EU data protection strategy for the Cloud

Caspar Bowden

independent privacy researcher

(Chief Privacy Adviser Microsoft 2002-2011,
Director of Foundation for Information Policy Research 1998-2002)

If you are interested in further analysis, or want to discuss a speaking engagement, please contact

caspar@PrivacyStrategy.EU
Twitter: @CasparBowden

This is <u>not</u> about Cloud as storage

parallel **processing power** as a commodity

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Fighting cyber crime and protecting privacy in the cloud

STUDY

EN 2012

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 ?"

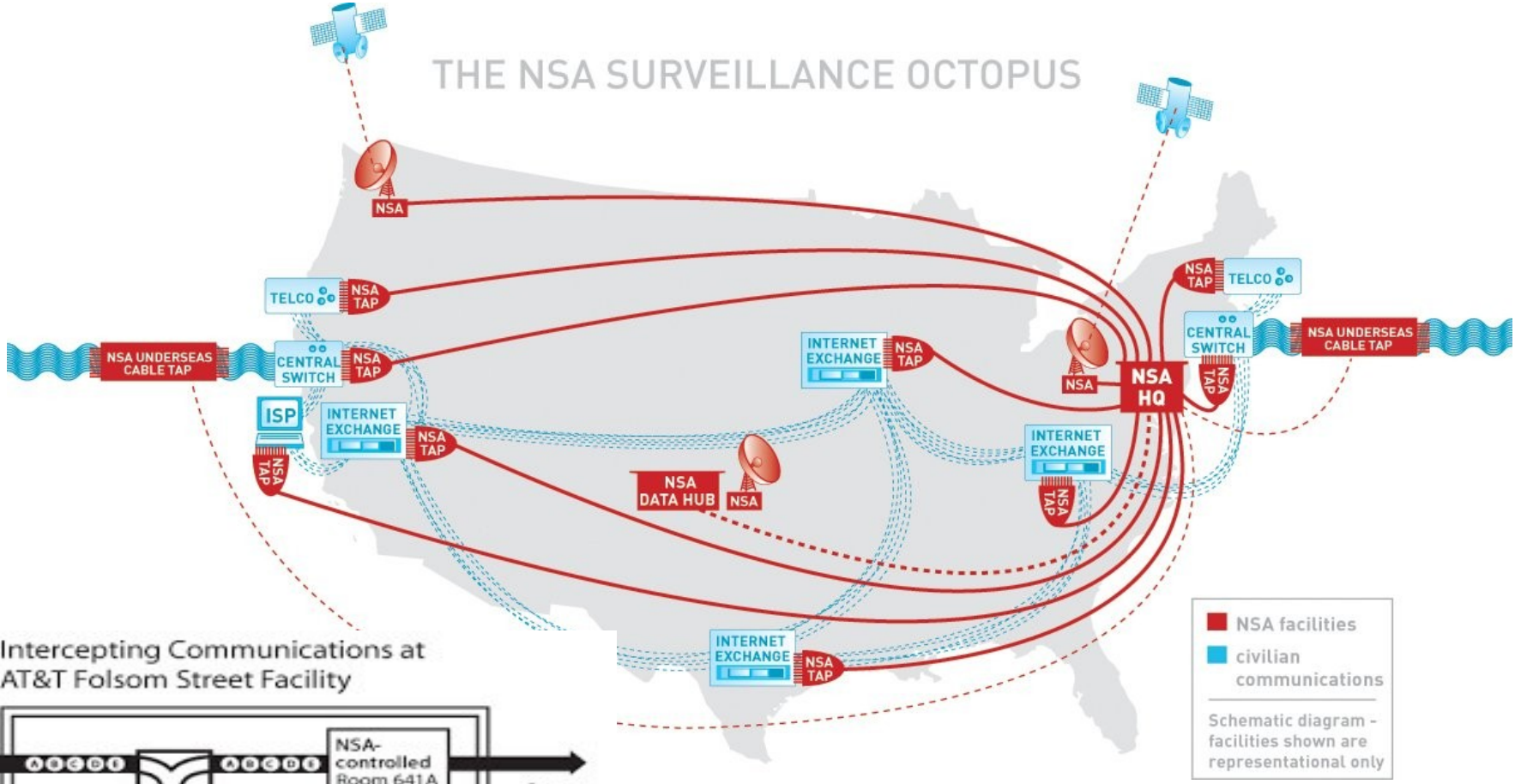
US blog reaction MUCH less, but typically

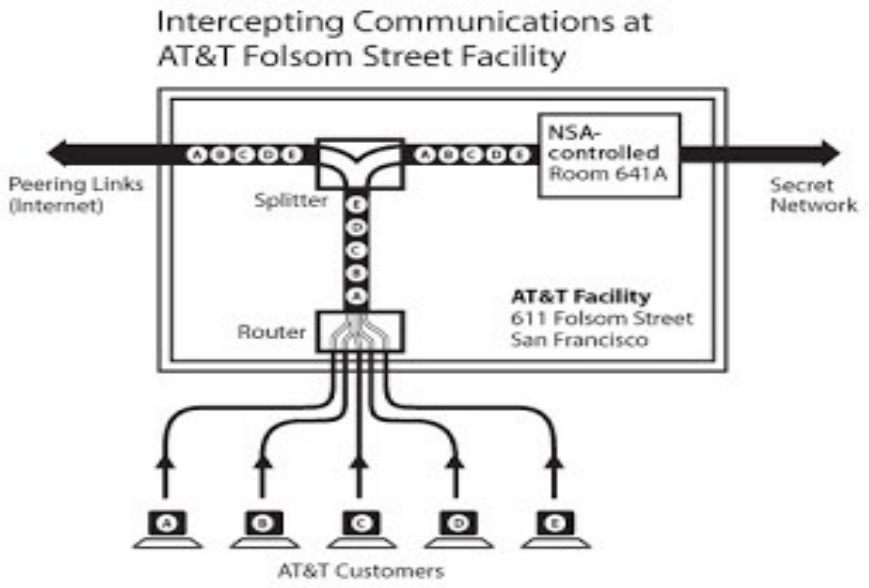
"who's going to stop us?"

“Warrantless Wiretapping” 2001-7

- NSA, FBI, and AT&T whistleblowers tried official channels and then media - ignored
- New York Times self-censored story for a year
  - published in 2005 (after 2004 election)
- “Stellar Wind”: database of phone call data
  - Traffic-analysis of call patterns and transaction data
- AT&T San Francisco switching centre
  - all Internet backbone data analysed by Narus 6400
  - triaged and forwarded to NSA
- “legalized” by Protect America Act 2007
  - retroactive immunity for telcos
  - new paradigm: “collect everything, minimize later”

This is <u>not</u> a “Request”





US Foreign Intelligence Surveillance Act §1801(e) - 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.

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**

Is Cloud-veillance a real risk ?

- encryption can only protect data to/from the Cloud
  - and “lawful” access (FISA §1881a) reaches inside the SSL!
- Platform-as-a-Service (PaaS) : software is re-written in new languages to scale **automatically** to thousands of machines
- **Scalable** mass-surveillance which adjusts elastically, is only practical* if scan data at the protocol layer where the data makes sense (files/e-mail/SNS); cannot reconstruct individual packets of data fast enough
- Therefore governments wishing to conduct mass-surveillance of Cloud in real-time will have to co-opt the Cloud providers to build capabilities on the inside
  - entirely different paradigm to telco interception
  - **potentially all EU data at risk**
    - (unlike ECHELON – only interception)

*ETSI developing “LIaaS” (using the Cloud to surveil the Cloud)

Cloud sovereignty risk matrix

Locus of control / Location

CONTROLLER PRIMARY JURISDICTION	EU*	US
EU	**SAFE**	**Tech: HIGH** **Legal: LOW**
US	**Tech: LOW** **Legal: HIGH**	**HIGH-RISK**

* location in UK ? – FIVE EYES member !

EU data sovereignty risk matrix by purpose

	intra-EU	EU data in US
CRIMINAL		
NATIONAL SECURITY		
POLITICAL/ FOREIGN POLICY	**ECHR/ TFEU**	

RED

NOT PROTECTED BY

- ✘ **US 4th Amendment**
- ✘ **EU DP**
- ✘ **CoE 108**
- ✘ **CoE Cybercrime**
- ✘ **ECHR**

Art.29 WP on BCRs-for-processors

Audit coverage**...**for instance**...decisions taken as regards mandatory requirement **under national laws that conflicts ..

NEWSFLASH for DPAs

"lawful" access for national security not part of auditors' threat model

- **but anyway loopholes already built-in**
  - *Request....shall be communicated to the data Controller **unless otherwise prohibited**, **such as** a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. In any case, the request for disclosure **should be** put on hold and the DPA competent for the controller and the lead DPA for the BCR **should be** clearly informed about it*

Technical defences don't exist

- Homomorphic (computing with encrypted data)
  - not semantically secure, trillion times too slow
    - optimists think > 3 years “usable”
      - (irrelevant unless DP mandates)
- 'Trusted computing', TPMs, TeFKAP
  - Consumer-grade threat-model, not NSA-proof
  - TPM 1.2 broken for $100,000
- Tokenizing encryption gateways
  - lose Cloud processing power, storage only
- Encrypted search – niche application

An EU Cloud “Airbus” to compete with US “Boeing”

- 15m Euro “Cloud partnership” is a marketing budget!
- “On Trusting Trust” problem is solved !
  - David A. Wheeler 2006-2009
  - crucial security advantage for FLOSS in Cloud
  - AGPL ~ copyleft on patches for offered services
- 0-day risk comparable FLOSS vs. Proprietary
  - **but back-door risk MUCH greater with proprietary**
- Maintain infrastructure under exclusive EU jurisdiction
  - 'cos plenty of bandwidth for remote-control ex-filtration
- Tough data export regime promotes EU Cloud investments
  - if US “Cloud dumping” allowed - no investment

Meanwhile...advice to Cloud customers

REMEMBER:

- **“lawful” access by government X is NOT part of the threat model of industry from country X**
- **What is lawful in X may be not be lawful in <u>your</u> country !**

AVOID providers which rely

- on Safe Harbor (**<u>especially</u>** offering Safe-Harbor-as-a-processor in DoC certification) with foreign jurisdiction in processor contracts
- on audit which excludes “lawful” foreign requests from threat model

SPECIFY providers with

- exclusively EU jurisdiction in processor contracts, heavy damages for acceding to foreign requests and generous whistleblower bounties
- open-source stacks, with a verifiable forensic operational trail of code from source to binary to load and run
- guaranteed non-retention of session keys, and publication of reasons (unless prohibited) of certificate revocations

Conclusions

- EU personal data is naked to FISAAA, contrary to much “Cloudwash” White Paper propaganda
  - PATRIOT is bad, FISAAA much worse for Cloud
- Astonishingly, EU Commission, DPAs, MS, MEPs, didn't know about FISAAA 1881a until 2012
- No satisfactory technical defences in sight
- Some LIBE Amendments to draft DPR tabled
  - **Consent-with-drastic-warning, Whistle-blower protection**
- Need massive vertical investment in indigenous EU Cloud software platforms and operations
  - FLOSS has crucial security advantages for Cloud
  - retain high-end of value chain in Europe

Thank you

Q & A ?

caspar@PrivacyStrategy.EU

Safe-Harbor-as-processor is an oxymoron

- **IaaS or PaaS are Cloud Processor services**
- Processors cannot execute **any** of the SHA Principles, because they just provide a platform – they do not know the function of the programs the Controller is running on the platform, who the individual subjects are, the purposes, algorithms used, transfers, the meaning (hence integrity and security) of the personal data.
- SaaS must be a (co-)Controller not a Processor because Identity Management requires autonomous security decisions about means and purposes ("is the person asking for a new password trying to break into this system"?)
- **If two parties have a deal based on 7 Principles, does that deal still hold in a situation in which all of the Principles are void? (No)**

✘ Notice

✘ Choice

✘ Onward Transfer

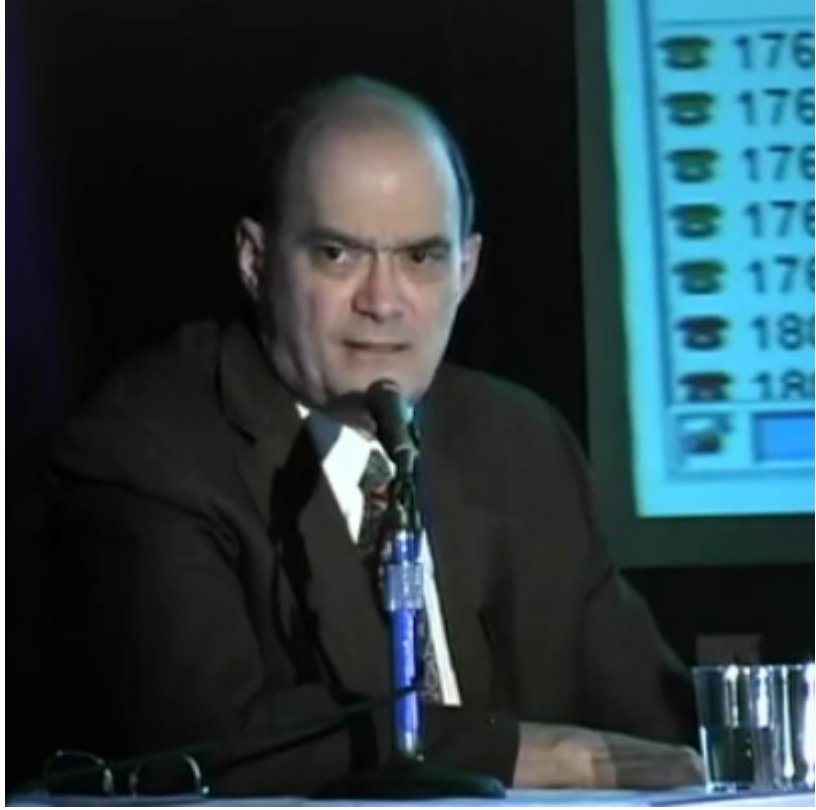
✘ Security

✘ Integrity

✘ Access

✘ Enforcement

Bill Binney
ex-NSA whistleblower



- mathematical analyst, 32 years at NSA
- 2001 Technical Leader, Intelligence
  - Sigint Automation Research Center
- New Yorker article May 2011
  - architect of “ThinThread” system
    - cancelled because too cheap and worked too well
  - TrailBlazer replacement was expensive failure
    - whistle-blowers filed complaint to DoD IG about waste, corruption
    - led to victimisation, harassment and malicious prosecution
- HOPE conference New York July 2012
  - Automatic targeting
  - Latent semantic indexing

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