Securing Private Communications

LEKENPRAATJE

Protecting Private Communications Security in E.U. Law: Fundamental Rights, Functional Value Chains and Market Incentives

25 November 2015, “Lekenpraatje” Ph.D. Thesis Defense, Aula @ University of Amsterdam

Securing Private Communications

Protecting Private Communications Security in EU Law: Fundamental Rights, Functional Value Chains and Market Incentives

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. D.C. van den Boom
ten overstaan van een door het college voor promoties
ingestelde commissie, in het openbaar te verdedigen in de Aula der Universiteit
op woensdag 25 november 2015, te 11:00 uur
door

Axel Martin Arnbak

geboren te 's-Gravenhage


zeker weten met wie u via
internet afspraken maakt
DigiNotar
sche handtekenin

Dutch government: stop using the internet

Donner ontraadt internet

Van onze parlementaire redactie

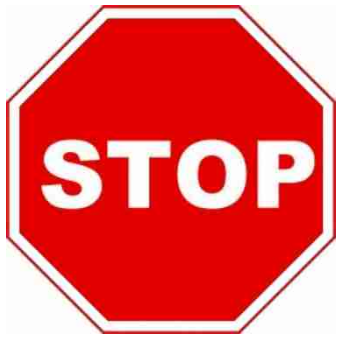
DEN HAAG, zaterdag

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

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

De Telegraaf, Frontpage, 5 Sept. 2011

"work with letters and bank cheques, just like me!"



"We Must Do Something.
This Is Something.
Therefore, We Must Do It"

cloud computing

&

“Patriot Act”

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

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

AP FILE

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

Reaction Dutch government: “NSA will respect Dutch patient privacy!”

Reaction Amazon: “Fearmongers!”

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

Johan Leupen
Amsterdam

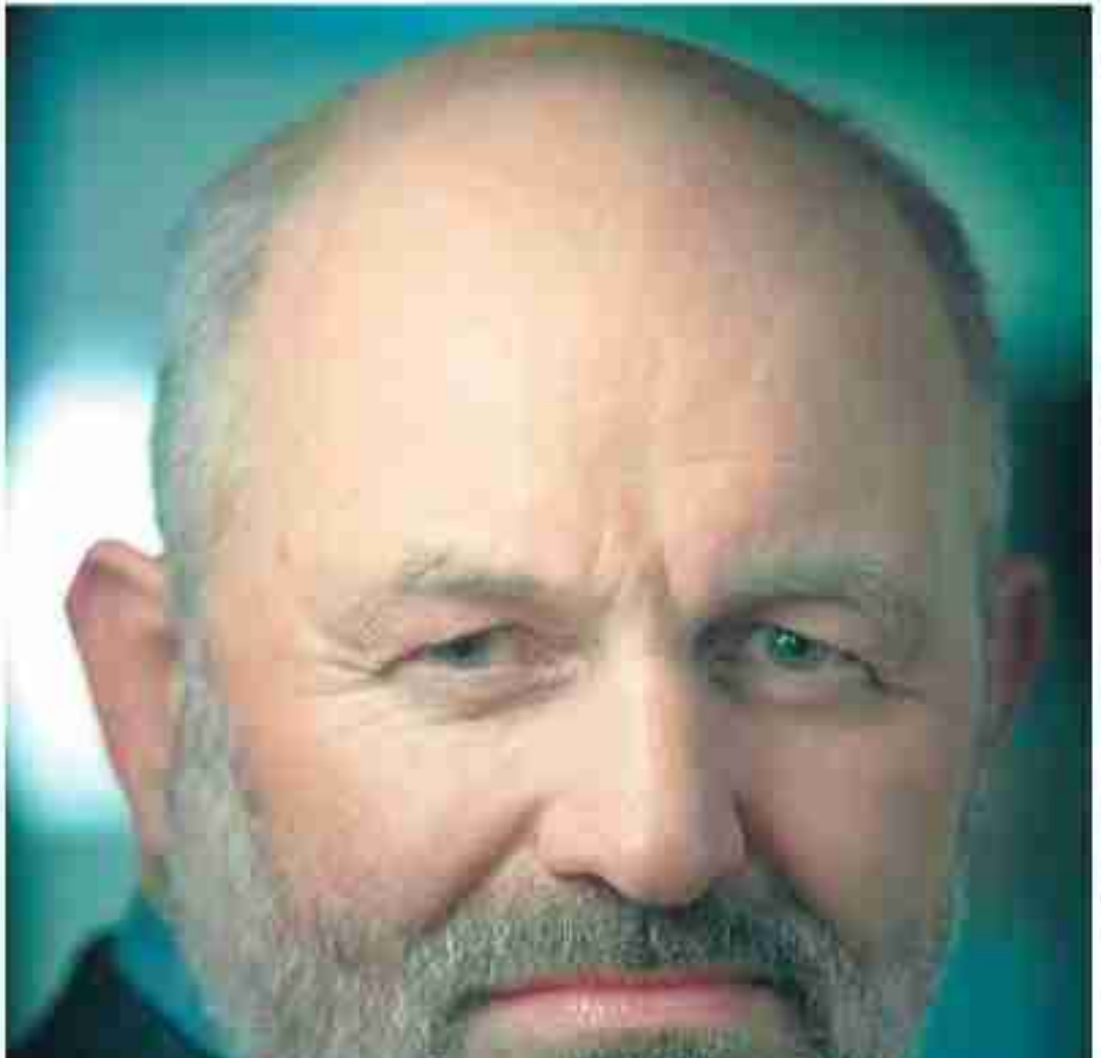
De privacydiscussie over de ‘cloud’ is opnieuw hooggeplaatst. Amerikaanse opsporingsdiensten kunnen gevoelige data van Nederlandse bedrijven of overheden inzien zonder hun medeweten, waarschuwt het Instituut voor Informatierecht (IViR). De anti-terreurwet Patriot Act geeft de Verenigde Staten zelfs toegang tot servers op Nederlands grondgebied, stipt het UvA-orgaan aan in zijn onderzoek.

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

Amazon-bestuurslid Werner Vogels, uitgerekend wel het voornaamste voorbeeld van de cloud-revolutie, verdraagt de commotie over zijn geesteskind slecht. De argumenten zijn vermoeibeld door propaganda van bedrijven die hun broodwinning zien verdwijnen, zegt hij. Daarmee dreigt het revolutionaire karakter van de cloud onderuit te sneeuwen.

V Schrikken uw klanten van de Patriot Act?

‘Die staat los van de cloud. De Patriot Act is gewoon een wet die gelkt voor iedereen. Het klopt dat de opsporingsdiensten toegang kunnen krijgen, maar die is niet laagdrempelig



V 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 bladla. Alle voordelen zijn dan weg. Je moet klanten juist ontlasten: van hun zorgen over datacenters, van onderhoudscontracten. Bij private loop 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-die nuveterner de baas, en kwam je onmogelijk van hem af. Wij pikken hun werk in.’

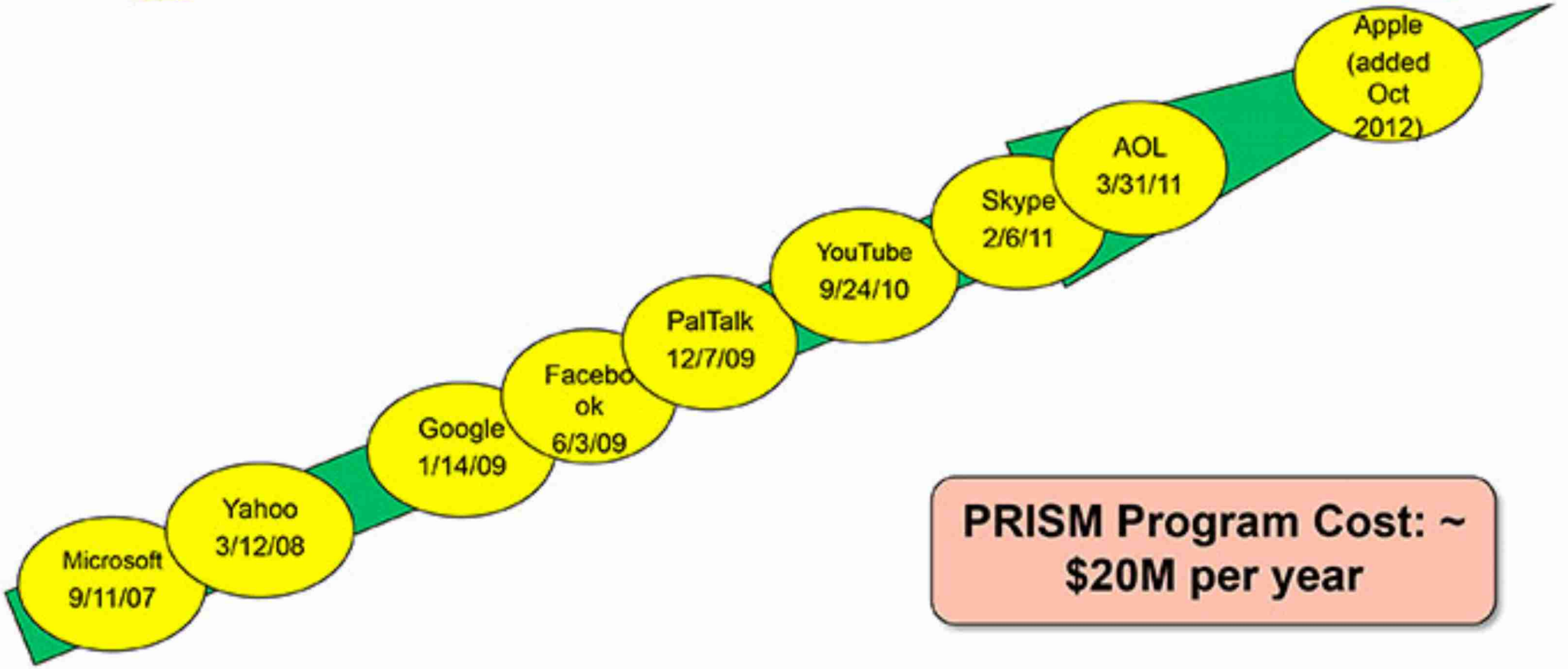
V De Duitse softwarereus SAP gebruikt zijn origine als verkoopargument: ‘Bij ons kijkt de Amerikaanse overheid niet mee’.

‘SAP is juist een heel grote klant en een belangrijke partner. Ze hebben zelf trainingsfaciliteiten, sales, en andere zaken bij ons belegd 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. Daarzit genoeg verstand.’

V De IT-volwassenheid laat bij overheden nogal eens te wensen over. Zie het debacle met Digitaal in Nederland.

‘Dat klopt. Mensen bouwen nu eenmaal slechte IT-architectuur, met alle risico’s van dien. Dat zou niet moeten kunnen. We zitten

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year

General Research Question
Thesis:

How should the EU lawmaker protect private communications security?

OUTLINE

Communications security

Why communications security fails

Systemic flaws in E.U. communications law

Recommendations

OUTLINE

Communications security

Why communications security fails

Systemic flaws in E.U. communications law

Recommendations

Communications Security ...

Protects:

Confidentiality

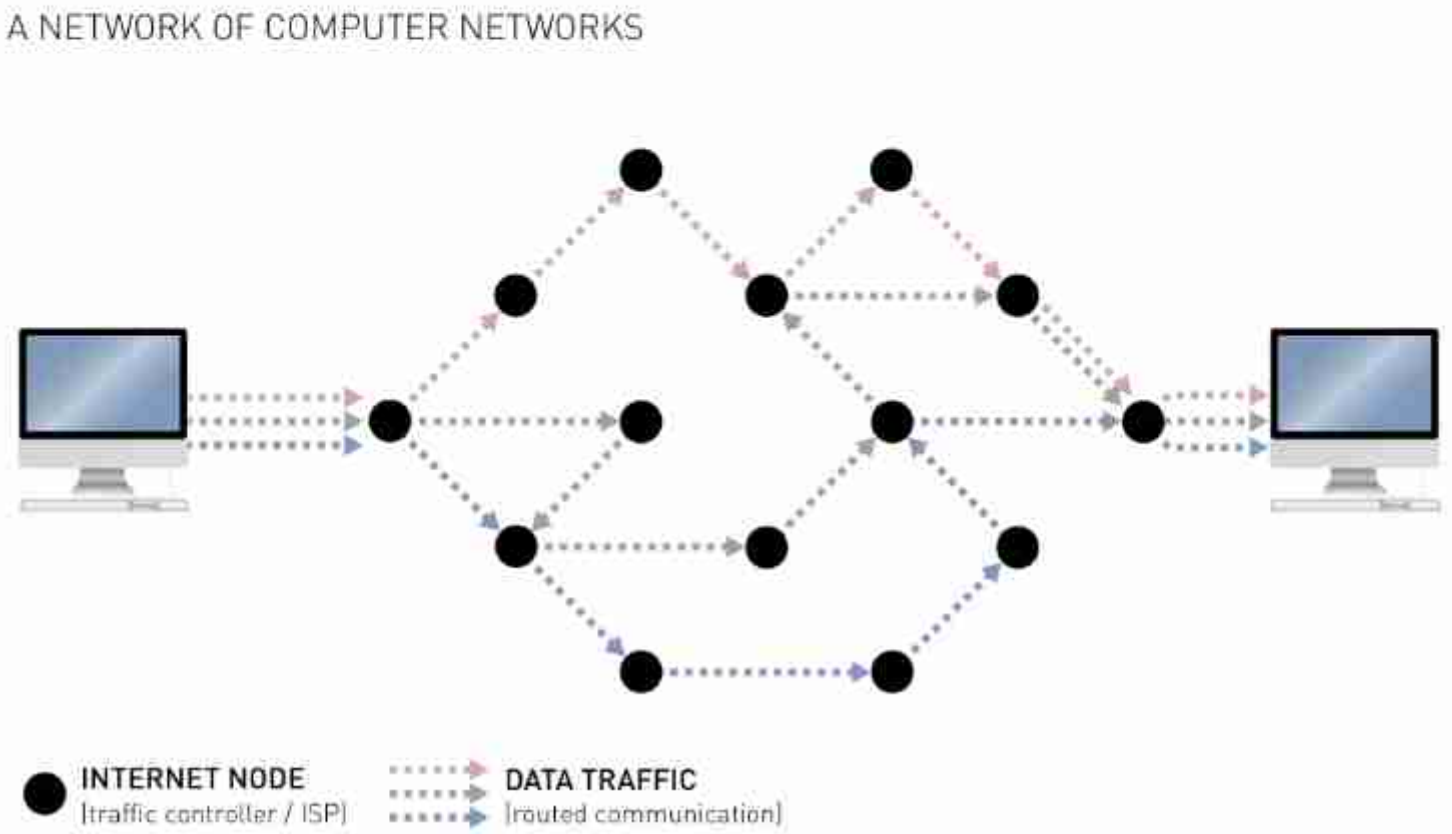
Integrity

Availability

of information transmitted through networks/systems

… has been around for a while

THE INTERNET



Based on 'IP‘: Internet Protocol (~1974)

1989: HTTP

p2p: files

SMTP: mail

IP = Foundation 'network' society

domestication: digital technology is our BFF

IP great for availability, but:

communications

... confidentiality?

... integrity?

OUTLINE

Communications security

Why communications security fails

Systemic flaws in E.U. communications law

Recommendations

Failure classes:

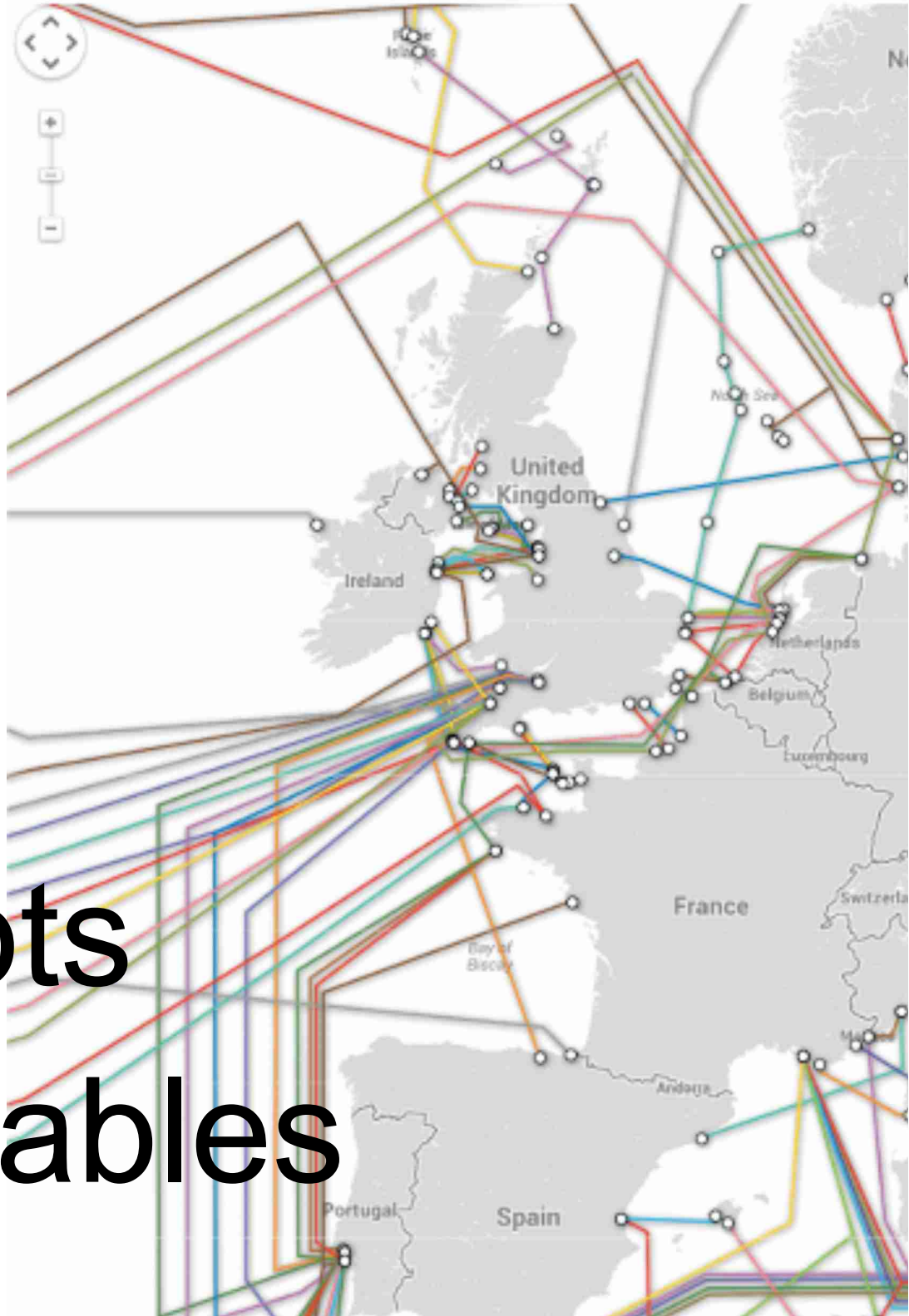
Technology
Users
Markets
Surveillance

Failure classes:

Technology
Users
Markets
Surveillance

Snowden Disclosure: TEMPORA

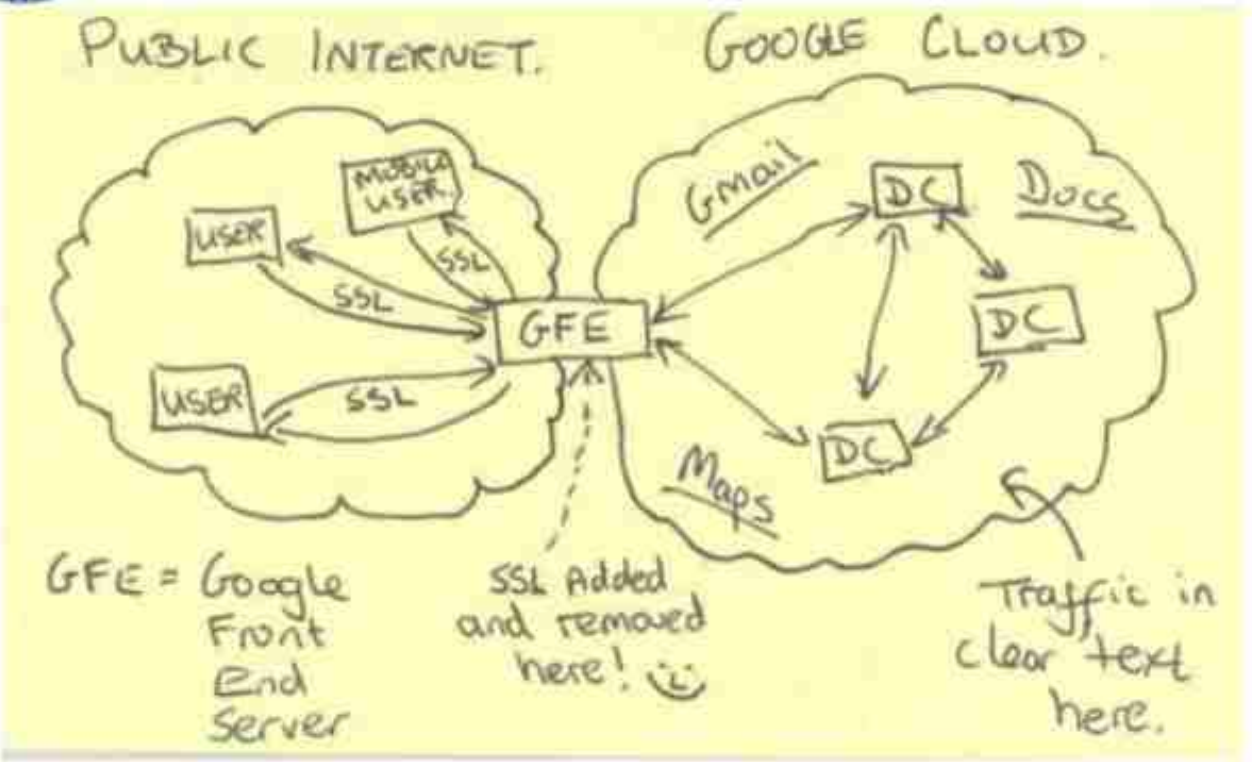
Bulk intercepts
Submarine cables



HTTPS: Snowden disclosure MUSCULAR

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

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.

CBSNEWS Video US World Politics Entertainment Health MoneyWat

By ZACK WHITTAKER / CBS NEWS / June 30, 2014, 4:02 PM

Legal loopholes could allow wider NSA surveillance, researchers say

CBS News

Shares / Tweets / Stumble / Email

NEW YORK -- Secret loopholes exist that could allow the National Security Agency to bypass Fourth Amendment protections to conduct massive domestic surveillance on U.S. citizens, according to leading academics.

The research paper released Monday by researchers at Harvard and Boston University details how the U.S. government could "conduct largely unrestrained surveillance on Americans by collecting their network traffic abroad," despite constitutional protections against warrantless searches.

One of the paper's authors, Axel Arnbak of Harvard University's Berkman Center for Internet & Society, told CBS News that U.S. surveillance laws presume Internet traffic is non-American when it is collected from overseas.

article:
"Loopholes
to Circumvent
the Constitution"

in both law
and technology

File Says N.S.A. Found Way to Replace Email Program

By CHARLIE SAVAGE NOV. 19, 2015

The National Security Agency headquarters at Fort Meade, Maryland in 2010.
Saul Loeb/Agence France-Presse — Getty Images

Email

Save

WASHINGTON — When the National Security Agency's bulk collection of records about Americans' emails came to light in 2013, the government conceded the program's existence but said it had shut down the effort in December 2011 for "operational and resource reasons."

Last Week!

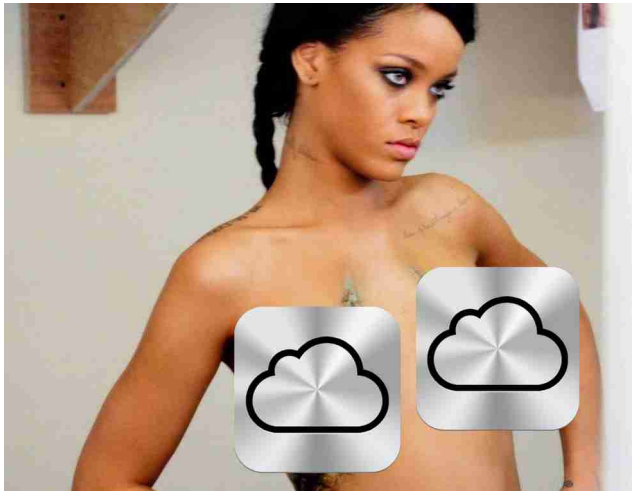
If you secure one part of communications network,

Breaches move to the next part of the network.

Ergo:
Law should secure the entire communications value chain

Failure classes:

Technology
Users
Markets
Surveillance



• 1 september 2014, 12:38

Privéfoto's beroemdheden online na hack

Jennifer Lawrence. Foto EPA/Claudio Onorati

iCloud Fail!

Lesson 1:
protect against "brute force" password guessing hack

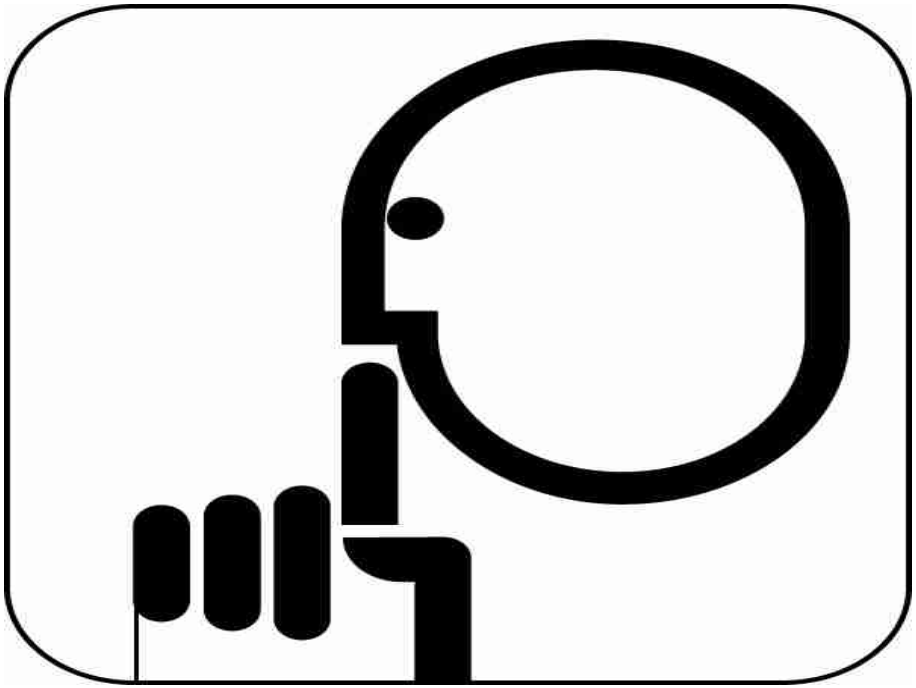
Why? “market failure” by user lock-in

Not Apple, but users feel the pain of hack


zeker weten met wie u via
internet afspraken maakt
DigiNotar
sche handtekenin

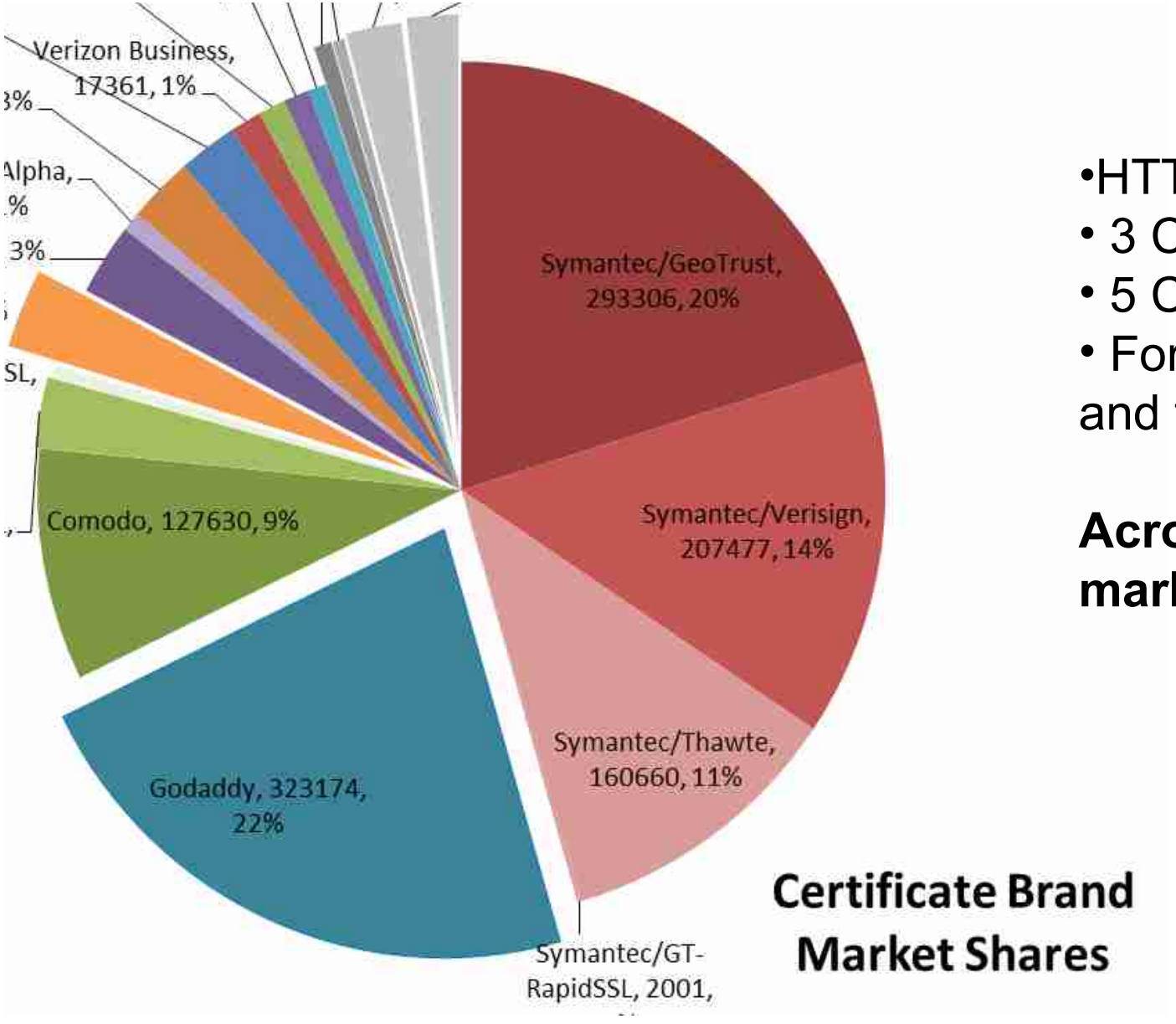
Known for long
HTTPS: deep security flaws

Many CAs hacks
All kept silent



All CAs are a weakest link!

Across communications security: Highly concentrated security markets

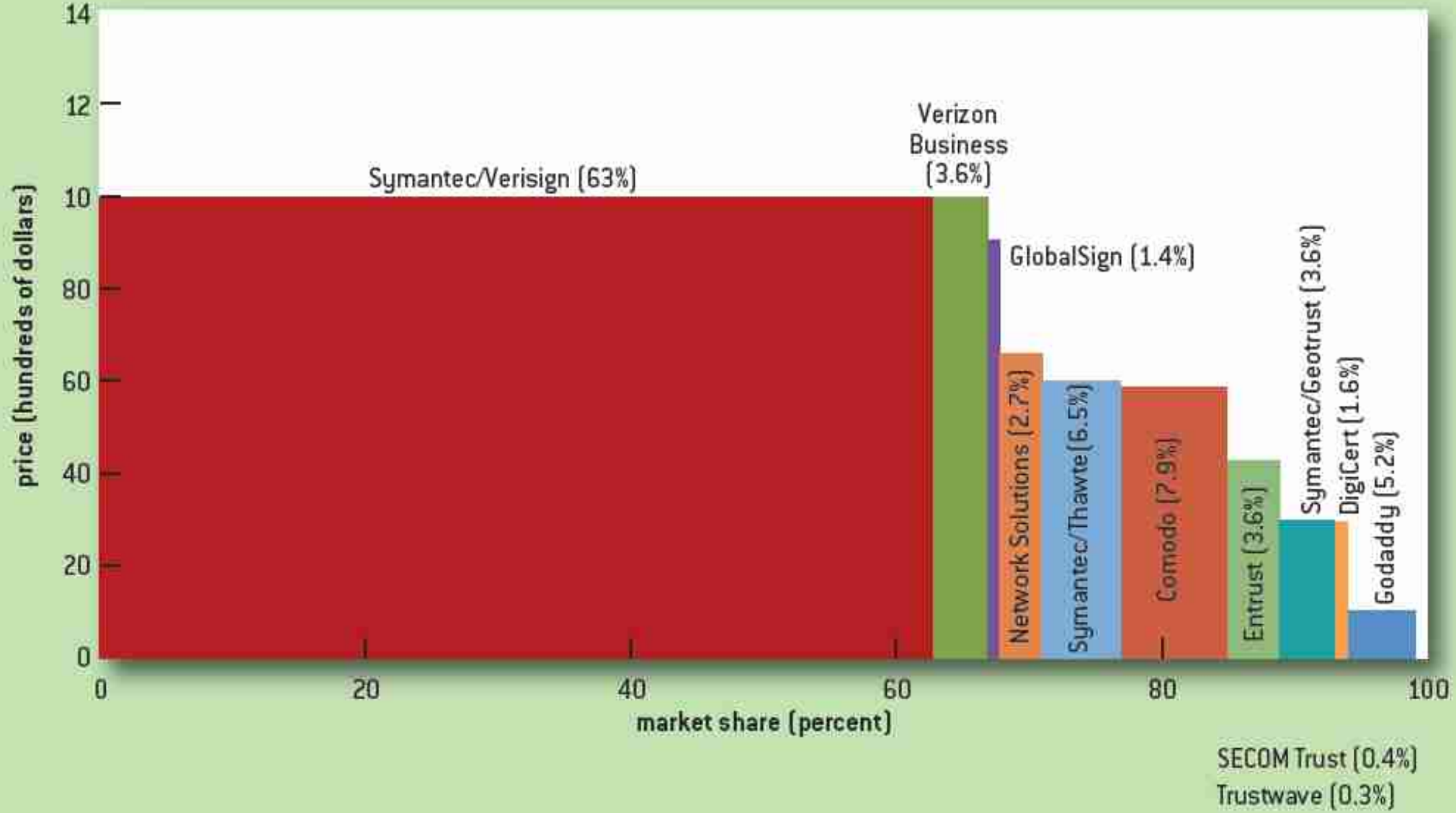


- HTTPS market
- 3 CAs sell 75% certs
- 5 CAs sell 90% certs
- For top 1k, top 100k and top 1m domains

Across web, similar market dynamics

FIGURE 3

Price and Market Share of EV Certificates



Market failures across security markets:

Information asymmetries
Negative externalities
User lock in

OUTLINE

Communications security

Why communications security fails

Systemic flaws in E.U. communications law

Recommendations

PART I: A HISTORY OF EU COMMUNICATIONS SECURITY LAW

2. Five EU Communications Security 'Policy Cycles'

Regulatory failure can often be attributed to shortcomings in legal definitions.[53] The apparent lack of a comprehensive overview of the EU regulatory framework of communications security is not a good omen in this respect.[54] A 2013 policy study commissioned by the European Parliament calls the exercise of providing such an overview 'undoubtedly highly complex', and in the end dodges the question at hand.[55] This chapter seeks to fill the gap, as it maps over three decades of information and communications security conceptualizations in E.E.C., E.C. and EU policies, sketching the relevant regulatory framework of EU communications security law in the process.

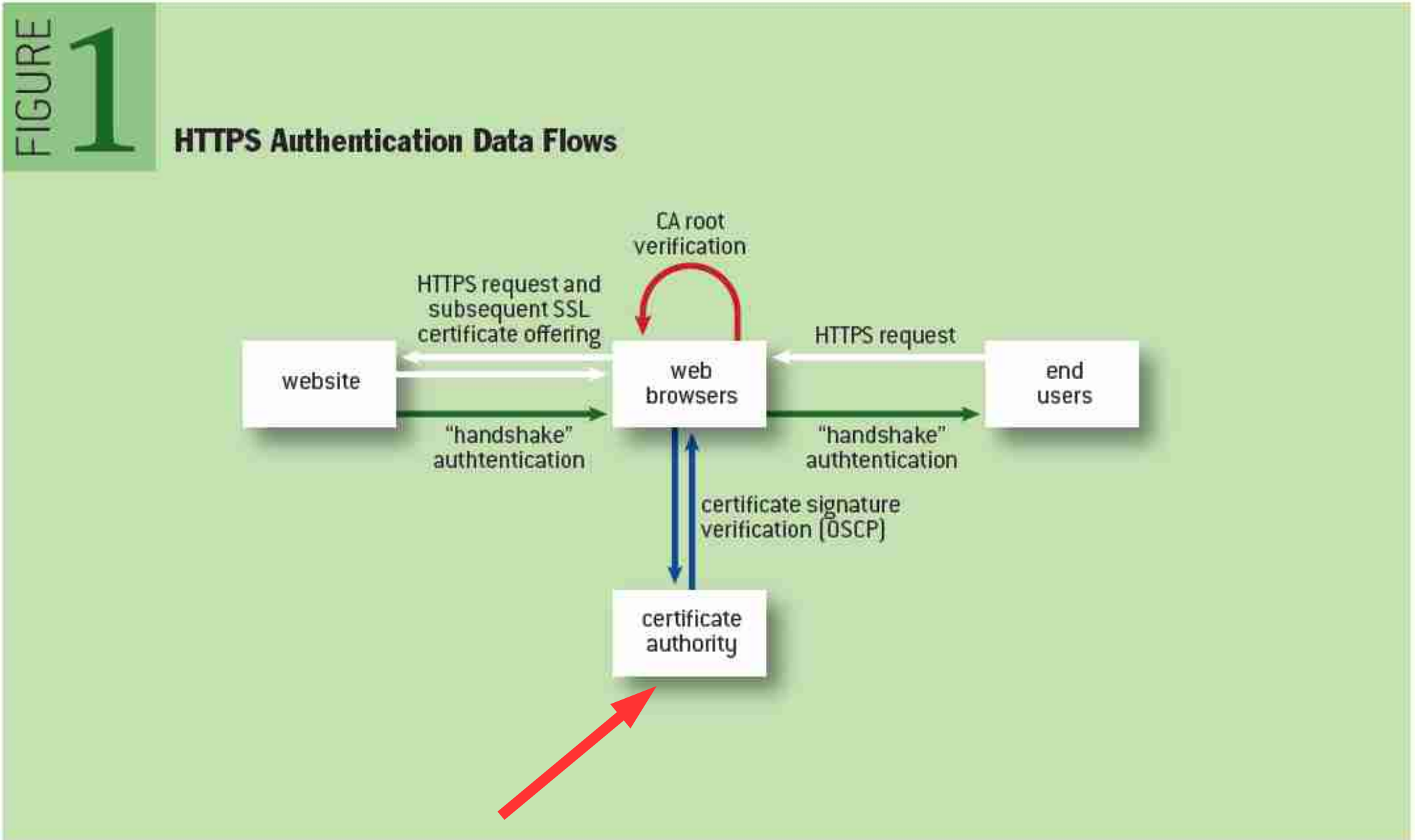
Historical analysis: 25 years of EU communications law

Current laws have old legacies:
fx. Breaking state monopolies
Not 'scoped' to same functionality

kpn

Ziggo

regulated

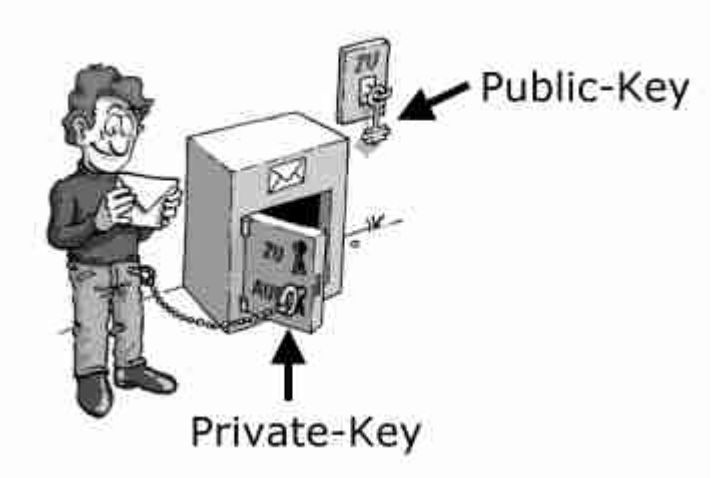


HTTPS communications: Only CAs (weakly) regulated

Not exactly securing the entire communications value chain

EU law offers a patchwork of protection

Intensely successful lobbying
Some gems of the mid 90s



СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

CVRIA
LUXEMBOURG

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

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 connection with the provision of such services — Validity — Articles 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, received at the Court on 11 June and 19 December 2012, in the proceedings

Digital Rights Ireland Ltd (C-293/12)

8 april 2014, E.U. Court Data Retention Directive Void

Landmark ruling: Human Right to Communications / Data Security

1. Para. 66 on c.i.a.-triad: “no sufficient safeguards to ensure full **confidentiality and integrity**”:
   - Quantity Data
   - Sensitivity Data
   - Risk of Abuse
1. 67: Wrongly permits **economic considerations** for IT-security

A Constitutional First Line of Defense

OUTLINE

Communications security

Why communications security fails

Systemic flaws in E.U. communications law

Recommendations

Research Question:

How should the EU lawmaker protect private communications security?

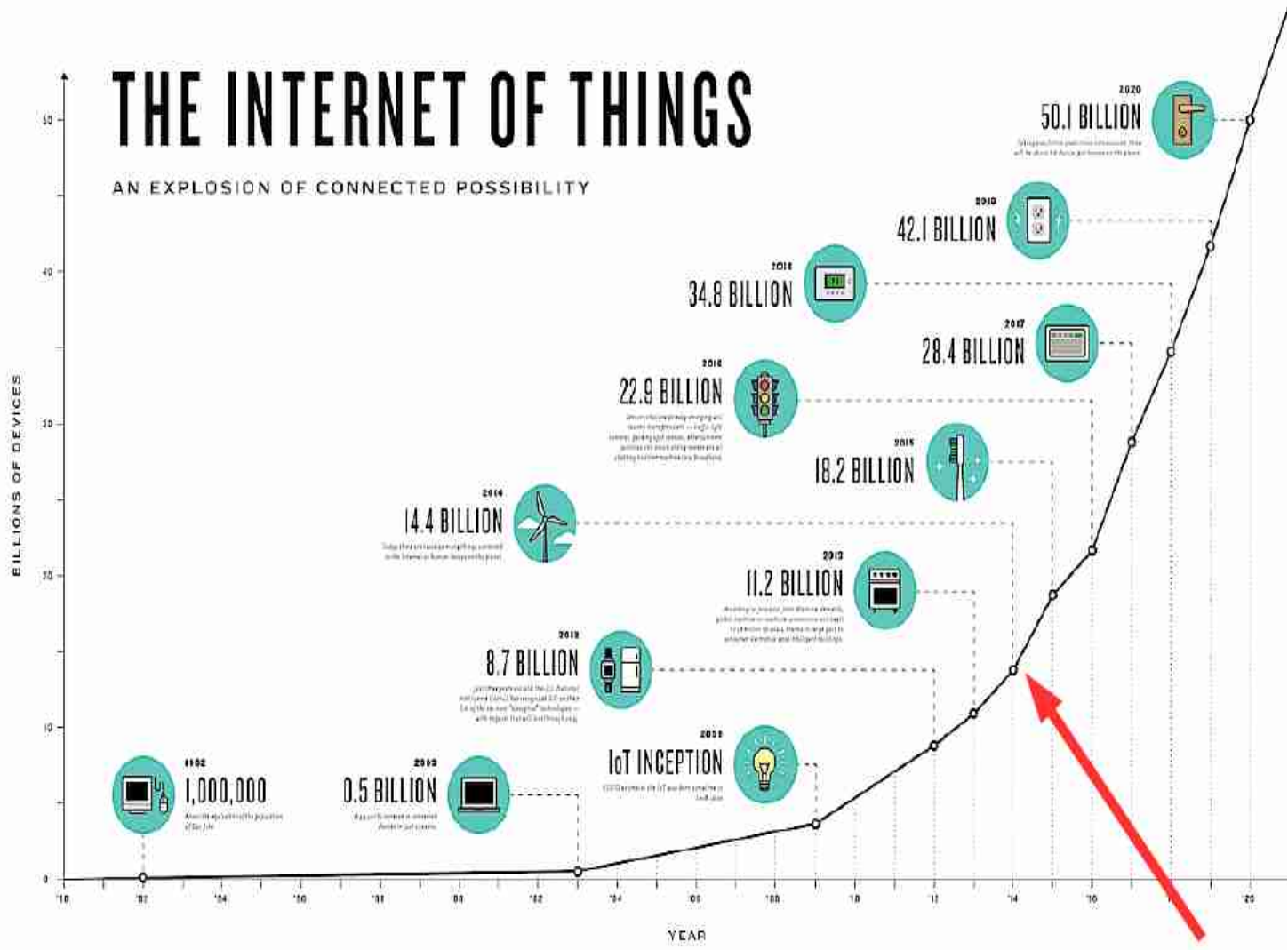
5 general recommendations:

The EU lawmaker should:

1. Implement human rights obligations
2. Resist regulatory capture by national security
3. Definition: ensure all elements of the c.i.a.-triad
4. Scope: technology-neutral along entire communications value chain
5. Intervene in persistent market failures

BONUS!
Use analytical model developed in case studies :)

reform inevitable on long term



Or else….

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 veiligheidscertificaten.

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

De Telegraaf, Frontpage, 5 Sept. 2011

work with letters and bank cheques, just like Mr. Donner!

Securing Private Communications

LEKENPRAATJE

Protecting Private Communications Security in E.U. Law: Fundamental Rights, Functional Value Chains and Market Incentives

25 November 2015, “Lekenpraatje” Ph.D. Thesis Defense, Aula @ University of Amsterdam

Securing Private Communications

Protecting Private Communications Security in EU Law: Fundamental Rights, Functional Value Chains and Market Incentives

Thesis, papers, presentations:
https://www.axelarnbak.nl

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. D.C. van den Boom
ten overstaan van een door het college voor promoties
ingestelde commissie, in het openbaar te verdedigen in de Aula der Universiteit
op woensdag 25 november 2015, te 11:00 uur
door

Axel Martin Arnbak

geboren te 's-Gravenhage