QCon

Please evaluate my talk via the mobile app!

Reflections on Mistrusting Trust

Caspar Bowden
independent privacy researcher

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

QCon - London 4th March 2014

Reflections on Trusting Trust

Ken Thompson 1984

suppose put a backdoor in a compiler binary...
which replicates itself when compiling a compiler!

- implications for “trusted computing” tool-chains

insoluble for 3 decades, but David A.Wheeler

- *Fully Countering Trusting Trust through Diverse Double-Compiling (2006)*

Computer science. It changes. Deal with it.

Policymaker sense of “trust”

- Warm fuzzy feeling
- can “trust” this person/company/government not to act against my interests
  - belief that they won't
- Often meant as “blind” trust which cannot verify
  - “you have to trust something/someone”
- “Trusted Third Party”
  - originally from Kerberos-type authentication
  - perversely appropriated by UK government to mean key-escrow, 1996-1999

Information security sense of “trust”

- *“A trusted party is somebody who can break my security policy*”
  - Robert Morris Snr (Chief Scientist NSA 1980s) [apocryphal?]
- “Trusted parties” imposed on you by **Policy**
  - not your choice!
- In this sense of “trusted” you may well be suspicious and *mistrustful* of your trusted parties (and employ other precautions!)

So that means....

- technical and policy communities use “trust” in diametrically opposite senses!
  - InfoSec
    - “trust” is bad : minimize it
  - Policymaker
    - “trust” is good : don't worry, be happy
- Who has written about this ?
  - Ross Anderson, Dieter Gollmann, Claudia Diaz
- Why don't more people notice?
  - It's all about the Five Eyes....

EU “Trust and Security” Policy

- EU old-timers will tell you something bad happened in mid '90s
  - ECHELON inquiry 1999-, US-EU Safe Harbor 2000
- EU treaty: MS sole competence for “national security”
  - ...but EU responsible for “Data Protection” (?!)
- EU Commission weren't allowed to put NSA in their Threat Model (basically UK subverted EU policy)
  - no EU institutions acknowledged foreign intelligence threats (intra- or extra-EU) from 9/11 until Snowden
  - all EU “Trust & Security” for 20 years using T-word in warm fuzzy sense (don't worry about spying!)
  - they do not like people realizing these things !

But I came here for a talk on US FISA law, Cloud Computing, and Edward Snowden

Oh, alright, if you insist

Cloud *computing*
parallel processing power as commodity

Consumer: Facebook, Skype, Microsoft, Google

Business : Microsoft Azure/Office365, Google Apps, Amazon

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

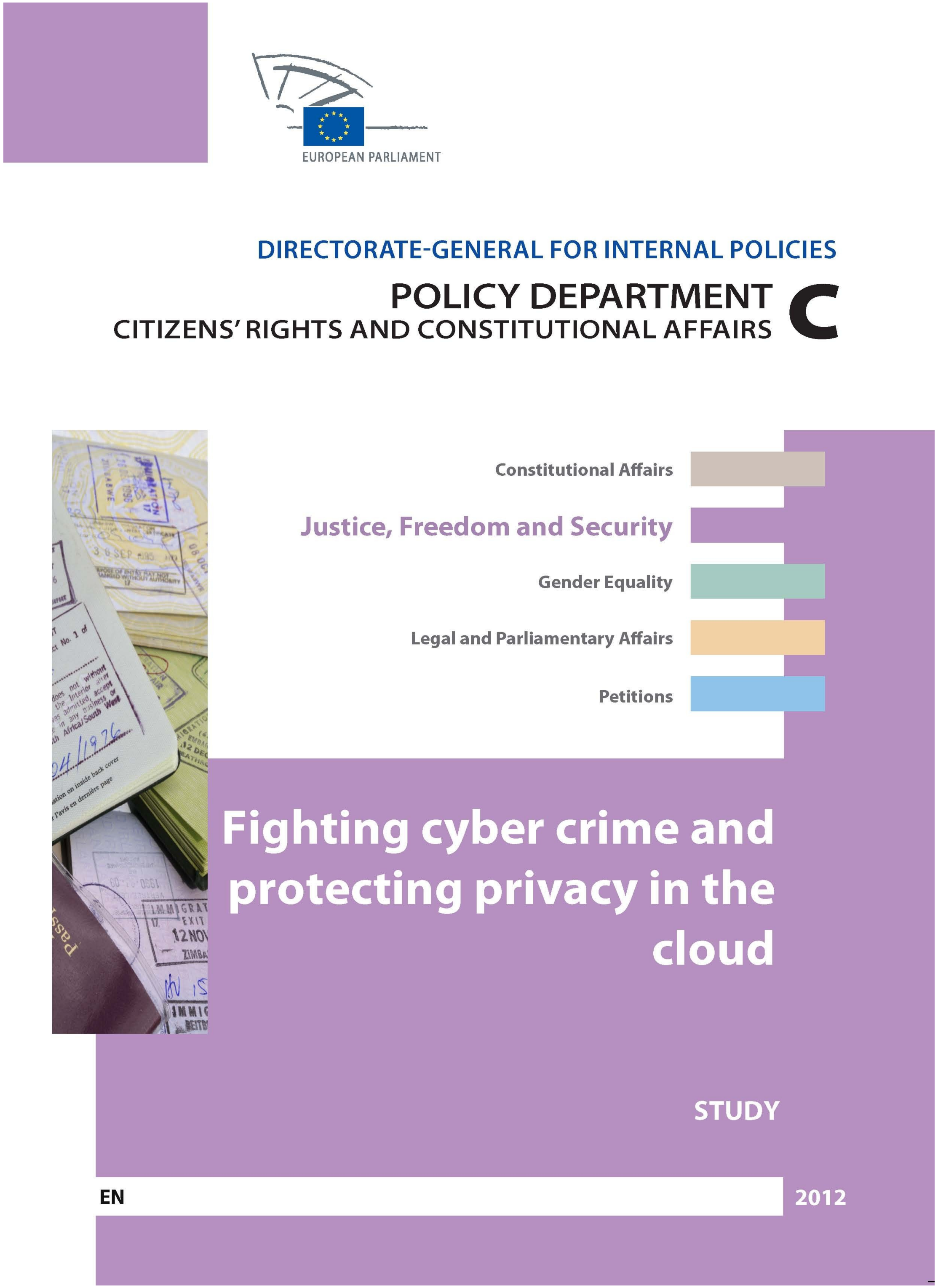
→ **designed for mass-surveillance of any Cloud data relating to US foreign policy**

- **"double-discrimination" by US nationality**
  - **completely unlawful under ECHR**

US Judiciary Subcommittee 31.5.12

Hearing on 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: 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?"

EU data sovereignty risk matrix by purpose

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

RED

<u>NOT PROTECTED BY</u>

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

Main programmes revealed by Snowden (1/2)

- PRISM/“Upstream”
  - full-take of metadata & content
  - fibre-optic cables, public/private networks
- 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 (NSA), EDGEHILL (GCHQ)
  - “aggressive multi-pronged effort to break into widely used encryption technologies”
- MUSCULAR (GCHQ)
  - intercepting unencrypted data between Cloud datacentres

Main programmes revealed by Snowden (2/2)

- Spying on 35 foreign government leaders
  - #MerkelPhone
- Quantum Insert
  - injecting vulnerabilities into packet stream
  - “shadow Internet” of ~100,000 pwned boxes
- “PORNINT”
  - Surveillance of sexual interests/behaviour for foreign policy objectives
- Global surveillance of cellphone locations
  - intersection attacks, “developing targets”
- “Anticrisis Girl” – targeting political activist networks

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.*

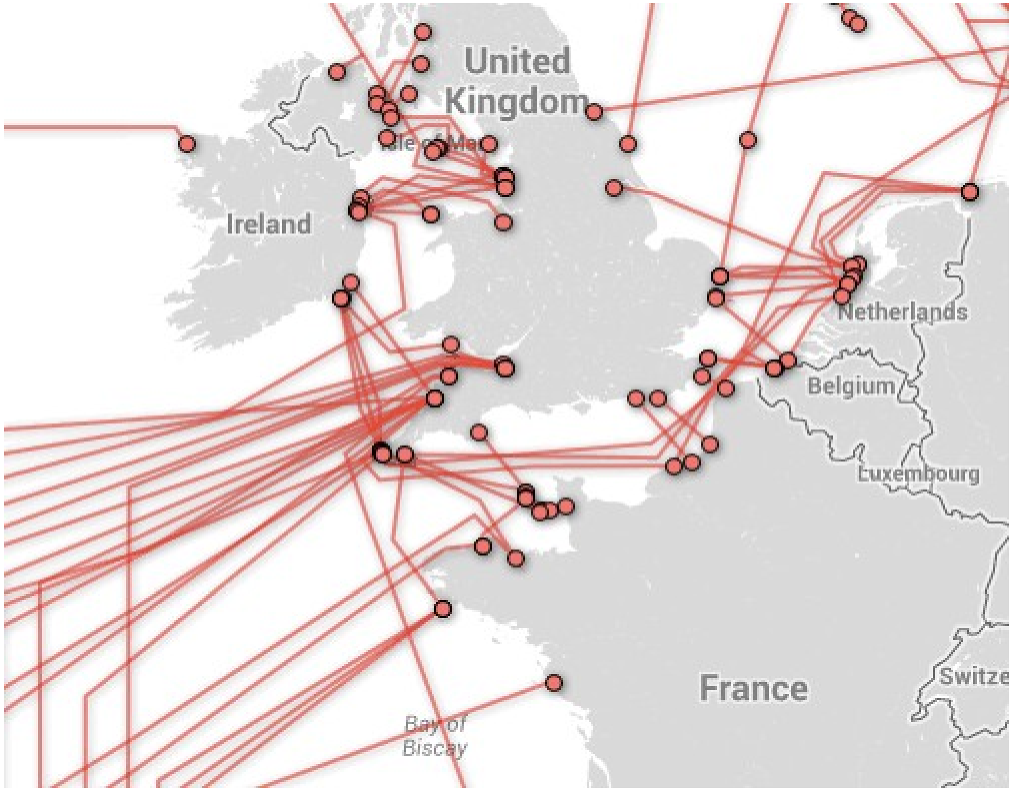
89. Regulatory action against the cloud provider, in its role as data controller when disclosing data to the enforcement agency, ***would also be unlikely*** *provided the disclosure was made by the cloud provider* ***in accordance with a legal requirement to comply*** *with the disclosure request by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

What do we know about TEMPORA ?

Interception at cable-heads since 2008

Guardian reports 21.6.13

- Internet “buffer”
  - 3 days content
  - 30 days metadata
    - “larger amount than NSA”
- May 2012: 300 GCHQ and 250 NSA analysts
- trawling EU traffic?
- Is NSA buffering too ?
  - or maybe 702 50% stops?



“Mastering the Internet"

GCHQ

Is TEMPORA lawful ?

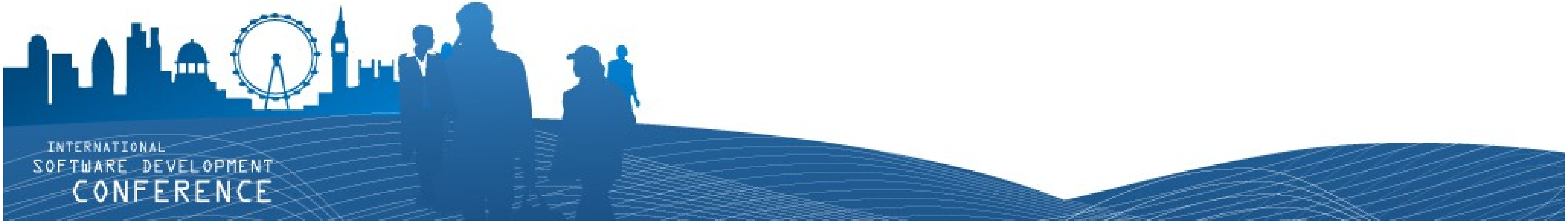
- RIPA “certificated warrant” for “external” communications
  - s.8(4)b(i) descriptions of intercepted material the examination of which SoS considers necessary
  - s.5(6) conduct authorised by an interception warrant shall be taken to include..all such conduct (**including the interception of communications not identified by the warrant**) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;
- HoC Standing Comittee discussion of “recklessness”
  - SoS does <u>not</u> have to consider proportionality
- HoL Committee non-discussion of “black-boxes”
    - “that's the best answer we are going to get”
- **HRA/ECHR – separate discussion**

What happened on Monday & Tuesday?

- **Monday**, Labour made a speech (Yvette Cooper, Shadow Home Sec)
  - keep blanket data retention (in coded language)
  - ISC are feeble and IPT lacks any credibility
  - IoCC/ISC are useless - scrap 'em - maybe Inspector General
    - and maybe not senior judges
  - Demos & Sir David Omand (Director GCHQ 1996-2000)
- **Tuesday**, LibDems made a speech (Nick Clegg, Deputy PM)
  - Problem is “external” data is not external any more
  - RUSI “private” inquiry
    - (no Conservative buy-in for reforms or inquiries)
  - “Don't accept” inevitability of blanket data retention
  - IoCC/ISC are useless - scrap 'em – maybe Inspector General
    - and not a senior judge

QCon

Please evaluate my talk via the mobile app!



Thank you

Q & A ?

Research Note to LIBE Ctee:

The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights

caspar@PrivacyStrategy.eu

“Prediction is very difficult, especially about the future”
Niels Bohr

Advice to Cloud providers

Providers subject to EU jurisdiction

- use open-source stacks, prefer AGPL-style licenses where possible
- establish an audit process for documenting not just the static code-base, but also all updates and patches, and establish a forensic trail from the source to the compiled code to the binaries which are loaded and run on every machine, from bare-metal upwards
- ensure all your sub-contractors can meet the same requirement, and keep your supply chain short and verifiable
- cut-out any extraterritorial legal access affecting your supply chain
- show stats on law enforcement requests and document compliance
- declare exact data retention polices and periods, including crypto keys
- ***tell customers and take credit for your transparency !***

Providers subject to non-EU jurisdiction

- plan on meeting above requirements
- lobby your legislature for treaties which extend the same privacy rights to EU residents as the citizens of your home jurisdiction

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