Encryption and Fundamental Rights

The XXXI Nordic Conference on Law & IT
10-11 November 2016

---

Joris van Hoboken, PhD
Senior Researcher, Institute for Information Law (IViR), University of Amsterdam
Affiliate Scholar, Stanford Center for Internet & Society, Stanford University
Affiliate Researcher, LSTS, VUB
Overview

- The post-Snowden turn to encryption;
  - Van Hoboken, Arnbak and Van Eijk, Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad, PLSC 2013.

- Encryption and human rights
  -- Forthcoming study for UNESCO;

- Encryption in the upcoming amendments to the ePrivacy Directive;
The post-Snowden turn to encryption
**PRISM Program Cost:** ~ $20M per year

**Current Efforts - Google**

**Exploitation of Common Internet Encryption Technologies**

- **Upstream**
  - Collection of communications on fiber cables and infrastructure as data flows past.
  - (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

- **PRISM**
  - Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.
The Post-Snowden Turn to Encryption

• Snowden revelations:
  – Large scale access to cloud and electronic communication service data (content as well as meta-data);
  – Demonstration of the lack of limitations vis a vis the data and communications of non-US persons;
  – ‘Circumvention’ of legal process by intelligence agencies (under 12333), e.g. Muscular program.
  – Deliberate introduction of backdoors in NIST encryption standards and covert financial incentives for adoption of such standards/

• Reactions:
  Legal (US system, International, European/elsewhere)
  Civil society:
  Industry: Transparency reporting and encryption
Reactions to the Revelations

- Legal/Government
  - US: Review Committee PPD-28, USA Freedom Act; Encryption debate;
  - International: UN Rapporteur on privacy, stipulation of international norms;
  - Europe/elsewhere: CJEU (Schrems/Safe Harbor), Germany/EP/EC/CoE; Brazil;

- Industry:
  - Intensified transparency reporting;
  - Quick adoption of better security of internal communications and channel to users (https);
  - More limited: end-to-end encryption (especially messenger services);

- Internet engineering community
  - New efforts to address mass surveillance in IETF and other forums;

- Civil society:
  - Litigation and campaigns against mass surveillance;
  - Campaigns to promote encryption adoption;
Analysis:

• Distinguish backdoor and front door lawful government access;

• Distinguish meta-data: much harder to protect and much more widely available to government;

• Back door access. Examples: Muscular program. Encryption backdoors. Intercepting unencrypted traffic from the wire.

• Front door: legal access through legal channels established by law and the procedures in relevant cloud service companies.

• Industry players could be using crypto to prevent government access to data, but most of all, it has been using it to shape lawful access in terms of the channels and locations where lawful access can take place.
Mass versus Targeted Surveillance

• Encryption promoted by civil society campaigns to protect against mass surveillance by the government (passive interception);

• Significant portion of counter-surveillance advocacy appears to be based on distinction between
  – targeted surveillance (bad guys, terrorists =>) and
  – mass surveillance.

• Definition of mass surveillance?
  – Technical: Bulk/indiscriminate/dragnet collection of data
  – Legal: General warrant / FISAAA 702 acquisitions / 12333;
  – Political: everyone, the innocent, the good, the privileged;

• ‘Nothing to hide’?
Human Rights and Encryption
Human rights and encryption
Overview of the Study

• Encryption in media and communications;
• Encryption and the law;
• Case Studies: (Germany, India, Unites States, Brazil and a selection of developments on the African continent);
• Normative implications of international human rights frameworks for the regulation of encryption. In-depth discussion of:
  1. the relevant notion of ‘uninhibited communications’,
  2. transparency about state action restricting availability of secure encryption;
  3. The notion of ‘security intermediaries’
• Recommendations.
Implications of HR framework for encryption policy

Analysis building on international human rights framework, in particular the right to freedom of expression and the right to privacy in article 17 and 19 ICCPR.

General requirement: restrictions on encryption should be proportional, necessary and pursue a legitimate aim;

The availability and free deployment of encryption supports the essential characteristic of ‘uninhibited communications’, which is an essential element of the effective enjoyment of freedom of expression and the right to private life;

For the protection of the rights to be effective, it is essential that there is transparency about state action restricting availability of secure encryption;

As individuals are increasingly dependent on private sector implementation of encryption by cloud services (‘security intermediaries’), these have an important role to play to ensure the availability of trustworthy security.
Thank you!

vanhoboken@uva.nl

Twitter: jorisvanhoboken

www.ivir.nl / jorisvanhoboken.nl