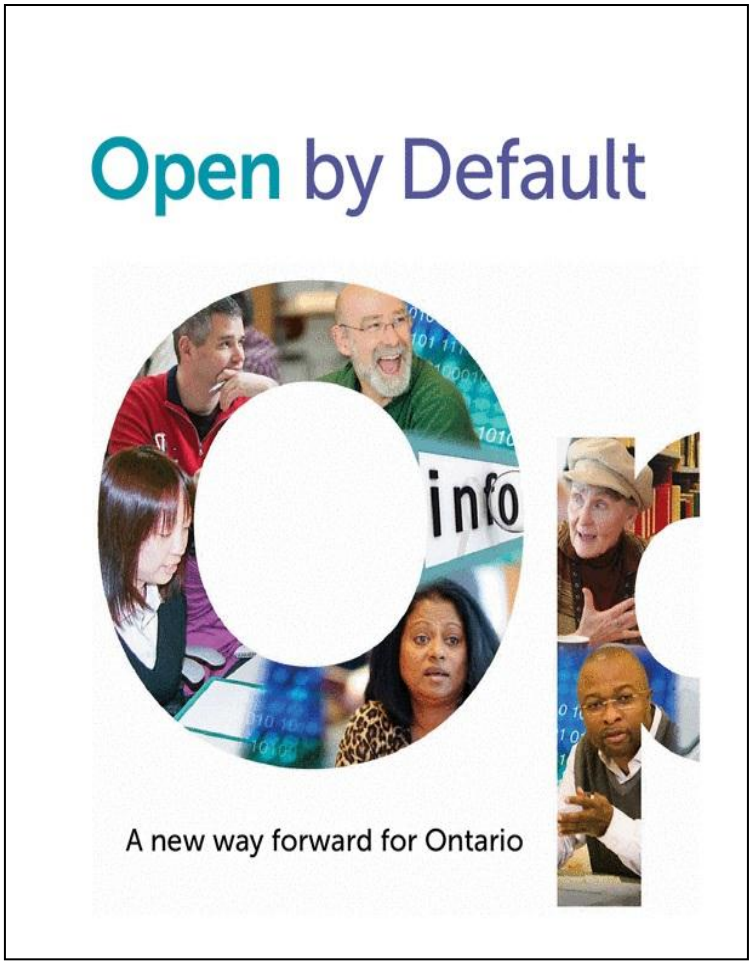


Total Orders Issued



Open Government Engagement Team
Open by Default Report

- Reform Acts by basing them on the principals of Open by Default and requiring the proactive publication of certain types of information;
- Reform the FOI process so that government systems can receive, process and respond to information requests online and in machine-readable formats;
- Publish FOI responses online.



Open Government

Ontario issues draft **Open Data Directive** [May 1/15]

- Directive aims to make data like school enrollment, highway traffic volume, open to public
  - Public uses include building maps, apps, models to tackle gridlock, make health care service more accessible
- Data should be public unless privacy, legal, security, commercial sensitivity concerns
- Province seeks public feedback; IPC now evaluating, will provide comments

Open Government

City of Guelph

- Received **award** this year from Institute of Public Administration of Canada (IPAC) and Deloitte
- One of **top three cities** for advancing local government, responding to citizens' needs
- Included:
  - comprehensive Open Government Action Plan
  - Open Government Community Leadership Team
  - turned Council orientation into an online resource everyone can access

Open Government

IPC will issue **guidelines** to help institutions advance open government agenda

- Focus on smaller institutions, including municipalities, school boards
- **Small steps** approach: IPC recognizes moving to open by default can be daunting task
- We will engage with individual institutions to identify their needs, give advice on how to move forward

Procurement Records

Procurement records

- IPC recommends routine publication of contracts (allowing for withholding of **truly proprietary** information)
- Becoming routine for some institutions (e.g., Infrastructure Ontario, LAO, some municipalities)
- Key is **managing expectations**: parties engaging with government should expect public scrutiny [*e.g.*, include in RFP materials]
- Procurement highlighted in draft **Open Data Directive**

Russell Williams DNA Case

FOI request for dates when DNA samples were collected

- MCSCS "unjustified invasion" of privacy
- IPC ordered release of dates as they was a compelling public interest in disclosure which clearly outweighs privacy interests
- Released March 2015

> STAR INVESTIGATION

Troubling DNA delay in Williams murder case

Getting result faster might not have stopped another killing, but could have linked crimes

SANDRO CONTENTA AND JIM RANKIN
STAFF REPORTERS

In mid-September 2009, air force colonel Russell Williams broke into a neighbour's home in the village of Tweed. He beat, blindfolded and sexually assaulted a young woman as her 8-week-old daughter slept in another room.

When police arrived, a DNA sample was lifted from behind the woman's neck. It took less than two weeks for the Centre of Forensic Sciences in Toronto to identify a DNA profile and upload it to the RCMP's National DNA Data Bank.

Days before that upload, Williams unleashed the same violence on another neighbour, Laurie Massicotte, though no useful DNA sample was found. Massicotte lived on Williams' dead-end street called Cosy Cove Lane.

On Nov. 24, he took his crime spree to Brighton, 60 kilometres south of Tweed, and escalated to murder. He broke into the home of Marie-France Comeau, a 38-year-old corporal under his command at Canadian Forces Base Trenton. He rained blows on her head with a flashlight and sexually assaulted her for hours, capturing much of it on video, before suffocating her.

This time, a Star investigation has revealed, DNA results from that murder — which would have helped investigators by linking the crimes — took 10 weeks to process and upload from the day crime scene items began arriving at Toronto's forensic lab.

DNA continued on A21

Convicted killer Russell Williams was commander at CFB Trenton.

Province cited killer's privacy in withholding DNA documents

SANDRO CONTENTA
AND JIM RANKIN
STAFF REPORTERS

The Star's quest for the DNA dates in the Russell Williams case began with a simple question: Were the samples tested and uploaded to a national DNA data bank in a timely fashion?

In an October 2011 freedom-of-information request, the Star asked for dates when samples were collected, when they were sent to the Centre of Forensic Sciences, and when DNA profiles were uploaded to the RCMP's National DNA Data Bank.

The Star asked only for dates involving samples that were later determined to match Russell Williams' DNA profile. These dates were not part of the 96-page agreed statement of facts introduced during Williams's 2010 guilty plea. The statement did include, however, the crime scenes from which DNA profiles were obtained. The Ministry of Community Safety and Correctional Services, which oversees the Ontario Provincial Police and the Centre of Forensic Sciences, fought the release of the requested dates for more than three years.

Citing the provincial Freedom of Information and Protection of Privacy Act, it called the release of DNA collection and processing dates an "unjustified invasion" of the privacy of Williams' victims, their families — and of Williams himself. The information, the ministry added, was not of "compelling" public interest.

The ministry also suggested in submissions to the information and privacy commissioner that sharing the dates would set a "dangerous precedent" that "may lead to victims of crime being less co-operative with the police, especially during high-profile investigations."

The IPC invited responses on the request for dates from victims, their representatives, and Williams. Only Williams chose to reply. While he asked the IPC that his submission not be shared publicly, the IPC indicated that he expressed concerns about the privacy of his victims.

The Star argued that the DNA dates from such a high-profile case would either instill confidence in the investigation and forensics lab or highlight areas for improvement, particularly in light of gaps in the submitting and testing of DNA samples identified by Justice Archie Campbell nearly 20 years ago in the Paul Bernardo case.

IPC adjudicator Brian Beamish, now Ontario's information and privacy commissioner, agreed with the Star.

In ordering the ministry to release the DNA dates, Beamish wrote they "will inform the citizens of Ontario when crucial and time sensitive evidence was collected and catalogued by law enforcement."

A court challenge by the province prolonged the process. The dates were released to the Star in March after a second order from the IPC, affirming Beamish's order.

Wrote assistant commissioner David Goodis: "I find that there is a compelling public interest in disclosure . . . that clearly outweighs the privacy interests of the individuals whose personal information is contained in the record."

The dates are contained in charts in a document that outlines where and when the samples — later determined to match Williams' DNA profile — were collected by police. It also notes when they were sent to Toronto's Centre of Forensic Sciences and when DNA profiles were uploaded to the national DNA data bank.

Privacy

Challenges Ahead

Law Enforcement Surveillance

- Bill C-51, CCTV cameras, body-worn, etc.

Cloud Computing

- Public/health sector moving to the cloud?

Service Integration

- More efficient public services may mean sharing personal information

Big Data

- Profiling citizens, consumers

Body Worn Cameras

Body-Worn Cameras

- Working with Toronto Police on pilot project
- Important accountability tool, but privacy must be respected
- Scope of collection, notice, retention, training
- Mission creep concern: combine with facial recognition technology?

Surveillance

Bill C-51:

- Concerns about expanded information sharing among agencies, insufficient oversight
- Joint statements with cross-Canada counterparts, support federal Privacy Commissioner Therrien
- What next?

Police Record Checks

Continuing privacy concern

- Checks now routine for many jobs, volunteer positions
- Growing concern that employers obtain irrelevant information, particularly **non-conviction** information

IPC calls for guidance/consistency

- IPC worked with OACP, MCSCS to develop solution
- Optimistic about legislative solution

Crossing the Line

Crossing the Line investigation report [2014]:

- Toronto woman denied entry to US at Pearson Airport due to mental health concern
- 2012 suicide attempt on **CPIC** due to 911 call
- US border officials have direct, instant CPIC access

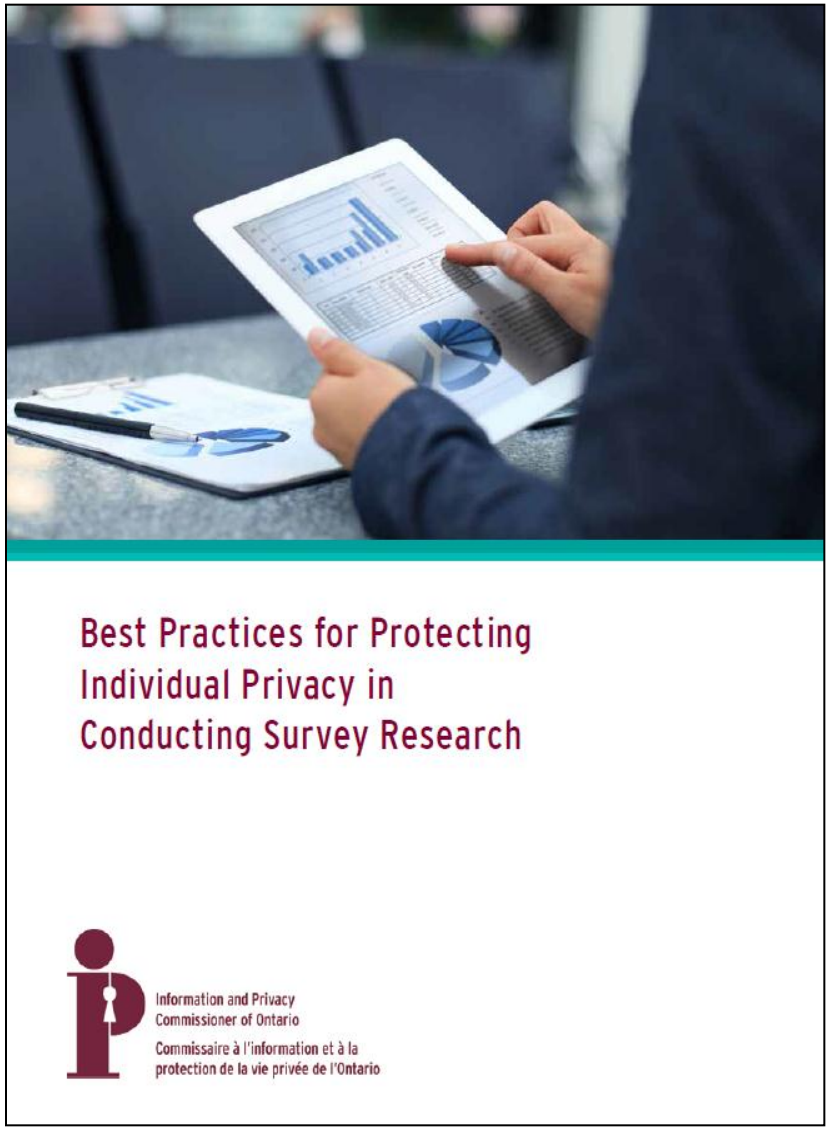
IPC finds police uploading info about suicide attempt/threat is improper disclosure [*FIPPA*, s. 42]

- Disclosure permissible only where valid public safety concern

Crossing the Line - Response

- Most police services comply
- Toronto Police Service refuses
- IPC brings application for judicial review, asks Divisional Court to order compliance
- Hearing expected in fall 2015

Survey Guidelines



- Updated from 1999 version, co-authored with Ontario Public Service.
- Changes reflect use of online survey tools, and use of mobile devices.

Planning for Success: Privacy Impact Assessment Guide

- A PIA is a process used to identify actual or potential risks to privacy.
- A privacy best practice – PIAs are widely recognized as essential tools in the analysis of the privacy implications of new systems, programs and technological tools.
- While *FIPPA* and *MFIPPA* do not require that institutions conduct PIAs, PIAs can help proactively address privacy and provide evidence of due diligence.

Planning for Success: Privacy Impact Assessment Guide

- This guide will help institutions subject to *FIPPA* and *MFIPPA* conduct PIAs to assess compliance with the acts.
- It includes a user friendly step by step guide on how to do a PIA from the beginning to the end and some tools or checklists to assist with the analysis.

Planning for Success:
Privacy Impact Assessment
Guide

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

IPC PIA Methodology

STEP 1: PRELIMINARY ANALYSIS

- Examine the project to determine if it will involve the collection, use, retention, disclosure, security or disposal of personal information.

If you determine that the project WILL involve personal information, proceed with the PIA process. If the project WILL NOT involve personal information, you do not need to proceed with the PIA process.

STEP 2: PROJECT ANALYSIS

- Collect specific information about the project, the key players and stakeholders and the type of and manner in which personal information will be collected, used, retained, disclosed, secured or disposed of.

STEP 3: PRIVACY ANALYSIS

- Using information gathered in the previous step, identify *FIPPA* or *MFIPPA* requirements and potential risks and impacts to privacy.
- Consider ways to reduce or eliminate the risks and impacts identified.
- Assess proposed solutions and their benefits.

STEP 4: PIA REPORT

- Obtain approval to proceed with recommended solutions.
- Document your findings and chosen solutions in a PIA Report.
- Proceed with the project, ensuring that the recommendations from your PIA are fully incorporated in the project plans and implemented.

Privacy and the Internet: A Guide for Municipalities

- The Internet is now seen as a pillar of the Open Government movement which promotes publishing records online – a highly effective means of ensuring that the public has access to information.
- However, when records include personal information, there are privacy implications that must be considered.

10 YEARS OF THE PERSONAL HEALTH INFORMATION PROTECTION ACT

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

The Need for PHIPA is Clear!

The need to protect the privacy of individuals' personal health information has never been greater given the:

- Extreme sensitivity of personal health information
- Greater number of individuals involved in the delivery of health care to an individual
- Increased portability of personal health information
- Emphasis on information technology and electronic exchanges of personal health information

Consequences of Inadequate Attention to Privacy

- Discrimination, stigmatization and psychological or economic harm to individuals based on the information
- Individuals being deterred from seeking testing or treatment
- Individuals withholding or falsifying information provided to health care providers
- Loss of trust or confidence in the health system
- Costs and lost time in dealing with privacy breaches
- Legal liabilities and ensuing proceedings

Challenges Posed by Shared Electronic Health Record Systems

- Health information custodians may have custody or control of personal health information they create and contribute to, or collect from, shared electronic health record systems
- No custodian has sole custody and control
- All participating custodians and their agents will have access to the personal health information
- These pose unique privacy risks and challenges for compliance with *PHIPA*

The Need for ePHIPA

A governance framework and harmonized privacy policies and procedures are needed to:

- Set out the roles and responsibilities of each participating health information custodian
- Set out the expectations for all custodians and agents accessing personal health information
- Ensure all custodians are operating under common privacy standards
- Set out how the rights of individuals will be exercised

Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies and procedures should address:

- Governance
- Consent Management
- Logging, auditing and monitoring
- Privacy training
- Privacy breach management
- Privacy complaints and inquiries management
- Access and correction

Orders HO-002, HO-010 and HO-013

Our office has issued three orders involving unauthorized access:

Order HO-002

- A registered nurse accessed records of the estranged spouse of her boyfriend to whom she was not providing care
- They were accessed over six-weeks during divorce proceedings

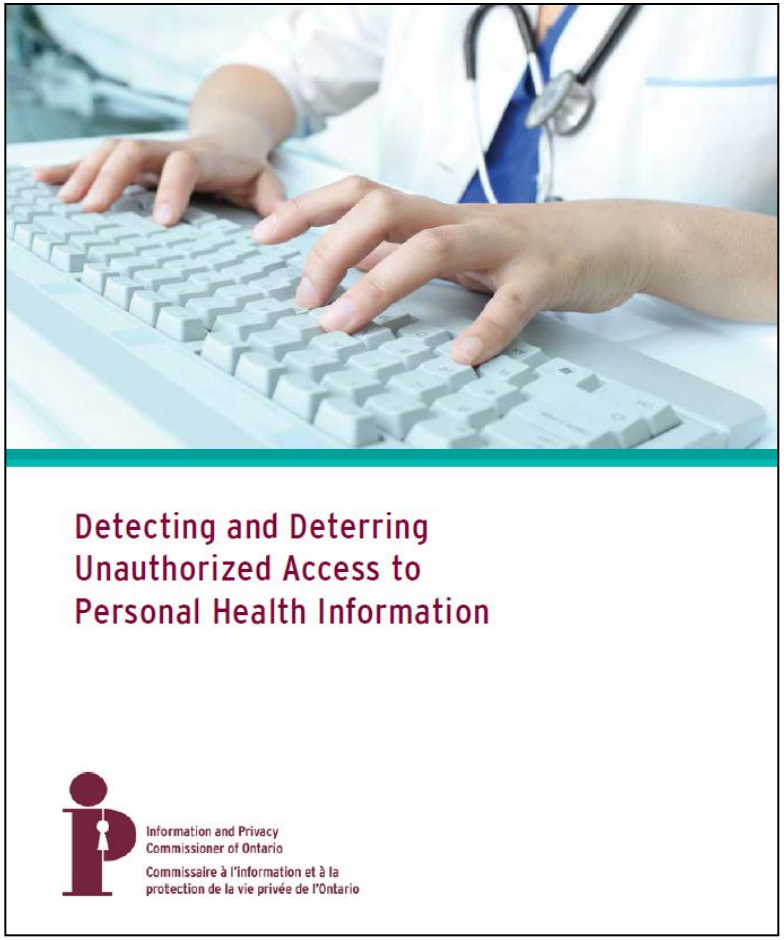
Order HO-010

- A diagnostic imaging technologist accessed records of the current spouse of her former spouse to whom she was not providing care
- They were accessed on six occasions over nine months

Order HO-013

- Two employees accessed records to market and sell RESPs

Detecting and Deterring Unauthorized Access



- Impact of unauthorized access
- Reducing the risk through:
  - Policies and procedures
  - Training and awareness
  - Privacy notices and warning flags
  - Confidentiality and end-user agreements
  - Access management
  - Logging, auditing and monitoring
  - Privacy breach management
  - Discipline

Privacy Class Actions

Hopkins v. Kay, 2015 ONCA 112

- Ontario Court of Appeal affirms patients' right to sue hospitals for **invasion of privacy tort** (*Jones v. Tsige*)
- Court says limiting right to cases where IPC issues *PHIPA* order too restrictive
- IPC intervenes, argues in favour of common law right, since IPC will exercise discretion not to conduct review/issue order, for wide variety of reasons (SCC leave application)

Contact Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca