

Privacy and Accountability in the Cloud: Is this a new problem?

Colin J. Bennett,
Department of Political Science
University of Victoria
BC, Canada
www.colinbennett.ca
cjb@uvic.ca

Keynote address to the International
Workshop on Trustworthiness,
Accountability and Forensics in the Cloud ,
Malaga Spain, June 6, 2013



OECD Privacy Guidelines 1980

INTERNATIONAL ASPECTS OF PRIVACY AND DATABANKS

7. For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.

8. One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements.

9. There are other reasons why the regulation of the processing of personal data should be considered in an international context: the principles involved concern values which many nations are anxious to uphold and see generally accepted; they may help to save costs in international data traffic; countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in view of the international mobility of people, goods and commercial and scientific activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved.

A Test Case: Canadian Access to Social Media Information Project

www.catsmi.ca

- **23 top SNSs in terms of usage in Canada**
- **Content Analysis of Privacy Policies**
- **Tests of Subject Access to PII by researchers**
- **Law Enforcement Compliance Guides**

Funded by Social Sciences and Humanities Research Council of Canada (SSHRC) and Office of the Privacy Commissioner



Find out what some of your favourite Social media providers have to say about your privacy...

We posed these questions to **WIKIPEDIA**:

1.

What counts as personally identifiable information (PII) that the site collects?

Information includes username, email address, IP address, and other raw log data.

The company does not mention non-PII.

2.

How can you complain? Is there a specific privacy officer listed?

No process specified. There is a general 'Questions for Wikimedia?'

3.

Does the PII collected change depending on whether you're an adult or a child?

No.

a Network

Find out how one of your social networks treats your privacy...

a Question

Find out how social networks responded to a question...



Home / Learn About... / A Network

A NETWORK



TBDF: Organization to Organization approach

- Section 4.1.3 of Schedule One of the Canadian Personal Information Protection and Electronic Documents Act (*PIPEDA*):

“An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.”



The “Real and Substantial Connection to Canada” Test

- Acusearch Decision – www.abika.com (2009)
- Facebook Investigations (2009-2012)
- WhatsApp Investigation with Dutch DPA (2012-13)
- Cloud-Computing Applications

Compliance of top Social Network Services with Canadian law?

- **Inconsistent and incomplete statements of privacy principles**
- **Confusion about jurisdictional issues**
- **Instruments of recourse/complaint unclear**
- **Unresponsiveness to inquiries about policies**
- **Unresponsiveness to access to information requests**



Transborder Data Flows: country-country approaches

- **European Union: 1995 Directive**

The “adequacy” test

- **European Union: 2012 Draft Regulation**

The “adequacy and/or” test



Transborder Data Flows: Country-country approaches

- **The Council of Europe 1981 (Convention 108): an “equivalent” test**
- **The draft “modernized Convention” (2013): an “appropriate” test**



Transborder data flows: A hybrid approach

**Asia Pacific Economic Cooperation (APEC):
“The Cross-Border Privacy Rules system”**



Accountability Mechanisms

- Model contracts
- Binding Corporate Rules (BCRs)
- Privacy Management frameworks
- Technical standards
- Management standards
- Privacy Seals

BEWARE!

NEW DEFINITIONS AND FORMULATIONS



BEWARE!

THE REINVENTION OF THE WHEEL!



BEWARE!

VAGUENESS ABOUT WHO SHOULD
BE ACCOUNTABLE, FOR WHAT, AND
TO WHOM



BEWARE!

FLEXIBILITY AND SCALEABILITY



BEWARE!

INTEROPERABILITY



In Conclusion...

- Issues surrounding the transborder flow of personal data have been around for a long time, and have not been solved
- Dominant motivations are free flow, trust and risk management NOT the enforcement of the rights of the data subjects
- Accountability measures are valuable, but a means to an end not an end in itself