The Evolving Role of Cyber Surveillance in Public Sector Decision-Making

Office of the Privacy Commissioner of Canada
Contributions Program

Tamir Israel
Staff Lawyer, CIPPIC
www.cippic.ca
tisrael@cippic.ca

June 2, 2011
University of Ottawa – Faculty of Law

Semi/Publicly Available Info

- Increasing use of publicly available online data in various decision-making processes
- Specific examples of uses are still difficult to track
- Did manage to get glimpse of general scope/character

Semi/Publicly Available Info

Used across the board:

- 'Facebook' averages about 6 QL hits/week
- Many Tort/family lawsuits; Discovery
  - Lawyer's Professional Responsibility to use/pursue available data sources
  - Issues concerning context
- Courts have generally recognized some privacy expectation in semi-public data in discovery context

Semi/Publicly Available Info

PUBLIC SECTOR

- Expanded use of online data evident in various investigative and decision-making capacities
- Drivers: Community outreach initiatives; community presence; efficiency in surveillance techniques; and ‘more data = better decision-making’
- Rationales: reputation management; community presence; specific investigative purposes; more general investigative purposes

Semi/Publicly Available Info

PUBLIC SECTOR

- Types of Relevant Info: meta-data, 'social network', location, opinions/thoughts, political affiliations, identity, recreating specific interactions/events; undercover fact-finding
- Evident in: politics, social services enforcement, crime enforcement, national security, crowd control, immigration, teenage party control
- Some ad hoc, some within a policy framework

Semi/Publicly Available Info

PUBLIC SECTOR: Range of Approaches

< 40% of surveyed Gov organizations had policies

- In some contexts, use of such data is "done by…investigators on an ad hoc basis (often after seeking direction from…local Crown counsel)."

– Saskatoon Police Services, email correspondence, February 2, 2011

Semi/Publicly Available Info

PUBLIC SECTOR: Range of Approaches

- Some explicitly refrain from using online data sources such as SNSs in investigations because “the reliability of information found on these sites (such as Facebook) would always be suspect.”

– BC Ministry of Housing & Social Development, Prevention and Loss Management Branch

Semi/Publicly Available Info

PUBLIC SECTOR: Range of Approaches

- Some are forward looking, putting in place governance structures tasked with overseeing future expansions of SNS use/interactions as part of service delivery

– Health Canada

Semi/Publicly Available Info

PUBLIC SECTOR: Range of Approaches

- Some have comprehensive policies and training courses for investigators covering the range of
- TC0106 Computer and Technology Facilitated Investigations, offered as of 2010 for TPS

– Toronto Police Services

Semi/Publicly Available Info

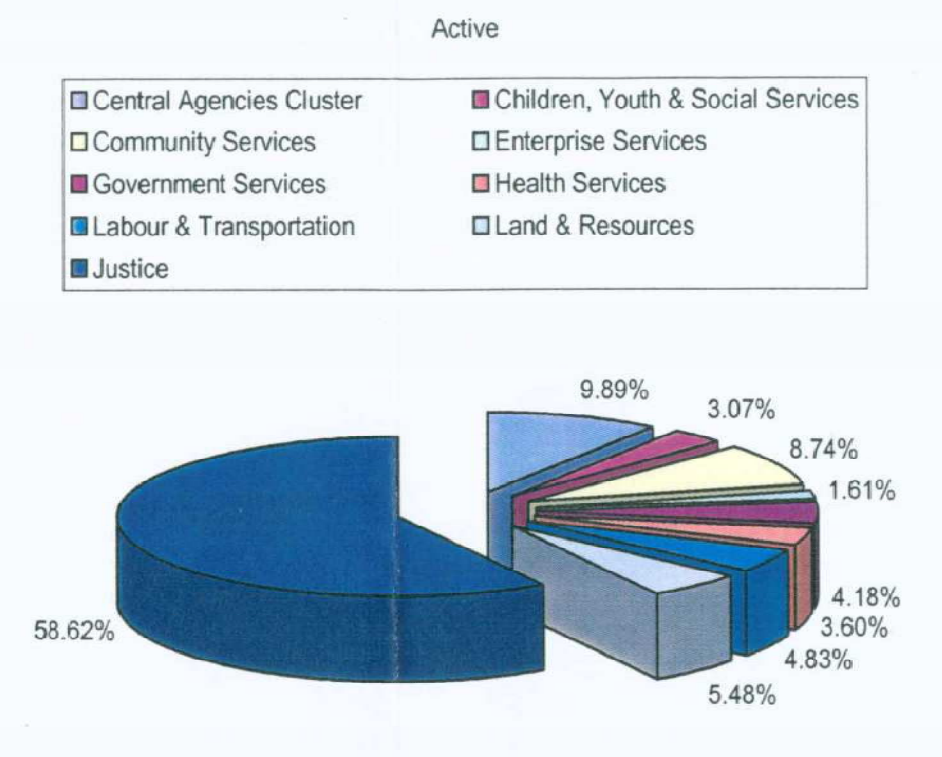
PUBLIC SECTOR: Definitely happening

- "The Canada Border Services Agency utilizes both open source information as well as information from law databases during the course of immigration investigations. Open source information can include websites, directories, maps, etc. to assist in locating individuals of interest."

– CBSA ATI response, February 21, 2011

Publicly Available Info

Web Filtering Exemptions: Ontario, Ministry of Government Services



Category/Purpose	#
Ministry Communications & Issues Management	256
Policy, Marketing, Research, Analysts	455
Staff Employed by O.P.P.	273
Inspection & Enforcement	1333
Ministry Corporate Offices	293
TOTAL	**2610**

Obtained by CIPPIC via ATI Request filed January 2011

Semi/Publicly Available Info

RCMP – Web Filtering/Equipment Requests

- 'Mobile Command Posts': developed/configured during G8/G20; used for "information gathering during operations/major events"; access to Twitter, Facebook required.
- Purposes: Financial crimes; drug enforcement; major events; organized crime unit 'covert operations'; "general policing"; national security criminal investigations; critical infrastructure criminal intelligence; national gun registry application assessment.
- Scope: ranges from individual officers for specific types of operational purposes to entire units involved in a specific class of investigations, to entire divisions for general policing purposes.

Semi/Publicly Available Info

OF GENERAL NOTE

- Some awareness of potential inaccuracy of data: future inteligence analysts “will need to be more comfortable with technology but there is also that danger of relying on the tools too much and not recognizing the limitations.” [Privy Council Office, Intelligence Analysts – Future Competency Requirements]
- Some recognition that open source data can be ‘secret’: “while information from websites are open source, the final designation will be dependent on the sensitivity concerning the criminal intelligence product that references website information.”
- Some expressed interest in “websites related to…any activities undertaken for political/religious/ideological motivations” or where relevant “opinions or ideas” might be presented by individuals.

Publicly Available Info

Types of Potential Concerns:

- Potential for misuse of information that would not historically have been available to decision-makers (i.e. discrimination based on political beliefs)
- New medium, new methodologies. Context of information not always fully understood, and may lead to inaccurate outcomes (can be mitigated by better training)
- Growing disconnection between subjective and objective privacy expectations
- Amount and scope of information now available

Publicly Available Info

While Mr. DeWaard's Facebook profile is not completely consistent with his evidence at trial, I am prepared to accept that Facebook profiles may contain an overly positive perspective regarding one's abilities and interests or a certain amount of puffery. Mr. DeWaard is currently able to maintain a reasonably active life style, but it is less active than before and he can no longer engage in some of the activities he previously enjoyed.

DeWaard v. Capture the Flag Indoor Ltd, 2010 ABQB 571,
http://www.canlii.org/en/ab/abqb/doc/2010/2010abqb571/2010abqb571.html

Shifting Role of Online Intermediaries

‘Hands off the Net’

‘Regulation of Individual Online Activity’

‘Mobilization of Online Intermediaries’

- Increasing international pressure for online intermediaries to assist in achieving public policy objectives
- Can be mandatory, discretionary, or ‘voluntary’
- G8/OECD

Shifting Role of Online Intermediaries

CONCERNS:

- Potential normative impact of online intermediaries is great in scope.
- Private sector lacks institutional capacity for objective judicial-like decision making.
- Safeguards traditionally applicable to state information collection do not apply to private sector.
- Civil society has salient concerns but no way to voice them.

Shifting Role of Online Intermediaries

ABSENCE OF SAFEGUARDS:

- Private sector subject to different signaling (market pressures vs. democratic pressures). Less responsive to minority concerns. Increasingly responsive to government pressures. *Are* responsive to costs, where present.
- *Charter*; Legislation; Common Law – to date, not helpful.
  - Potential: fiduciary-like duties; Public Utility/Common Carrier-based obligations; 'Agency' doctrine
  - Narrow interpretation of wiretapping/communication interception [*R. v. Telus*, 2011 ONSC 1143, 'general warrant' for all text messages, proactive, not 'interception']
- Private sector seen as individual: has *always* had free discretion to assist law enforcement.

Shifting Role of Online Intermediaries

ATI Response on policies governing information requests from CIRA

2/21 pages excluded for their capacity to reveal investigative methods or techniques

7/21 pages excluded for their capacity to reveal third party (i.e. CIRA) ‘financial, commercial, scientific or technical’ information that has been treated as confidential

Shifting Role of Online Intermediaries

Online Intermediary mechanisms for setting reasonableness of privacy expectations

Standard form contracts [appear definitive] + individual intermediary disclosure decisions

Public Policy-driven Industry Practices

Governance models

Shifting Role of Online Intermediaries

Case Study: CNA Data Disclosure

- Terms of Use: many online service providers include blanket terms ‘may assist law enforcement upon request’.
- Canadian ISPs: Have jointly decided to provide CNA data in child exploitation investigations.
  - Some (Shaw, for example) have begun disclosing in other contexts (online harassment investigation)
- CIRA: public consultations on WHOIS led to limited CNA disclosure policy. Only for child exploitation, malware, fraud investigations, critical infrastructure threats.

Shifting Role of Online Intermediaries

GENERAL FINDINGS OF NOTE:

- RCMP production order templates for CIRA CNA data concede that such data implicates a ‘biographical core’ of personal information.
- In the majority of CNA voluntary disclosure cases, law enforcement has quite clear reasonable grounds to believe the anonymous individual in question had committed an offence.
  - In most cases, the CNA data does not even avoid the requirement for a warrant down the road.