Privacy and Collecting Identity-Based Data (IDbD)

David Weinkauf, Ph.D. Senior Policy and Technology Advisor



Commissaire à l'information et à la protection de la vie privée de l'Ontario AERO-AOCE Spring Special Interest Group (SIG) Presentation

May 10, 2019

Overview

- IDbD case study
- What is privacy?
- Lessons from IPC reports MC06-63 and MI10-5
- Topics from Anti-Racism Act
 - De-identification
 - Age requirements for consent

IDbD Case Study: TTC's "Field Information" Cards

TTC officers have collected more than 40,000 records on riders who weren't charged with an offence

By Ben Spurr Transportation Reporter Mon., March 11, 2019

TTC suspends use of forms used to document riders' personal information after Star investigation

By **Ben Spurr** Transportation Reporter Thu., March 14, 2019

Characteristics of the Program

- Purpose
 - To assist TTC fare inspectors in their daily functions, e.g., to detect multiple warnings
- Information collected
 - E.g., person's name, address, driver's licence, physical appearance and race
- Number of records
 - 40,000 cards between 2008 and 2018
- Retention period
 - 20 years

What Is Privacy?

- Interpretations change in response to challenges of new and emerging technologies
- Since 1970s, dominant interpretation has been "individual control over personal information"
- Why? "Information record-keeping systems" emerged in 1970s
 - Today we call them "databases"
- Information in databases can be:
 - Inaccurate, incomplete or outdated
 - Shared / accessed indiscriminately
 - Used for illegitimate, unknown purposes

Fair Information Practices (FIPs)

- Set of privacy principles formalized in 1980 by OECD
- Form the basis of virtually all modern privacy laws, including Ontario's
- Eight basic principles:
 - Collection Limitation
 - Data Quality
 - Purpose Specification
 - Use Limitation
 - Security Safeguards
 - Openness
 - Individual Participation
 - Accountability

Brief History of IDbD in Ontario

- IDbD has been the topic of two Information and Privacy Commissioner (IPC) investigations:
 - Privacy Complaint Report MC06-63 (January 17, 2008)
 - Privacy Complain Report MI10-5 (March 3, 2011)
- Anti-Racism Act (ARA) passed in 2017
 - Regulations currently "authorize" school boards to collect IDbD
 - As of January 1, 2023, collection will be "required"

IPC Reports MC06-63 and MI10-5

- Both reports stem from parent complaints about board-wide student surveys
- In both cases, the IPC found that the collection of IDbD was authorized under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Provisions in ss. 169.1(1), 170(1) and 171(1) of the *Education Act* make the collection compliant with s. 28(2) of MFIPPA
- Other issues discussed include:
 - Appropriate notice
 - Linking of IDbD with other data sources
 - Security measures

Important Points to Consider

- Tension between consent and MFIPPA
 - Participation in both student surveys was voluntary, opt-out
 - However, consent is not an authority to collect under MFIPPA
 - Is consent then only a best practice for IDbD under MFIPPA?
- Functional separation between IDbD and administrative data
 - IDbD was deemed necessary for planning, management, resource allocation and policy development purposes
 - Addressing "achievement gap"
 - Distinct from service delivery / administrative purposes
 - Surveys were described as "confidential"
 - Could IDbD in this context be used to make educational / administrative decisions about individuals?

Storage and Security of IDbD

- Board in report MI10-5 had three separate databases:
 - Database 1: student data, achievement data and OENs
 - Database 2: survey data and survey numbers
 - Database 3: linked survey data and achievement data (no names / identifiers)
- Access to databases only on a "need-to-know" basis
- Database 3 only accessible to research officers

Anti-Racism Act, 2017

- Consent-based statute that authorizes and/or requires the collection of specific IDbD by certain public institutions
- Purpose of collection is to "eliminate systemic racism and advance racial equity" (s. 7(2))
- Regulations for school boards specify IDbD fields:
 - Indigenous identity, race, religion, ethnic origin
- Also specify areas of potential disparity:
 - Credits granted, graduation, special education, suspension / expulsions, refusal to admit under clause 265(1)(m) of Education Act
- Data standards set out rules for the collection, use, de-identification, reporting and retention of personal information

De-Identification

- Process of **removing personal information** from a record or dataset
 - Basic technique is to ensure result contains a minimum number of individuals with the same attributes ("cell size")
- In general, privacy laws, including Ontario's, **do not apply** to de-identified information
 - Privacy laws apply only to "identifiable" information
 - Thinking is that if no individual can be identified, then no potential privacy harm
- However, also important to consider the privacy of **groups** of individuals
- Non-identifiable information can still be **stigmatizing**
 - "Big data" has made this a more pressing issue

Attribute Disclosure Fictional Example

- The population of students who identify as race X in school Y is 87
- Linking ARA data with other school data shows that 55 of these students receive special-needs education
- 55 / 87 = 0.63 (63%)
- Important statistic, but should it be publicly released?
- Can somebody potentially learn something new / sensitive about race X students in school Y through inference?

De-Identification / Disclosure Control Best Practices

- Address both identity and attribute disclosure
- See IPC's "De-identification Guidelines for Structured Data" for reference / introduction to basic issues
- Consult with your legal counsel, privacy officer or MFIPPA coordinator
- Establish a disclosure review / avoidance committee to ensure public releases protect privacy and meet ethical obligations

Age Requirements for Consent under ARA

- ARA is a consent-based statute, yet it is silent on age requirements
- At what age can a student provide consent under the ARA? When can parents consent on behalf of a child for ARA purposes?
- Question of statutory interpretation, so ultimately seek legal advice
- MFIPPA and Education Act have different age requirements
 - MFIPPA: parent or guardian of child may consent on child's behalf only if **under 16**
 - Education Act: parent or guardian of student may provide written consent for use or disclosure of information in child's OSR only if **under 18**
- In general, Education Act applies to OSR, MFIPPA to information not part of the OSR
- So key question is whether ARA data forms part of the OSR

HOW TO 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 TDD/TTY: 416-325-7539 Web: www.ipc.on.ca E-mail: info@ipc.on.ca Media: media@ipc.on.ca / 416-326-3965