The Cloud Conspiracy 2008-2014

Caspar Bowden
independent advocate for privacy rights

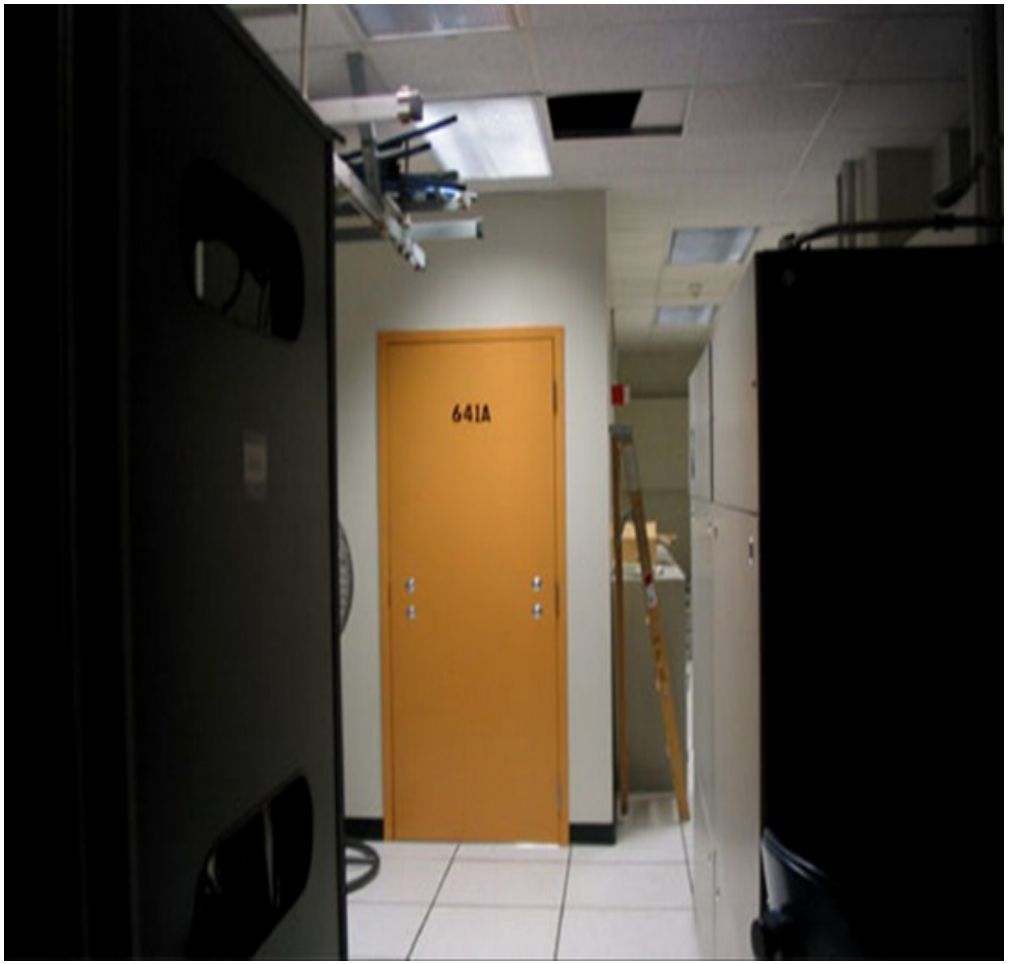
(Tor Board, Qubes-OS Policy Adviser,
Chief Privacy Adviser - Microsoft 2002-2011,
Director of FIPR 1998-2002)

31C3 Hamburg – 27th December 2014

Preliminaries

- 2002-2011 Chief Privacy Adviser Microsoft
  - **advising** 40 “National Technology Officers”
  - not compliance, not US privacy
- I did not know about PRISM at Microsoft
  - deduced from open-sources
  - never had a security clearance
- Microsoft made me “redundant” in 2011, two months after I warned them about FISA
  - now 100% FLOSS advocate

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



parallel **processing power** as a commodity

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**
  - **THIS MEANS IF YOU ARE NOT AMERICAN, YOU CANNOT TRUST U.S. SOFTWARE SERVICES !!**
- contempt of FISC for non-compliance
- providers have complete immunity from civil lawsuits
- "**in a manner consistent with the 4th Amendment**"

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)

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**

The 4th Amendment does not apply to non-US persons outside US

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized

1990: US v. Verdugo-Urquidez (Supreme Court)

2008: FISCR judgement on Protect America 2007 (opened door for §1881a !)**)**

- no 4th for "foreign powers reasonably believed to be located outside US"

2008: "probable cause" conspicuously absent in FISA §1881**(a)**

- but explicit in §1881**(b)** and §1881**(c) which <u>can</u> target US persons**

2010: ACLU FOIAs (redacted) on FBI use of s.702

- "probable cause" becomes
  "reasonable belief user is non-USPER located outside US"

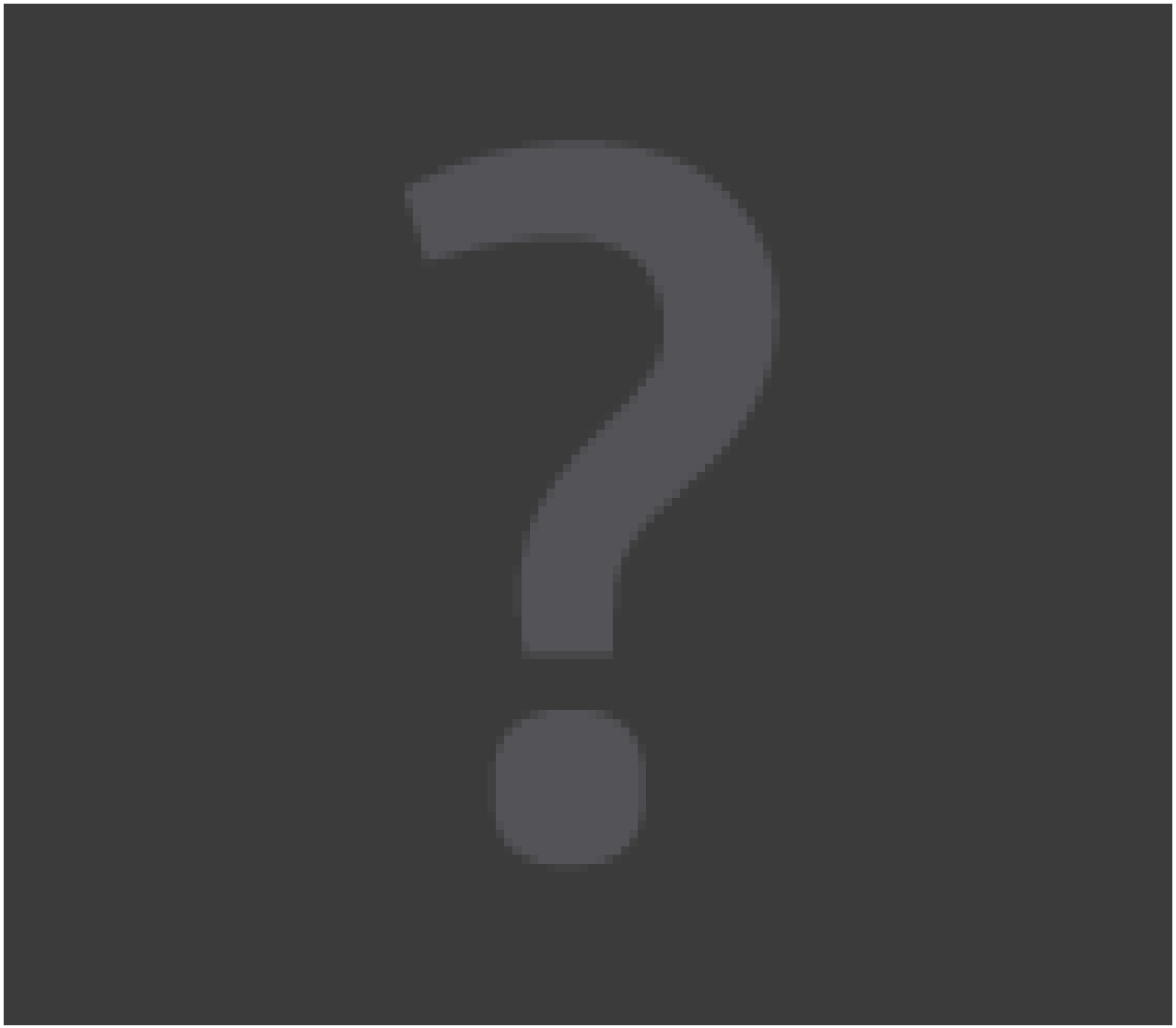
2012: House Judiciary Subcommittee hearing on FISAAA 2008

- EPIC (Rotenberg) and ACLU (Jaffer) concede it does not !

US Judiciary Subcommittee 31.5.12

Hearing on renewal of FISAAA 2008

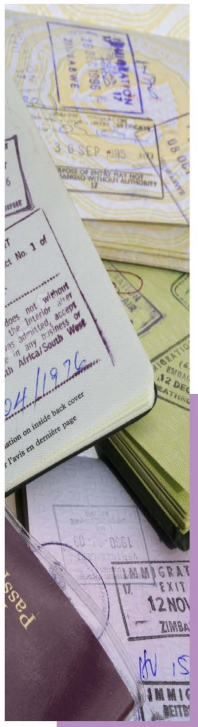
4th Amendment does not apply to non-USPERs' data



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 2013

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?"

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

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
  - 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)

Abracadabra

1) Microsoft/Google/etc. gets BCR certified
2) DPA must accept
3) Data transferred into US controlled Cloud

Sleight-of-hand:

- questions of mass-surveillance disappear in puff-of-audit

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**

(17.1.14) PPD28 - Sec.2 Limitations on Use

Footnote 9.

- This directive is not intended to alter the rules applicable to US persons in EO12333, the FISA , or other applicable law.
- New rules drafted by AG + DNI will treat US and non-US persons equally (with national security exemption), but only regarding **dissemination** & **retention**

So discrimination by US nationality will continue...

- **If a US Person, need a particular justified FISC warrant**
- **If not a US Person, NSA just adds selectors to list**

...and different legal standards apply (relates/necessary)

(July 2014) PCLOB 702 report

- **Analysis for non-Americans is 5 pages out of 196**
- **misleading, tautologous, credulous junk**

- **Vast amount of FISC declassifications,**
  - **guess what, stuff about non-Americans redacted !**

Warnings given on 702 before Snowden

- Jan '11: OSF (Soros) - “only fund existing NGOs”
- Jun '11: Privacy International - “no resources”
- Sep '11: EDRi, DG-JUSTICE, Poland DPA
  - evasion, inaction, 1 footnote in a DPA article
- Jun '12: EP Greens - helpful
- Sep '12: ENISA, EDPS, CNIL(Art.29), Council
  - stunned silence, total inaction
  - ENISA refused action before (“no mandate”), afterwards falsely claimed had foreseen and covered in Cloud advice
- Oct '12: EP Inter-Parliamentary Forum – stunned silence
- Feb '13: EP LIBE
  - asked for GDR Amendments in 3 days, mostly ignored/diluted
- May '13: DG-CONNECT + DigitalEurope – laughter

EU Commission Cloud policy (-2014)

- DG-CONNECT (was Neelie Kroes)
  - rejected a pan-EU Cloud (no enthusiasm MS)
- European Cloud Partnership
  - Steering Board (big US/EU industry)
  - Trusted Cloud Europe (yada yada)
  - 2013 “Cloud Contract” WG (Snowden oblivious)
    - “recursive” sub-processing contracts [endorsed by Art.29]
- 7th Framework “research” projects
  - “Accountability” (A4Cloud), v.dodgy papers
- senior (non-tech) Cloud official has new job: EU CISO (!)
- (ENISA) certification schemes blind to mass-surveillance
- **NO SUBSTANTIVE CHANGE - assumes NSA problem will just be fixed politically**

EU Parliament

- first LIBE EP Report in Oct 2012 and Feb 2013 presentation
  - Asked me for GDPR amendments, mostly ignored watered down
  - Warned again in Sep 2013 report and presentation
- After Snowden, LIBE lock-down in purdah 3 months, LIBE draft totally inadequate to stop NSA
  - Art.43a : proposed deliberate conflict of law
  - “special” direct transfers must be DPA approved
  - removed BCRs for processors (good!)
    - likely COM and Council and Art.29 try to restore

What's not to like about GDPR?

- Widens 1995 DPD Cloud loopholes in floodgates
  - BCRs-for-processors, Code of Conduct, Seals (?)
- No reform of DPAs or DPC appointments
- colossal bureaucracy, inchoate PET mandates, theological consistency mechanism for DP Board
- certification schemes doomed to diverge, ignoring realistic comp.sci threat models
- no effective subject rights in pseudonymised data, carte blanche exemptions for 'archives' and (commercial) 'research'
- “fantasy computer science” - 450 refs to “processing”
- (and much more) – needs complete re-boot

Art.29 WP 228 (5.12.14)

on surveillance of electronic communications for intelligence and national security purposes

- *"exemption in the treaties offers no possibility to invoke the national security of a third country alone in order to avoid the applicability of EU law"*
- *"DPAs may suspend data flows...also awaiting the outcome of the Max Schrems case"*
- *"Art.43a may be a step in the right direction, but it will not be the* deus ex machina *solving all other questions"*
- *"competent supervisory authority should be the EU national authority dealing with the request* ***rather than the DPA****"* **[they don't want the job!]**

Art.29 evades own responsibility

(2005) WP114

- *transfers..repeated, mass or structural ..precisely because of..importance, be carried out **WITHIN**..contracts or BCR*

(2014) WP228

- *BCRs, SafeHarbor, [contract] exceptions ..could **NOT** be a basis for massive, structural or repetitive transfers*

Art.29 endorsed contracts, invented BCRs, to control “massive” transfers in 2005. Now they contradict themselves, walk away, without acknowledging absurdity...

Art.29 never mention...

- Discrimination by nationality in US law/policy
- In ~150 Opinions since 9/11, PATRIOT mentioned once in a footnote (2001), FISA, PAA, FAA, “foreign intelligence” not mentioned **at all.**
- Their endorsement for Cloud Computing under existing legal model (WP196) and volte-face on BCR4P (WP195/204)
- EDPS + Deputy, Council, COM, CNIL (Art.29) warned in comprehensive detail at ERA (21.9.12)
- In 1999/2000, Safe Harbour “national security” Annex, even though ECHELON reports published and EP inquiry in progress (Peter Hustinx was Chair)
- In 2001 approved “model clauses” without demur (WP38)

Art.29 “political statement” 8.12.14

- conference with UNESCO in Paris, but Snowden barely on agenda
- CNIL schmooze for civil society
- Statement of 15 points on “European values”, “open for comment through 2015”
- Transparent ploy to evade Art.29/DPA responsibility to enforce **existing** law, shut down US dataflows
- In WP228, Art.29 say they don't want job of arbitrating 3rd country requests anyhow, and Art.43 (conflict of law) no solution
- Art.29 deadlocked – no consensus job for DPAs

US is “exceptionally exceptionalist”

- References in surveillance law to discrimination by citizenship/nationality (NOT geography of communication path)
  - US 40 (FISA+PATRIOT+FISAAA, 1st & 4th Amndt)
  - UK zero (sic)
  - DE 1 (G10 – oops, ECHR, that's embarrassing)
  - CA ~2
  - NZ ~2
  - AU ~2
  - Any others ? At all? In EU ?

What have NGOs done?

- Not 1 word said on discrimination by nationality vs. human rights equality in Brazil NetMundial, Istanbul IGF
- Not one word said either at 30c3 :-(
- CDT, ACLU, EFF very little on non-USPER rights
  - Access has done more than most
- EPIC - not 1 word on FISA, 18yrs visiting EU
- USA Freedom Act failed – Good !
  - introduced **extra** 40 protection only for Americans
  - nothing at all for non-Americans
- EDRi - nothing, before or after Snowden
- Privacy International – nothing before Snowden
  - dubious handling of UK TEMPORA case
  - told UN Geneva “vast majority” surveillance is “one country on own citizens” - blew off extraterritoriality issue

Is a real EU/US Treaty even possible?

- Suppose a full EU/US Treaty
  - because concept of **"adequacy"** per company is absurd
  - giving EU data equal protection to that of US Persons
  - **criminalizing** abuse of EU data in US law
  - full rights to access/deletion/portability, breach notification
  - class-actions possible in US for violations of EU citizens' data
- Spying on foreigners abroad is "inherent" Presidential prerogative
  - cannot be restricted by Congress (FISA 1978, hence EO12333)
  - any POTUS assurance today can be reversed in secret tomorrow
- Basically need to change US Constitution
  - or Supreme Court could reverse/embellish V-U 1990 decision

How could EU respond?
3-Prong Strategy

1) progressively terminate selected flows in phased escalation
   - audit current flows for:
     - risk to Fundamental Rights and EU interests
     - strategic value for US interests
     - ease of substitution
2) EU industrial policy for software and Cloud services
   - open-source software (and ultimately hardware)
   - if Cloud so important, EU ought to do anyway!
     - but much easier to attract investment with strong GDPR
   - but DG-CONNECT policy so far unchanged by Snowden !!
3) Whistle-blower protection (and rewards for enormous risks)
   - only transparency mechanism proved effective
   - only deterrent from future policy deception

Welcome to the Meta-Panopticon

- “who cares – I have nothing to hide”
  - most people don't think they have anything to hide
- but people vote for politicians, and must trust bureaucracies to take decisions fairly in collective interest.
- how do people know politicians and officials aren't influenced by fear of NSA spying in their own private life?
  - one tabloid story about private life can ruin a career
  - or at least prevent a promotion in a hierarchy
- this is highly corrosive to democracy!
  - But people don't think about this...
  - ...and they should, even if it is “corrosive”

Thank you

Q & A ?

caspar@PrivacyStrategy.EU

@CasparBowden

GPG: 2051 D1A8 231B 66AA 0935 1363 1442 D4AC 0B66 330A

Research Note to LIBE Ctee

The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights, European Parliament 2013