FISA, PRISM and Data Protection

Caspar Bowden
independent advocate for privacy rights

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

Congress on Privacy and Surveillance
30th September 2013 – Lausanne
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... ;-)
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”
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
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
US mission to EU
misdirection and omission : no mention of FISA

US Ambassador Kennard speech (Dec 4\textsuperscript{th} 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 \textit{criminal} investigators \textbf{equal to or greater} than the protections provided within the European Union.

- \textbf{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 \textit{criminal} investigations.

  - but FISAAA 1881a \textbf{did} eliminate these restrictions in non-criminal cases (and “foreign intelligence information”)


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
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>Green</td>
<td>Yellow</td>
</tr>
<tr>
<td>NATIONAL SECURITY</td>
<td>Green</td>
<td>Red</td>
</tr>
<tr>
<td>POLITICAL/FOREIGN POLICY</td>
<td>ECHR/TFEU</td>
<td>Red</td>
</tr>
</tbody>
</table>

**RED**

**NOT PROTECTED BY**

- US 4\textsuperscript{th} Amendment
- EU DP
- CoE 108
- CoE Cybercrime
- ECHR
Main programmes revealed by Snowden

- **PRISM**
  - are there other s.702 programmes (e.g for business Cloud computing)?

- **“Upstream”**
  - 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”
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
Procedures used by NSA to target non-US persons (Guardian 20.6.13)

- Confirms there are zero substantive privacy protections for non-US persons
- Solely concerned with establishing “foreignness” of target
- No restriction on full breadth of “foreign intelligence information”
WP29, EDPS silent about “foreign intelligence”

DPAs did not react to 2yrs of warnings?

~ 150 Opinions since 9/11

- PATRIOT mentioned in one footnote in 2001
  • Absent: FISA, PAA, FAA, “foreign intelligence”

Ambiguities:

• “legally binding request”

• “national security” - of Member States or United States?
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
This talk was not about PATRIOT Act

- 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
What is to be done?

- EU DPR amendments
  - consent “political” warning, and whistle-blower protection
  - insist DG-CONNECT, ENISA protects vs. foreign intel
- Need changes in US law – recognition, reciprocity
  - “lost Art.42”? fooling ourselves, US corps will ignore
- Reform of DPAs – WP29 ignored problem for 12 years
  - independent NGO monitoring of DPAs
- an EU Cloud
  - 'Airbus' to match US's Boeing
- ECHR litigation
  - GCHQ hacks into Belgacom switches
Call to action

- You want InfoSec? Buy an exercise book + Biro
  - assume NSA/GCHQ will target anti-NSA activism
  - small, independent, unconnected groups
- European + national advocacy
  - universal rights
  - targeted data preservation, no blanket retention
  - use tools that work: GPG, self-hosting, Tor (hops?)
  - no more secret laws & secret interpretations
  - reject “Carl Bildt” doctrine:
    - nobody knows, no “chilling effect”, no problem
Mes chers frères, n'oubliez jamais, quand vous entendrez vanter le progrès des lumières, que la plus belle des ruses du diable est de vous persuader qu'il n'existe pas!

Charles Baudelaire - Le Joueur Généreux
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.