Privacy at the Border

Transborder Data Flows and Privacy Considerations

Karim Benyekhlef
Professor, Université de Montréal
Director, Centre de recherche en droit public

Université de Montréal

CENTRE DE RECHERCHE EN DROIT PUBLIC

I

The Right to Privacy in the *Canadian Charter of Rights and Freedoms*

Canadian Charter of Rights and Freedoms

- Section 8: Everyone has the right to be secure against unreasonable search and seizure.
  - Protects individual vs. government only
    - Reasonable expectation of privacy
    - Search / seizure reasonable

Canadian Charter, cont'd

- Reasonable Expectation of Privacy
  - Protects Territorial Privacy, Personal Privacy and Informational Privacy
  - Protects biographical core of information
  - Applies to commercial records
  - Varies according to context
  - Balancing State interest vs. individual interest

Canadian Charter, cont'd

- Very low expectation of privacy at the border
  - For example, no reasonable expectation of privacy for information from Customs declaration when shared with social security agency for data matching
- Reasonableness standard for intrusive searches: « Reasonable grounds to suspect »
- No reasonableness standard for non-intrusive examination of goods

II

Statutory Protection of Privacy in Canada

Privacy Legislation

- ***Privacy Act*** *&* ***Access to Information Act*** (federal public sector)
- ***PIPEDA: Personal Information Protection and Electronic Documents Act*** (federal & provincial* private sectors)
- ***Customs Act***, ***Criminal Code*** and other sector-specific statutes
- Provincial Privacy Legislation (public & private* sectors)

Privacy Act, *R.S.C., 1985, c. P-21*

- Applies only to federal government institutions
- Broad definition of personal information (s. 3)
- Collection must be relate directly to operating a program or activity (s .4)
- Collection from person to whom information relates (s. 5(1))
- Institution must identify purpose of collection (s. 5(2))
- Institutions must ensure information is accurate, up-to-date and complete as possible (s. 6)
- Principle of consistent use (s.7) and non-disclosure (s.8)
- Right to access and request correction (s.12)
- Ombudsman role of Privacy Commissioner (ss. 53-68)

Privacy Act, Cont'd

- Section 8 provides list of exceptions to prohibition of disclosure, including:
  - Any purpose in accordance with federal law (2(b))
  - Law enforcement and investigation (2)(e)
  - Under an agreement with a foreign state ((2)(f))
  - For any purpose where public interest outweighs invasion of privacy (as judged by department head) (2)(m)
- Use by receiving institutions still limited (s. 7)
- Ss. 18-28 provide exceptions to right to access, including:
  - Law enforcement and national security (s. 21 & 22)

Personal Information Protection and Electronic Documents Act (PIPEDA), 2000, c. 5

Governs private sector organizations

CSA Ten Privacy Principles:

1. Accountability.
2. Identifying purposes.
3. Consent.
4. Limiting collection.
5. Limiting use, disclosure and retention.
6. Accuracy.
7. Safeguards.
8. Openness.
9. Individual access.
10. Challenging compliance.

PIPEDA Cont'd

Exceptions to non-disclosure:

- Disclosure made to a government institution that has made a request for the information and that
  - (i) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
  - (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law. (s.7(3)(c.1))
- Disclosure required by law (s.7(3)(i))

- The federal institution that collects this data must then comply with the *Privacy Act* and its consistent use principles

III

Privacy at the Border

Disclosure of Customs Information Permitted by Law

- S. 107 *Customs Act,* 1985, c. 1 (2nd Supp.), prohibits disclosure of Customs information to third parties, with numerous exceptions:
  - S. 107(4&5) allows sharing with law enforcement with or without warrant, voluntary or upon request solely for criminal investigations or national security purposes, to designated persons only
  - S. 107(6) allows sharing with "any person" by the Minister if public interest outweighs invasion of privacy. He must, however, notify Privacy Commissioner in advance
  - S. 107(8) *Customs Act* permits disclosure of customs information to a foreign government or international organization solely in accordance with purposes and procedure stated in an international agreement:
    - Mutual Legal Assistance Treaty (MLAT)
    - Customs Mutual Assistance Agreement (CMAA)

Program 1

Integrated Customs Enforcement System Database (ICES) and the Shared Lookout Initiative

Collection and Disclosure of Customs Information

- Canadian Border Security Agency (CBSA) is empowered by the *Customs Act* to collect information from customs violations, declarations, through searches, etc. from persons entering Canada

- Stored in Integrated Customs Enforcement System (ICES database):
  - Customs information collected at the border, infractions, violations, customs officers notebooks etc.
  - Information from law enforcement and intelligence agencies
  - Information stored in databank used to identify individuals who have committed or are suspected of infractions against the *Customs Act*
  - Information retained for a maximum of 6 years.

Shared Lookout Initiative and U.S./Canada Data Sharing

- Lookout is created based on analysis of Integrated Customs Enforcement System Database (ICES), and through information from intelligence and law enforcement services
- Lookouts received from foreign governments, including U.S.
- Flags travellers for automatic secondary screening based on intelligence and risk indicators
- Lookout information electronically shared with U.S. customs
- Information is also shared with U.S. through more informal, non automated mechanisms at regional level

Shared Lookout Initiative Cont'd

Privacy Commissioner Concerns –Exchange of Customs Information

- CBSA cannot report on the extent to which it shares personal information with the United States, or how much and how often it does
- Not all lookouts subjected to review process prior to being shared with the U.S.
- Some lookouts identify travellers by name only
- Lack of data to indicate effectiveness

Program 2

PAXIS Passenger Information Database and High Risk Traveller Initiative

Airline Passenger Information

- CBSA requires airline companies to provide passenger information prior to arrival in Canada (s. 107.1 *Customs Act, Passenger Information (Customs) Regulations)*:
  - Advance Passenger Information (API)
    - Name, date of birth, gender, citizenship, passport or travel document information, reservation number
  - Passenger Name Record Information (PNR)
    - Travel itinerary, address, phone number, check-in information, manner in which ticket paid…
    - Only airline companies are required provide this information along with API, upon departure
  - This information stored in the Passenger Information System (PAXIS Database)

Disclosure of Customs Airline Passenger Information

- Disclosure of Passenger Information System (PAXIS) data is more restricted than other forms of customs information:
  - It may only be retained and/or disclosed to another government department or foreign state “for the purpose of identifying persons who are or may be involved with or connected to terrorism or terrorism-related crimes or other serious crimes, including organized crime, that are transnational in nature” (*Protection of Passenger Information Regulations)*

Airline Passenger Information PAXIS Database

- Airline company provides to CBSA API/PNR information on a traveller
- Entered into PAXIS database and run against established risk patterns
- Officials use pattern-based analysis of database used to create lookouts that subject travellers to secondary screening each time they cross the border
- If high risk score, automatically shared with the U.S. to query against its databases (High Risk Traveller Initiative Framework)
  - Item 8 U.S. / Canada Smart Border Action Plan
- If data match exists, U.S. sends back information from its databases
- Information only stored in PAXIS for purposes connected to terrorism or transnational crime

Airline Passenger Information PAXIS Database, Cont'd

- Advance Passenger Information (API) and Passenger Name Record (PNR) information stored separately
- After 72 hours of receiving data, access is restricted and depersonalized for trend analysis
- API may not be used to gain access to PNR information unless related to terrorism or transnational crime
- After 2 years, PNR information can only be linked to passenger name upon permission from the President of CBSA
- After 3 ½ years, information can be transferred to an enforcement system for maximum 6 years

Airline Passenger Information PAXIS Database, Cont'd

Privacy Commissioner Concerns

- PAXIS – High Risk Travel Initiative
  - Access and logging of data base activity by CBSA officials
  - Volume of information exchanged: s. 4 *Privacy Act*: collection of personal information should be limited to that information which is necessary for the organization to carry out its legislative mandate.
  - No formalized agreement with U.S. covering security and accuracy of information (s. 8(f) Privacy Act)
  - No formal assessment of High Risk Travel Initiative program to assess effectiveness and to ensure accuracy of information
    - False positives
  - Lack of transparency and publicly available information on transborder data flows

IV

Passenger Protect Program
“No-Fly List”

Passenger Protect Program – "No-Fly List"

- Transport Canada, Royal Canadian Mounted Police (RCMP), and Canadian Security Intelligence Service (CSIS) can also request API/PNR information from airlines, under *Aeronautics Act*
  - For purposes related to aviation security or national security
  - Must purge data within 7 days, unless held for national security purposes
- Passenger Protect Program ("No-Fly list")
  - List of names compiled based on intelligence information
  - Airlines required to contact Transport Canada if passenger information match and send API/PNR data
  - Passengers unable to board flight until clearance from Transport Canada

Passenger Protect Program – "No-Fly List", Cont'd

Privacy Commissioner Concerns

- Program high priority for privacy audit
- Lack of clear, transparent criteria for inclusion of name on list – suspicion basis
- CSIS and RCMP able to use information for purposes unrelated to aviation security
- Nothing to prevent airlines from sharing information with foreign countries
- Reconsideration process inadequate: lack of procedural fairness
- Great consequences of individuals denied boarding

V

Conclusion

General Concerns- Transborder Data Flows

- Right to access and to ensure accuracy (s. 12 *Privacy Act)*
  - National security or law enforcement exceptions
- Lack of transparency, clarity and information on use of personal information
- Absence in the US of a privacy commissioner to overview data collection and storage (audit, control)
- Long-term storage, use and disclosure of information on the basis of suspicion
- Lack of safeguards once information shared with foreign authorities