Cloud Computing at Risk? The Political Impact of the Surveillance Revelations

Ninja Marnau

Independent Centre for Privacy Protection
Schleswig-Holstein

What happened?

National security authorities' surveillance activities :

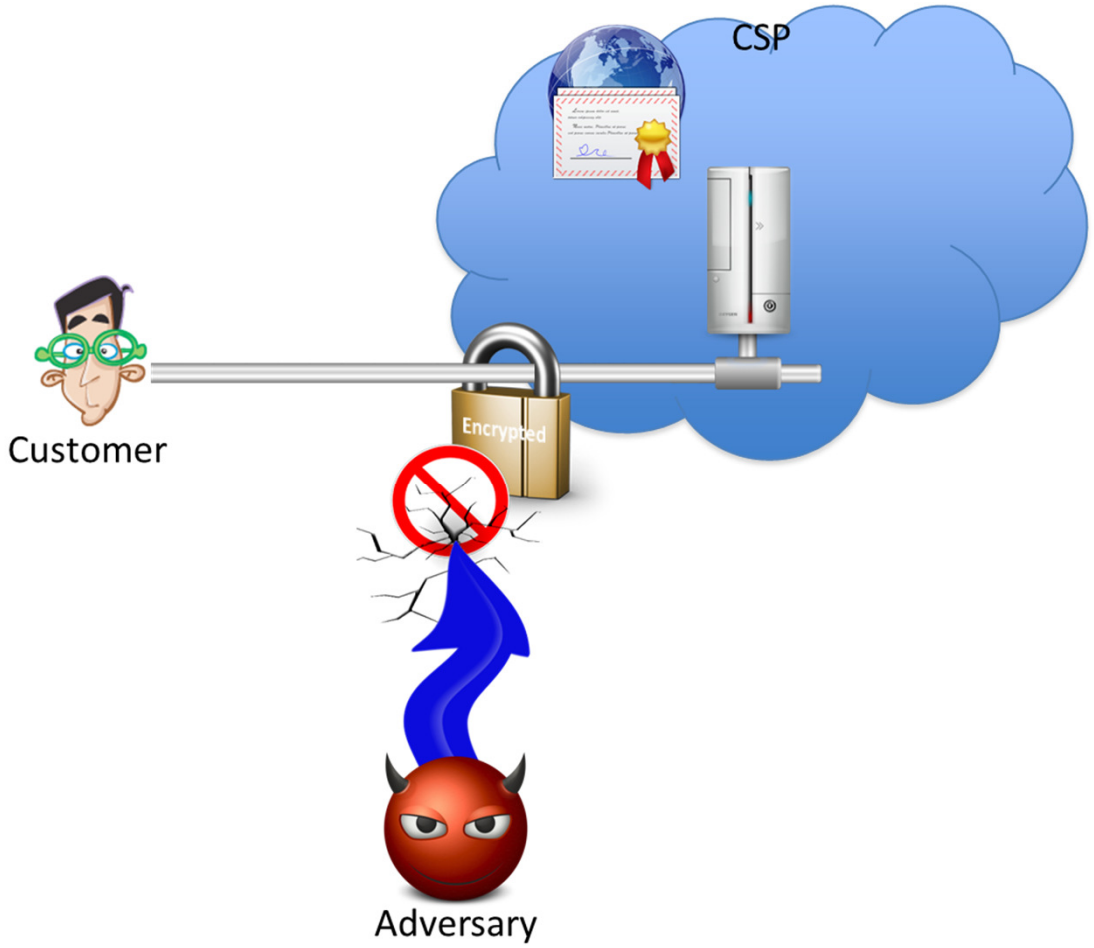
- Massive collection, retention and analysis of metadata around the globe
- Wiretapping of international communication cables and Internet Exchange Points
- Backdoors/direct access to commodity software and communication infrastructure
- Excessive options to force providers to hand out users' data
- Access to financial transactions via SWIFT network
- Purposeful vulnerabilities of encrypted communication (SSL, VPN)
- Compromising of other encryption standards?

Why is that problematic?

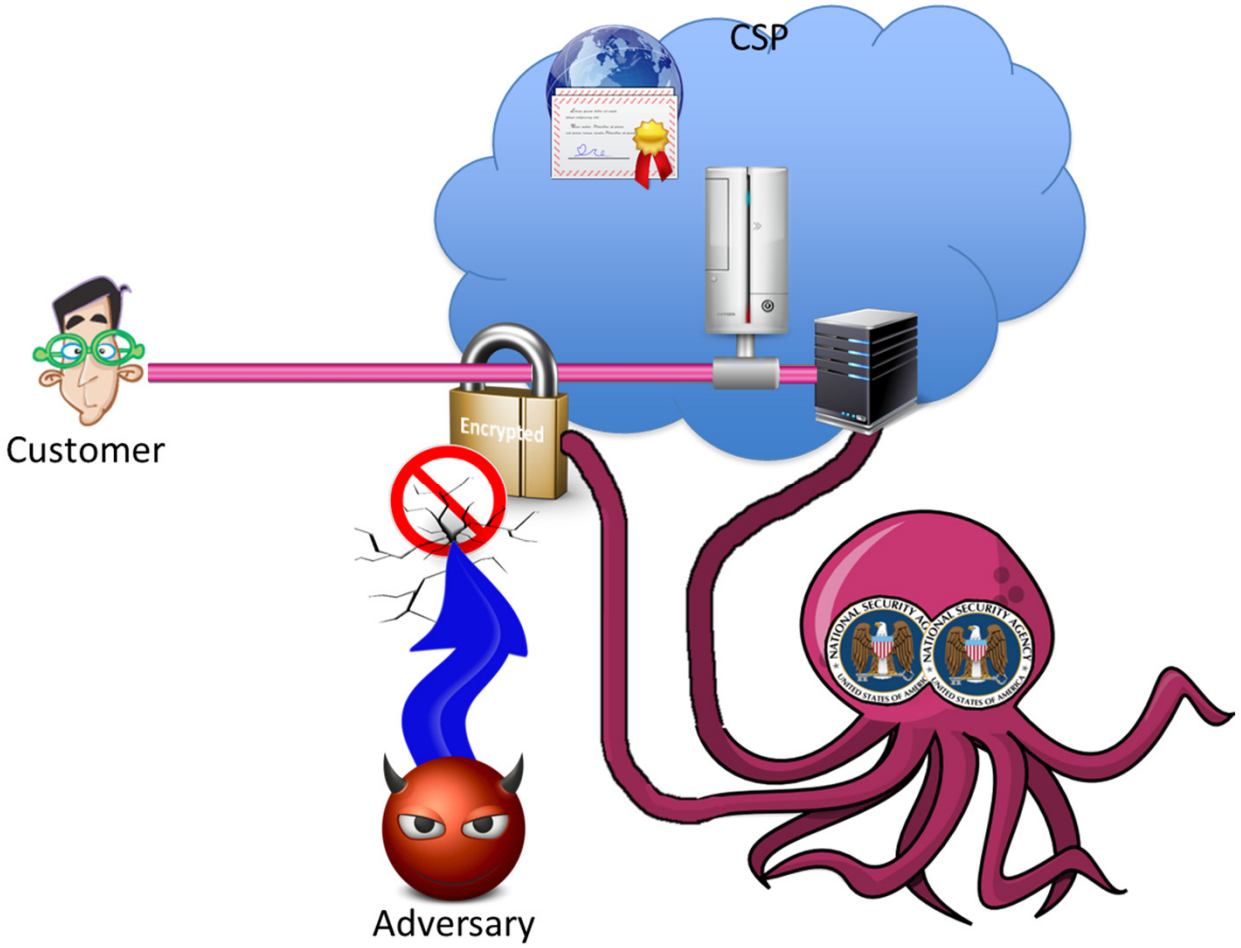
- National security provisions got completely out of hand since 2001
  - Lack of proportionality of laws and measures
  - Lack of transparency (secret laws and gag orders)
  - Non-functioning national democratic control
  - Non-functioning judicial scrutiny (secret courts with dubious staffing, secret decisions)
  - No information to the subjects
  - No possibility for legal actions
  - Discrimination of foreign citizens

The actual power of national security authorities infringes the essential **separation of powers** of a democratic state.

Trustworthy Clouds



~~Trustworthy~~ Clouds



Economic Consequences

- Asian countries:
  Mandatory PRISM security checks for authorities, review of used software and providers
- Global:
  CSA survey on the impact of th revelations (207 non US anwers, most from Europe)
  - 56% less likely to use US CSP
  - 10% cancelled at least one project with an US CSP
  - 31% no impact on usage of US CSP
  - 3% more likely to use a US CSP

Economic Consequences

- Global:
  Information Technology & Innovation Foundation (ITIF) forcast:
  - Between 21.5 and 35 billion US dollars drop in revenue over the next 3 years for US CSPs

- Germany:
  BITKOM survey
  - 2/3 of internet users have lost trust in communication confidentiality
  - 19% will reduce their usage of US-based internet services

Political Consequences

- Transfers of personal data within the EU rely on the fiction of comparable data protection levels
- Certain level of trust between the member states regarding industrial espionage
- EP *Committee on Civil Liberties, Justice and Home Affairs* is investigating QCHQ's activities

Political Consequences

- For legitimization of personal data transfer to the USA, the EU has acknowledged the Safe-Harbor Principles, PNR records and to some extent SWIFT
- Safe Harbor has always been criticised by DPAs
- All big US CSPs are Safe Harbor self-certified
- Actual Wording of the principles:
  "adherence to these principles may be limited [...] to the extent necessary to meet national security, public interests, or law enforcement requirements"

Political Consequences

After PRISM/Bullrun:

- Commissioner Reding announced a re-evaluation of Safe Harbor until the end of the year
- Article 29 Working Party will independently assess PRISM and especially the role of the FISA court
- German DPAs refrain from further data transfer authorization on basis of Safe Harbor

Is the EU Data Protection Regulation the solution?

A look at the proposal

One directly applicable data protection law for the EU

BUT: Article 2 (2) "This Regulation does not apply to the processing of personal data"

- a) "in the course of an activity which falls outside of the scope of Union law, in particular concerning national security"
- b) "by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."

Is the UN International Covenant on Civil and Political Rights (ICCPR) the solution?

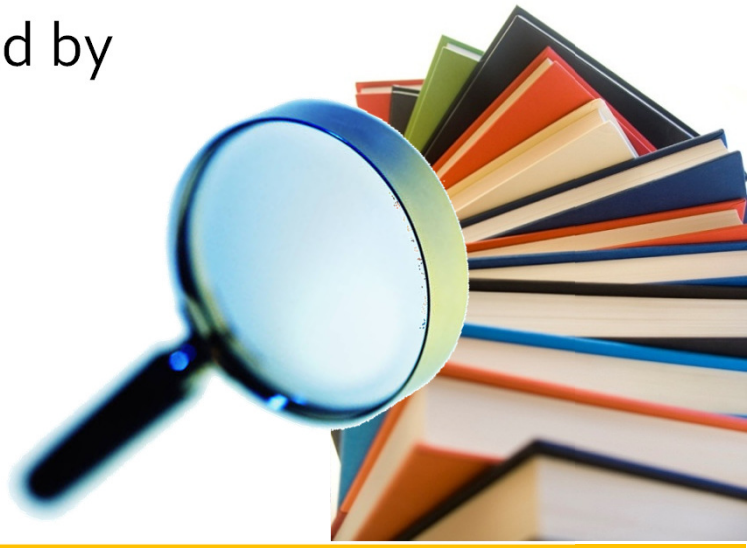
A look at the ICCPR

- UN treaty from 1966 (most states of the world have signed)
- Signing parties commit to respect the civil and political of individuals
- Art. 17 (1) "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence"

A look at the ICCPR

Problems:

1. What is considered "unlawful"?
2. National implementation is lacking (e.g. USA)
3. UN Human Rights Committee has no enforcement power
4. Only an optional protocol allows citizens to enforce their rights legally (not signed by many states, e.g. USA)



<u>ICCPR is nice but toothless</u>

So, what now?

References

- CSA "CSA Survey Results: Government Access to Information", July 2013 https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-July-2013.pdf
- ITIF "How Much Will PRISM Cost The U.S. Cloud Computing Industry?", August 2013 http://www2.itif.org/2013-cloud-computing-costs.pdf
- BITKOM "Internetnutzer werden misstrauisch", July 2013 http://www.bitkom.org/de/presse/8477_76831.aspx
- Art. 29 WP's Letter to Viviane Reding, August 2013 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf
- Conference of German data protection commissioners' press release "intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe", July 2013 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile

Thanks!

www.tclouds-project.eu

"The TClouds project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-257243."