SECURITY LAWS AND PRIVACY: THE BALANCE

A Case Study: Privacy Vs. Security

Riley Information Services - Seminars
Ottawa, October 20, 2003
Eloïse Gratton
INTRODUCTION

The legal system is undergoing major changes due to emerging technologies:

- In arresting criminals:
  - Using wireless technologies to locate the accused at the time of a specific crime

- In convicting criminals:
  - Introducing as evidence, location data, to convict a criminal
RIGHT TO PRIVACY: CANADA

- Personal Information and Protection of Electronic Documents Act;
- Privacy Act;
- Criminal Code;
- Articles 7 and 8 of the Canadian Charter of Rights and Freedom;
- Article 12 of the Universal Declaration of Human Rights;
- Article 17 of the International Covenant on Civil and Political Rights;
RIGHT TO PRIVACY: QUEBEC

- An Act respecting the protection of personal information in the private sector;
- An Act respecting Access to documents held by public bodies and the Protection of personal information;
- Quebec Charter of Human Rights and Freedoms;
- Articles 35 to 41 of the Civil Code of Quebec.
RECENT SECURITY INITIATIVES

- Anti-Terrorism Act (Bill C-36);
- Public Safety Act, 2002 (Bill C-17) (replacing C-55 that died on September 16, 2002, which was replacing Bill C-42 (2001));
- Lawful Access Initiative;
- CCRA Big Brother Database;
- National ID card;
- Police Video Surveillance.
Employer Forcing Consent to Security Screening

- PIPED Act case # 65 = Not well founded;
- Field: Operations involved in the nuclear products;
- Security clearance check – criminal check;
- Consent forms with details that employees had to execute in order to keep their job;
- Given the enhanced concerns about possible acts of terrorism at nuclear facilities after 911, the security check was found to be reasonable.
PRIVACY Vs SECURITY CASE NO 2

- Employer Forcing Consent to Security Screening
  - PIPED Act case # 127 = Not well founded;
  - Field: Telecommunications company – position at a restricted area of an airport;
  - Security clearance check / screening processes;
  - Employee initially signed an acknowledgment form but never enforced until terrorist attacks on the U.S., increased vigilance on the part of the security personnel;
  - Decision: Reasonable for airport personnel to take such measures given the increased threat of terrorism.
Video Surveillance Activities in a public place

- PIPED Act Case #1 = Well Founded;
- Complaint that personal information is collected by a security company;
- Security company admitted that the surveillance activity was a marketing demonstration;
- However, the Commissioner specifies that the monitoring public places for public safety reasons are appropriated “if there is a demonstrable need”.
PRIVACY Vs SECURITY: Video Surveillance

Video Surveillance Activities in a public place - Quebec perspective:

- In 1992, the CAI refused to allow the police force to use video surveillance for monitoring residents of a certain neighborhood where many criminal activities were taking place;

- In May 2003, the CAI, following the incidents of September 11th, has published minimum requirements that should be followed when using video surveillance for security purposes.
Quebec minimum requirements that should be followed when using video surveillance for security purposes:

- Study and analysis of risks, dangers and criminal activity with police force / insurance companies;
- Analysis of less intrusive alternatives and solutions;
- Limited to certain periods;
- Informing the public with appropriate notice;
- Only registration / retention of relevant data;
- Cameras never directed to certain sensitive areas;
- Access rights.
Wireless Profiling and Data mining for National Security Purposes

- E911 may be a market driver for accurate location data;
- E911 is an exception to the non-disclosure of location data: U.S legal framework:
Telecommunications Act, Section 222 (d):

“Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary information (..) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user’s call for emergency services”
Wireless Profiling and Data mining for National Security Purposes

Quebec: Article 43 of an Act to establish a legal framework for information technology (2000):

“A person may not be required to submit, for identification purposes, to a process or device that affects the person’s physical integrity. Unless otherwise expressly provided by law for health protection or public security reasons, a person may not be required to be connected to a device that allows the person’s whereabouts to be known at all times”
Wireless Profiling and Data mining

Europe: Article 15 (1) Privacy Directive 2002/58/EC (July 2002) provides for the possibility to override wireless privacy restrictions with legislative measures:

“if necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system.”
Catching a Specific Target Using Wireless Technologies

  - Tracking of serial killer using a GPS receiver installed in the suspect’s car.

- The effectiveness of this method in order to solve a crime:
  - Many assumptions: Specific target can be tracked/located at each crime scene location.
  - Success Rate: How many arrests? / convictions?
PRIVACY Vs SECURITY: Wireless Tracking

- Wireless Profiling and Tracking:
  - Is the intrusion of fundamental rights proportional to the security benefit pursued?
  - Only in presence of a clear demonstration that no less privacy intrusive measures would achieve the same result.
CONCLUSION

- Access to location data should only be used with legal authority;

- Authorizations to collect and track location data should ONLY be used to:
  - Target specific criminals;
  - Carried out for a specific period of time.

- Warrant to search and seize data should ONLY be granted if:
  - Reasonable grounds to believe that an offence has been committed.
Eloïse Gratton
MENDELSON
Email: egratton@mendelsohn.ca
Tel: (514) 987-5093
Website: www.mendelsohn.ca