

INTERNATIONALE DATAFLOWS & CLOUD SURVEILLANCE: RECHT, TECHNOLOGIE OF ILLUSIE?



@axelarnbak

12 mei 2014, College 7, Privacy & Gegevensbescherming

1E ONDERZOEK IN SEPT. '12: PAS OP PATRIOT ACT EN FISA



By ZACK WHITTAKER / CBS NEWS / December 4, 2012, 3:59 PM

Patriot Act can "obtain" data in Europe, researchers say



AP FILE

3 Comments / 1 Shares / 1 Tweets / 0 Stumble / 0 Email

More +

LONDON | European data stored in the "cloud" could be acquired and inspected by U.S. law enforcement and intelligence agencies, despite Europe's strong data protection laws, university researchers have suggested.

The research paper, titled "[Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act](#)," written by legal experts at the University of Amsterdam's Institute for Information Law, support previous reports that the anti-terror Patriot Act could be theoretically used by U.S. law enforcement to bypass

REACTIE AMAZON OP ONS ONDERZOEK IN FD, SEPT. '12

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

Johan Leupe n
Amsterdam

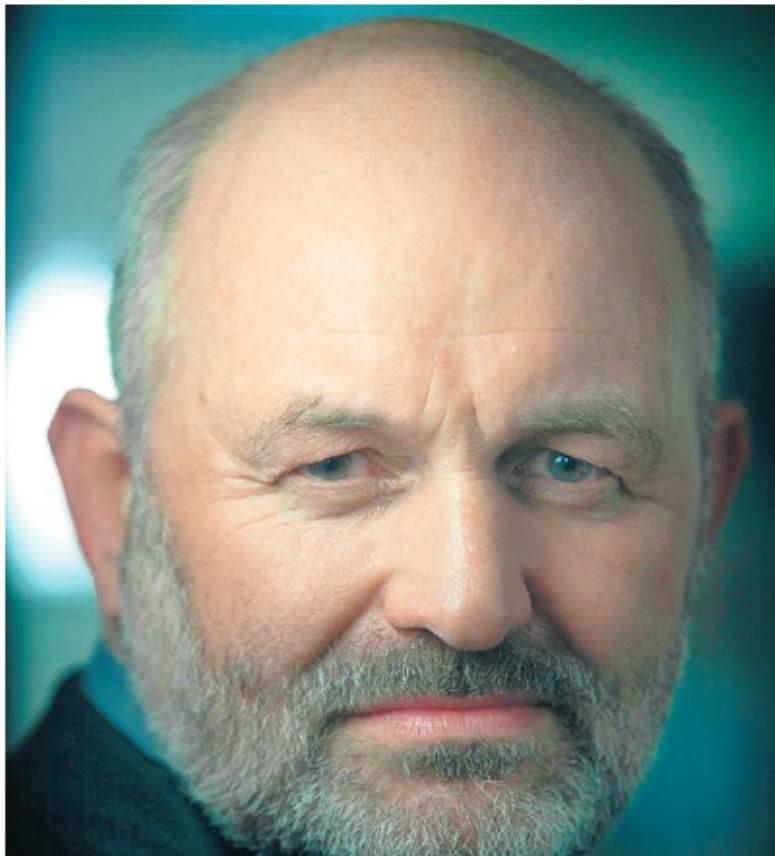
De privacydiscussie over de 'cloud' is opnieuw hoog opgetaaid. Amerikaanse opsporingsdiensten kunnen gevoelige data van Nederlandse bedrijven of overheden inzien zonder hun medeweten, waarschuwt het instituut voor Informatierecht (IVIR). De antiterrorismewet Patriot Act geeft de Verenigde Staten zelfs toegang tot servers op Nederlands grondgebied, stipt het UvA-onderzoek aan in zijn onderzoek.

Die bezwaren leidden tot Kamervragen en wakkeren een al langer bestaande discussie aan: is het welveilig om cruciale gegevens of zelfs complete IT-systemen te verhuizen naar Amerikaanse hostingbedrijven? Wegen de kostenwoedeën op tegen de risico's?

Amazon-bestuurslid Werner Vogels, misschien wel het voornaamste boegbeeld van de cloudrevolutie, vondraagt de commotie over zijn geesteskind slecht. De argumenten zijn vertrouwd door propagandisten van bedrijven die hun broodwinning zien verdwijnen, zegt hij. Daarmeer dreigt het revolutionaire karakter van de cloud onder te sneeuwen.

V Schrikken uw klanten van de PatriotAct?

'Die staat los van de cloud. De Patriot Act is gewoon een wet die geldt vooriederden. Het klopt dat de opsporingsdiensten toegang kunnen krijgen, maar die is niet langduriger dan drie uren. En dan moeten ze wel met een geldige dagvaarding komen. Wijlichten dan de klant in. Tenzij er een geheimehoudingsclausule geldt. In het geval dat er illegale content wordt aan-



Uw concurrenten Cisco en Oracle propageren de 'private cloud', een open IT-omgeving die wel binnen de muren van de klant blijft. 'Private cloud is een hoop blabla. Alle voordelen zijn dan weg. Je moet klanten juist onlasten: van hun zorgen over datacenters, van onderhoudscontracten. Bij private koop je nog je eigen hardware.'

'Het komt allemaal neer op wat ik "FUD" noem: "fear, uncertainty en doubt". Bangmakerij, propaganda van bedrijven die vroeger dominant waren en willen dat je hun spullen blijft kopen. Vroeger was de IT-dienstverlener de baas, en kwam je onmogelijk van hem af. Wij pikken hun werk in.'

V De Duitse softwarereus SAP gebruikt zijn origine als verkoopargument: 'Bij ons kijkt de Amerikaanse overheid niet mee'.

'SAP is juist een heel grote klant en een belangrijke partner. Ze hebben zelf trainingsfaciliteiten, sales, en andere zaken bij ons beladen in de cloud. Dat zouden ze niet doen als het slecht zou zijn voor hun klanten. We hebben ook overheden van over de hele wereld. Daar zit genoeg verstand.'

V De IT-volwassenheid laat bij overheden nogal eens te wensen over. Zie het de haken met Diginotar in Nederland.

'Dat klopt. Mensen bouwen nu eenmaal slechte IT-architectuur, met alle risico's van dien. Dat zou niet moeten kunnen. We zitten nu met zijn allen vijftien, twintig jaar op internet. De wereld is veranderd.'

'Kijk naar banken. Internet wordt het dominante kanaal voor alle bankzaken. Ik sta ervan ver-

ONDERTUSSEN: \$600M 'BIG DATA' CONTRACT MET C.I.A. - MRT '13



TRENDING: Shutdown NSA Federal List FY2014

POLICY MANAGEMENT EXEC TECH WHO & WHERE TI

Cloud Services

Sources: Amazon and CIA ink cloud deal

By Frank Konkel Mar 18, 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 electronic commerce giant Amazon, worth up to \$600 million over 10 years.

Amazon Web Services will help the intelligence agency build a private cloud infrastructure that helps the agency keep up with emerging technologies like big data in a



SCHIPPERS DEC '12: GEEN ZORGEN EPD, 'MEDISCH BEROEPSGEHEIM'

NOS.nl



"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

DATACENTER IN UTAH: TOTALE SURVEILLANCE, WIRED MRT '12



CIA CTO GUS HUNT (MRT. '13): CIA RECRUITMENT SLIDE 1



It is nearly within our grasp to
compute on all human
generated information

A slide from Hunt's presentation.

CIA CTO GUS HUNT (MRT. '13): “BIG DATA IS A BIG DEAL”



CIA Home
About CIA
Careers and Internships
Offices of CIA
News & Information
Press Releases & Statements
Speeches & Testimony
CIA & the War on Terrorism
Featured Story Archive
2012 Featured Story Archive
Big Data is a Big Deal at the CIA
What's New on CIA.gov
Your News
Library
Kids' Page
Contact CIA
Mission

CENTRAL INTELLIGENCE AGENCY

THE WORK OF A NATION. THE CENTER OF INTELLIGENCE.

... | 中文 | English | Français

Sea

Featured Story Archive

[CIA Home](#) > [News & Information](#) > [Featured Story Archive](#) > [2012 Featured Story Archive](#)
> [Big Data is a Big Deal at the CIA](#)



Big Data is a Big Deal at the CIA

 RSS

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.

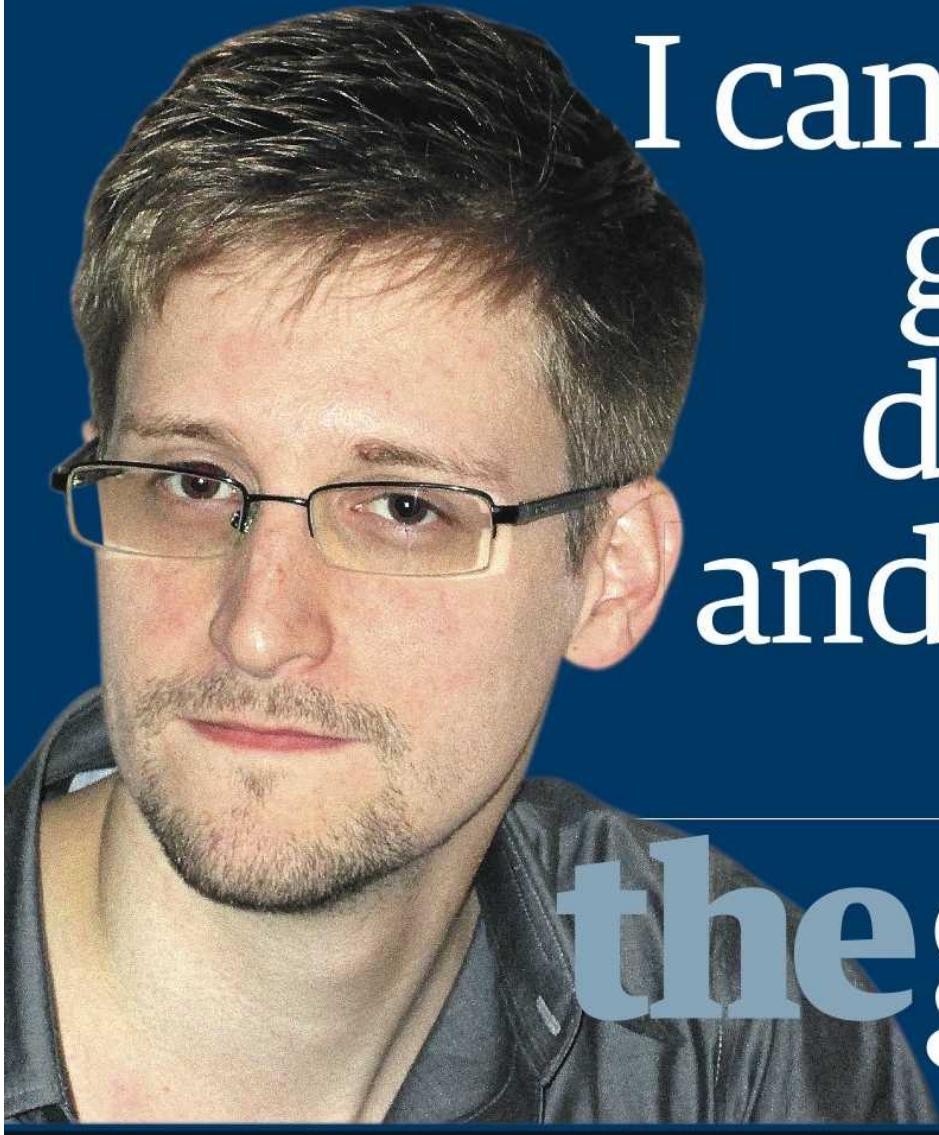
3E ONDERZOEK MEI '13: ‘OBSCURED BY CLOUDS’



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

The whistleblower

I can't allow the US government to destroy privacy and basic liberties



the guardian

guardian.co.uk

OUTLINE

VS wetgeving & Snowden's onthullingen

Waarom alle data, van iedereen?

Pauze

Oplossingen: Recht, Technologie of Illusie?

OUTLINE

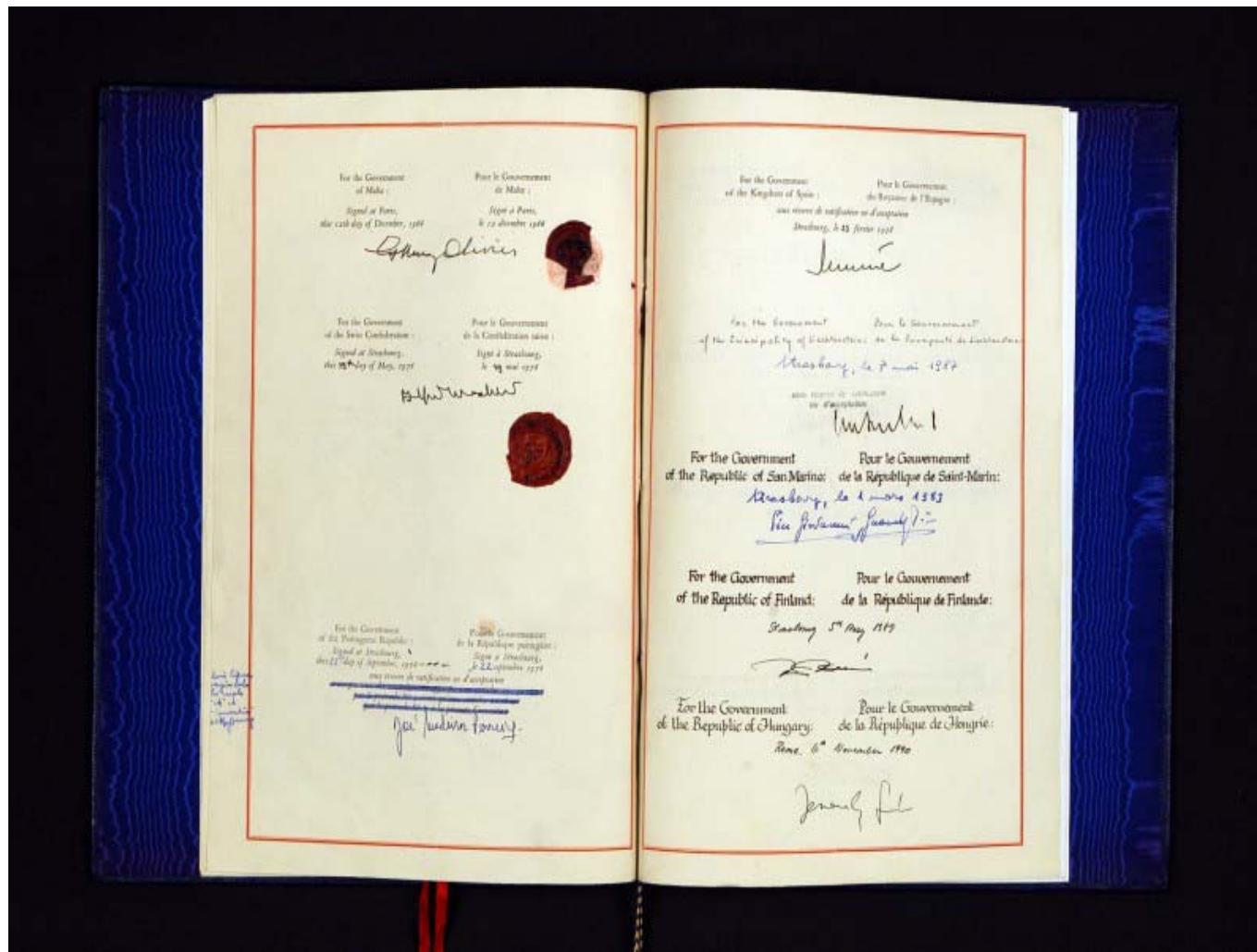
VS wetgeving & Snowden's onthullingen

Waarom alle data, van iedereen?

Pauze

Oplossingen: Recht, Technologie of Illusie?

47 LANDEN RAAD V. EUROPA: VERDRAG RECHTEN VD MENS



HAYDEN: “US CONSTITUTION IS NOT AN INTERNATIONAL TREATY”



DAT VINDT HET AMERIKAANSE MINISTERIE VAN JUSTITIE OOK

- “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.”

FORMELE REACTIES NA SNOWDEN: ‘LAWFUL & AUTHORIZED’

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.



President George W. Bush, joined by members of his Cabinet and members of Congress, signs the FISA Amendments Act of 2008 Thursday, July 10, 2008, in the Rose Garden at the White House. White House photo by Eric Draper



DE BERUCHTE “SECTION 702” FISA AMENDMENTS ACT (FAA)

- Reactie AT&T Warantless Wiretapping Schandaal
- Meer bescherming Amerikanen
- Geen juridische waarborgen “non-US persons”
 - Reguleert “Foreign Intelligence Information”
 - Militaire, politieke, economische surveillance
 - Van wie? personen, organisaties, regio's
 - Zoals: Alle VPN connecties in Nederland (*xKeyscore*)
 - Geheime Rechtbank: geen toets surveillance niet-Amerikanen
 - Geheime Rechtbank: maakt ook zelf ‘recht’
 - Sealed Case, 310 F.3d 717: re-use in criminal proceedings
- Geruisloze 5 jaar verlenging op 31 dec. 2012

WIE MOETEN MEEWERKEN? FYSIEKE LOCATIE IRRELEVANT!

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.

US SUPREME COURT: 'ER IS EEN WET, DUS NOT OUR BUSINESS'

Clapper v. Amnesty, Feb. '13; 5 - 4 conservatieve meerderheid over 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;*

ORWELIAANSE TWIST: ‘NO PROOF OF SURVEILLANCE, NO HARM’

Amnesty, ACLU en de rest hebben geen zaak, want:

‘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’

De wet geen enkele transparantie, dus je kan nooit weten wat er gebeurt, dus je hebt geen zaak

The whistleblower

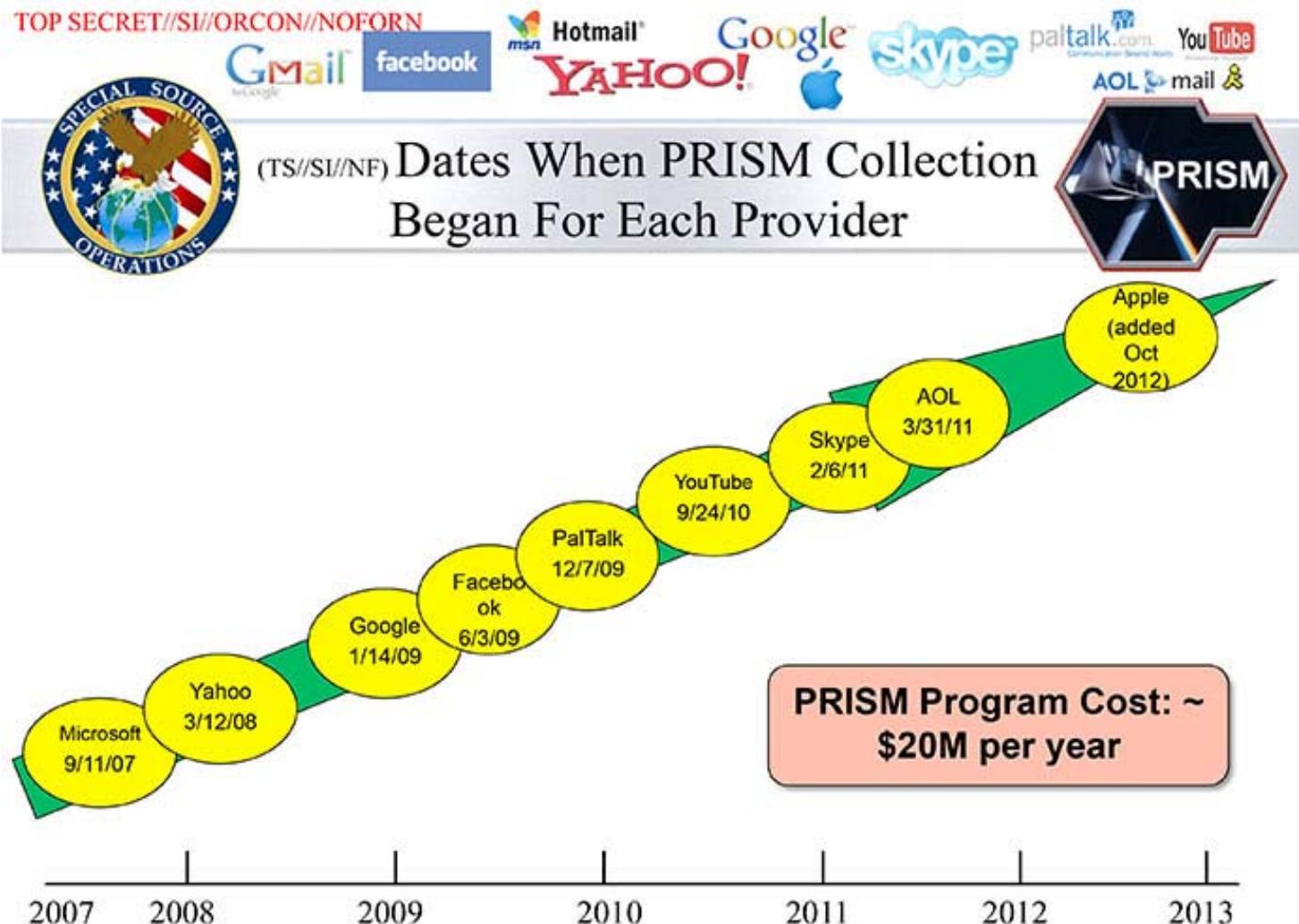
I can't allow the US government to destroy privacy and basic liberties



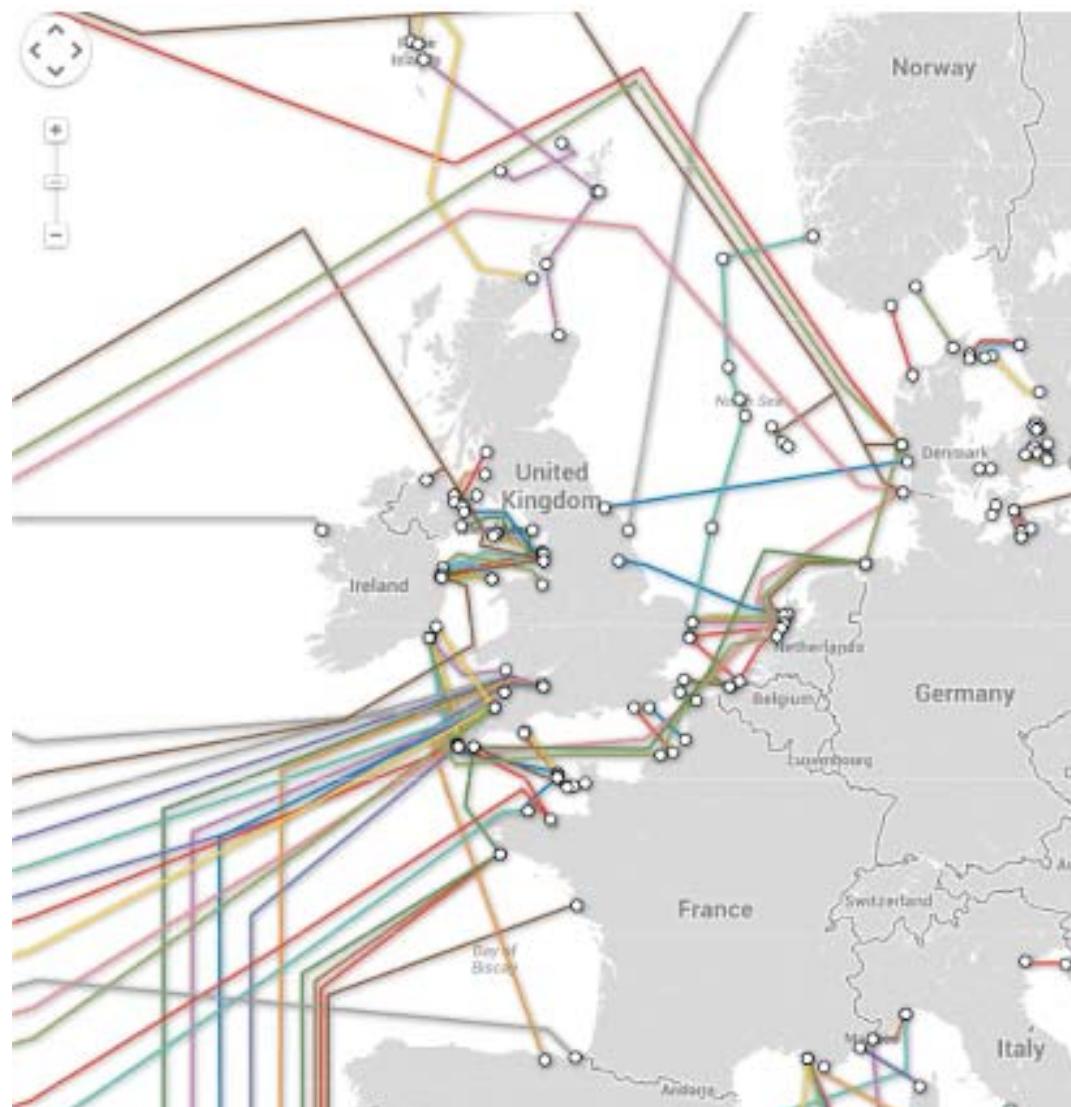
the guardian

guardian.co.uk

SNOWDEN ONTHULLING [1]: PRISM



SNOWDEN ONTHULLING [2]: TEMPORA



SNOWDEN ONTHULLING [3]: BULLRUN

TOP SECRET STRAP1

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

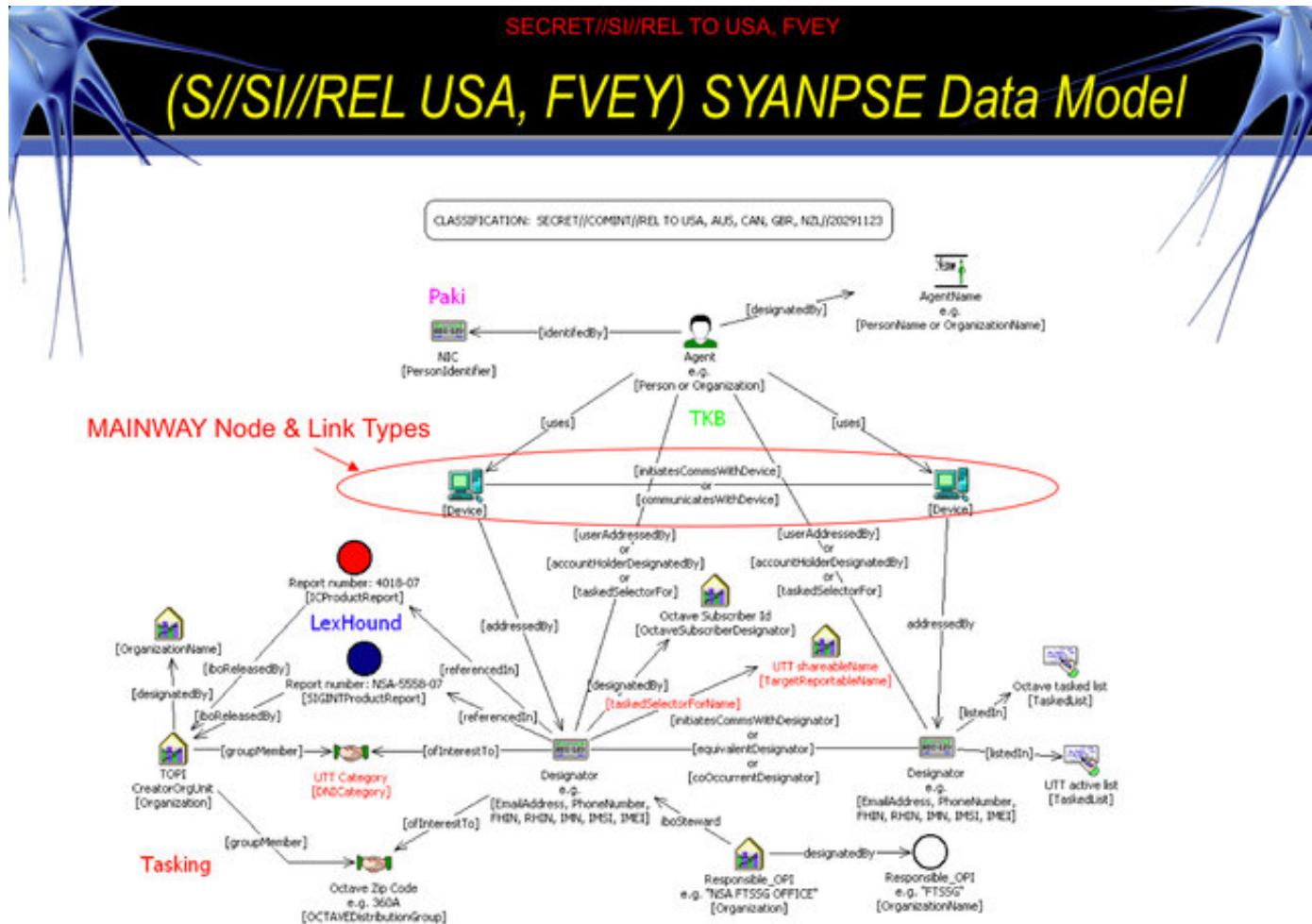
PTD "We penetrate targets' defences."



This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email infoeg@gchq.gov.uk

© Crown Copyright. All rights reserved.

SNOWDEN ONTHULLING [4]: ‘THE SOCIAL GRAPH’



NYTIMES 29 SEPT. '13: ‘THE SOCIAL GRAPH’

“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.”

SNOWDEN ONTHULLING [5]: ‘XKEYSCORE’ ZOEKMACHINE

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

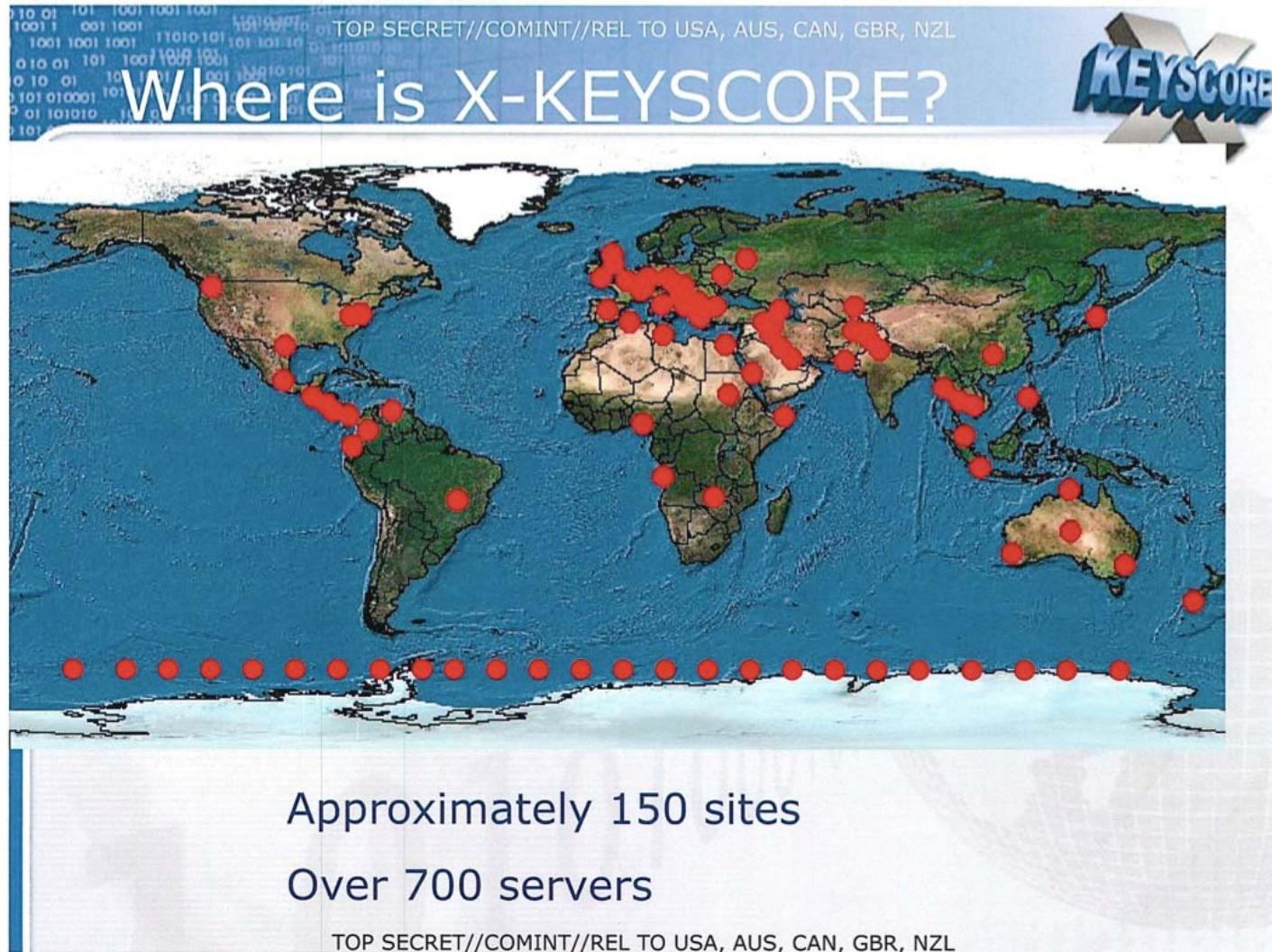
What is XKEYSCORE?



1. DNI Exploitation System/Analytic Framework
2. Performs strong (e.g. email) and soft (content) selection
3. Provides real-time target activity (tipping)
4. “Rolling Buffer” of ~3 days of ALL unfiltered data seen by XKEYSCORE:
 - Stores full-take data at the collection site – indexed by meta-data
 - Provides a series of viewers for common data types
1. Federated Query system – one query scans all sites
 - Performing full-take allows analysts to find targets that were previously unknown by mining the meta-data

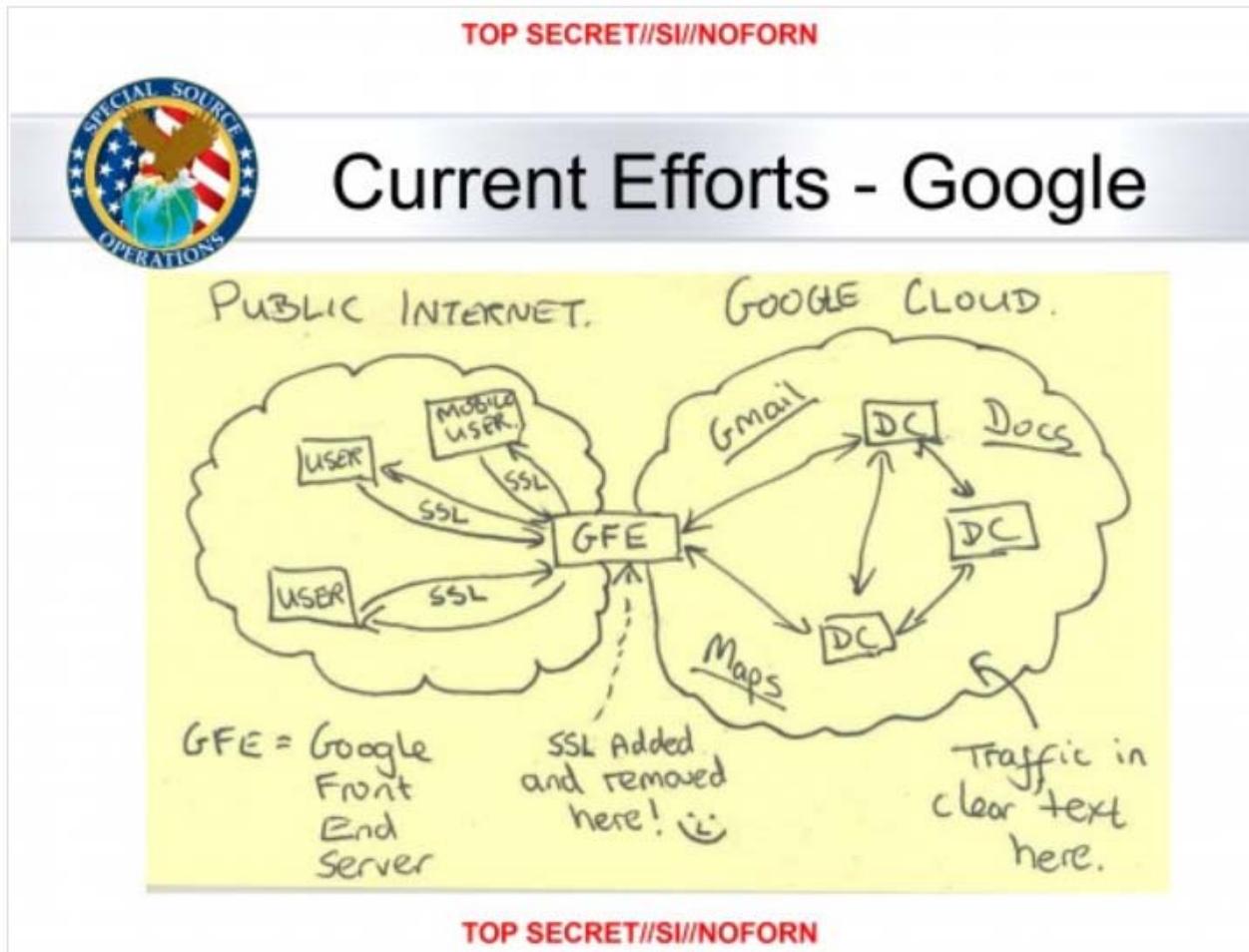
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

SNOWDEN ONTHULLING [5]: ‘XKEYSCORE’ DATALOCATIES



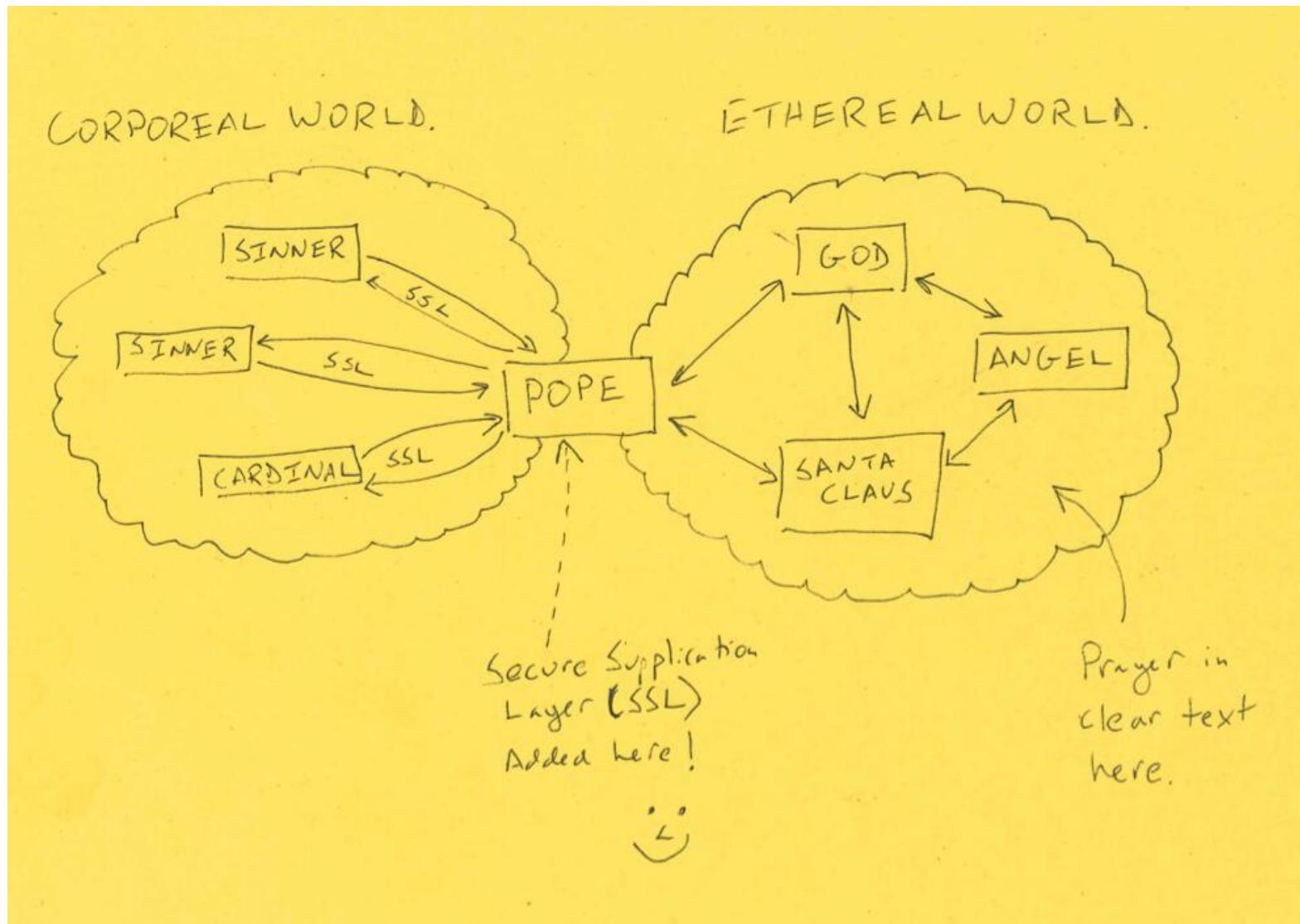
SNOWDEN ONTHULLING [6]

MUSCULAR: 181M RECORDS P/MND



In this slide from a National Security Agency presentation on "Google Cloud Exploitation," a sketch shows where the "Public Internet" meets the internal "Google Cloud" where user data resides. Two engineers with close ties to Google exploded in profanity when they saw the drawing.

COLLEGA RYAN BUDISH GAAT LOS: HOE DE NSA RELIGIE AFLUISTERT ☺



SNOWDEN ONTHULLING [7]: QUANTUM CATALOG, HACKING

TOP SECRET//COMINT//REL USA, FVEY

(U) There is More Than One Way to QUANTUM



TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
CNE				
QUANTUMINSERT	<ul style="list-style-type: none"> • Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation 	2005	Operational	Highly Successful <small>(In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)</small>
QUANTUMBOT	<ul style="list-style-type: none"> • Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel 	Aug 2007	Operational	Highly Successful <small>(over 140,000 bots co-opted)</small>
QUANTUMBISCUIT	<ul style="list-style-type: none"> • Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity. 	Dec 2007	Operational	Limited success at NSAW due to high latency on passive access <small>(GCHQ uses technique for 80% of CNE accesses)</small>
QUANTUMDNS	<ul style="list-style-type: none"> • DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers. 	Dec 2008	Operational	Successful <small>(High priority CCI target exploited)</small>
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	Successful
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	N/A
CNA				
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	Successful
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live Tested	N/A
CND				
QUANTUMSMACKDOWN	Prevents target from downloading implants to DoD computers while capturing malicious payload for analysis.	Oct 2010	Live Tested	N/A

TS//SI//REL

TOP SECRET//COMINT//REL USA, FVEY

1

SNOWDEN ONTHULLING [8]: TURBINE, MALWARE

THE//INTERCEPT

[NEWS](#)[GLENN GREENWALD](#)[VOICES](#)[DOCUMENTS](#)[STAFF](#)[ABOUT](#)[ARCHIVES](#)

NEWS

How the NSA Plans to Infect ‘Millions’ of Computers with Malware

By Ryan Gallagher and Glenn Greenwald

12 Mar 2014, 9:19 AM EDT

122

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

One presentation outlines how the NSA performs “industrial-scale exploitation” of computer networks across the world.

SHARE

 [Facebook](#) [Google](#) [Twitter](#) [LinkedIn](#) [Email](#)

ABOUT THE AUTHORS



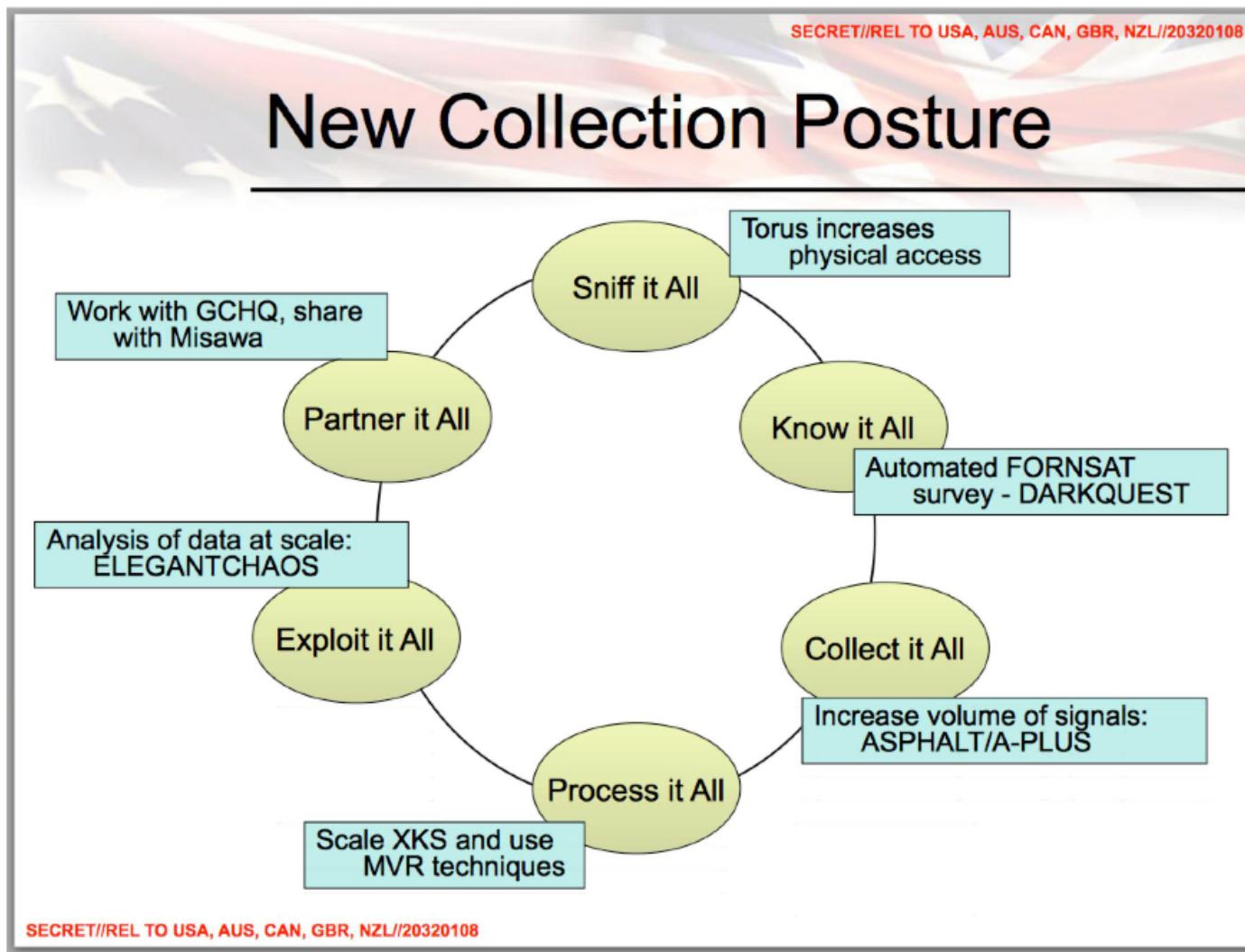
Ryan Gallagher
Reporter: [Read more](#)



Glenn Greenwald
Editor: [Read more](#)

SNOWDEN ONTHULLING [9]: GISTER!

Page 97



SNOWDEN ONTHULLING [10] GISTER

Page 102

TOP SECRET//COMINT//X1

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSA Strategic Partnerships

CENTRAL SECURITY SERVICE
UNITED STATES OF AMERICA

Alliances with over 80 Major Global Corporations Supporting both Missions

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators

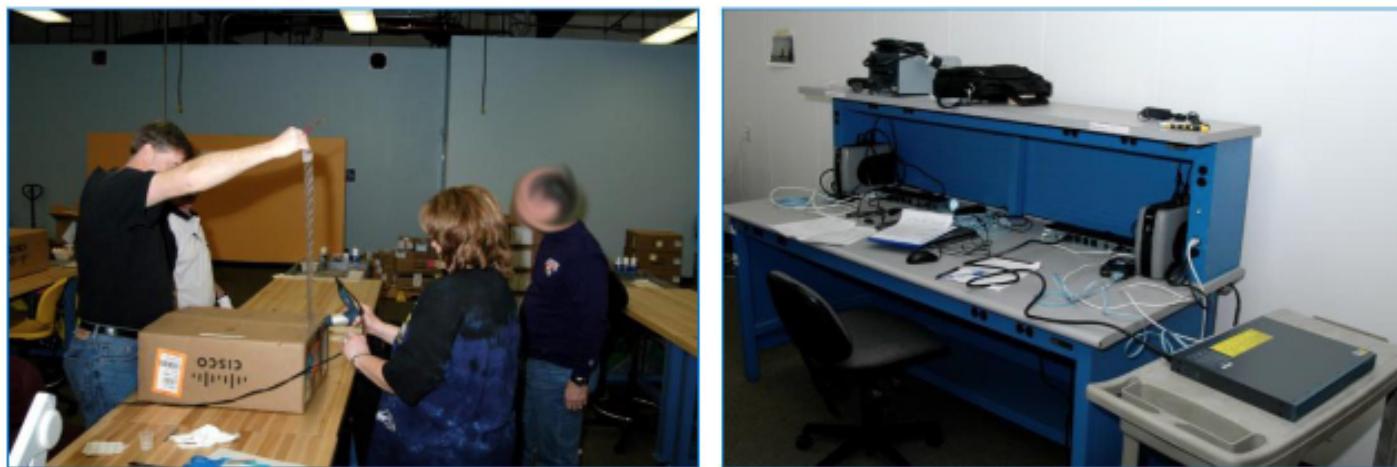
AT&T
EDS
Qualcomm
IBM
CISCO
Oracle
Microsoft
Verizon
Motorola
Intel
Qwest

TOP SECRET//COMINT//X1

SNOWDEN ONTHULLING [11] GISTER ROUTER INTERCEPTS, IN DE POST!

Page 149

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

" ALL THE NEWS
YOU NEED TO KNOW "

News.Today

FOUNDED 1851

MONDAY, OCTOBER 2012
Vol. MCMXX, No. 144672

WHAT'S NEXT?

newspaper |

Stemming AMS-IX: Europa niet bang voor Patriot Act



2 okt. 2013 door René Schoemaker



Nieuws - De Nederlandse leden van AMS-IX hebben in meerderheid tegen een uitbreiding naar de Verenigde Staten gestemd, maar dat was te weinig om die stap tegen te houden. De meeste leden uit andere (Europese) landen en de VS stemden voor.

Uit gegevens die de Amsterdam Internet Exchange vandaag heeft vrijgegeven blijken vooral de Nederlandse leden tegen een nieuwe dochteronderneming in de Verenigde Staten te hebben gestemd. Een indicatie dat een meerderheid van de Nederlandse leden tegen zou stemmen, was al eerder bekend. Met name leefde de vrees dat daardoor de Amerikaanse opsporingsdiensten toegang zouden krijgen tot het internetverkeer dat via AMS-IX de wereld wordt rondgepompt. De stemming was vorige week vrijdag.

Major Communications Cables

- Points of Convergence -

ATT

New York
Chicago
Los Angeles
Salt Lake City
Denver
Phoenix
Kansas City
Atlanta
Miami
Washington DC
Seattle
San Francisco
Dallas

Verizon

New York
Chicago
Los Angeles
Salt Lake City
Denver
Phoenix
Kansas City
Atlanta
Miami
Washington DC
Seattle
San Francisco
Dallas

British Telecom

New York
Chicago
Los Angeles
Salt Lake City
Denver
Phoenix
Kansas City
Atlanta
Miami
Washington DC
Seattle

T-Mobile

New York
Chicago
Los Angeles

San Francisco
Dallas

Major Cable Convergence Points (Cont.)

ATT

Amsterdam
Frankfurt
Paris
London
Tokyo
Hong Kong
Singapore

Sydney
Toronto
Redditch
Sophia
Antipolis
Bangor
Shanghai

Verizon

Amsterdam
Paris
London
Tokyo
Hong Kong
Singapore

British Telecom

Frankfurt
London
Tokyo
Hong Kong
Singapore
Stockholm
Sydney

T-Mobile

Amsterdam
Frankfurt
Paris
London
Tokyo
Stockholm

Copenhagen
Marseille
Hamburg
Hanover
Nuremberg
Zurich
Vienna

Buenos Aires
Rio De Janeiro
Santiago
Lima
Mexico City
Bogota
Mumbai

Loopholes for Circumventing the Constitution: Warrantless Surveillance on U.S. Persons by Collecting Network Traffic Abroad

Working Paper; Last updated May 1, 2014.

Axel M. Arnbak¹ and Sharon Goldberg²

¹ Berkman Center for Internet & Society, Harvard University, Cambridge, MA 02138.

² Computer Science Department, Boston University, Boston, MA 02215.

Abstract. In this multi-disciplinary paper, we reveal interdependent legal and technical loopholes that intelligence agencies of the U.S. government could use to circumvent 4th Amendment and statutory safeguards for U.S. persons. We outline known and new circumvention techniques that can leave the Internet traffic of Americans as vulnerable to surveillance, and as unprotected by U.S. law, as the Internet traffic of foreigners.

Keywords: surveillance, legal frameworks, network protocols, DNS attacks, BGP attacks.

1 Introduction

As the general public and the media becomes overloaded by the string of recent NSA revelations, the academic community has the important task of precisely describing the legal and technical realities under which these programs operate, and to offer informed recommendations on how to overcome the current status quo of apparent surveillance overreach. This multi-disciplinary paper takes steps in this direction, by discussing legal and technical loopholes that enable U.S. authorities to circumvent the 4th Amendment and statutory safeguards in place for U.S. persons when conducting network surveillance. We describe known and new circumvention techniques which, if the authorities choose to employ them, leave Americans as unprotected against ubiquitous surveillance as foreigners.

N.S.A. '03: POLITIEK GEBLOKKEERD, ZONDER POLITIEK VOORTGEZET



OUTLINE

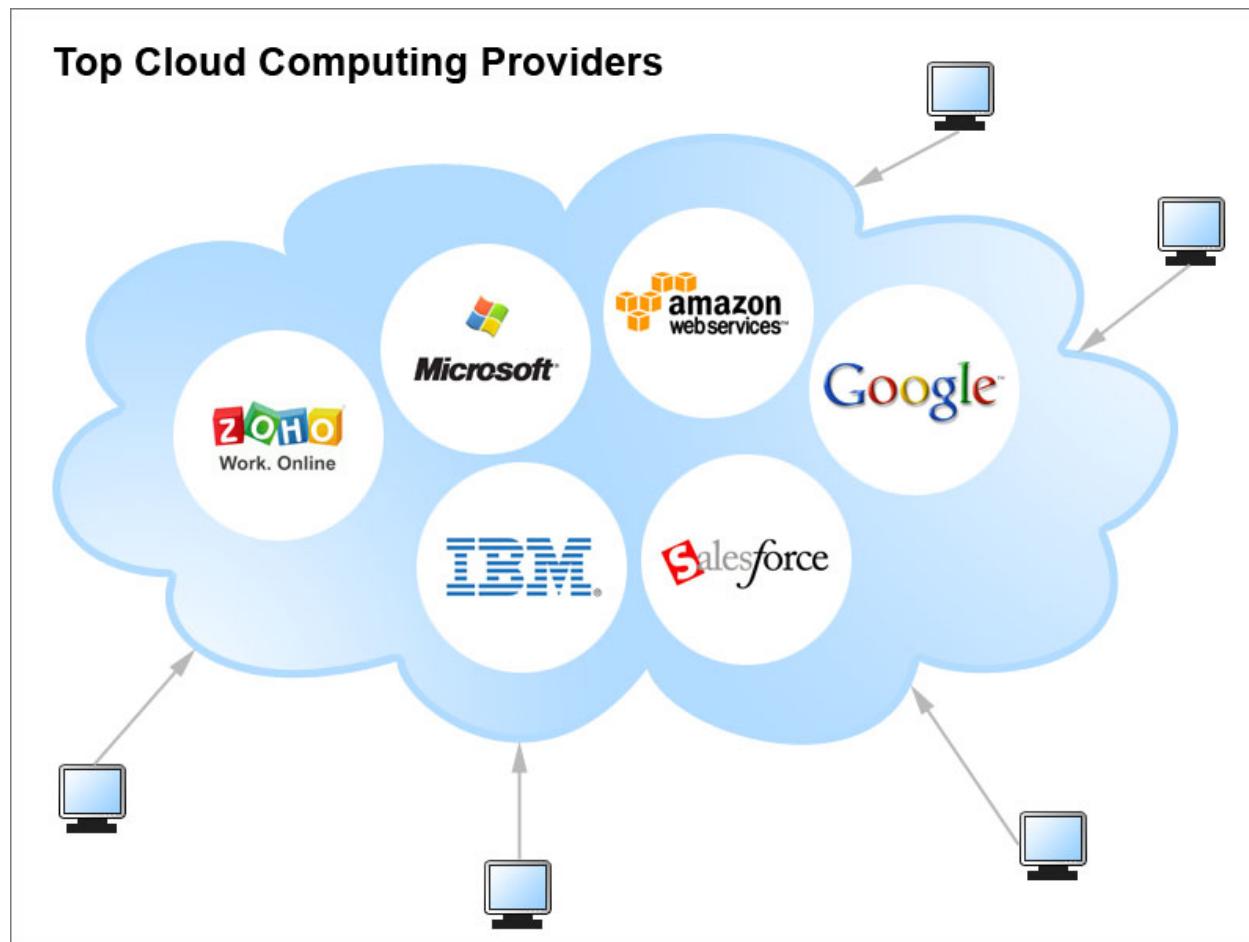
VS wetgeving & Snowden's onthullingen

Waarom alle data, van iedereen?

Pauze

Oplossingen: Recht, Technologie of Illusie?

HET KAN: CLOUD COMPUTING & OLIGARCHISCHE MARKTEN



VERKOOPTRUC AAN PUBLIEK: VAN TERRORISME NAAR 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

<http://clarke.dickinson.edu/wp-content/uploads/Dickinson-Constitution-Day-Talk-12-Sept-2013.pdf>

MAAR ONDERTUSSEN: POLITIEKE & ECONOMISCHE SPIONAGE



Edição do dia 02/09/2013
02/09/2013 20h33 - Atualizado em 03/09/2013 13h25

Veja os documentos ultrassecretos 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 ultrassecretos, 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.

GISTER! GREENWALD'S BOEK ECONOMISCHE SPIONAGE

Page 136

CONFIDENTIAL//X1

SERVING OUR CUSTOMERS

Major Finished Intelligence Producers:

- CIA
- DIA
- State/INR
- NGA
- National Intelligence Council

**Policymakers/
Law Enforcement:**

- White House
- Cabinet Officers
- Director Central Intelligence
- U.S. Ambassadors
- U.S. Trade Representative
- Congress
- Departments of:
 - Agriculture
 - Justice
 - Treasury
 - Commerce
- Energy
- State
- Homeland Security

Military/Tactical:

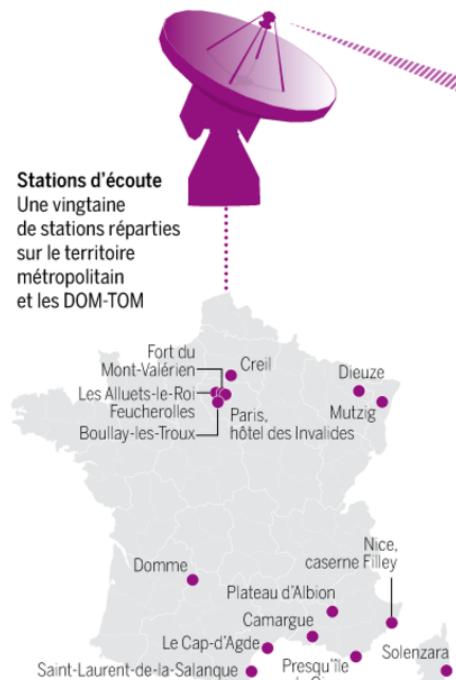
- JCS
- CINCs
- Task Forces
- Tactical Commands
- All Military Services
- Department of Defense
- Alliances
- UN Forces
- NATO

CONFIDENTIAL//X1

INLICHTINGENDIENSTEN EUROPA? DOEN 'T ZELFDE, OF HELPEN NSA

Comment la France intercepte les communications

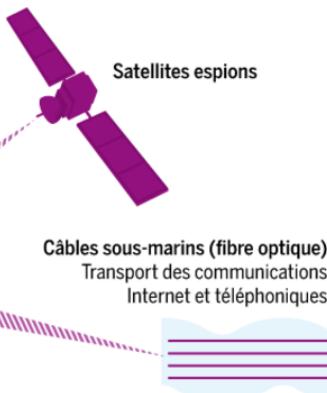
1 La captation



Communications téléphoniques, e-mails, SMS, fax... L'expéditeur et le receveur sont identifiés ; la durée, la fréquence et la localisation sont enregistrées.



Données électromagnétiques interceptées



2 Le stockage



3 L'accès aux données

- DGSE Direction générale de la sécurité extérieure
- DCRI Direction centrale du renseignement intérieur
- DNRED Direction nationale du renseignement et des enquêtes douanières
- DPSD Direction de la protection et de la sécurité de la défense
- DRM Direction du renseignement militaire
- Tracfin Traitement du renseignement et action contre les circuits financiers clandestins
- Service du renseignement de la Préfecture de police de Paris

La DGSE en chiffres

€ 600 millions d'euros de budget et
40 millions d'euros de fonds spéciaux

4 991 personnes
dont 28 % de militaires



687 embauches de 2009 à 2014,
essentiellement des ingénieurs

INFOGRAPHIE LE MONDE PHOTO AFP

NET UIT EL MUNDO: TIER A EN B LANDEN, SAMENWERKEN MET NSA

CONFIDENTIAL//NOFORN//20291123

TIER A Comprehensive Cooperation	Australia Canada New Zealand United Kingdom
TIER B Focused Cooperation	Austria Belgium Czech Republic Denmark Germany Greece

	... Iceland Italy Japan Luxembourg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey
--	--

DATADELEN INLICHTINGENDIENST: “QUID PRO QUO” (CTIVD ‘09)



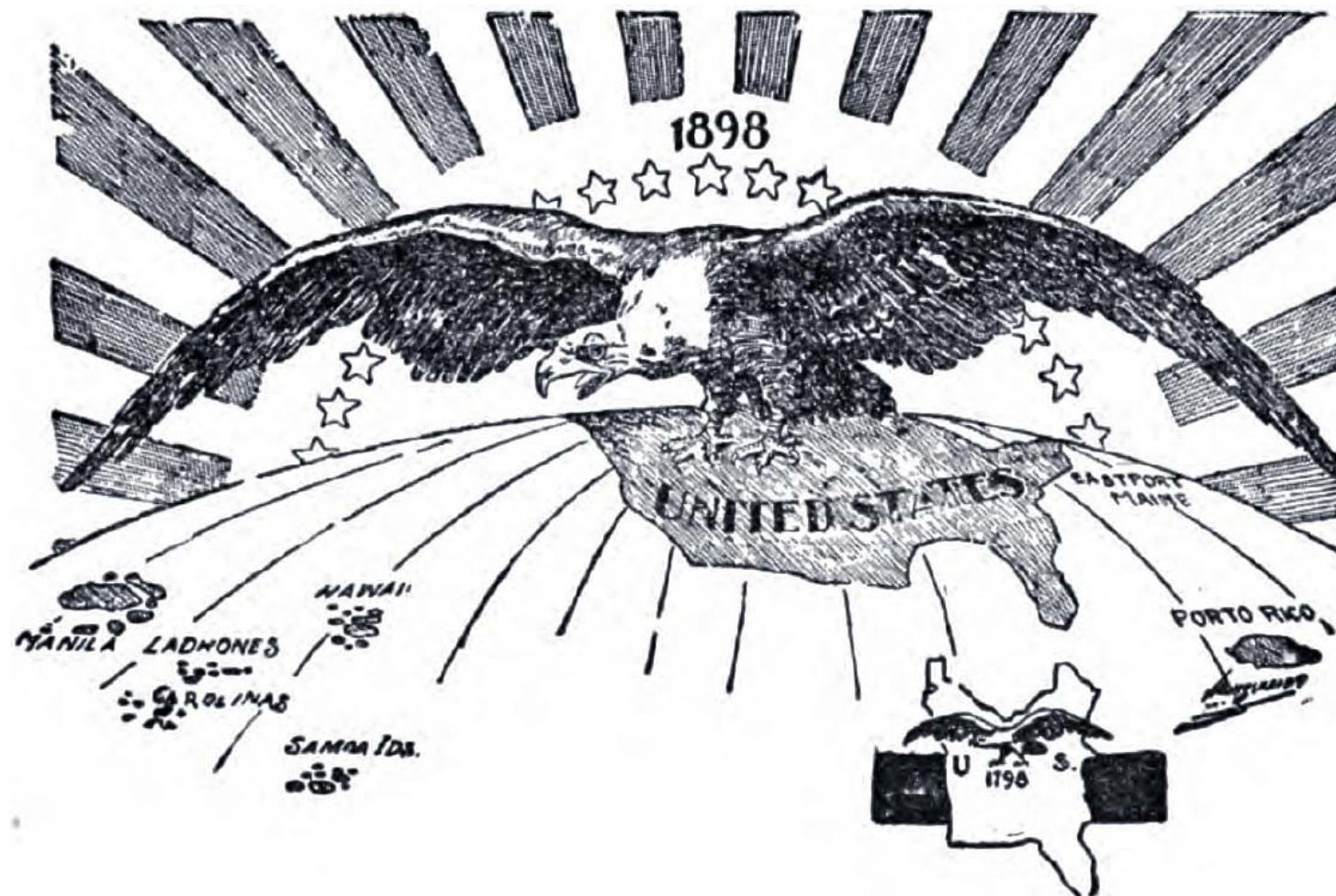
TRANSNATIONALE SURVEILLANCE NSA IN UK; GCHQ IN VS



SPELTHEORIE: 'RACE TO BOTTOM' TE VERGELIJKEN MET WIELRENNEN



ANDERE METAFOOR: 'INFORMATIE HEGEMONIE VAN KEIZERRIJK V.S.'



Ten thousand miles from tip to tip.—Philadelphia Press.

GORÉ VIDAL ('98): NA WWII, US NATIONAL SECURITY STATE



Veel betere lezing dan de mijne:
https://www.youtube.com/watch?v=oD_YSRZjLx0



TOP SECRET AMERICA

*THE RISE OF THE NEW AMERICAN
SECURITY STATE*

DANA PRIEST AND WILLIAM ARKIN

5M. SECURITY CLEARANCE, 2 STAF: ~15M OP 136M ARBEIDSBEVOLKING



Offficiële data zeggen niks over national security:
<http://www.bls.gov/news.release/empsit.t17.htm>

VEILIGHEIDSINDUSTRIE ... BANENPOLITIEK !??!!?!!?



POLITIEKE LEIDERS KOMEN, GAAN EN ZIEN INFO.SECURITY-STERRETJES

Donner ontraadt internet

Van onze parlementaire redactie

DEN HAAG, zaterdag

Minister Donner (Binnenlandse Zaken) heeft een opmerkelijk advies voor mensen die twijfelen aan de betrouwbaarheid van internet door de problemen met veiligheids-certificaten.

„Doe dat niet meer, werk net als ik met brieven en overschrijvingsbiljetten”, aldus de 62-jarige bewindsman.



“Werk net als ik met brieven en overschrijvingsbiljetten”



De Telegraaf, Frontpage, 5 Sept. 2011

SURVEILLANCE VEELKOPPIGE DRAAK INFOSEC, PRIVACY TEGEN MUUR



OUTLINE

VS wetgeving & Snowdens onthullingen

Waarom alle data, van iedereen?

Pauze

Oplossingen: Recht, Technologie of Illusie?

OUTLINE

VS wetgeving & Snowden's onthullingen

Waarom alle data, van iedereen?

Pauze

Oplossingen: Recht, Technologie of Illusie?

SCHIPPERS/EPD, PLASTERK/NSA: VERTROUWEN IN POLITIEK?

NOS.nl



"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

WEET JE NOG - STAS. TEEVEN? VERTROUWEN IN POLITIEK?

State Secretary Teeven reassured the parliament that upon bringing the issue up with their U.S. counterparts, the American authorities had assured him that when data are physically located in the EU, they always go through mutual legal assistance procedures to gather these data.

This is simply not true, not even in the law enforcement context (that U.S. authorities always go through MLATs), let alone a requirement for foreign intelligence gathering under FISA.

Bron: <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/03/16/antwoorden-kamervragen-over-dat-de-vs-mogelijkheden-heeft-om-in-clouddata-te-graaien.html> en 'Obscured by Clouds', p. 32-33

GEEN ACCOUNTABILITY IN BESTUUR BIJ SERIEUZE BEVEILIGINGSLEUGENS



DRUK OP VS VOOR WETSWIJZIGING PATRIOT ACT / FISA?

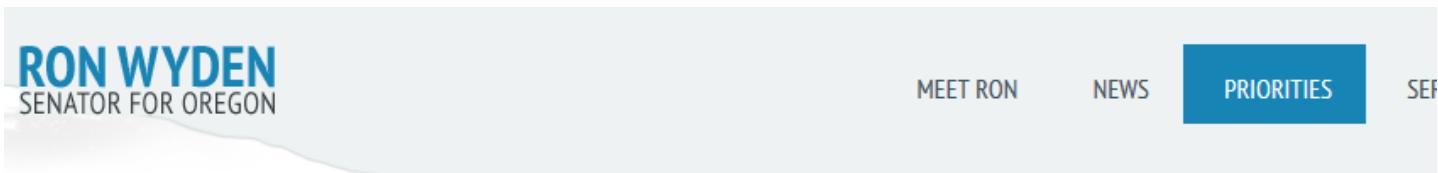


President George W. Bush, joined by members of his Cabinet and members of Congress, signs the FISA Amendments Act of 2008 Thursday, July 10, 2008, in the Rose Garden at the White House. White House photo by Eric Draper



WHITE HOUSE PHOTOS

RECHTSPOSITIE NIET-AMERIKANEN AFWEZIG IN POLITIEKE DEBAT



Home > Priorities

DOMESTIC SURVEILLANCE REFORM

Revelations of the National Security Agency's bulk collection of Americans' records and reliance on secret law and secret courts have made clear the need for reform of surveillance law immediately. [The Intelligence Oversight and Surveillance Reform Act](#) - introduced by U.S. Senators Ron Wyden (D-Ore.), Mark Udall (D-Colo.), Richard Blumenthal (D-Conn.), and Rand Paul (R-Ky) - will preserve constitutional liberties while maintaining the government's ability to protect national security. It will amend the Foreign Intelligence Surveillance Act to end dragnet domestic surveillance and other unjustified intrusions on Americans' constitutional rights, make improvements to the Foreign Intelligence Surveillance Court (FISC), and provide for greater transparency from government entities and the private sector.

[Summary](#) | [Bill Text](#) | [Press Release](#)

WATCH: Wyden, Mark Udall, Blumenthal, & Paul Unveil Bipartisan Surveillance Reform Bill



DHILMA ROUSSEFF: AANPASSEN INTERNET INFRASTRUCTUUR?

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

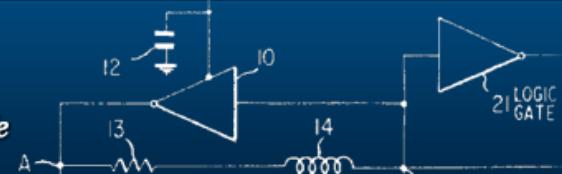


NSA HEEFT OVERAL TOEGANG, VS WET MAALT NIET OM GRENZEN

OCTOBER 1, 2013 POSTS COMMENT

FREEDOM TO TINKER

research and expert commentary on digital technologies in public life





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.

Freedom to Tinker is hosted by Princeton's Center for Information Technology Policy, a research center that studies digital technologies in public life. Here you'll find comment and analysis from the digital frontier, written by the Center's faculty, students, and friends.

CITP
CENTER FOR INFORMATION TECHNOLOGY POLICY

Search this website ...

What We Discuss

AACS Broadband CD Copy
Protection censorship CITP
Competition Computing in the Cloud
Copyright Cross-Border Issues

DHILMA ROUSSEFF: HERONTWERP 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



VS, RUS, CHI, EU, IRAN, ISR, SAUDI: SURVEILLANCE CONSENSUS?



STERKEREU BESCHERMING BIJ HERZIENING DATAPROTECTIE?



CONTEXT: STOF DEZE WEEK

- Handboek p. 135-149
- LIBE rapport NSA surveillance
- Statement Edward Snowden, EP

CONTEXT: STOF DEZE WEEK

- Hoofdstuk IV Richtlijn: doorgifte persoonsgegevens naar derde landen (art 25, 26)
- Art 25: Alleen doorgifte naar landen met 'passend beschermingsniveau'.
 - *EC kan beslissen: land 'passend'*
- Art 26: doorgifte naar land zonder passend beschermingsniveau, bijv.
 - *Toestemming (kan ingetrokken worden)*
 - *Binding Corporate Rules*
 - *Modelcontracten (26(4))*
 - *Zie Kuner 2013 & Moerel 2011 (literatuurlijst)*
 - *Uitzondering voor Verenigde Staten:*
 - *'Safe harbor': <http://export.gov/safeharbor/>*



EU COMPETENTIEPROBLEEM / PARLEMENT VS. LIDSTATEN

- Misschien politiek aantrekkelijk als doekje voor het bloeden, maar...
- EU recht geen ‘competentie’ nationale veiligheid, art. 3(4) TFEU
- ‘Dataprotectie’ beperkte oplossing
 - *Niet alle cloud data zijn ‘persoonsgegevens’*
 - *BCR & S. Harbor: toezicht op inlichtingendiensten door CBP?*
 - *Maar gisteren: ECJ Google v. Spain*
 - Google valt integraal onder EU Dataprotectierecht
 - *Catch 22 voor bedrijfsleven*
 - Onmogelijk voldoen aan zowel VS als EU regulering

ROUSSEFF & MERKEL BIJ DE VN: INTERNATIONAAL RECHT?

theguardian

[News](#) | [US](#) | [World](#) | [Sports](#) | [Comment](#) | [Culture](#) | [Business](#) | [Money](#) | [Environment](#) | [Science](#)

[News](#) > [World news](#) > [United Nations](#)

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

 [Follow Julian Borger by email](#) BETA

Julian Borger New York
The Guardian, Tuesday 24 September 2013 12.27 EDT

 [Jump to comments \(755\)](#)



[Article history](#)

World news

[United Nations](#) · [NSA](#) ·
[Brazil](#) · [Dilma Rousseff](#) ·
[Barack Obama](#) ·
[Surveillance](#) · [United States](#) · [US foreign policy](#)
· [Privacy](#) · [US national security](#)

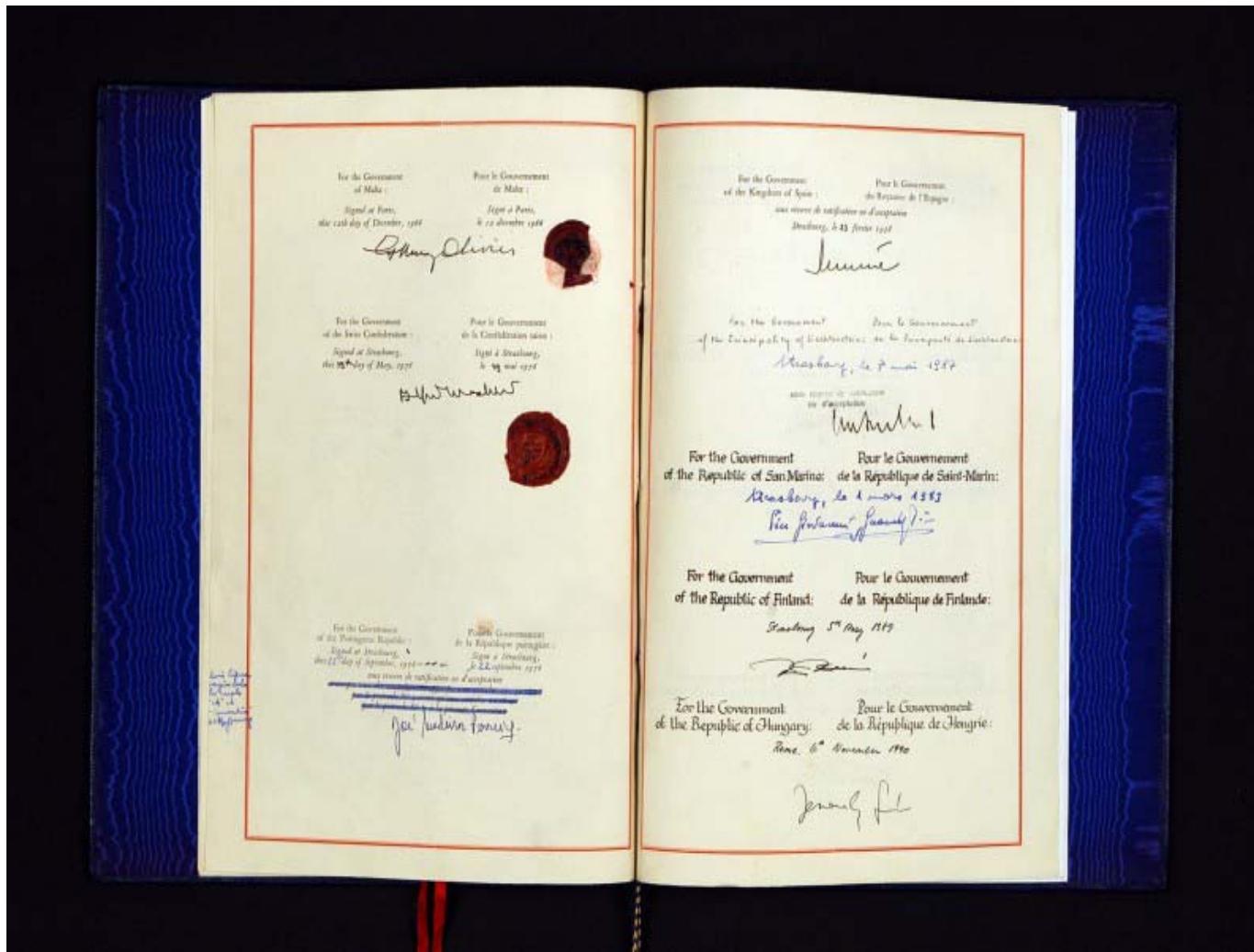
Technology



INTERNATIONAAL RECHT: GEWOONTERECHT SIGINT?

- Transnationale surveillance vanuit je eigen land
 - Vroeger: Sigint, satellietcommunicatie
- Schending soevereiniteitsbeginsel?
 - *Geen 'handhavingsjurisdictie'*
 - *Nauwelijks jurisprudentie*
- Iedereen doet het: niemand brengt de zaak op
 - Brazilië politiek goed gepositioneerd?
 - Gaat nooit steun krijgen?
- Bovendien: de VN grondrechten zijn er al sinds 1948, worden alleen stelselmatig genegeerd

HOE ZIT HET MET EUROPEES VERDRAG RECHTEN VAN DE MENS?



LIBERTY, PRIVACY INTERNATIONAL BEGINNEN ZAAK TEGEN UK

LIBERTY PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

» JOIN
» TAKE ACTION
» GET ADVICE

Home	Campaigns	About Liberty	About Human Rights	Support Us	Policy and Lobbying	Media Centre
----------------------	---------------------------	-------------------------------	------------------------------------	----------------------------	-------------------------------------	------------------------------

You are here » [Homepage](#) » [Media centre](#) » [Liberty issues claim against British Intelligence Services...](#)



25 June 2013

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.

Join our email list for regular campaign updates

 [JOIN](#)

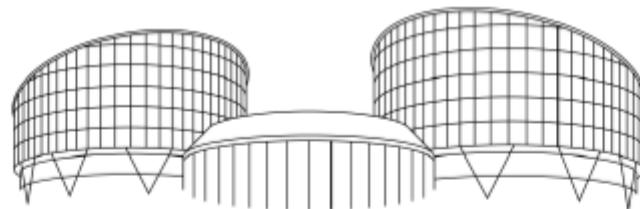
.....

JOIN US ON :



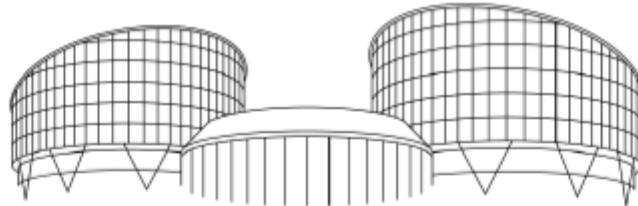
KLASS: ‘NOT ACTUAL HARM, MERE EXISTENCE OF LAW SUFFICES’

- Vgl. Clapper v. Amnesty’s Orwellian Twist!



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

NIET ALLEEN PERSOONSGEGEVENS, MAAR 'ALL DATA ON SERVER'



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)

'UNTARGETED MONITORING': CRITERIA 'OPEN TO THE PUBLIC'



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)

TOTALE SURVEILLANCE AFGEREMD OP PROCEDURELE GRONDEN

- Bekeek alleen 1 v 3 toetsen: 'Accordance with Law'
 - §64-§66 in 2002, leest als Snowden's onthullingen!
 - *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"*
 - *"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."*

'INDISCRIMINATE COLLECTION' ONVERDACHTE BURGERS ONWETTIG



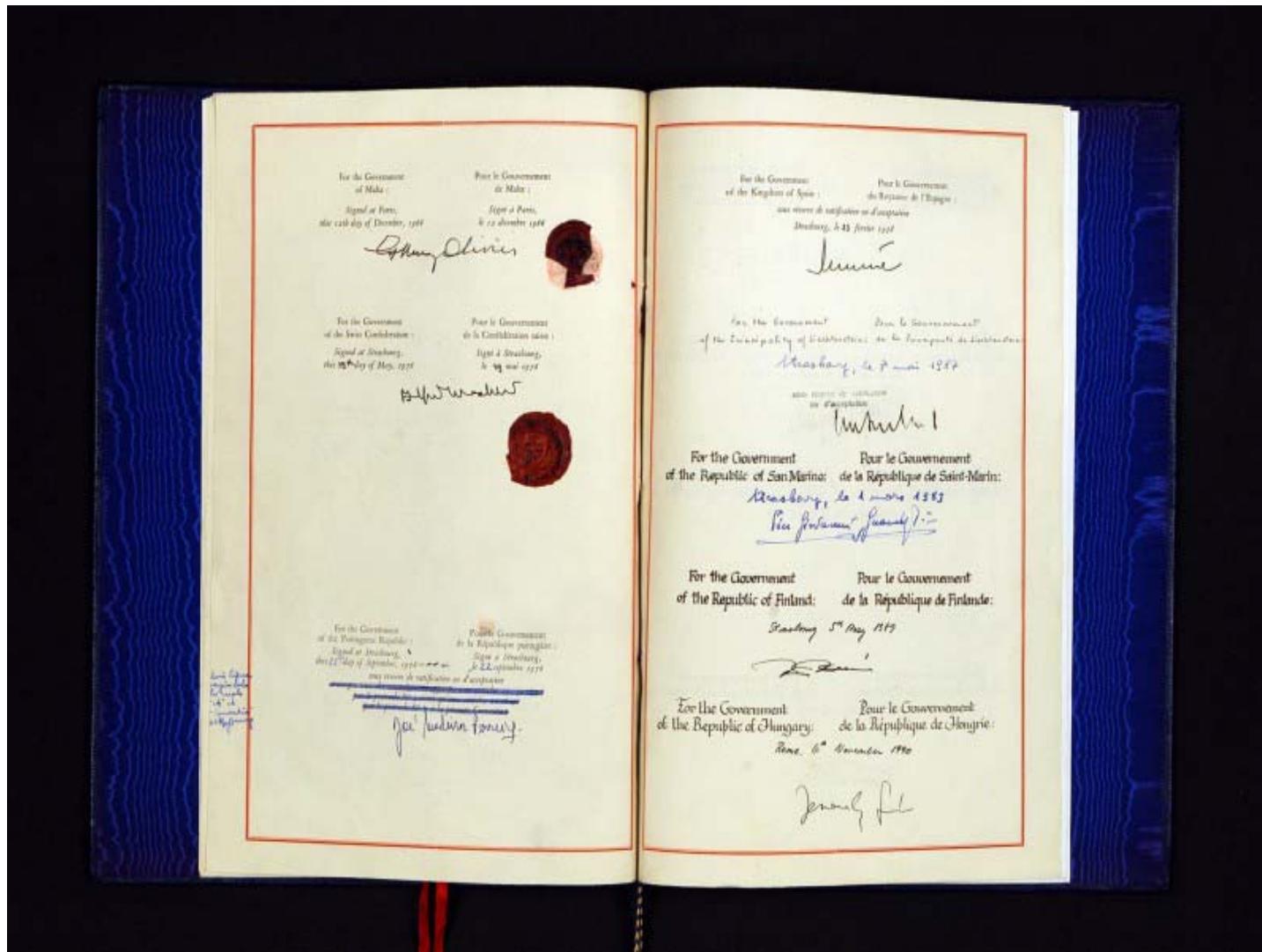
COUR EUROPÉENNE DES DROITS DE L'HOMME
EUROPEAN COURT OF HUMAN RIGHTS

GRAND CHAMBER

CASE OF S. AND MARPER v. THE UNITED KINGDOM

(Applications nos. 30562/04 and 30566/04)

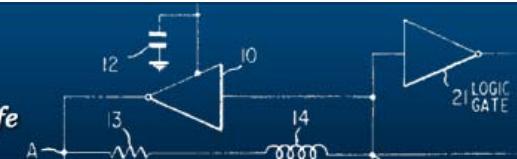
DUURT NOG JAREN VOORDAT WE HET ZULLEN WETEN



OF...? EHRC VERSNELT ZAAK BIG BROTHER WATCH VS UK

FREEDOM TO TINKER

research and expert commentary on digital technologies in public life





ECHR Fast-tracks Court Case on PRISM and TEMPORA (and VERYANGRYBIRDS?)

JANUARY 29, 2014 BY AXEL ARNBAK

So. The NSA and GCHQ piggyback on Angry Birds to spy on its 1.7 billion users, potential terrorists. Not only that, but everything on smartphones can be compromised: "if its on the phone, we can get it". Will it ever stop? A few days ago, the European Court of Human Rights ('ECHR') made the unique move to fast-track a case on the legality of mass surveillance practices by the GCHQ. A judgement is now expected in months, rather than years – in time to have a huge impact on the global debate on mass surveillance. Time for some analysis.

In September 2013 'Privacy not PRISM', a group of NGOs and activists, challenged the UK government's surveillance directly with the ECHR. Last week, the ECHR wrote to the group [[pdf](#)] that it gives the case priority – which it hardly ever does. Then again, the practices attack the core of the right to privacy. 2 May 2014 is the deadline for the UK government to provide information to the ECHR on three essential questions. The letter also reveals some interesting details on how the ECHR will approach the third, critical question.

Firstly, "can the applicants claim that their privacy rights have been violated?" This seems a no-brainer. As I [blogged](#) before, in contrast with the U.S. Supreme Court's stance on 'actual harm' in *Clapper v. Amnesty*, the ECHR accepts the 'mere existence' of vague surveillance law and practices as a sufficient basis for applicants.

Secondly, have the 'domestic means been exhausted'? The UK government told the group to file their case with the "Investigatory Powers Tribunal" of the executive branch. Not so smart: in 2010, *Kennedy v. The UK*, the ECHR ruled that this UK Tribunal does not provide an effective judicial remedy for privacy victims. While the UK government will try everything in its power to let the case proceed on a national level, it would be surprising if the ECHR allows that to happen.

The third question is the most relevant. Actually, three sub-questions need to be separated. Are PRISM and TEMPORA i) 'in accordance with the law'; ii) 'necessary in a democratic society' and, what the ECHR did not ask the UK government, iii) what about all those other revelations?

Freedom to Tinker is hosted by Princeton's Center for Information Technology Policy, a research center that studies digital technologies in public life. Here you'll find comment and analysis from the digital frontier, written by the Center's faculty, students, and friends.

 **CITP**
CENTER FOR
INFORMATION TECHNOLOGY POLICY

What We Discuss

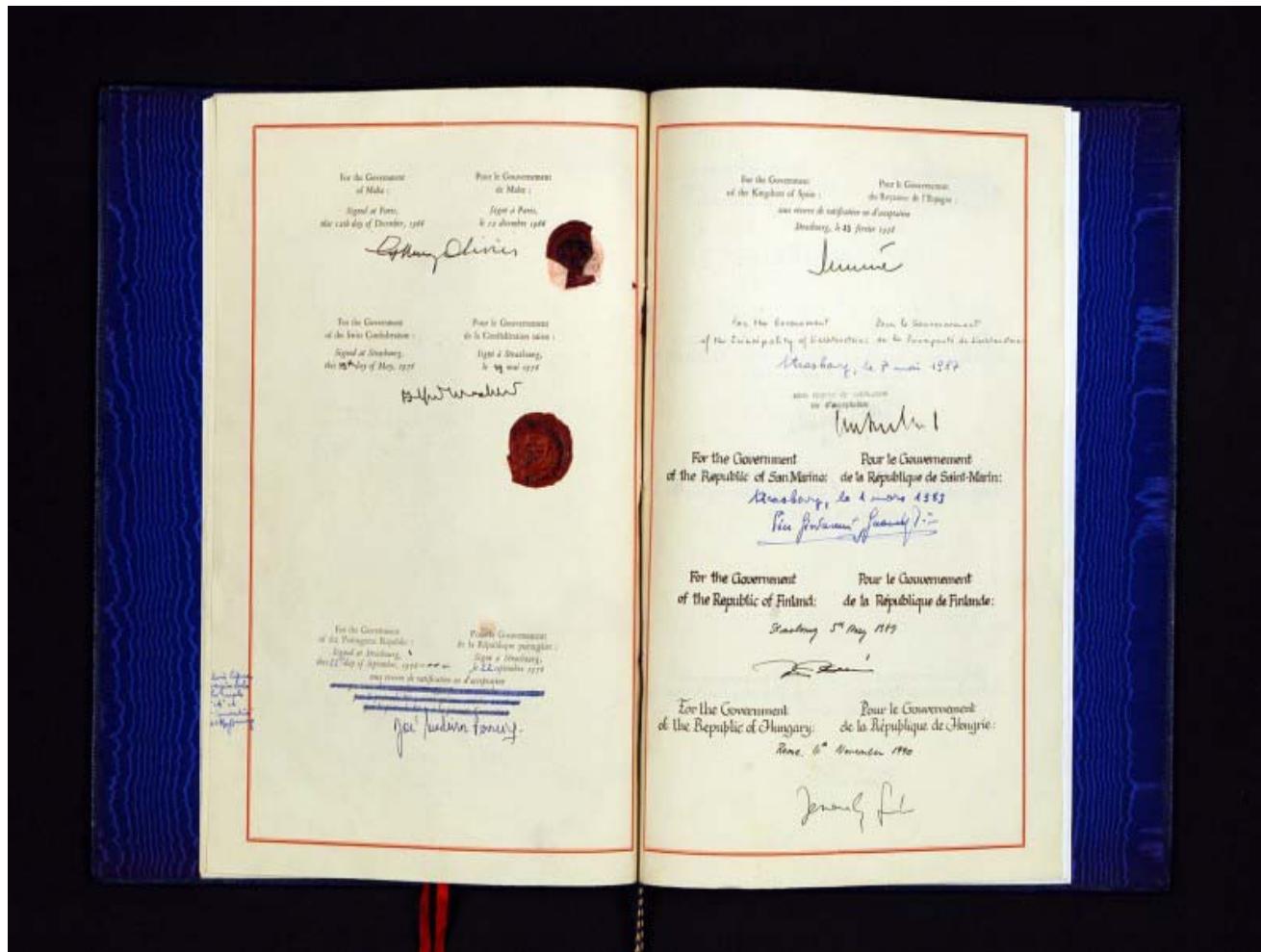
AACS bitcoin Broadband CD Copy
Protection censorship CITP
Competition Computing in the Cloud
Copyright Cross-Border Issues
DMCA DRM Education Events
Facebook FCC Government Government transparency Grokster Case Humor Innovation Policy Law

86

EN TOCH... TRANSCONTINENTAAL: NSA IN UK; GCHQ IN VS



KUNNEN EVRM PARTIJEN BURGERS BESCHERMEMEN TEGEN VS? ONZEKER



EN E.U. HVJ, APR. 2014: RICHTLIJN BEWAARPLICHT VERNIETIGD

JUDGMENT OF THE COURT (Grand Chamber)

8 April 2014 ([*](#))

(Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in the course of providing those services — Article 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)

In Joined Cases C-293/12 and C-594/12,

REQUESTS for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, in the proceedings

Digital Rights Ireland Ltd (C-293/12)

v

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Siochána,

Ireland,

The Attorney General,

intervener:

Irish Human Rights Commission,

and

Kärntner Landesregierung (C-594/12),

Michael Seitlinger,

Christof Tschohl and others,

HvJ OVER BEWAARPLICHT, OVER BULK METADATA SURVEILLANCE

- **49:** bewaarplicht kan ‘appropriate’ zijn
- **50:** gebrekke effectiviteit geen tegenargument
- **51/52:** dataprotectie essentieel privacy, inbreuk ‘strikt noodzakelijk’, waarborgen crucial
 - *Take away: gaat dus vooral om dataprotectie !!!*
- Richtlijn geen waarborgen – strijd art. 7/8 Charter
 - *59: geen relatie verdenking <-> data subject, locatie, tijd*
 - *60/61: geen beperking soort misdrijf, toegangscriteria*
 - *62: geen rechterlijke toetsing*
 - *63/64: geen relatie bewaartijd, ernst misdrijf*

HvJ OVER BEWAARPLICHT, BAANBREKEND RE: DATA SECURITY

- Geen waarborg re: misbruik/onwettige toegang
- §66: Criteria when security measures need to go beyond general delegation to private sector:
 - *Quantity Data*
 - *Sensitivity Data*
 - *Risk of Abuse*
- §67: DRD wrongly permits economic considerations for data security
- §67: DRD has no explicit data destruction rules
- §68: DRD does not prohibit storing data outside E.U., insufficient control over retained data

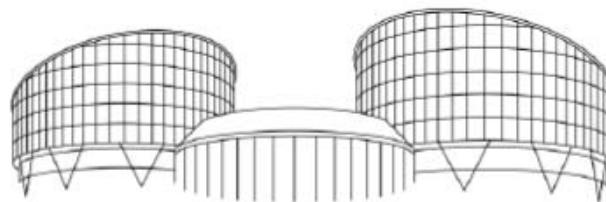
STERKERE REGULERING TOEZICHT EN TRANSPARANTIE SURVEILLANCE?



INSTITUTIES GEFAALD, LEKKEN ENIGE ROBUUSTE TOEZICHTSMODEL?



EVRM VRIJ STEVIGE BESCHERMING: “DUTY CIVIL SERVANTS”



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

THIRD SECTION

CASE OF TELEGRAAF MEDIA NEDERLAND LANDELIJKE
MEDIA B.V. AND OTHERS v. THE NETHERLANDS

(Application no. 39315/06)

ENCRYPTIE? TEGEN SLEEPNET WEL, TEGEN GERICHTE AANVAL NIET

Where Do All The Attacks Go?

Dinei Florêncio and Cormac Herley
Microsoft Research
One Microsoft Way
Redmond, WA, USA

“Many attacks cannot be made profitable, even when many profitable targets exist.”

5 AANBEVELINGEN BRUCE SCHNEIER

- DIE DOCUMENTEN HEEFT GEZIEN

- 1. Hide in the network** – gebruik TOR
- 2. Air Gap** – PC nooit verbonden met internet
- 3. Gebruik open source** – Linux, Free Software
- 4. Gebruik open encryptie** – TLS, Ipsec
- 5. Publieke compatibiliteit** – wederkerige controle

NB. Er bestaat geen magic bullet

Maatregelen maakt het veel moeilijker, maar niet onmogelijk voor overheden en cybercriminelen

SECURITY ECONOMICS REGULERING: BEVEILIGINGSPRIKKELS AFDWINGEN

Security Economics in the HTTPS Value Chain

Hadi Asghari*, Michel J.G. van Eeten*, Axel M. Arnbak[†] & Nico A.N.M. van Eijk⁺¹

* h.asghari@tudelft.nl, m.j.g.vaneeten@tudelft.nl
Delft University of Technology, Faculty of Technology Policy and Management

[†] a.m.arnbak@uva.nl, vaneijk@uva.nl
University van Amsterdam, Faculty of Law, Institute for Information Law

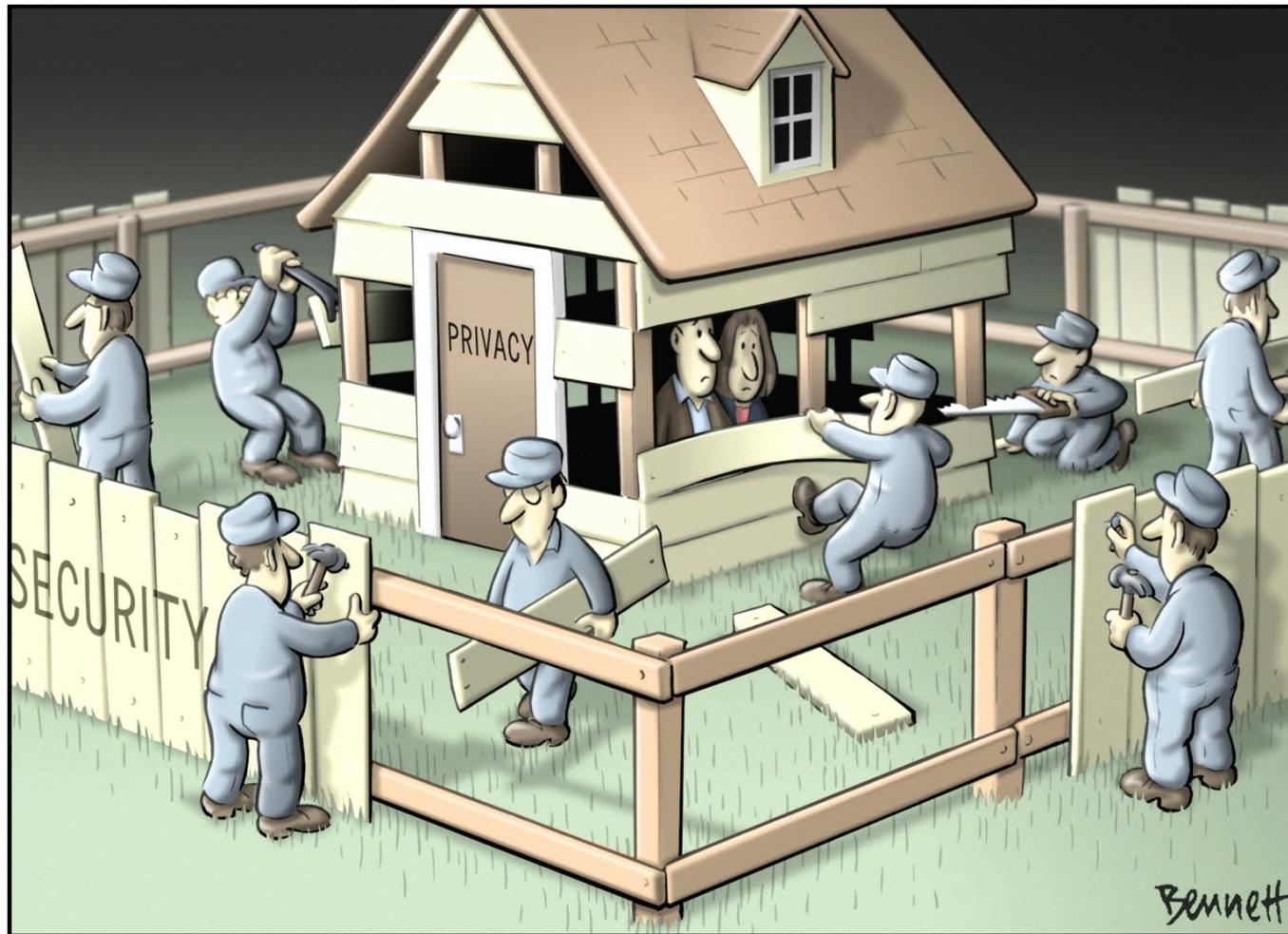
Abstract. Even though we increasingly rely on HTTPS to secure Internet communications, several landmark incidents in recent years have illustrated that its security is deeply flawed. We present an extensive multi-disciplinary analysis that examines how the systemic vulnerabilities of the HTTPS authentication model could be addressed. We conceptualize the security issues from the perspective of the HTTPS value chain. We then discuss the breaches at several Certificate Authorities (CAs). Next, we explore the security incentives of CAs via the empirical analysis of the market for SSL certificates, based on the SSL Observatory dataset. This uncovers a surprising pattern: there is no race to the bottom. Rather, we find a highly concentrated market with very large price differences among suppliers and limited price competition. We explain this pattern and explore what it tells us about the security incentives of CAs, including how market leaders seem to benefit from the status quo. In light of these findings, we look at regulatory and technical proposals to address the systemic vulnerabilities in the HTTPS value chain, in particular the EU eSignatures proposal that seeks to strictly regulate HTTPS communications.

Keywords: HTTPS, Cybersecurity, Internet Governance, Constitutional Values, E-Commerce, Value Chain Analysis, Security Economics, eSignatures Regulation, SSL, TLS, Digital Certificates, Certificate Authorities.

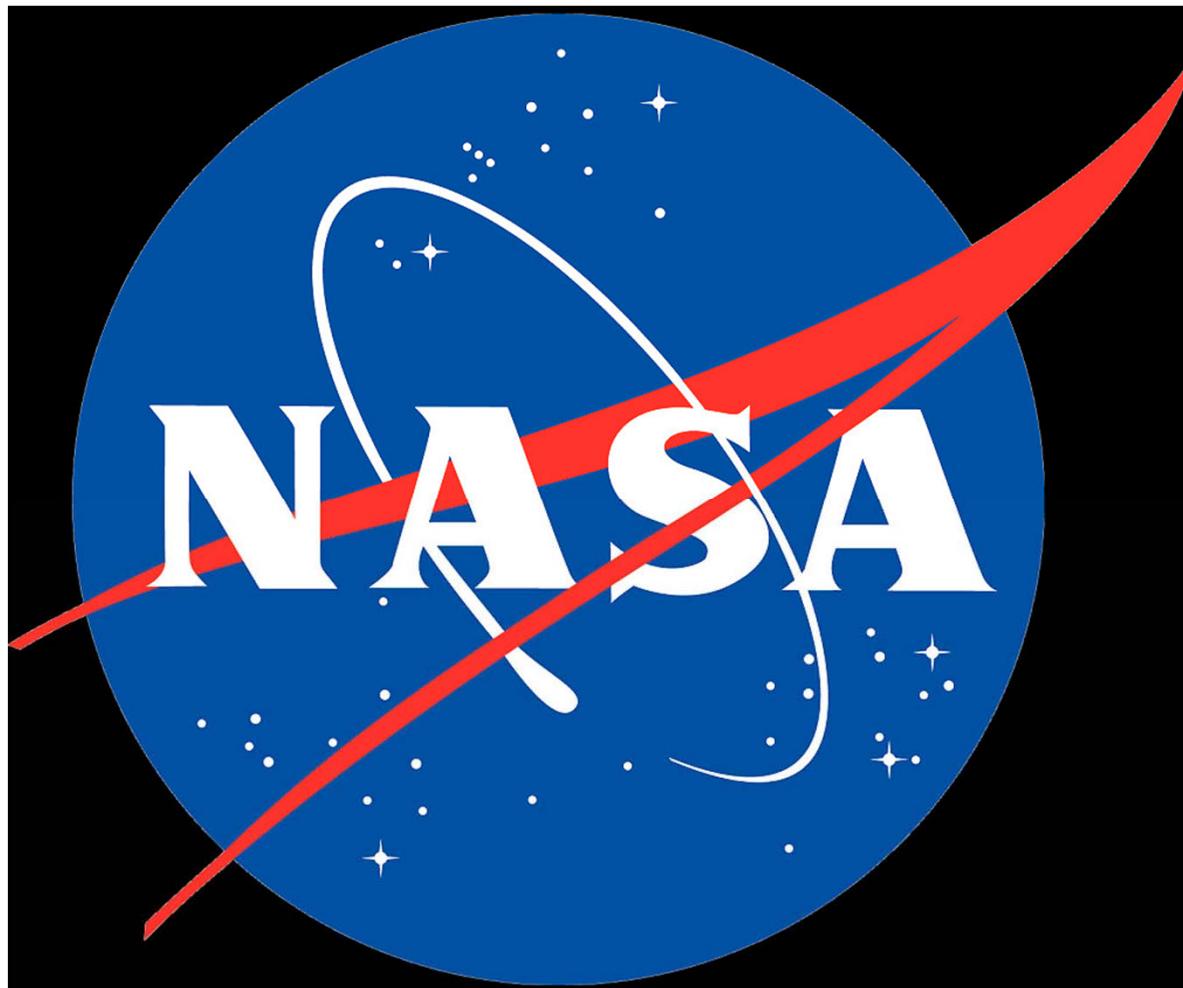
REGULEREN SURVEILLANCETECH & CYBERWAPENS ESSENTIEEL



HOOGSTE TIJD VOOR HERIJKING 'SECURITY'; PRIVACY ESSENTIEEL



BANENPOLITIEK? DOE MAAR GOEDS: PUT THE A BACK IN NSA!



VRAGEN?

Twitter @axelarnbak

Cybersecurity & Information Law Researcher

Ph.D. Cand. Institute for Information Law, University of Amsterdam

2013/14 Fellow CITP @ Princeton, Berkman Center @ Harvard

<https://www.axelarnbak.nl/>