

Global IT Law
Privacy
January 11, 2017

professor michael geist
university of ottawa, faculty of law

Emerging IT Issues

Data Localization

Data Localization

- Growing trend in response to Snowden
- Requirements to retain data locally
- Changing architecture of cloud services
- British Columbia case
 - Health processing data
 - Retention requirements in province
- TPP requirements (data localization and data transfer)
- Future challenge: EU/Data localization demands vs. TPP/corporate pressure

Standard of Consent

Opt-in vs. Opt-out

– Examples

- Bell RAP
- Anti-spam laws
- EU law
- U.S. lower standard

– Shift away from consent?

- Is consent fictional?
- Alternatives – focus on use?

WHOIS

Whois

Registrant:

Michael Geist
57 Louis Pasteur
Ottawa, ON K1N6N5
Canada

Registrar: DOTSTER

Domain Name: MICHAELGEIST.COM

Created on: 27-FEB-00
Expires on: 27-FEB-07
Last Updated on: 05-JUN-06

Administrative Contact:

Geist, Michael mgeist@netcom.ca
57 Louis Pasteur
Ottawa, ON K1N6N5
US
6135625800

Technical Contact:

Geist, Michael mgeist@netcom.ca
57 Louis Pasteur
Ottawa, ON K1N6N5
US
6135625800

Domain servers in listed order:

NS1.NAMERESOLVE.COM
NS2.NAMERESOLVE.COM
NS3.NAMERESOLVE.COM
NS4.NAMERESOLVE.COM

End of Whois Information

END WHOIS RECORD -----

Whois

Whois

Whois Information For: michaelgeist.com

BEGIN WHOIS RECORD -----

The information in this whois database is provided for the sole purpose of assisting you in obtaining information about domain name registration records. This information is available "as is," and we do not guarantee its accuracy. By submitting a whois query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) enable high volume, automated, electronic processes that stress or load this whois database system providing you this information; or (2) allow, enable, or otherwise support the transmission of mass, unsolicited, commercial advertising or solicitations via facsimile, electronic mail, or by telephone to entities other than your own existing customers. The compilation, repackaging, dissemination or other use of this data is expressly prohibited without prior written consent from this company. We reserve the right to modify these terms at any time. By submitting an inquiry, you agree to these terms of usage and limitations of warranty. Please limit your queries to 10 per minute and one connection. If you have a legitimate purpose for whois information please contact our customer service department.

Whois

Two Key Issues:

- What information is collected?
- What information is disclosed?
 - To whom?
 - In what circumstances?

Whois

ICANN Registrar Agreement

At its expense, Registrar shall provide an interactive web page and a port 43 Whois service providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar for each TLD in which it is accredited. The data accessible shall consist of elements that are designated from time to time according to an ICANN adopted specification or policy. Until ICANN otherwise specifies by means of an ICANN adopted specification or policy, this data shall consist of the following elements as contained in Registrar's database:

Whois

ICANN Registrar Agreement

3.3.1.1 The name of the Registered Name;

3.3.1.2 The names of the primary nameserver and secondary nameserver(s) for the Registered Name;

3.3.1.3 The identity of Registrar (which may be provided through Registrar's website);

3.3.1.4 The original creation date of the registration;

3.3.1.5 The expiration date of the registration;

3.3.1.6 The name and postal address of the Registered Name Holder;

3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and

3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

Whois

Required Provisions in Service Agreements with Registrants

Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the following provisions:

3.7.7.1 The Registered Name Holder shall provide to Registrar **accurate and reliable contact details** and promptly correct and update them during the term of the Registered Name registration, including: the **full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder**; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8.

Whois

Required Provisions in Service Agreements with Registrants

Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the following provisions:

3.7.7.2 A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration.

Whois

Intersection with:

- Intellectual property
- Security/Law Enforcement
- Privacy
- Spam/Phishing
- Free Speech
- Government

CIRA Whois

- Major change in 2008
- Remove data on individual registrants (personal info) --> 70% of registrations
- CIRA serves as intermediary for contacting registrants
- Exceptions for:
 - Law enforcement
 - IP issues

Network Privacy Case Study

Emmanuel Goldstein, a well-known computer programmer, calls you in a panic. “I need to talk to you right away”, he says, barely able to catch his breath. “You’re the leading privacy expert in the country and I’ve just experienced the most bizarre hour of my life. I’m hoping you can provide some quick advice.” You tell Goldstein to calm down and tell you what happened.

“Well, I was walking my dog around the neighbourhood, when suddenly a policeman approached me. He said that there had just been a robbery a few blocks away and they were investigating. He asked me to hand over identification and my mobile phone. My phone was on without password protection and he proceeded to search through my recent text messages. When I asked what he was doing, he told me that I was a suspect and that he was searching to see whether there was any relevant information on my phone. He then told me that he would be contacting my Internet provider to ask for my IP address in order to see if there were any online clues that might help the investigation as well as my wireless provider to check whether my cell phone contacted the tower near to the robbery. He told me he could obtain this information immediately without a warrant. Is that possible?”

Network Privacy Case Study

Goldstein needs immediate answers:

1. Do you think the police search of the cellphone without a warrant is lawful? If so, why?
2. Do you think the ISP will provide the IP address without a warrant?
3. Do you think the wireless provider will provide the tower information on users in the area? How broad (timing, users, etc.) the disclosure might be? With or without a warrant?

ISPs – Subscriber Information

Who Wants It?

- Surveillance Agencies
- Law Enforcement
- Private Sector

Israel

- Communications Data Law (2007) aka “Big Brother Law”
 - Court order (details on investigation, carried out within 30 days)
 - Police can order disclosure in emergent circumstances for 24 hours, insufficient time for court order
 - Information covers location data, IP address, subscriber data, traffic data
 - Database on basic subscriber information
- Law challenged before Israeli Supreme Court in 2012
 - Upholds the validity of the law
 - Says can only be used for specific subjects or incidents, not general investigations

Law Enforcement

- CRTC
 - 1980s - Prohibit disclosure unless written consent or legally required, exception for name, address & telephone number
 - LSPID
 - provider info subject to tariff (2001)
 - Requires law authority
 - Expanded to emergency situations in 2002

Law Enforcement

- PIPEDA

Section 7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it 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, or

iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

Law Enforcement

- 2005 – Canadian Coalition Against Internet Child Exploitation (“CCAICE”) creates form to allow for “pre-warrant” disclosures
- Most TSPs adopt position CNA disclosures do not require a warrant
- But...not all
- Becomes lawful access issue

Lawful Access Subscriber Info (Beta)

- 2007 – CNA consultation
 - Assumes mandatory disclosure of subscriber information
 - Consultation about parameters of disclosures
 - Minister Stockwell Day backtracks when consult becomes public

Lawful Access Subscriber Info 1.0

- name and address
- telephone number
- electronic mail address
- Internet protocol address
- mobile identification number
- electronic serial number (ESN)
- local service provider identifier
- international mobile equipment identity (IMEI) number
- international mobile subscriber identity (IMSI) number
- subscriber identity module (SIM) card number that are associated with the subscriber's service and equipment.

Lawful Access Subscriber Info 2.0

- name and address
- telephone number
- electronic mail address
- Internet protocol address
- local service provider identifier

Lawful Access Subscriber Info 3.0

- No mandatory disclosure
- Expanded voluntary disclosure
 - Bill C-13 – full civil and criminal immunity for voluntary disclosures
 - Bill S-4 – expanded investigative bodies provision – permits voluntary disclosure to any private sector organization

SCC – R. v. Spencer

“in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.”