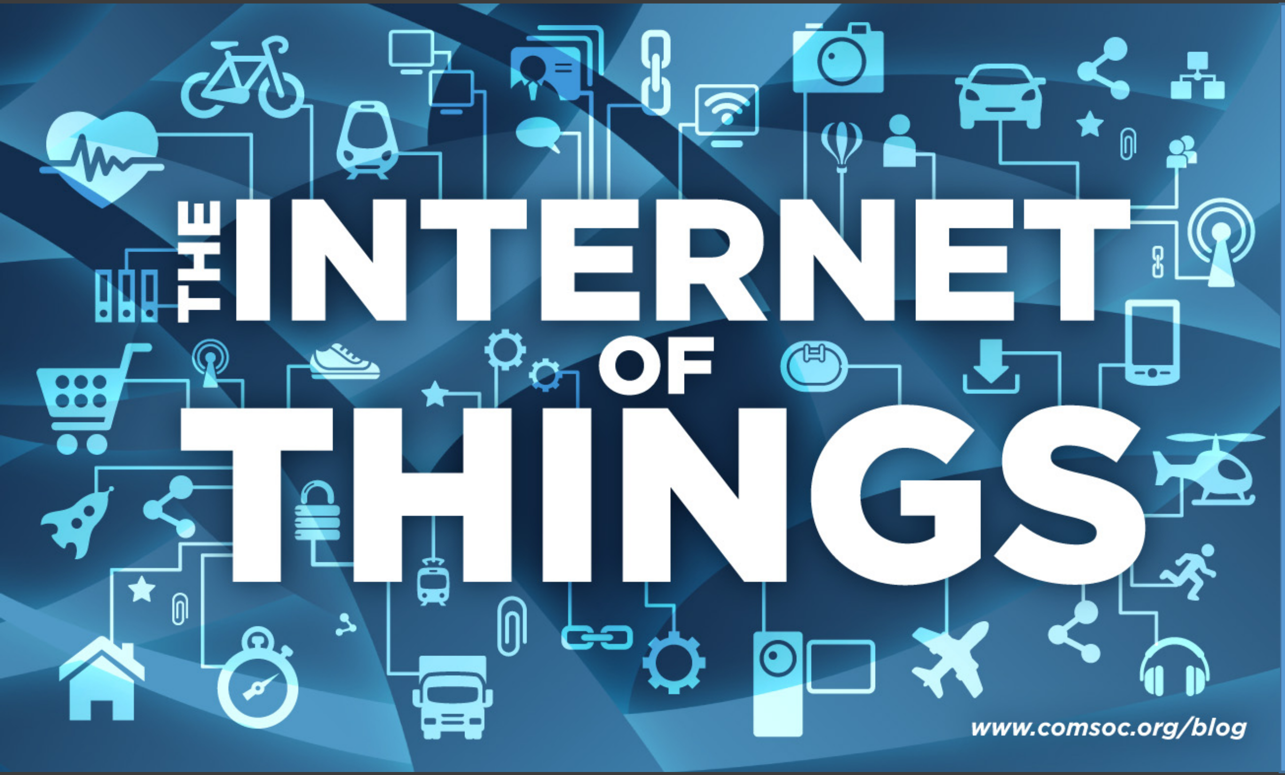
The Future of Security and Privacy

Bart Preneel

imec-COSIC KU Leuven

Trend 1

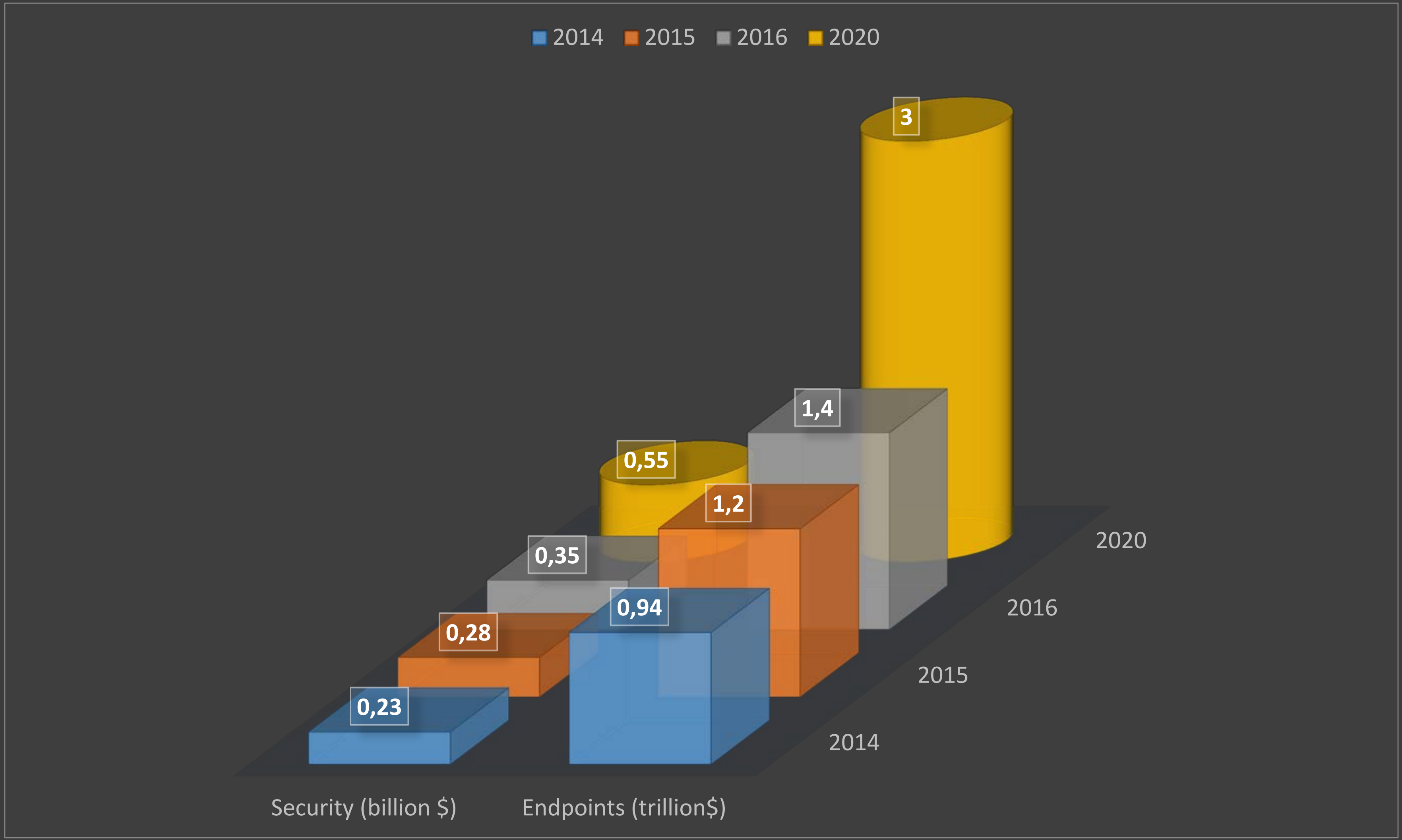
IoT makes IT more intrusive



Intrusive
unavOidable
sTealthy

IoT: security vs. endpoint spending

[Gartner, Apr 2016]



Trend 2

Big Data and Data Analytics for Security

Neerpelt.in - Stijn Philippe

Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization.

veracity

Gartner, 2010

Big Data for Security

If you have no visibility of your systems, how can you secure them?

Prevention is hopeless: if you detect all incidents, you can stop the bad guys in a cost effective way (read: you can reduce investments in prevention)

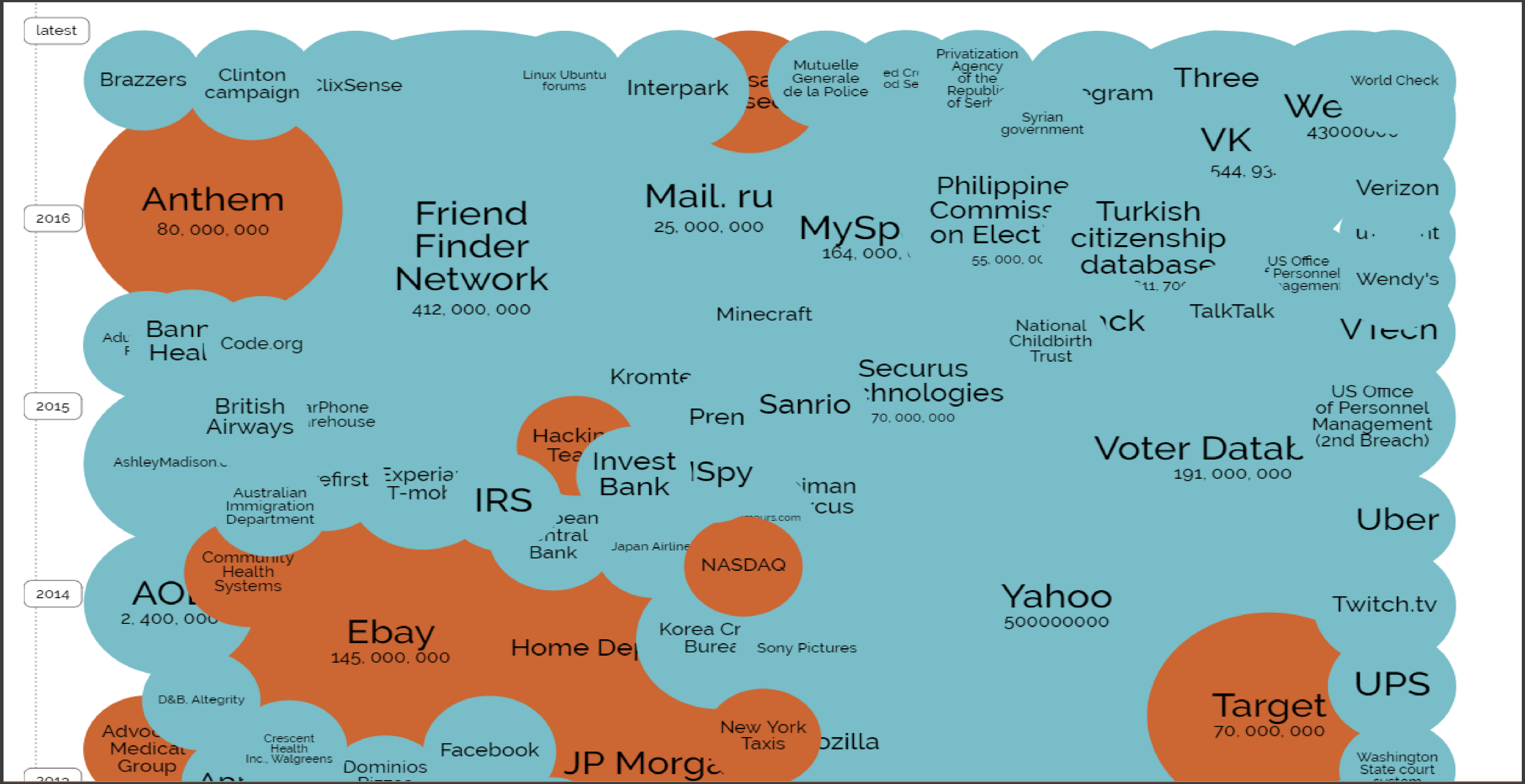
By applying analytics to incident data sets, we can learn how the bad guys behave and detect them even faster next time around

Trend 3

Big Data means ever bigger breaches

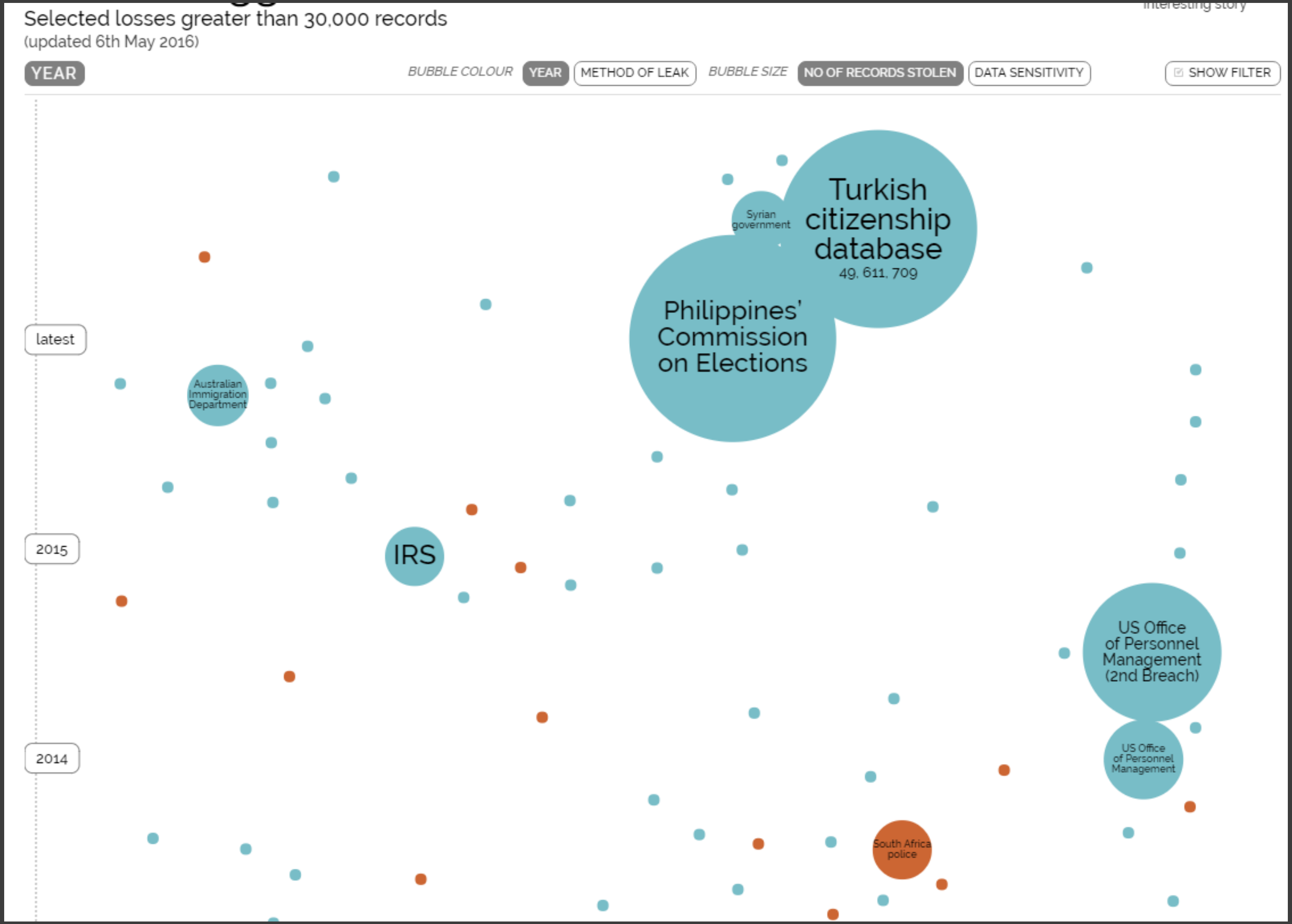
World’s Biggest Data Breaches

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks



World’s Biggest Government Data Breaches

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks



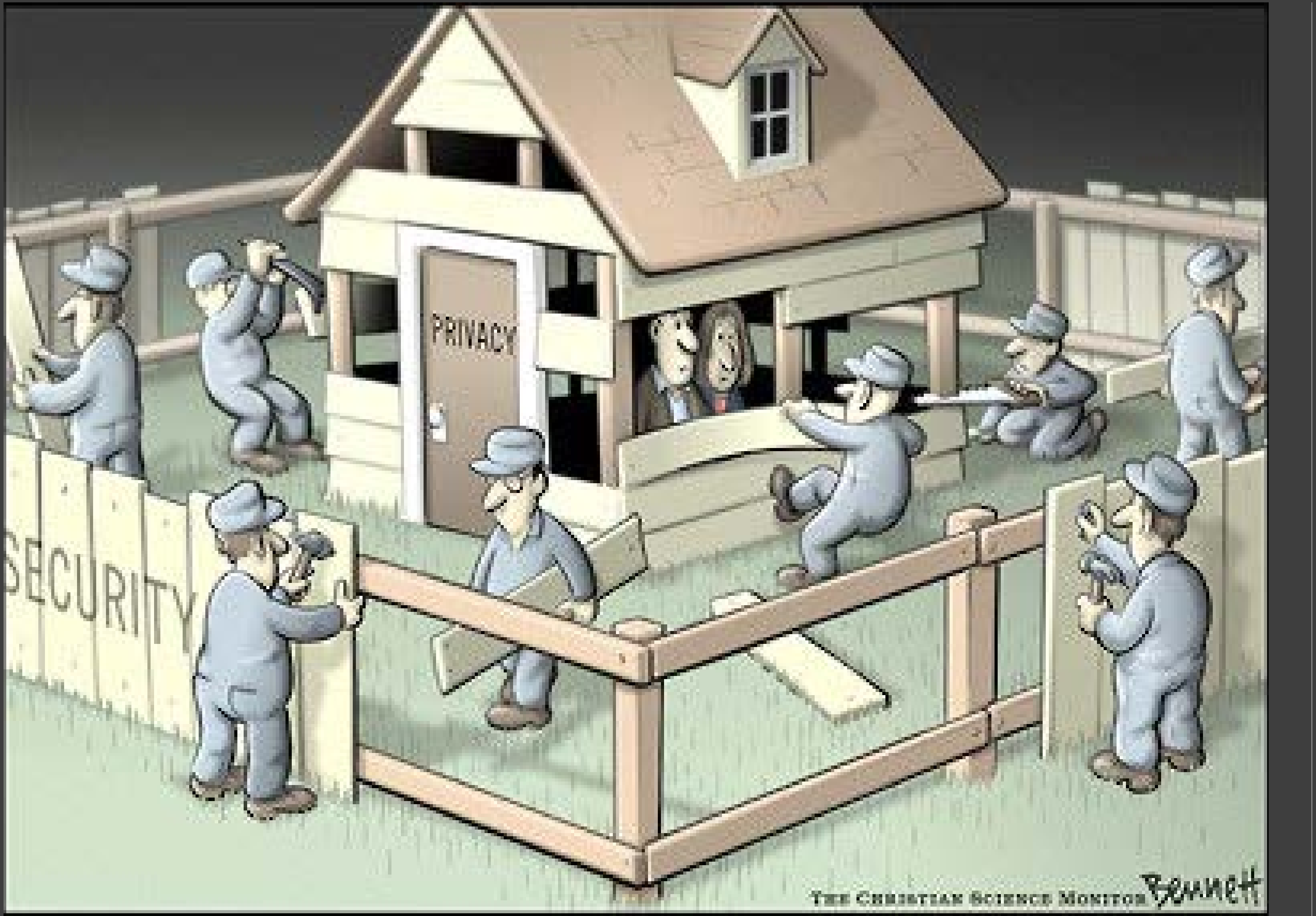
Selected losses greater than 30,000 records

(updated 6th May 2016)

YEAR
BUBBLE COLOUR
YEAR
METHOD OF LEAK
BUBBLE SIZE
NO OF RECORDS STOLEN
DATA SENSITIVITY
SHOW FILTER
latest
2015
2014
Turkish citizenship database
49, 611, 709
Syrian government
Philippines' Commission on Elections
Australian Immigration Department
IRS
US Office of Personnel Management (2nd Breach)
US Office of Personnel Management
South Africa police

OPM – 21 million people
Forms submitted by military and intelligence personal for security clearances
(eye colour, financial history, substance abuse)

Privacy is a security property



A metafor

Thinking of

Big Data in terms of pollution

Trend 4: Big Data for mass surveillance

« Who knew in 1984…

… that this world would be big Brother … »

… and the Zombies would be paying customers ? »

https://www.authcom.com/going-crazy-for-apples-iphone-6/

http://phys.org/news196665821.html

http://stacks.org/wp-content/uploads/2014/09/iphone-6-wait-660x330.png

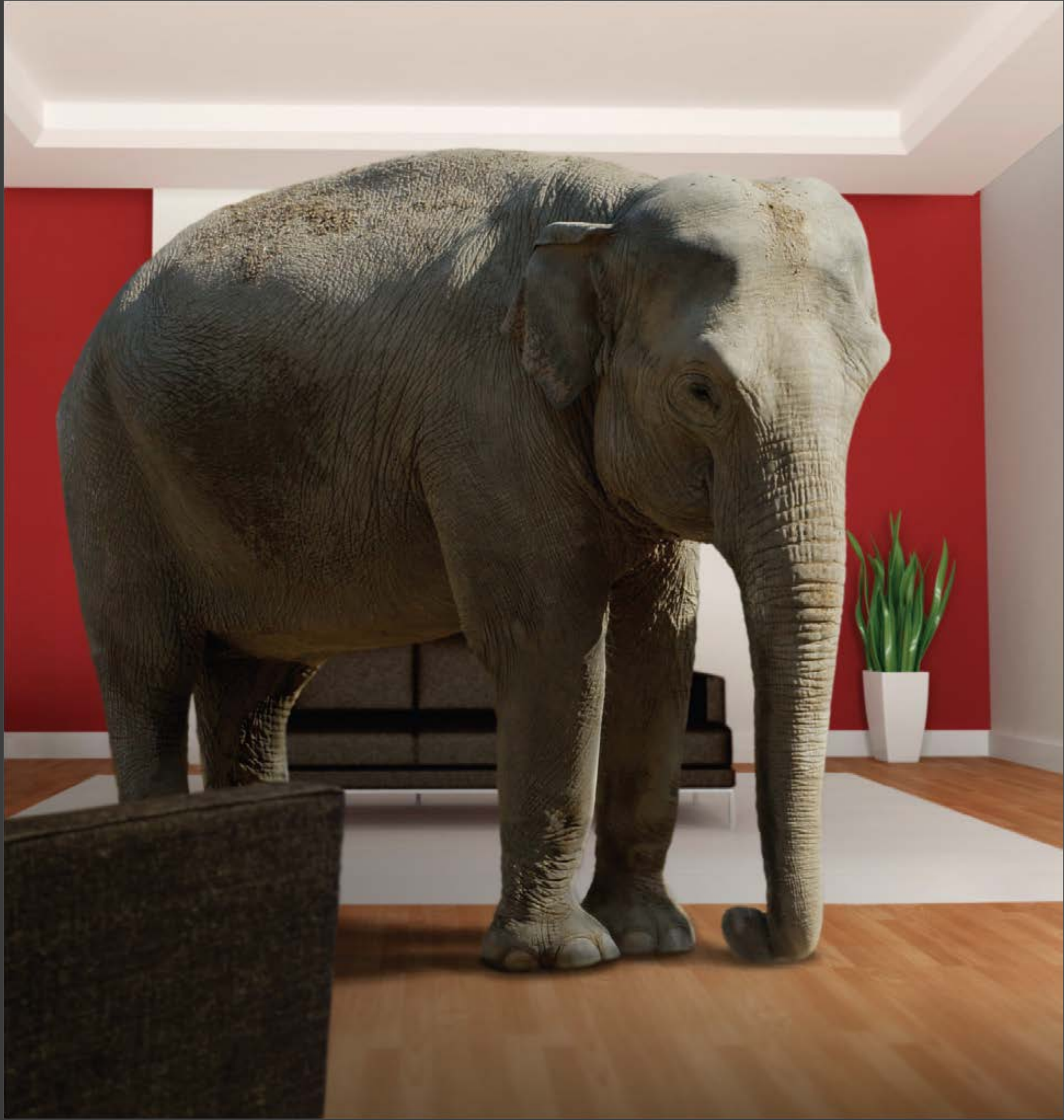
http://www.rjgeib.com

NSA calls the iPhone users public 'zombies' who pay for their own surveillance

It’s the

metadata

stupid

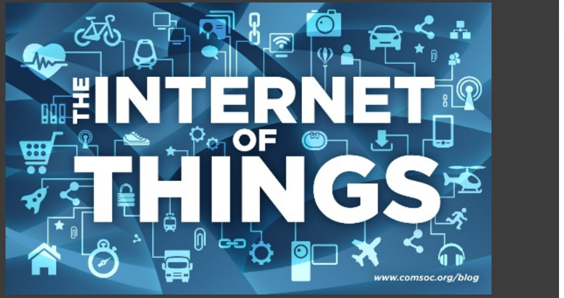


Which questions can one answer with mass surveillance systems/bulk data collection?

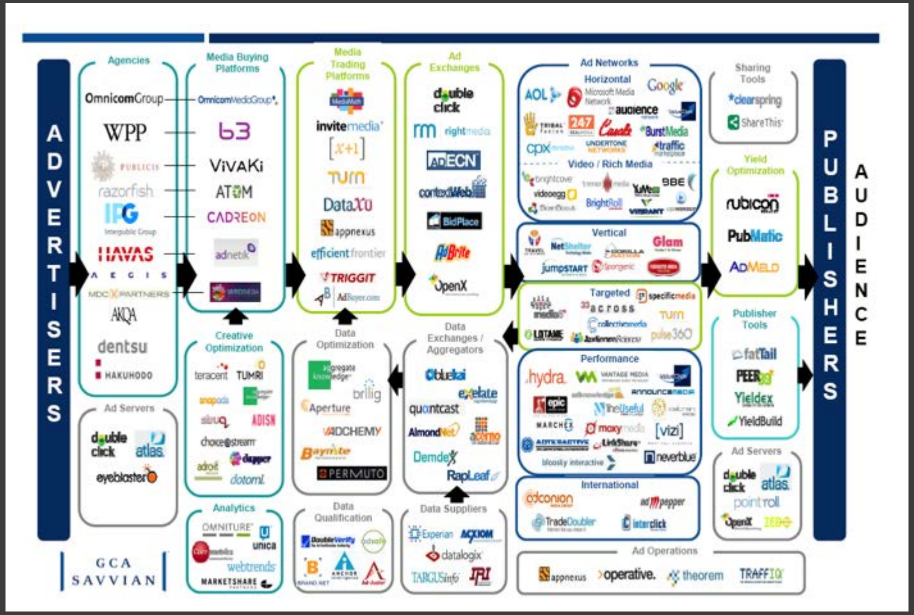
Tempora (GCHQ) ~ Deep Dive Xkeyscore (NSA)

- I have one phone number – find all the devices of this person, his surfing behavior, the location where he has travelled to and his closest collaborators
- Find all Microsoft Excel sheets containing MAC addresses in Belgium
- Find all exploitable machines in Panama
- Find everyone in The Netherlands who communicates in French and who use OTR, Signal or Telegraph

BND has spied on EU (incl. German) companies and targets in exchange for access to these systems



industry



users

government

Mass Surveillance

panopticon

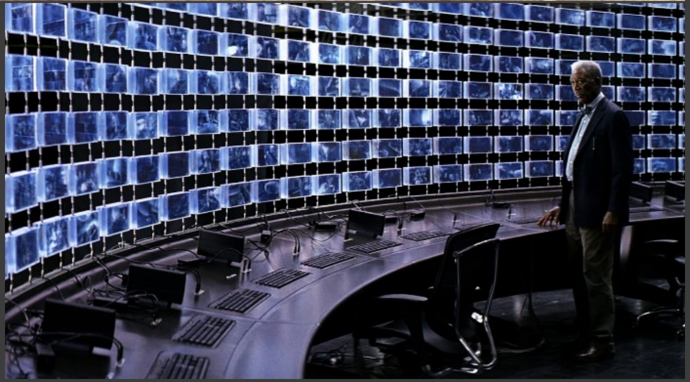
[Jeremy Bentham, 1791]

discrimination

fear

conformism - stifles dissent

oppression and abuse

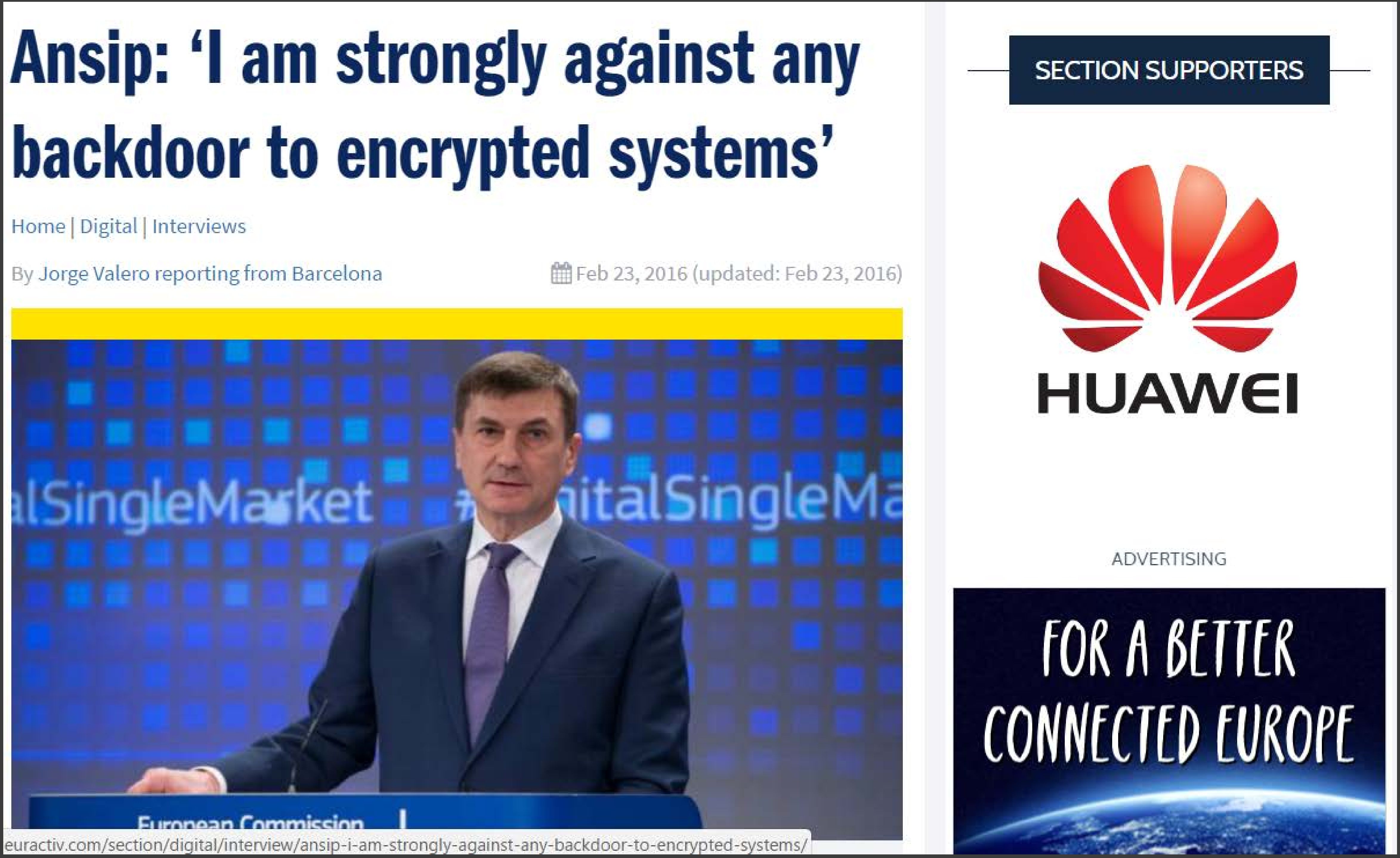


Trend 5

The Crypto Wars will ~~return~~ continue

France and Germany push for encryption limits

AP



Ansip: 'I am strongly against any backdoor to encrypted systems'

Home | Digital | Interviews

By Jorge Valero reporting from Barcelona

Feb 23, 2016 (updated: Feb 23, 2016)

eurativ.com/section/digital/interview/ansip-i-am-strongly-against-any-backdoor-to-encrypted-systems/

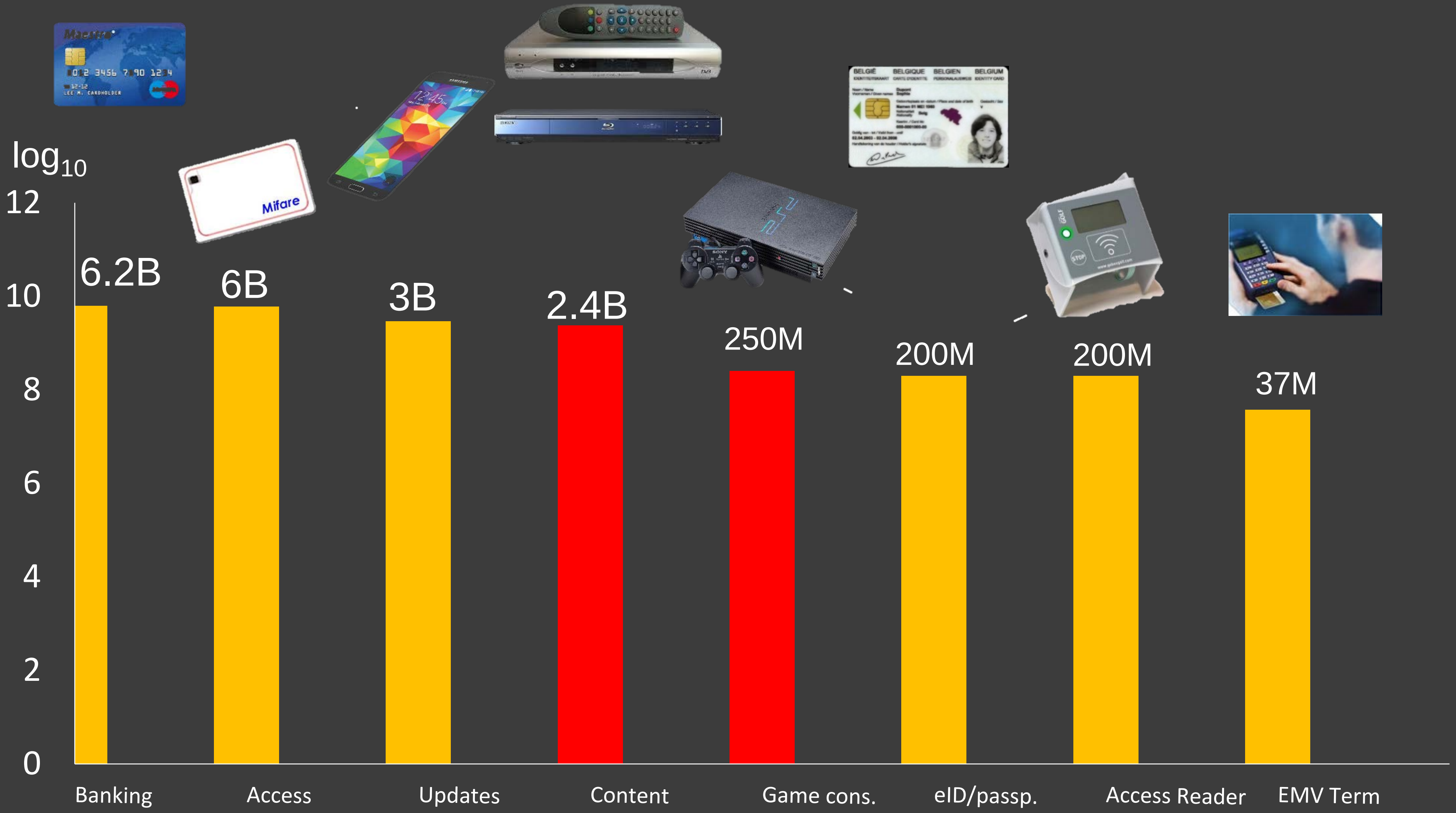
SECTION SUPPORTERS

HUAWEI

ADVERTISING

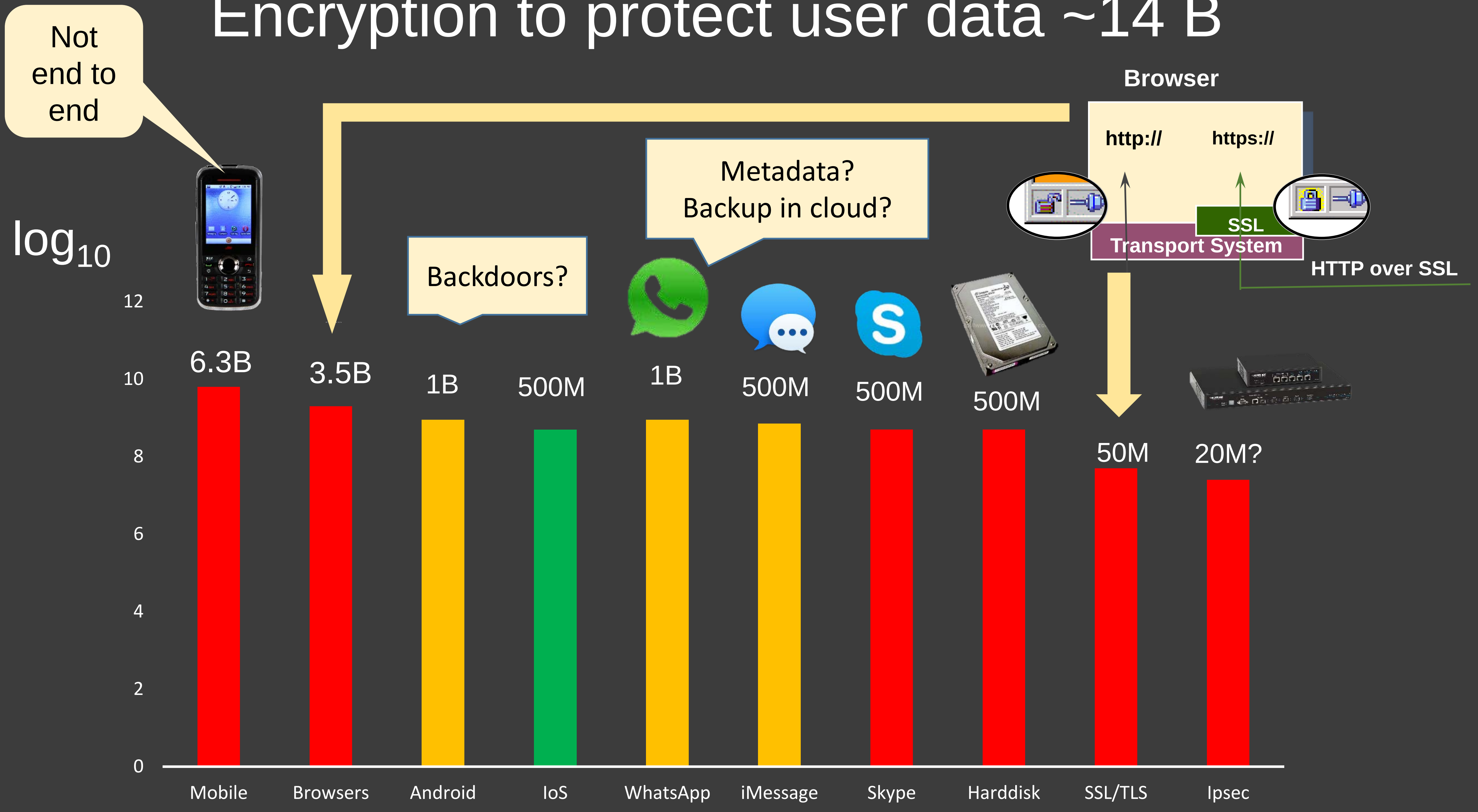
FOR A BETTER CONNECTED EUROPE

Encryption to protect industry ~18.3B



© Bart Preneel

Encryption to protect user data ~14 B



Not end to end

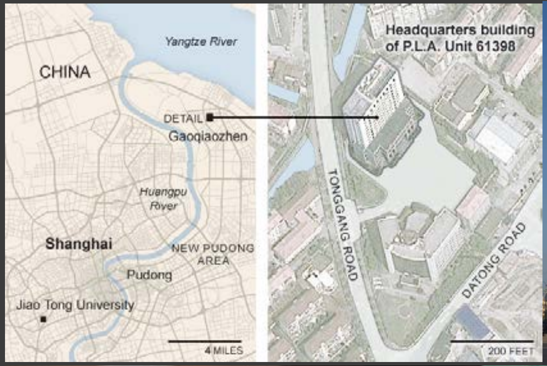
Backdoors?

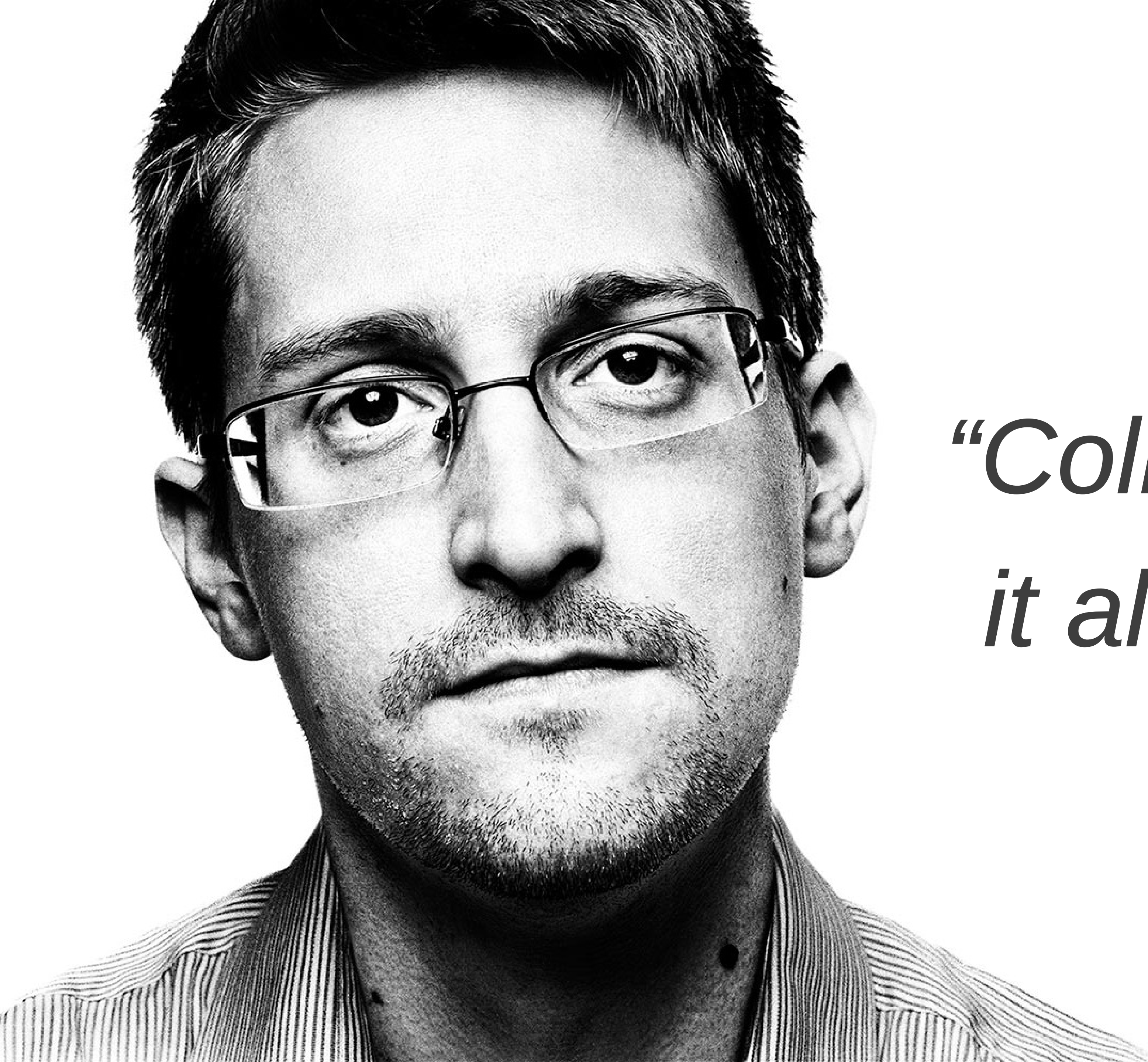
Metadata? Backup in cloud?

© Bart Preneel

Trend 6

Nation state hacking and cyber arms proliferation





NSA:

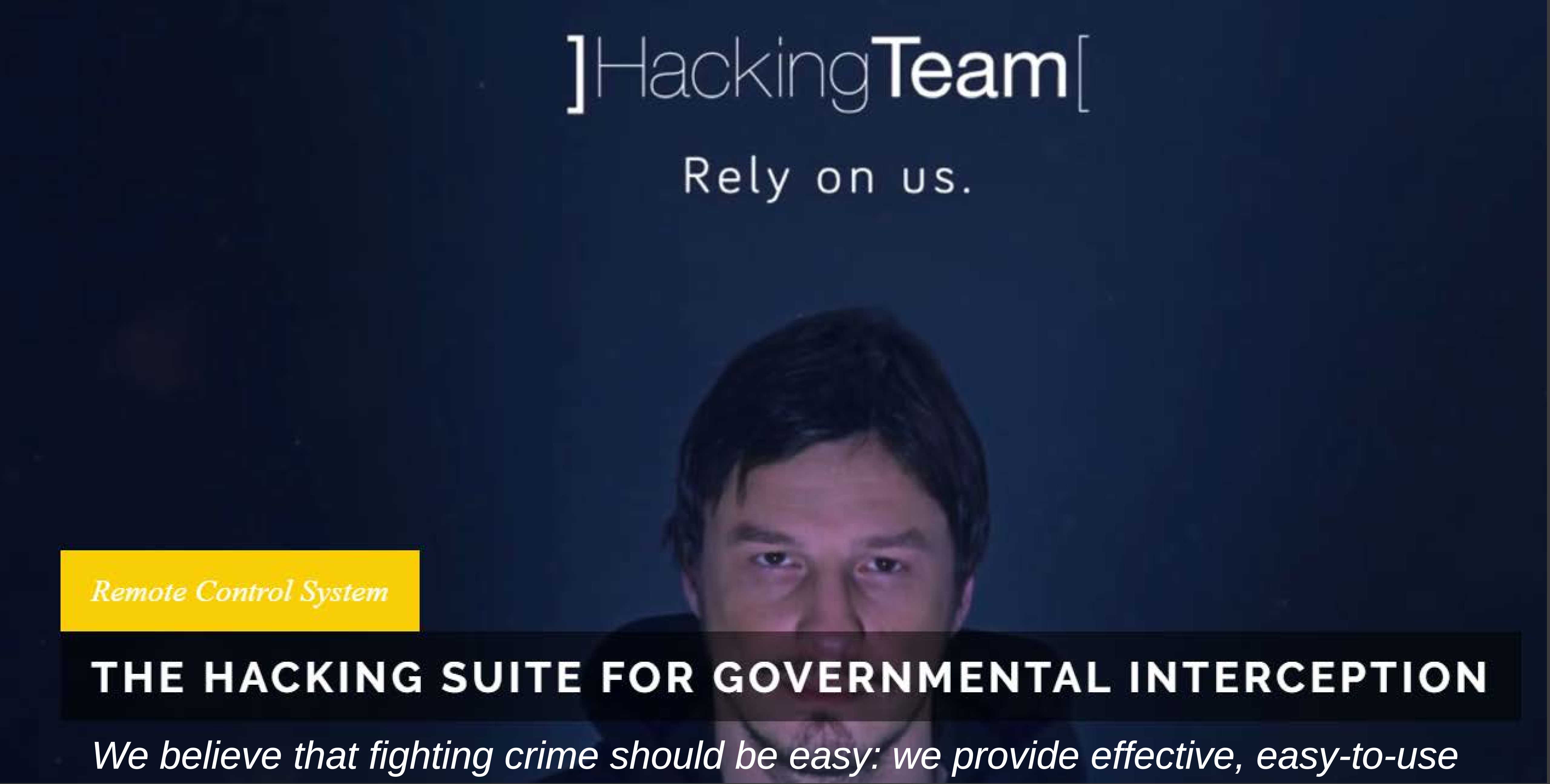
“Collect it all, know it all, exploit it all”

www.wired.com

Names and definitions of leaked CIA hacking tools

Posted Mar 9, 2017 by Devin Coldewey

www.techcrunch.com



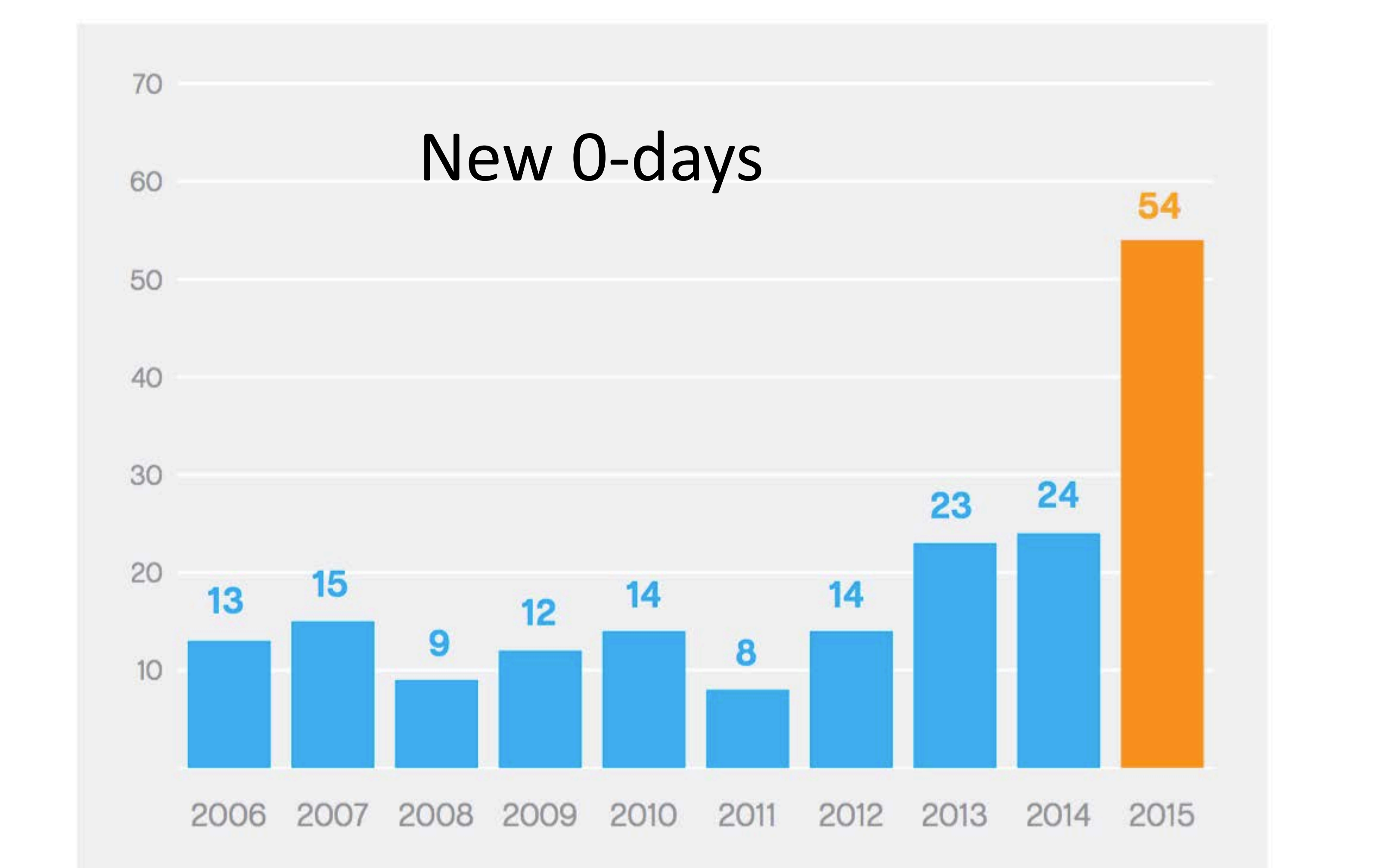
We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities

(Part of) government seems to prefer offense over defense

How many 0-days does the FBI and the NSA have?

Are they revealed to vendors?

If so when?



New 0-days

We need a Digital Geneva Convention

Microsoft President Brad Smith:

“Nation states are hacking civilians in peace time”

Optimism is a moral duty

Architecture is politics [Mitch Kaipor’93]

Avoid single point of trust that becomes single point of failure

COMSEC - Communication Security

Secure channels: still a challenge

- authenticated encryption studied in CAESAR http://competitions.cr.yp.to/caesar.html

Simplify internet protocols with security by default: DNS, BGP, TCP, IP, http, SMTP,…

Or start from scratch: Gnunet [Grothoff+], SCION [Perrig+]

Hiding communicating identities

Location privacy: problematic

COMPUSEC - Computer Security

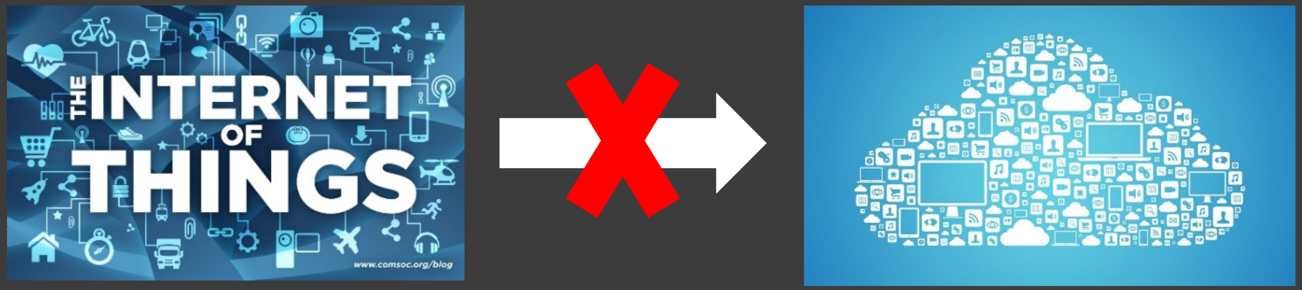
Protecting data at rest

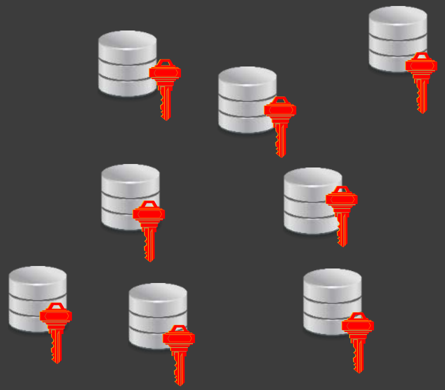
- – well established solutions for local encryption:
- – infrequently used in cloud

Secure execution

- essential to avoid bypassing of security measures

From Big Data to Small Local Data





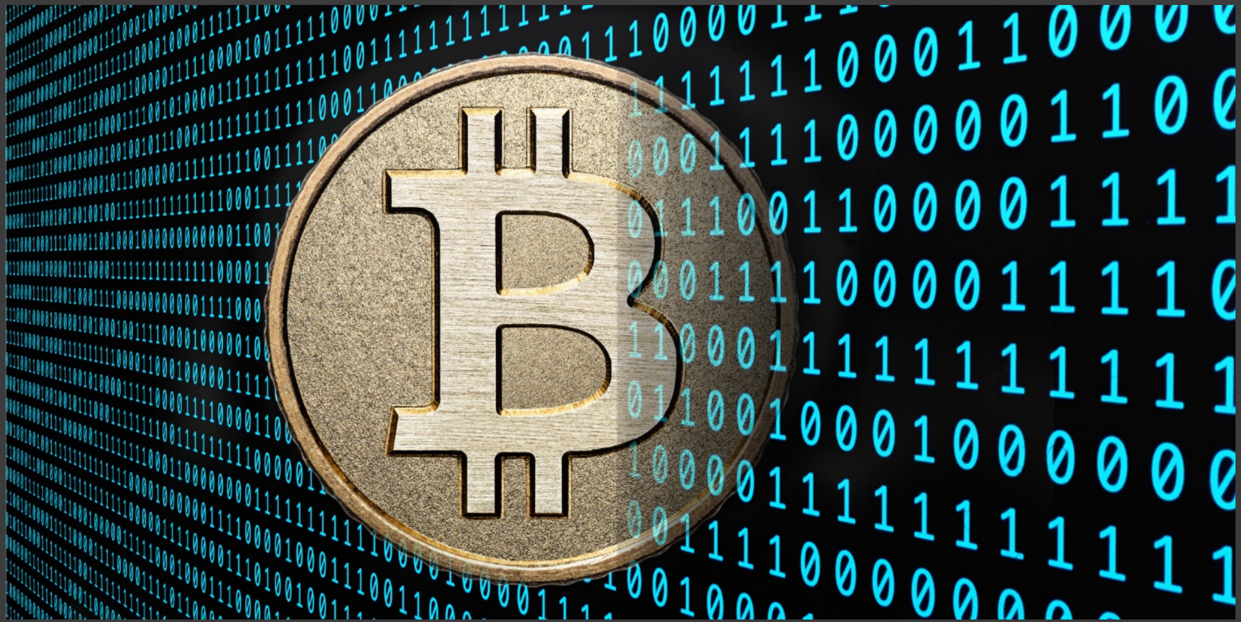
Data stays with users

Distributed solutions work

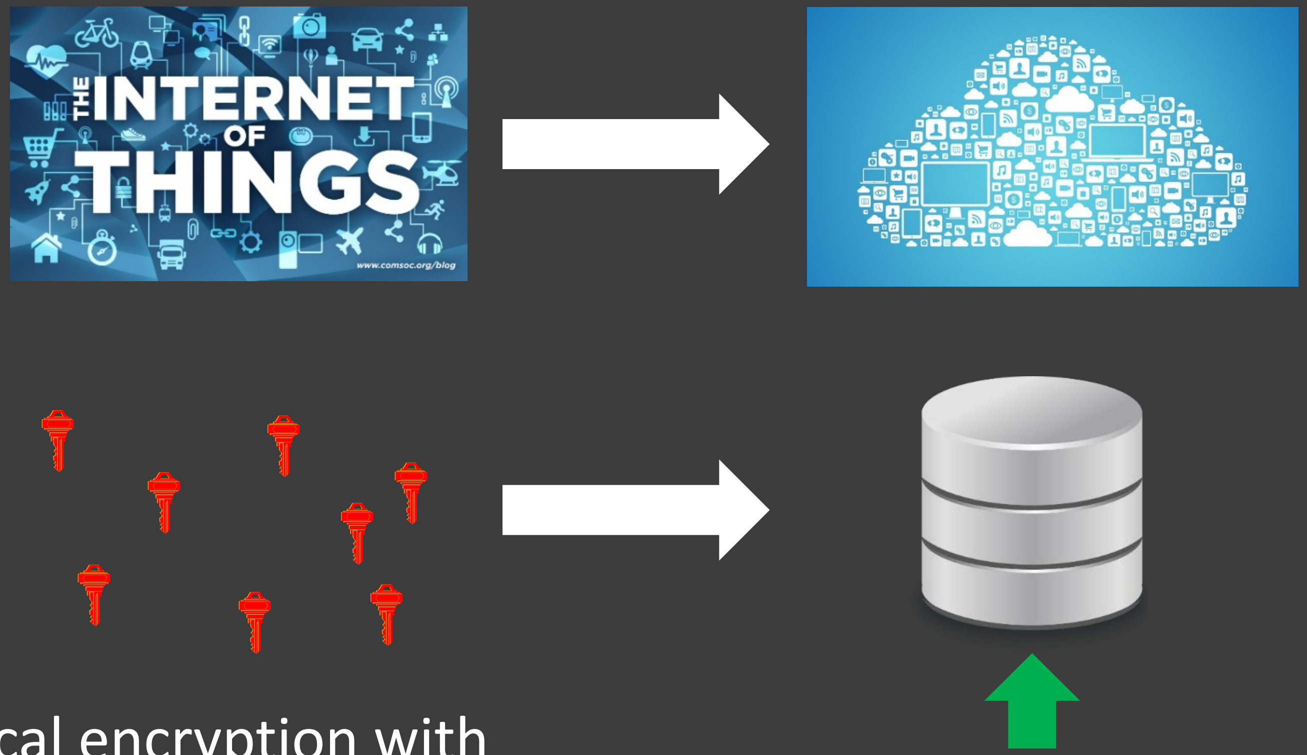
Root keys of some CAs

Skype (pre -2011)

Cryptocurrencies



From Big Data to Encrypted Data



Local encryption with low multiplication depth

Encrypted data

Can still compute on the data with somewhat Fully Homomorphic Encryption

Open (Source) Solutions

Effective governance

Transparency for service providers

EU-FOSSA

EU Free and Open Source Software Auditing

Conclusions (research)

Rethink architectures: distributed

Shift from network security to system security

Increase robustness against powerful opponents who can subvert many subsystems during several lifecycle stages

Open technologies and review by open communities

Cryptomagic can help

Conclusions (policy)

Pervasive surveillance needs **pervasive collection** and **active attacks** with massive collateral damage on our ICT infrastructure

Back to targeted surveillance under the rule of law

- avoid cyber-colonialism [Desmedt]
- need industrial policy with innovative technology that can guarantee economic sovereignty
- need to give law enforcement sufficient options

Bart Preneel, imec-COSIC KU Leuven

ADDRESS:	Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE:	homes.esat.kuleuven.be/~preneel/
EMAIL:	Bart.Preneel@esat.kuleuven.be
TWITTER:	@CosicBe
TELEPHONE:	+32 16 321148

ECRYPT CSA

http://www.ecrypt.eu.org

Further reading

Books

Glenn Greenwald, No place to hide, Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014

Documents:

https://www.eff.org/nsa-spying/nsadocs

https://cjfe.org/snowden

Articles

Philip Rogaway, The moral character of cryptographic work, Cryptology ePrint Archive, Report 2015/1162

Bart Preneel, Phillip Rogaway, Mark D. Ryan, Peter Y. A. Ryan: Privacy and security in an age of surveillance (Dagstuhl perspectives workshop 14401). Dagstuhl Manifestos, 5(1), pp. 25-37, 2015.

More information

Movies

Citizen Four (a movie by Laura Poitras) (2014) https://citizenfourfilm.com/

Edward Snowden - Terminal F (2015) https://www.youtube.com/watch?v=Nd6qN167wKo

John Oliver interviews Edward Snowden https://www.youtube.com/watch?v=XEVlyP4_11M

Snowden (a movie by Oliver Stone) (2016)

Zero Days (a documentary by Alex Gibney) (2016)

Media

https://firstlook.org/theintercept/

http://www.spiegel.de/international/topic/nsa_spying_scandal/

Very short version of this presentation: https://www.youtube.com/watch?v=uYk6yN9eNfc