How the US crafted secret mass-surveillance laws for foreign Cloud data, without any legal rights or redress

Caspar Bowden
independent advocate for privacy rights

(Chief Privacy Adviser - Microsoft 2002-2011,
Director of FIPR 1998-2002)

University of Toronto
16th November 2013

Cloud *computing*
parallel processing power as commodity

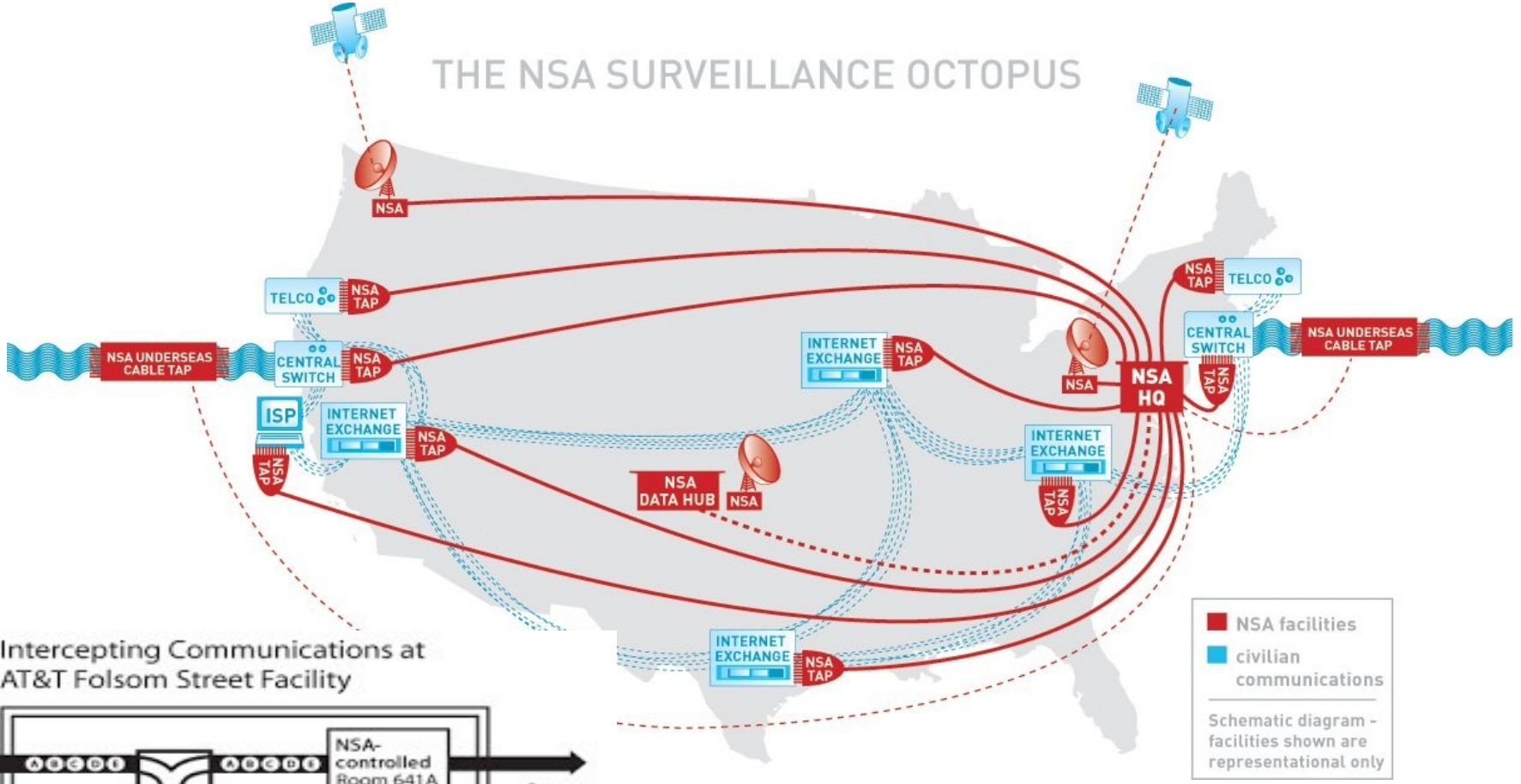
Consumer: Facebook, Skype, Microsoft, Google

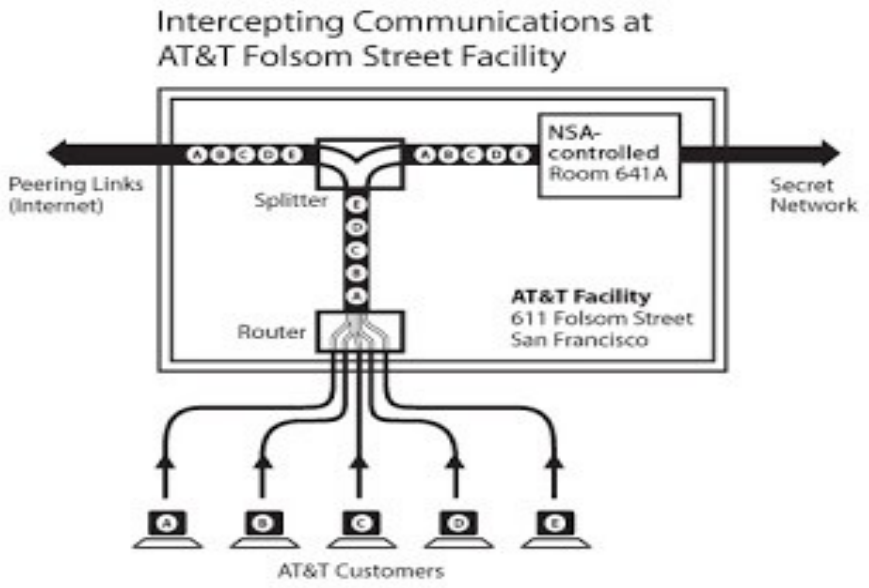
Business : Microsoft Azure/Office365, Google Apps, Amazon

“Warrantless Wiretapping” 2001-7

- 2003: AT&T San Francisco switching centre
  - Internet backbone split to DPI and forwarded to NSA
- 2005 New York Times broke story
  - media self-censored story until after 2004 election
  - several whistleblowers NSA, FBI, and AT&T
    - tried official channels and then media – ignored, prosecuted
  - Traffic-analysis of call patterns and transaction data
- 2007: “legalized” by Protect America Act
  - retroactive immunity for telcos
  - new paradigm: “collect everything, minimize later”
  - no more particular warrants
  - FISC approves “procedures”

This is <u>not</u> a “Request”





What is *"foreign intelligence information"*?

- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against -
  - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
  - (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
  - (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; **or**
- (2) **information with respect to a foreign power or foreign territory that relates to**, and if concerning a United States person is necessary to -
  - (A) the national defense or the security of the United States; or
  - (B) **the conduct of the foreign affairs of the United States**.

information with respect to a foreign-based political organization or foreign territory that relates to the conduct of the foreign affairs of the United States.

US Foreign Intelligence Surveillance Act §1801(e)

2008 FISA Amendment Act **§1881a** (Sec.702)

- ***foreign intelligence information***
- *intentionally* targets only non-US persons outside US
- authorization for 1 year
- "minimize" access on US persons after collection
- provide all facilities/information to accomplish in **secret**
- contempt of FISC for non-compliance
- providers have complete immunity from civil lawsuits
- "**in a manner consistent with the 4th Amendment**"

FISAAA 2008 combined 3 elements for 1st time

1) §1881a only targets non-US persons located outside US

2) "remote computing services" (defined ECPA 1986)

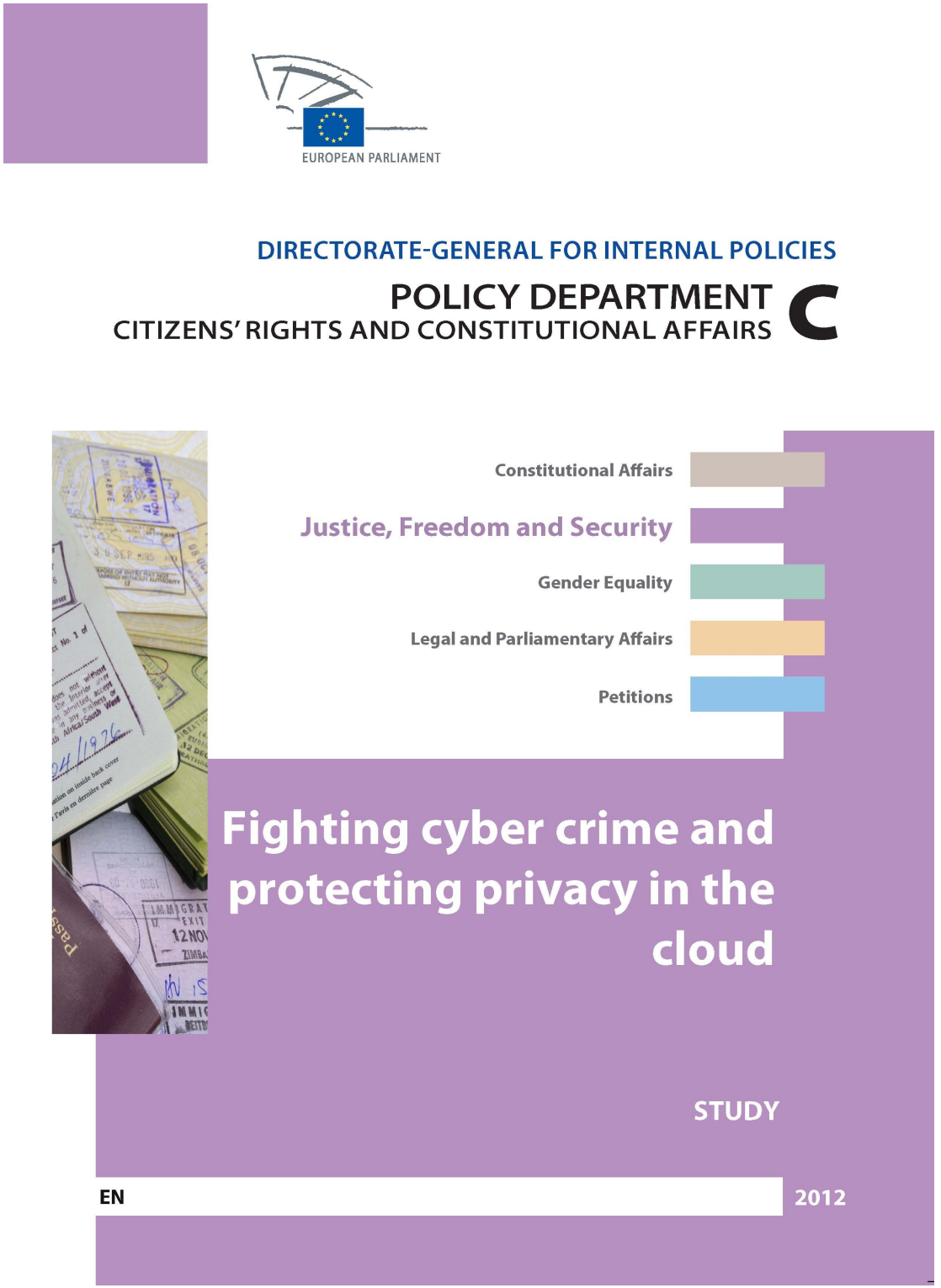
- *provision to the public of computer storage or processing services by means of an electronic communications system* (today = **Cloud**)
- **Nobody noticed addition of RCS!**

3) not criminality, not "national security"

- **purely political surveillance**
- ordinary lawful democratic activities

→ designed for mass-surveillance of any Cloud data relating to US foreign policy

- **"double-discrimination" by US nationality**
  - **completely unlawful under ECHR**



SLATE 8th Jan: Ryan Gallagher

U.S. Spy Law Authorizes Mass Surveillance of European Citizens: Report

1500 Tweets in a week

Most apparently from Europe, without comment, but general reaction of "WTF? How can this be allowed ?"

US blog reaction MUCH less, but typically

"who's going to stop us?"

NEW post-Snowden research briefing

European Parliament September 2013

Main programmes revealed by Snowden

- PRISM (FISA 702)
- “Upstream” (EO1233)
  - fibre-optic cables, public and private telco/ISP networks
  - Internet exchanges
- Xkeyscore - “exploitation system/analytic framework”
  - indexes/searches “3 day rolling buffer” of “full take” data stored at 150 global sites on 700 database servers.
- BULLRUN - “aggressive multi-pronged effort to break into widely used encryption technologies”
- MUSCULAR – NSA intercepting to Google/Yahoo fibre
  - flows between datacentres not encrypted (or defeated)
  - **Microsoft** admits to European Parliament no encryption “server-to-server”

Procedures used by NSA to target non-US persons (Guardian 20.6.13)h

- Confirms there are zero substantive privacy protections for non-US persons
- solely concerned with establishing “foreigness” of target
- no restriction on full breadth of “foreign intelligence information”

Cloudwash

US law offers good protection to its citizens

as good or better as foreign law for foreigners

►►► don't worry about the US Cloud

FALLACY: FISAAA offers zero protection to foreigners' data in US Clouds

And these materials don't mention FISAAA at all...

- “Five Myths...” (US mission to EU)
- Hogan Lovells report (for “media and political purposes”)
- Linklaters
- **Peter Hustinx (April 2010)**
  - **“streamlining the use of BCRs”**
- ENISA - “procure secure”
- WTO (Kogan)
- RAND Europe
- QMUL Cloud Project* (sponsored by Microsoft)

*one paper has one footnote

(some) Privacy regulators acquiesce to "don't worry be happy about the Cloud"?

~ 150 Opinions on EU Data Commissioners since 9/11

- PATRIOT mentioned in one footnote in 2001
  - Absent: FISA, PAA, FAA , "foreign intelligence"

- 24.11.11 **Anne Cavoukian** – Ontario Privacy Commissioner
  - **"Privacy in the Clouds –Yes, You Can Have Both" (?!!)**
  - "**Don't waste your time** by focusing on the Patriot Act, there are several U.S. investigatory powers that rival the Act and grant similar authority"
  - no mention of FISA in an OPC materials until May 2013
    - no analysis of discrimination by nationality/implications under Canadian Charter
- Regulators conceive their job as enabling and obfuscating mass-surveillance (especially by the state)

US political and media debate entirely focussed on rights of Americans

- PRISM not controversial in Congress
  - Controversy about s.215 of PATRIOT and domestic + international “metadata”
- non-Americans rights non-existent, unmentioned
- ex-NSA Dir. Hayden
  - *“4th Amendment is not an international Treaty”*
  - *“home field advantage”* data transiting/stored US
- But until 2012 US State Department extolling protections of 4th at international conferences !!
  - 4th situation did not crystallise until 2012

Questions about outsourced e-services
RISK ≠ UNCERTAINTY

- Is metadata covered as “Enterprise customer data”?
  - How long is data retained, where are flows exposed?
- How do we trust (proprietary implementations) of encryption after BULLRUN/MUSCULAR ?
  - If data wasn't encrypted between datacentres, what does that imply about good faith and prudence of vendors?
  - Encryption is futile to protect webmail & hosted services against NSA if provider subject to US jurisdiction
- What are vendor assurances by worth given secrecy provisions in FISA/PATRIOT orders ?
- **What about the students ?**

Reduce risks & uncertainties, don't entrench them