THE QUESTION LAWYERS DON’T ASK: CAN LAW ADDRESS TOTAL TRANSNATIONAL SURVEILLANCE?

@axelarnbak
30 September 2013, Lausanne, Switzerland
Cloud Concerns after 1st Paper
Amazon sep ‘12: Fearmongering!

Amazon-topman Vogels ziet discussie over privacy en de cloud als ‘pure bangmakerij’

Johan Leupen
Amsterdam

De persconferentie over de ‘cloud-o-pie’ was hooggeëigend. Aanwezige sprekers en sprekerszittingen konden gevoelige data van Nederlandse bedrijven of overheidsinstanties onder het hoofd en voet van de medeweten, waarmee het in het vertrouwen van het publiek en het publiek in de bedrijven belijden van de in- en uitvoering van de drukst wonende rapport. De raadplegingen afleiding van de bedrijven en de bedrijven van de cloud als ‘pure bangmakerij’

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud

Voor clamor over privacy en de cloud
THIRD PAPER (MAY ’13)
‘OBSCURED BY CLOUDS’

With Joris van Hoboken and Nico van Eijk
http://ssrn.com/abstract=2276103
OUTLINE

The Law & Policy of Total Surveillance

National Security Incentives: Why Everything?

Can Law & Policy Stop Total Surveillance?
OUTLINE

The Law & Policy of Total Surveillance

National Security Incentives: Why Everything?

Can Law & Policy Stop Total Surveillance?
47 CoE COUNTRIES: EUROPEAN CONVENTION ON HUMAN RIGHTS
Also According to US Department of Justice

• “non-U.S. persons located outside the United States [...] lack Fourth Amendment rights altogether.”

• “Because the Fourth Amendment does not protect such persons in the first instance, it does not prevent the Government from subjecting them to surveillance without a warrant.”

• “Since its enactment in 2008, section 702 has significantly increased the Government's ability to act quickly.”

• “It lets us collect information about the intentions and capabilities of [...] foreign adversaries who threaten the United States.”
DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Saturday, June 08, 2013

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

June 8, 2013

DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Over the last week we have seen reckless disclosures of intelligence community measures used to keep Americans safe. In a rush to publish, media outlets have not given the full context—including the extent to which these programs are overseen by all three branches of government—to these effective tools.

In particular, the surveillance activities published in The Guardian and The Washington Post are lawful and conducted under authorities widely known and discussed, and fully debated and authorized by Congress. Their purpose is to obtain foreign intelligence information, including information necessary to thwart terrorist and cyber attacks against the United States and its allies.
THE NOTORIOUS “SECTION 702” FISA AMENDMENTS ACT (FAA)
THE NOTORIOUS “SECTION 702” FISA AMENDMENTS ACT (FAA)

- Explicitly adopted to facilitate total surveillance
- “Foreign Intelligence Information”
  - ‘US National Security & Foreign Affairs’
- Data subjects: persons, organizations, regions
  - xKeyscore: All VPN connections in Switzerland
- Threshold: from ‘primary’ to ‘a’ purpose
  - Sealed Case, 310 F.3d 717: re-use in criminal proceedings
- 5 year extension on 31 Dec. 2012
- **No** legal safeguards for non-US persons
The United States [...] takes the position that it can use its own legal mechanisms to request data from any Cloud server located anywhere around the world so long as the Cloud service provider is subject U.S. jurisdiction: that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States.

Even Acknowledged in U.S. Lobby paper:
Hogan Lovells 2012, p. 5.
US Supreme Court:  
FISA is not our business

Clapper v. Amnesty, Feb. ’13; 5 – 4 Conservative Majority on Section 702 FISA:

1. it eliminated the requirement that the Government describe to the court each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized basis.

2. it **eliminated** the requirement that a target be a “foreign power or an agent of a foreign power.”

3. it diminished the court’s authority to insist upon, and **eliminated** its authority to supervise, instance-specific privacy-intrusion minimization procedures;
ORWELLIAN TWIST: ‘NO PROOF OF SURVEILLANCE, NO HARM’

No Standing for Amnesty, ACLU and others in Clapper v. Amnesty. Supreme Court interprets of Section 702 FISA:

‘because para. 1881a [of section 702] at most authorizes – but does not mandate or direct – the surveillance that respondents fear, respondents’ allegations are necessarily conjectural’

But the section was designed for non-US persons not to know that total surveillance is conducted?!?!
WHAT ABOUT US CITIZENS?
“MINIMIZATION PROCEDURES”

• To Minimize Total Surveillance on US citizens
• But Flakey ‘51% probability’ of US Citizen
  • Based on Selector / Keywords in Database
  • So Data is Collected / Seen.
• Generous exemptions – indefinite storage of
  • Any information needed to expand cyberwarfare arsenal
    • For finding 0day exploits, cyber offense and defense.
  • Encrypted traffic
    • Facebook, Webmail, Online banking
    • Protection is suspect: TOR, VPN, HTTPS.
• Highly sensitive ‘Metadata’ indefinitely stored?
  • NYTimes 29 sept: 5 years ‘online’, then 10 yrs on a disk
NYTimes 29 Sept. ’13: A Social Graph of every US person
NSA Gathers Data on Social Connections of U.S. Citizens

“The agency can augment the communications data with material from public, commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS location information, as well as property records and unspecified tax data, according to the documents. They do not indicate any restrictions on the use of such “enrichment” data, and several former senior Obama administration officials said the agency drew on it for both Americans and foreigners.”

"the agency is pouring money and manpower into creating a metadata repository capable of taking in 20 billion “record events” daily and making them available to N.S.A. analysts within 60 minutes."

"an internal briefing paper from the N.S.A. Office of Legal Counsel showed that the agency was allowed to collect and retain raw traffic, which includes both metadata and content, about “U.S. persons” for up to five years online and for an additional 10 years offline for “historical searches.”"
Total Information Awareness: Defunded in ’03? Never away
FRANCE, UK, SWEDEN, GERMANY, HOLLAND, ... JOIN THE PARTY
DEMAND & SUPPLY MEET IN SHINY LOGO’S OF CLOUD COMPUTING
Total Surveillance Grid Built in Utah (Wired March ’12)
SNOWDEN CONTACTS FILMMAKER LAURA POITRAS (JAN. ‘13)

How Laura Poitras Helped Snowden Spill His Secrets
It is nearly within our grasp to compute on all human generated information.
CIA cto Gus Hunt (Mar. ‘13): “Big Data is a Big Deal”

Big Data is a Big Deal at the CIA

Every day, the world is flooded by data. Cell phones, smart houses, satellite sensors and countless other sources are creating huge amounts of information—known collectively as “big data.”

The CIA is currently hiring creative, technically savvy individuals who know how to organize and interpret this complex information.

Chief Technology Officer Ira “Gus” Hunt has explained the significance of big data to the CIA: “It’s the CIA’s job to leverage the world of big data, find out what actually matters, connect the dots and figure out what our adversaries are intending to do.”

An Opportunity to Make a Difference

Today’s job market features an increasing number of careers for people with experience in data analytics, computer science, mathematics and engineering. But the CIA offers big data specialists the opportunity to:

- inform US policymakers,
- help drive successful intelligence operations,
- shape future CIA technologies and
- define resource needs and investments.
BIG DEAL INDEED: $600M CIA – AMAZON CONTRACT (MAR. ’13)

Cloud Services

Sources: Amazon and CIA ink cloud deal

By Frank Konkel Mar 16, 2013

In a move sure to send ripples through the federal IT community, FCW has learned that the CIA has agreed to a cloud computing contract with e-commerce giant Amazon, worth up to $600 million over 10 years.
Recall Amazon Oct. '12: 'Fearmongering'. Was he lying?

Amazon-topman Vogels ziet discussie over privacy en de cloud als 'pure bangmakerij'

Johan Leenen

De persoonlijke discussie over de cloud is openlijk hooggepookt. Aanvankelijk was de discussie voornamelijk gericht op de privacy en de impact op de privacy van individuen. Toen het bliksemende opponenten van de cloud zagen dat de cloud de toekomst was en dat de oude bedrijven niet in staat waren om deze te handhaven, begon de discussie over de impact van de cloud op de toekomstige technologieën. De discussie is nu overgegaan naar de impact van de cloud op de privacy en de veiligheid van de internetgebruikers.

Van Schlimmen niet als klant van het bedrijf

Waarom is de cloud voornamelijk gericht op de privacy en de veiligheid van de internetgebruikers? Het is een feit dat de cloud de toekomst is en dat de oude bedrijven niet in staat zijn om deze te handhaven. De discussie is nu overgegaan naar de impact van de cloud op de privacy en de veiligheid van de internetgebruikers. Het is een feit dat de cloud de toekomst is en dat de oude bedrijven niet in staat zijn om deze te handhaven.
OUTLINE

The Law & Policy of Total Surveillance

National Security Incentives: Why Everything?

Can Law & Policy Stop Total Surveillance?
NEW THREAT METAPHORS: FROM TERRORISM TO CYBERATTACKS

James Baker, former senior DOJ official on FISA:

“Let me repeat that: there are arguments that in order to defend ourselves, the government needs to be able to monitor all Internet communications. All of them. Is this possible, even if it is necessary? Maybe. The key limiting factors are money and access. And you would need lots of both.”

13 Sep ‘13, Constitution Day address, Dickinson College
Veja os documentos ultrasecretos que comprovam espionagem a Dilma

Arquivos foram obtidos com o ex-analista da NSA Edward Snowden.

Neste domingo (1º), o Fantástico exibiu uma reportagem exclusiva que revelou como o maior sistema de espionagem do mundo está de olho no Brasil.

Os três documentos ultrasecretos, vazados pelo ex-analista da NSA (Agência de Segurança Nacional de Segurança dos Estados Unidos) Edward Snowden, a que o Fantástico teve acesso exclusivo estão reproduzidos abaixo.
**Prism & Bullrun: Bulk Access in Concentrated Web Markets**

One of many examples:
- HTTPS market
- 3 CAs sell 75% certs
- 5 CAs sell 90% certs
- For top 1k, top 100k and top 1m domains

- Across web, similar market dynamics

With H. Asghari, M. van Eeten & N. van Eijk (WEIS 2013)
http://ssrn.com/abstract=2277806
POLITICAL LEADERS COME AND GO; HARDLY GRASP ISSUES AT HAND

• Minister Donner: “Don’t do it; use letters and bank cheques, just like me”

De Telegraaf, Frontpage, 5 Sept. 2011:
ALLIES SHARE INTELLIGENCE INFO: “QUID PRO QUO” (CTIVD ’09)
GAME THEORY: ‘race to bottom’ to leverage information trade
Treat yourself to a far better lecture than mine: https://www.youtube.com/watch?v=oD_YSRZjLx0
5M. SECURITY CLEARANCE, 2 STAFF:
~15M OF 136M US WORKFORCE!

Here’s the official Data, but nothing on national security:
http://www.bls.gov/news.release/empsit.t17.htm
Through Denial: EU Political Leaders Protect US Jobs?

They took ‘er jobs!
A SOBERING THOUGHT: BIG TECH TRANSITIONS HAVE THEIR WAR?

- World War II – Computer
- Cold War – Electronic ‘Inter’ Networks
- War on Terror – Datamining, the ‘Social Graph’
ANOTHER SOBERING THOUGHT: THE DUBIOUS ROLE OF ACADEMIA?

• Recent Quotes from Leading Academics
• DISCLAIMER: Very Anecdotal, but:
  • “NSA Recruits Top 10% US Math Students”
  • “Hardly Top Cryptanalysts in US Academia”
  • “State of the Art in Science 10 Years Behind NSA”
A Multi-Headed Monster Privacy Up against the Wall
OUTLINE

The Law & Policy of Total Surveillance

National Security Incentives: Why Everything?

Can Law & Policy Stop Total Surveillance?
Policy: Trust Political Leaders?

"In Nederland kennen wij een medisch beroepsgeheim. Er kan dan ook geen sprake van zijn dat wie dan ook zonder toestemming in medische gegevens van anderen zit te neuzen."

Edith Schippers (VVD)
minister van Volksgezondheid
FOR YEARS: DENIAL AND NATIONAL SECURITY EXCEPTIONALISM
Even Post-Snowden: Nobody Gets Fired, No Accountability
PRESS FOR FOREIGN INTELLIGENCE REFORM IN US LAWS?
YES, SOME ACTION & PROPOSALS; NOTHING ON NON-US PERSONS (!)
DHILMA ROUSSEFF: REDESIGN INTERNET GOVERNANCE?

BRAZIL LOOKS TO BREAK FROM US-CENTRIC INTERNET

By BRADLEY BROOKS and FRANK BAJAK — Sep. 17 2:26 PM EDT

Home » Dilma Rousseff » Brazil looks to break from US-centric Internet

1 of 2
GLOBAL LEGAL DEAL (W/ RUSSIA & CHINA!) ON SPYING/SURVEILLANCE?
Dhilma Rousseff: Redesign Internet Infrastructure?

Brazil looks to break from US-centric Internet

By Bradley Brooks and Frank Bajak — Sep. 17 2:26 PM EDT

Home > Dilma Rousseff > Brazil looks to break from US-centric Internet
Bullrun: NSA Too Powerful to Trust Technological Solutions

NSA Apparently Undermining Standards, Security, Confidence

SEPTEMBER 9, 2013 BY ED FELTEN  18 COMMENTS

The big NSA revelation of last week was that the agency’s multifaceted strategy to read encrypted internet traffic is generally successful. The story, from the New York Times and ProPublica, described NSA strategies ranging from the predictable—exploiting implementation flaws in some popular crypto products; to the widely-suspected but disappointing—inducing companies to insert backdoors into products; to the really disturbing—taking active steps to weaken public encryption standards. Dan wrote yesterday about how the NSA is defeating encryption.

To understand fully why the NSA’s actions are harmful, consider this sentence from the article:

Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wants to keep it that way.

In security, the worst case—the thing you most want to avoid—is thinking you are secure when you’re not. And that’s exactly what the NSA seems to be trying to perpetuate.

Suppose you’re driving a car that has no brakes. If you know you have no brakes, then you can drive very slowly, or just get out and walk. What is deadly is thinking you have the ability to stop, until you stomp on the brake pedal and nothing happens. It’s the same way with security: if you know your communications aren’t secure, you can be careful about what you say; but if you think mistakenly that you’re safe, you’re sure to get in trouble.
EU law solutions: mixed bag – No Member States’ support?

• Solutions EU Law Inherently Limited
  • No Competence National Security

• ‘Data Protection’ Framework Inherently Limited
  • Not All Cloud Data are ‘Personal Data’
    • Research Data, Trade Secrets, Lawyer Dossiers, etc.
  • Oversight on Intelligence Agencies by DPAs?
    • Notoriously Weak Position on Safe Harbor / BCRs

• Nonetheless, Interesting Proposals MEP In ‘t Veld:
  • ‘Warning’: High-End Security Customer Awareness
  • Whistleblower Protection
  • Increased Penalties for Cloud Providers
    • Catch 22, however: US Law Silences
Brazilian president: US surveillance a 'breach of international law'
Dilma Rousseff’s scathing speech to UN general assembly the most serious diplomatic fallout over revelations of US spying
INTERNATIONAL LAW: SLIM CHANCE OF SEEING RESULTS

• Transnational Surveillance from Within One State to Another
  • Context: Sigint in Satellite Communications
    • Ius Commune
    • Everybody Is Doing It

• Probably No Violation of State Sovereignty
  • No ‘Enforcement Jurisdiction’
  • Hardly Case-Law, No Indication Otherwise
  • Who Would Bring Up a Case Anyway?
  • Everybody Complicit – Except for Rousseff?
What About the European Convention on Human Rights?
Today Liberty announced it has issued a claim against the British Intelligence Services over their suspected involvement in the PRISM and Project Tempora privacy scandal.

Earlier this month it emerged that the US Government has been routinely intercepting the electronic communications of non-Americans outside of the US via the PRISM programme, covertly run by the National Security Agency (NSA). It now emerges that GCHQ, the UK’s eavesdropping agency, may have subjected people in the UK to blanket internet surveillance in any event.

Liberty believes that its electronic communications – and those of its staff – may have been unlawfully accessed by the likes of the Security Services and GCHQ.
ON STANDING: ‘NOT ACTUAL HARM, MERE EXISTENCE OF LAW’ SUFFICES

- Klass v. Germany: Opposite Approach from US
- Remember Clapper v. Amnesty’s Orwellian Twist!
  - Amnesty & ACLU no standing; no obstacle under ECHR
NOT MERELY PERSONAL DATA, BUT ‘ALL DATA ON SERVER’ PROTECTED

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L’HOMME

FIRST SECTION

CASE OF BERNH LARSEN HOLDING AS AND OTHERS
v. NORWAY

(Application no. 24117/08)
ECHR protects ‘the essence of rights’, Narrow Exceptions

CASE OF CHRISTINE GOODWIN v. THE UNITED KINGDOM

(Application no. 28957/95)
‘UNTARGETED MONITORING’: CRITERIA ‘OPEN TO THE PUBLIC’

CONSEIL DE L’EUROPE
COUNCIL OF EUROPE

COUR EUROPÉENNE DES DROITS DE L’HOMME
EUROPEAN COURT OF HUMAN RIGHTS

FOURTH SECTION

CASE OF LIBERTY AND OTHERS v. THE UNITED KINGDOM

(Application no. 58243/00)
LIBERTY a.o. VS. UK PROBABLY MOST RELEVANT CASE TO DATE

• **ECHR**: Struck the Total Surveillance Down
  • Only Looked at 1\textsuperscript{st} of 3 Tests: ‘Accordance with Law’
  • §64-§66 in 2002, read like Snowden’s Revelations Today!
    • *the 1985 Act* allowed the executive an extremely broad discretion … virtually unfettered”
    • for example, “all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe”
    • “Information could be … listened to or read, if the Secretary of State considered this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom’s economy.”
    • “material was selected for examination by an electronic search engine, and search terms, falling within the broad categories covered by the certificates, were selected and operated by officials.”
NO ‘BLANKET, INDISCRIMINATE COLLECTION’ OF NON-CONVICTS

CONSEIL DE L’EUROPE  COUNCIL OF EUROPE

COUR EUROPÉENNE DES DROITS DE L’HOMME EUROPEAN COURT OF HUMAN RIGHTS

GRAND CHAMBER

CASE OF S. AND MARPER v. THE UNITED KINGDOM

(Applications nos. 30562/04 and 30566/04)
JURY IS OUT: SUM OF PRACTICES VIOLATE ECHR? I’M POSITIVE
Problem [1]: Transnational Spying NSA on EU; GCHQ on US
‘Obligation’ under ECHR to Protect Citizens against Foreign Countries? Debatable…
Problem [2]: Constitutions forgot to bring an Army
ONE MAN ARMY: LEAKING THE REMAINING OVERSIGHT MODEL
ECHR on leaking quite strong, but case specific: ‘Public interest’, Duty ‘Civil Servants’
STRENGTHEN INSTITUTIONAL OVERSIGHT ON INTELLIGENCE?
Meaningful Oversight Within the State Hardly Feasible

- Transnational Surveillance: Oversight at UN?
- EU Data Protection Authorities Have No Competence
- CTIVD, Dutch Oversight Body, Interesting Model
  - Installed Just Before 9/11
  - Occasionally Highly Insightful Reports
  - But the Juice is Classified
- Transparency Won’t Break Culture of Plausible Deniability When it Gets Controversial
OUTLINE

The Law & Policy of Total Surveillance

National Security Incentives: Why Everything?

Can Law & Policy Stop Total Surveillance?

Wrap-Up & Desert (if time permits)
Wrap-up [1]: The Law & Policy of Surveillance, Intel. Incentives

- Intelligence Incentives for Total Surveillance Have Always Been There, Cloud Makes it Possible
- Decade of Law & Policy Enables Total Surveillance
- Total Surveillance About Much More than Privacy – The Rule of Law, Self-Government, Democracy
Wrap-up [2]: Can Law & Policy Tame Total Surveillance?

- Solutions on Infrastructural/Technological & Governance/Policy Level Unrealistic
- US: Not Moving One Inch on Foreigners Rights
- European Union & International/UN Law Inherently Limited as a Solution
  - EU Can Focus on Providers, Not on Intel. Agencies
  - In’t Veld Amendments Don’t Raise Costs of Surveillance
- ECHR Looks Promising Substantively …
  - Strong on Unspecific Cloud Surveillance & Leaking
- … but (Im)possible Enforcement Transnational Surveillance Within Foreign non-ECHR States
MAKE 15M WORKFORCE SOURCE FOR GOOD: PUT THE A BACK IN NSA!
QUESTIONS?

Twitter @axelarnbak

Cybersecurity & Information Law Researcher
Ph.D. Cand. Institute for Information Law, University of Amsterdam
2013/14 Fellow CITP @ Princeton, Berkman Center @ Harvard
http://www.ivir.nl/staff/arnbak.html
ART AS A SOURCE OF INSPIRATION: 
THE TRANSPARENCY GRENADE
... Pul the Pin in the App and Enforce Constitutional Values
... AND SUBMIT YOUR REPORT!
WWW.TRANSPARENCYGRENADE.COM