



Lawful Access & Data Retention: A Civil Society Perspective

Philippa Lawson

Director

Canadian Internet Policy and Public Interest Clinic

University of Ottawa

www.cippic.ca



uOttawa

L'Université canadienne
Canada's university

“Lawful Access”

= the interception of communications and search and seizure of information carried out pursuant to legal authority under the *Criminal Code*, *CSIS Act*, *Competition Act*, and other federal legislation.



uOttawa

L'Université canadienne
Canada's university

“Data Retention”

- Mandatory laws requiring TSPs to retain certain subscriber/user data for a certain time period, so that it is available for police searches
- Data could include:
 - subscriber information (after cancellation)
 - message transmission information
 - web activity (URLs visited, etc.)
 - content of messages



EU Data Retention Directive

- applies to “providers of publicly available electronic communications services”
- “data” = “traffic data and location data and the related data necessary to identify the subscriber or user”
 - NOT content of messages
- retention period: 6 mos to 2 years
 - up to each member country
- no obligation to collect information not otherwise being collected



Civil Society Response

- coalition of over 60 civil liberties groups opposed to EU directive
- petition signed by >16,000 individuals in matter of days
- EU Privacy Commissioners opposed
- many EU Commissioners opposed



Canadian proposals

- no mandatory data retention proposal
- instead, “**Preservation Orders**”
 - specific communications only
 - temporary (90 day; 15 day interim)
 - judicial authorization required
 - reasonable grounds to suspect....
 - no LEA access w/o separate judicial order
 - process for TSP objection



Production Orders

- currently in place:
 - ss.487, Criminal Code
 - General Production Order
 - requires judicial authorization on a “reasonable grounds to believe” standard
 - Financial Institutions Production Order
 - name, account #, status/type of account, opening/closing dates
 - requires judicial authorization on a “reasonable grounds to suspect” standard



Proposed New Prod'n Orders

- “tracking information”
 - to locate a suspect – e.g., via debit card or cell phone usage
- “transmission data”
 - re: telecom dialling, routing, addressing or signalling; that identifies origin, date, time, duration, destination or termination of a telecommunication
- both to be granted on “reas. grounds to suspect” threshold



Other new powers

- *Public Safety Act, 2002*
 - amended PIPEDA to permit private organizations to collect personal information surreptitiously for “national security” purposes
- *Anti-terrorism Act (2001)*
 - warrantless interception of foreign communications
 - interception need not be “last resort” for terrorism-related investigations



Mandatory Intercept Capability



- applicable to all TSPs
 - phase-in for small TSPs
 - exceptions for charities, universities, etc.
- must build in new interception capability so that LEAs relieved of effort & so that more simultaneous intercepts are possible
 - incremental (as facilities are upgraded)
 - must ensure new facilities meet requirements
 - heavy penalties for non-compliance
- must provide intercepted comm's to LEAs
- must decode/decrypt where possible
- must permit simultaneous intercepts by multiple LEAs



uOttawa

L'Université canadienne
Canada's university

Access to Subscriber Data

- subscriber identifiers only
 - as defined in MITA regulations: name, billing address, e-mail address, tel #, Internet ID, other?
- mandatory, upon request by LEA
- no judicial authorization required
- gag orders re: LEA requests?
 - in original proposal

Access to Subscriber Data

- MITA safeguards:
 - must be re: specific individual (identifier required)
 - must be in writing
 - must be re: “duty or power” of LEA
 - can use only for consistent purpose
 - < 5% of LEAs allowed to make requests
 - except where urgent
 - requester must keep record of requests
 - subject to regular internal audit
 - LEAs must report important findings to Minister, cc'ing PrivCom, SIRC or provincial authority
 - subject to discretionary audit by PrivCom, SIRC, or provinces



Civil Society Concerns

- lack of justification: are the new powers really needed?
- building an architecture of surveillance
- mandated warrantless access to any personal info = serious breach of principle of judicial oversight
- inadequate oversight/accountability
 - proposal for new oversight body (SARC)
- inadequate data protection safeguards





www.cippic.ca



uOttawa

L'Université canadienne
Canada's university