How to wiretap the Cloud

almost
(without ^ anybody noticing)

Caspar Bowden
independent advocate for privacy rights
(Chief Privacy Adviser - Microsoft 2002-2011,
Director of FIPR 1998-2002)

FISAAA, Data Protection and PRISM

ORGcon 8th June 2013 – IET London
Preliminaries

• I did not know about PRISM
  – warning about FISAAA since 2011
  – deduced PRISM from open-sources
  – never had a security clearance
• don't trust Microsoft
  – now 100% FLOSS advocate
• why did I leave Microsoft ?
  – maybe later... ;-)
• Allies have always spied on allies
  – WW2 British Security Co-ordination 1939-1941
• declassified UKUSA treaties 2010
  – began when Alan Turing arrived in US 1942!
    • led to postwar “5 Eyes” US/UK/CA/AU/NZ
    • much more tension than “Special Relationship” rhetoric would suggest
• PRISM codeword for special programs
  – ORCON - “originator controlled”
  – BLARNEY – mass collection of metadata
This is not about the PATRIOT Act

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

- PATRIOT 2001 is complicated (100+ pages)
  - amends FISA 1978 + other statutes
  - wiretap, seize, bug data
  - secret “National Security Letters” for metadata
- s.215 (aka FISA 1861) “Library Records”
  - Verizon leak 5.6.13, power used to obtain...
  - ALL domestic/international call metadata
This is not about Cloud as storage

parallel processing power as a commodity
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)
“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*”
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 can 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
SLATE 8th Jan: Ryan Gallagher


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
 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”)
This is a request
(National Security Letter to Nick Merrill, gagged for 7 years)
This is not a “Request”
Is Cloud-veillance a real risk?
(er...yes, since 7.6.13)

- 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
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.
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 data sovereignty risk matrix by purpose

<table>
<thead>
<tr>
<th>Purpose</th>
<th>intra-EU</th>
<th>EU data in US</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRIMINAL</td>
<td>✅</td>
<td>✗</td>
</tr>
<tr>
<td>NATIONAL SECURITY</td>
<td>✅</td>
<td>✗</td>
</tr>
<tr>
<td>POLITICAL/FOREIGN POLICY</td>
<td>✅</td>
<td>✗</td>
</tr>
</tbody>
</table>

**RED**

NOT PROTECTED BY

- ✗ US 4th Amendment
- ✗ EU DP
- ✗ CoE 108
- ✗ CoE Cybercrime
- ✗ ECHR
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.
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 practical 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
Summary

- Cloudveillance is potentially about all EU data (ECHELON agenda was only about comms)
- 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 misdirection to EU policymakers
- EU institutions warned off “national security”
- DP Regulation published with loopholes built-in
What do we know about PRISM?

- Seen same Washington Post article you have
- Full slides not disclosed
  - “selectors,” or search terms, that are designed to produce at least 51 percent confidence in a target’s “foreignness.”
- Under FISAAA 1881a...
- “probable cause” = “probably not American”
- is GCHQ use of PRISM the main issue?
  - isn't US surveillance of UK as/more worrying?
- are there other 1881a “programs”?
Facebook

Facebook is not and has never been part of any program to give the U.S. or any other government direct access to our servers....never received a blanket request or court order from any government agency asking for information or metadata in bulk, like the one Verizon reportedly received. And if we did, we would fight it aggressively. We hadn't even heard of PRISM before yesterday.

Google

not joined any program that would give the U.S. government—or any other government—direct access to our servers. ... not heard of a program called PRISM until yesterday....

Press reports that suggest open-ended access to our users’ data are false, period. Until this week’s reports, we had never heard of the broad type of order that Verizon received... Any suggestion that Google is disclosing information about our users’ Internet activity on such a scale is completely false.

Microsoft

...only ever comply with orders for requests about specific accounts or identifiers (!)
Confirmation PRISM is about 1881a

James R. Clapper
Director of National Intelligence

The Guardian and The Washington Post articles refer to ... Section 702 of the Foreign Intelligence Surveillance Act. They contain numerous inaccuracies.

Section 702 ...designed to facilitate the acquisition of foreign intelligence information concerning non-U.S. persons located outside the United States...... only non-U.S. persons outside the U.S. are targeted...minimize the acquisition, retention and dissemination of incidentally acquired information about U.S. Persons.

6.6.13
Thank you

Q & A?

caspar@PrivacyStrategy.eu

“When you have eliminated the impossible, there's a good chance you have made a mistake along the way”

But not in this case...
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
  - ThinThread trialled in UK (mid 2000s ?)
(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).
(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.