How to wiretap the Cloud

(without anybody noticing)

Caspar Bowden
independent advocate for privacy rights

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

Cloud Computing And Data Sovereignty: Mass-Surveillance by 3rd countries

CPDP Brussels 25th January 2013

This is not about the PATRIOT Act

- PATRIOT is complicated (100+ pages)
- wiretap, seize, bug data
- National Security Letters for metadata
- s.215 “Business records”
  - “production of tangible things”
  - power for FBI in “international terrorism or clandestine intelligence activities”

...because there is something worse if you are not a U.S. citizen or resident (“US person”)....

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

parallel **processing power** as a commodity

“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”

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**"

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)

§1881a combined 3 elements for first time

1) only targeted at 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

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 FISAAA 2008

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

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

Hogan Lovells report (Wolf & Maxwell – May 2012)

"Debunks Faulty Assumption That US Access is Unique" (press release)

- drafted for “media and political purposes” for a government client (Wolf – in D.C)
- No mention of:
  - ECHR (universal rights) v. protections only for US persons in FISA, FISAAA, etc.
  - for non-US persons located outside US
    - mass-surveillance of Cloud data under FISAAA 2008 §1881a (aka FISA s.702)
    - “foreign intelligence”: democratic politics, US policy goals, “foreign territories”
    - no 4th Amendment rights (requiring probable cause and specific warrant)
      - misleading (and omitted) reference and to Suzlon case (only affects ECPA)
    - no 1st Amendment rights (free expression/association) re: NSL letters
  - “secret interpretations” of PATRIOT 215 (bypassing court orders for stored data)
- When challenged on above (Maxwell, Council of Europe, June):
  - no counter-rebuttal at all
  - Maxwell said “Everyone should read FISA for themselves” (115 pages !)
- >1000 search-engine refs, cited by Microsoft, IBM, OpenForumAcademy, ITIF

US mission to EU

misdirection and omission : no mention of FISA

US Ambassador Kennard speech (Dec 4th 2012)

- *contrary to concerns raised by some, electronic data stored in the United States—including the data of foreign nationals—receives protections from access by **criminal** investigators **equal to or greater** than the protections provided within the European Union.*
- ***For law enforcement** acquisition of electronic communications, the stringent U.S. Statutes protecting the privacy of email and voice communications, among the highest standards in the world, apply equally to foreign nationals and U.S. Citizens*
- *The Patriot Act ...did not eliminate the pre-existing, highly-protective restrictions on U.S. law enforcement access to electronic communications information in **criminal** investigations.*
  - **but FISAAA 1881a did eliminate these restrictions in non-criminal cases (and "foreign intelligence information")**

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
- **This is an entirely different paradigm to communications interception**
  - *ETSI developing “LIaaS” (using the Cloud to surveil the Cloud)

This is a request

(National Security Letter to Nick Merrill, gagged for 7 years)

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

[redacted] 2004

[redacted]
President
[redacted]

Dear [redacted]

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the names, addresses, lengths of service and electronic communication transactional records, to include existing transaction/activity logs and all e-mail header information (not to include message content and/or subject fields), for the below-listed email address:

[redacted]

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request personally to a representative of the [redacted] of the FBI. Any questions you have regarding this request should be directed only to the [redacted] Due to security considerations, you should neither send the records through the mail nor disclose the substance of this request in any telephone conversation.

MAR-25-2010 17:21 US ATTORNEY'S OFFICE 212 P.03

[redacted] Page 3

ATTACHMENT

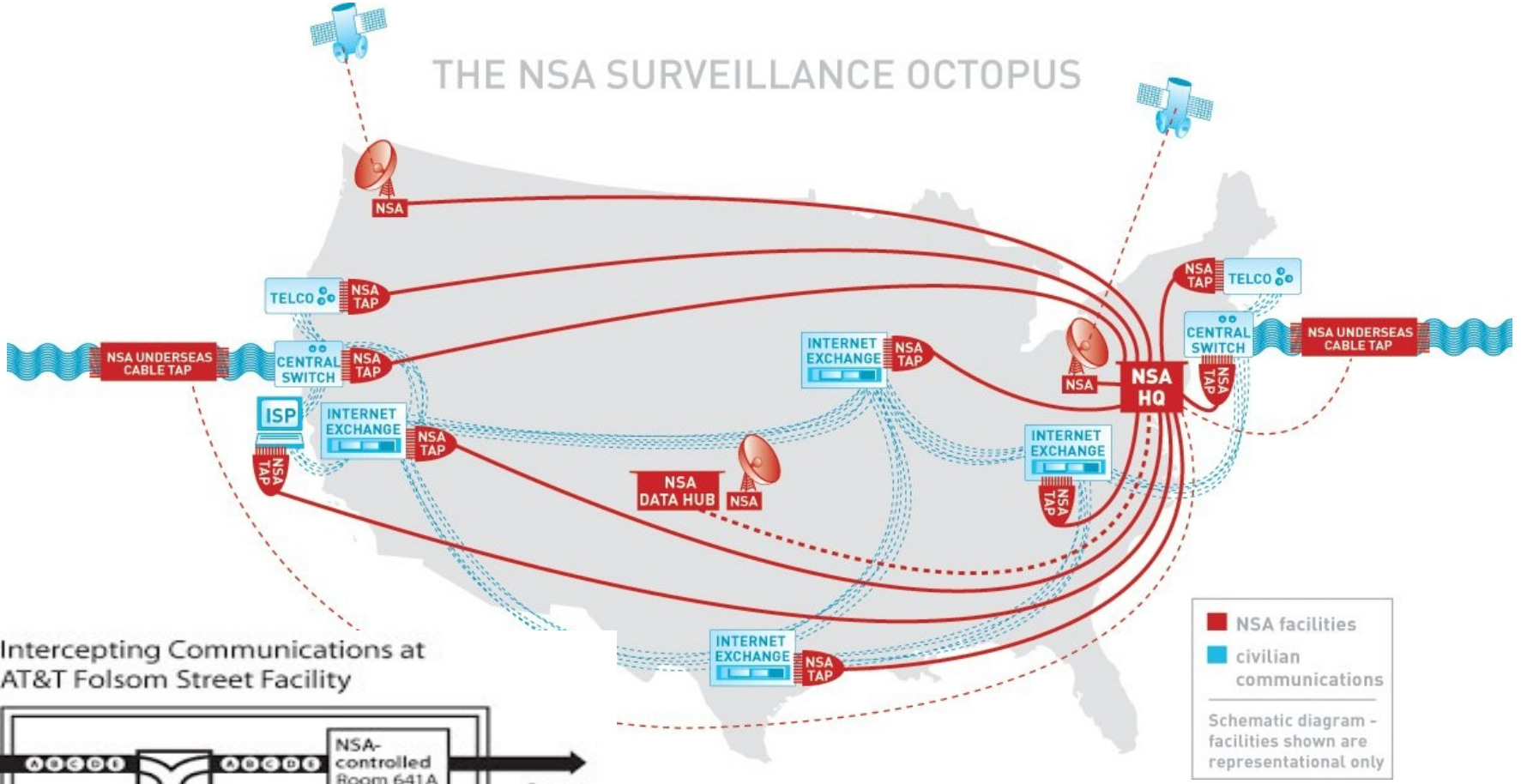
"In preparing your response to this request, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communication transactional record in accordance with Title 18, United States Code, Section 2709:

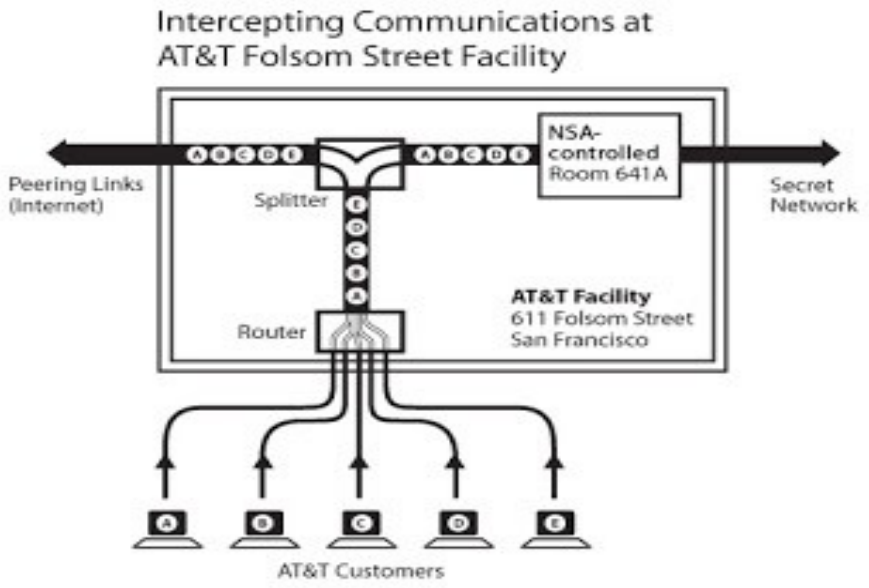
-- [redacted]
-- Subscriber name [redacted]
-- Account number
-- [redacted]
-- Address
-- [redacted] telephone number [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted] e-mail address
-- [redacted]
-- [redacted]
-- [redacted]
-- Any other information which you consider to be an electronic communication transactional record

We are not requesting, and you should not provide, information pursuant to this request that would disclose the content of any electronic communication as defined in Title 18, United States Code, Section 2510(8)."

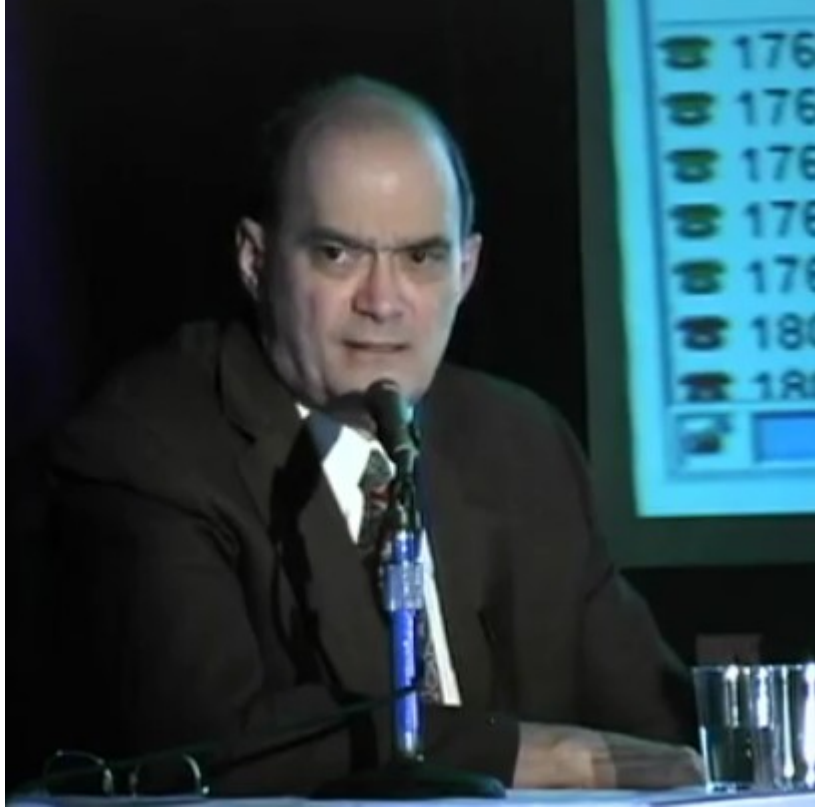
TOTAL P.03

This is not a “Request”





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

A Maginot Line in Cyberspace

Art.29 WP on Cloud Computing WP196 June 2012

Access to personal data for national security and law enforcement

*"It is of the **utmost importance"*** to ensure MLATs are used

Council Regulation (EC) No 2271/96 *is an appropriate example of legal ground for this.*

- **...But this example is about the overt consequences of extraterritorial US sanctions on Cuba, and an analogous instrument could not prevent covert surveillance on EU data.**
- Cloud data is continuously replicated on disks in US/EU/Asia (unless instructed otherwise), and the "software fabric" is (usually) remotely controlled and maintained in US (or e.g. India). The US could secretly order companies to comply.

Chronology of BCRs-for-processors

- 2010 “Working Group” of DPA/industry led by CNIL
- April 2010
  - EDPS speech to BSA: “streamlining the use of BCR and possibly extending the responsibility of controllers”
- Cloud vendors complain about model contracts (complex when location for taxation not location for DP jurisdiction)
- Jan 2012 - new DP Regulation published
  - BCRs for controller or processors
  - **Draft Regulation Art.42(3):**
    - **A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.**

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

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*

EU/US “Umbrella” discussions

Cloud surveillance via FISA would not be covered:

- US rejected should apply to data subsequently used for law enforcement “**transferred from private parties in the EU to private parties in the US**”

EU-US DATA PROTECTION NON-PAPER ON NEGOTIATIONS DURING 2011

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?"

Summary

- Cloudveillance is potentially about **all** EU data (ECHELON agenda was only about comms)
- encryption is futile
- surveillance by a foreign government has different risks than from own government
- US mass-surveillance over foreign political data in Clouds lawful since 2008
- pattern of US secrecy/misdirection in policy history
- EU institutions seem to be “complicit-by-design” ?
- DP Regulation published with loopholes built-in

Thank you

Q & A ?

caspar@PrivacyStrategy.eu

In the entire corpus of Art.29 WP

There is no recognition that surveillance occurs for foreign intelligence gathering

Not for law enforcement

Not for national security

….just purely political surveillance of ordinary lawful democratic activities, in pursuit of foreign policy objectives

150 Opinions since 9/11

references to **FISA: 0, FISAAA: 0, PATRIOT: 1** (footnote)

"*Requests*" ?

Foreign intelligence is not "*Law Enforcement*"

- April 2012: Sopot Memorandum (footnote 16)
  - "*allowing* foreign law enforcement powers access"
- Jun 2012: Art 29 WP
  - 196 on Cloud Computing, 195 BCRs-for-processors
  - 150 Opinions since 9/11
    - references to **FISA: 0, FISAAA: 0, PATRIOT: 1** (footnote in WP53)
- Nov 2012: EDPS on Cloud Computing
  - the conditions under which law enforcement bodies may seek access to data stored in cloud computing services would ***benefit from being further clarified*** *(*?)
  - *the use of encryption to protect the data* (?)

UK Information Commissioner - Oct 2012

Guidance on the use of cloud computing

If comply with FISA or PATRIOT, you get off scot free

88. If a cloud provider is required to comply with a request for information from a foreign law enforcement agency, and did comply, the ICO would be likely to take the view that, provided the cloud customer had taken ***appropriate steps*** *to ensure that the use of the cloud services would ensure an* ***appropriate level of protection*** *for the rights of data subjects whose personal data would be processed in the cloud, regulatory action against the cloud customer (in respect of the disclosure of personal data to the foreign law enforcement agency)* ***would not be appropriate as the cloud provider, rather than the cloud customer****, had made the disclosure.*

89. Regulatory action against the cloud provider, in its role as data controller when disclosing data to the enforcement agency, ***would also be unlikely*** *provided the disclosure was made by the cloud provider* ***in accordance with a legal requirement to comply*** *with the disclosure request by the agency.*

50 USC § 1881a - Procedures for targeting certain persons outside the United States other than United States persons

(h) Directives and judicial review of directives

(1) Authority

With respect to an acquisition authorized under subsection (a), **the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—**

(A) **immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition** and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) Compensation

The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(3) **Release from liability**

No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

50 USC § 1881a - Procedures for targeting certain persons outside the United States other than United States persons

(a) Authorization

Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the **Attorney General and the Director of National Intelligence may authorize jointly**, for a period of **up to 1 year** from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States **to acquire foreign intelligence information.**

(b) Limitations

An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted **in a manner consistent with the fourth amendment** to the Constitution of the United States.

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

US Judiciary Subcommittee (25.7.12)

(Intellectual Property, Competition, And The Internet)

Rep. GOODLATTE: “what are some of the misconceptions that they (Deutsche Telekom) are spreading about the PATRIOT Act..?”

Rackspace: “absurd ..that it allows almost any U.S. government agencies to, without notice or warrant, access any private data that is on a server contained within the US”

Rep. GOODLATTE. “**Well, that is totally false.**”

Rep. WATT: “If we are allowing our national security apparatus access to information in the cloud, would it not be **a legitimate concern** for other countries to be concerned about the extent to which **our national security apparatus** would have access to **their information in the cloud**?” (emphasis added)