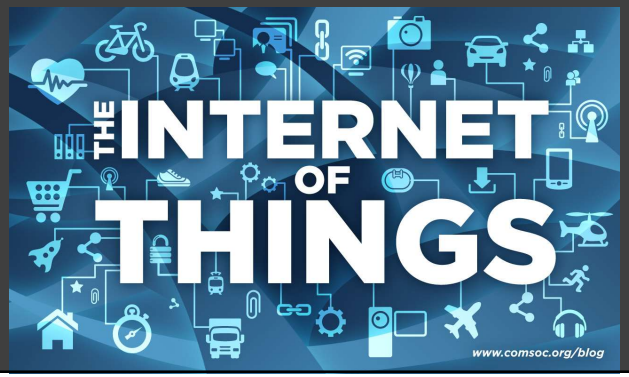
The Future of Security and Privacy

Bart Preneel
COSIC, an imec lab at KU Leuven

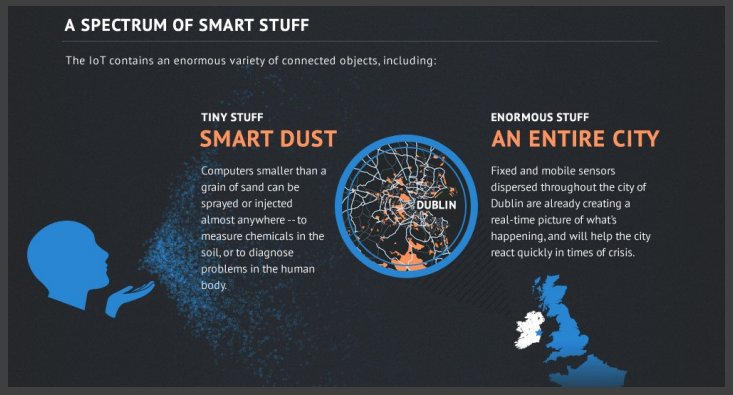
imec embracing a better life
KU LEUVEN
COSIC

Trend 1

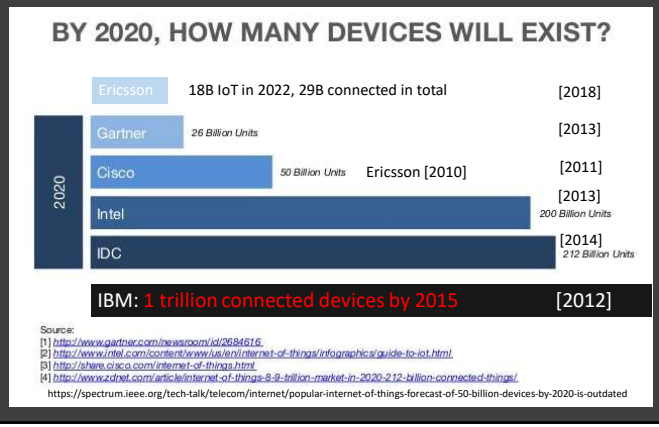
IoT makes IT more intrusive

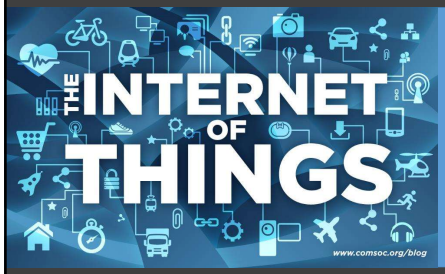


IoT markets (source: Intel)



How fast will IoT grow?





Intrusive
unavOidable
sTealthy

IoT security risks

IoT security risks

Massive deployment
Low cost
Limited resources
Large attack surface
Hard to update
Insecure programming
Lack of expertise

Complex ecosystem
Fragmentation
Security vs. safety

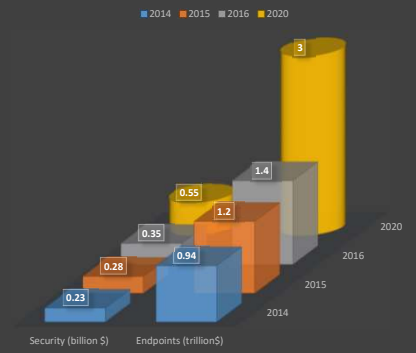
ENISA Baseline Security Recommendations for IoT in the context for critical information infrastructures, 2017

IoT security risks

Unclear liabilities
Market for lemons
Tragedy of the commons
Lack of regulation

IoT: security vs. endpoint spending

[Gartner, Apr 2016]



[Gartner, Oct 2017]
Through 2022, half of all security budgets for IoT will go to fault remediation, recalls and safety failures rather than protection

[Gartner, Mar 2018]
Worldwide IoT security spending will reach B$1.5 in 2018 (M$900 in 2016 and B$3.1 in 2020)

https://www.gartner.com/newsroom/id/3869181

How will we look back in 2039 to today?

1961 Chevrolet Corvair

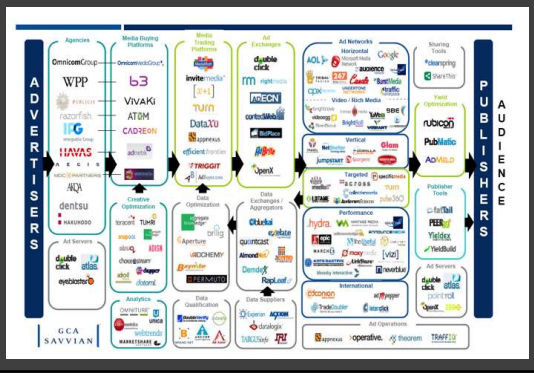
Trend 2

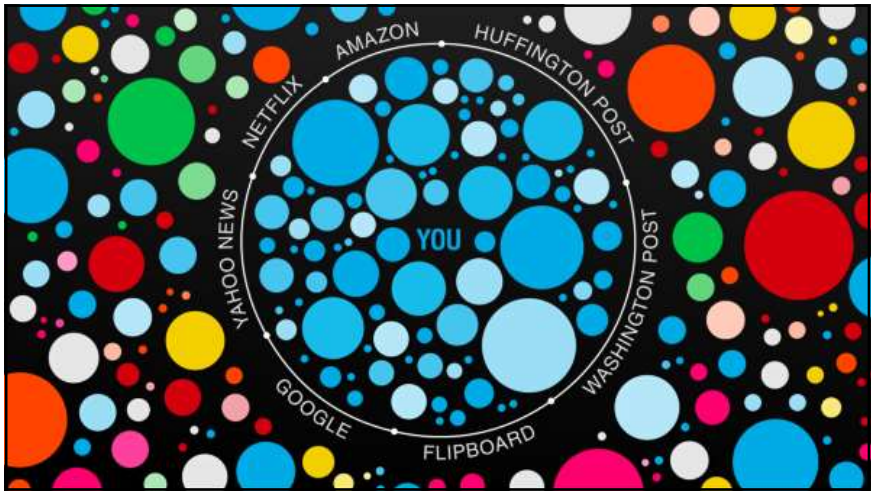
Big Data and Data Analytics (AI) for Security

Richard Stallman:
the cloud is someone else's computer

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 [Gartner 2010]

Andrew Lewis: If you are not paying for it, you're not the customer; you're the product being sold





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)

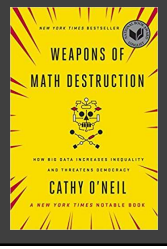
By applying analytics to incident data sets, we can learn how the bad guys behave and detect them even faster next time around

AI and privacy

Leakage of training data

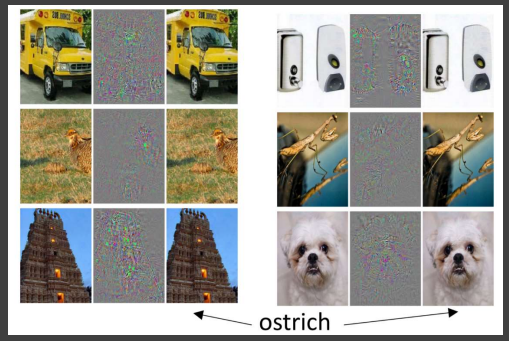
Leakage of models

Algorithmic fairness



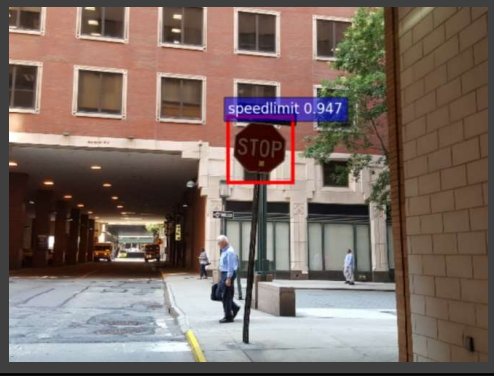
https://towardsdatascience.com/a-gentle-introduction-to-the-discussion-on-algorithmic-fairness-740bbb469b6

AI and security: adversarial machine learning



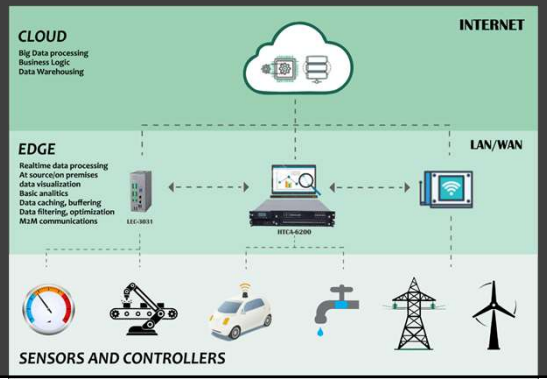
Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., Fergus, R. Intriguing properties of neural networks. ICLR 2014

AI and security: adversarial machine learning



Trend 3

Integration of IoT-Edge-Cloud



Edge (or Fog) computing

Latency: real-time processing

Reduce communication overhead

Decentralization: more privacy

Less secure?

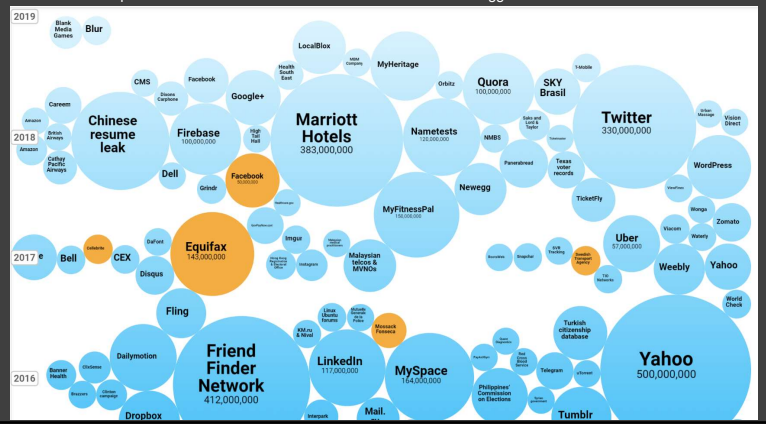
- Open to physical attacks
- Less control

ENISA Towards Secure Convergence of Cloud and IoT, 2018

Trend 4

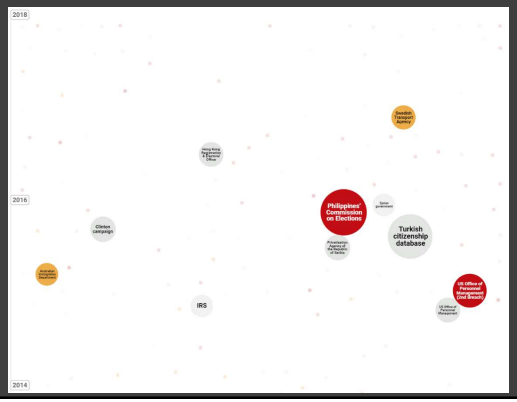
World's biggest data breaches

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



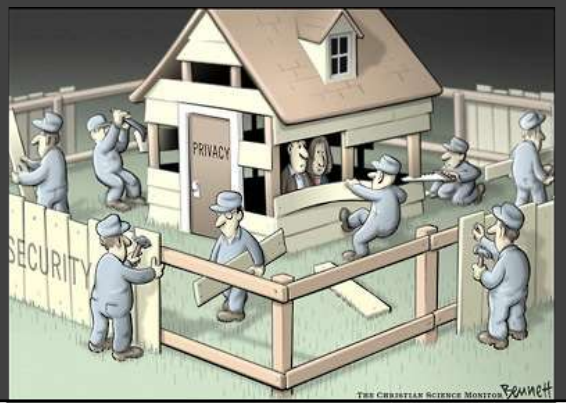
World's biggest government data breaches

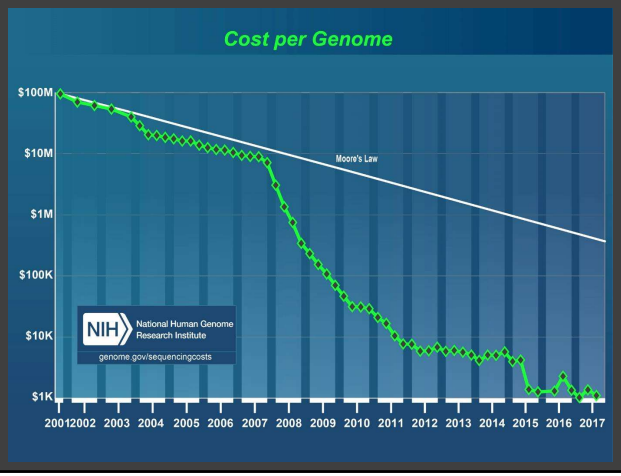
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks



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

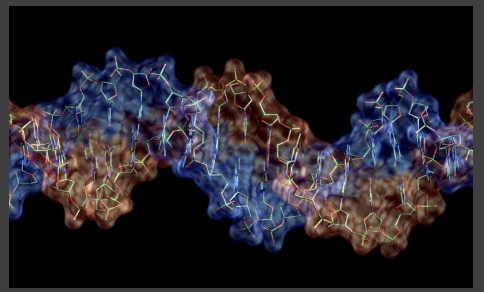




Your family DNA can be used against you

Data from Ancestry.com and 23andMe used to solve crimes

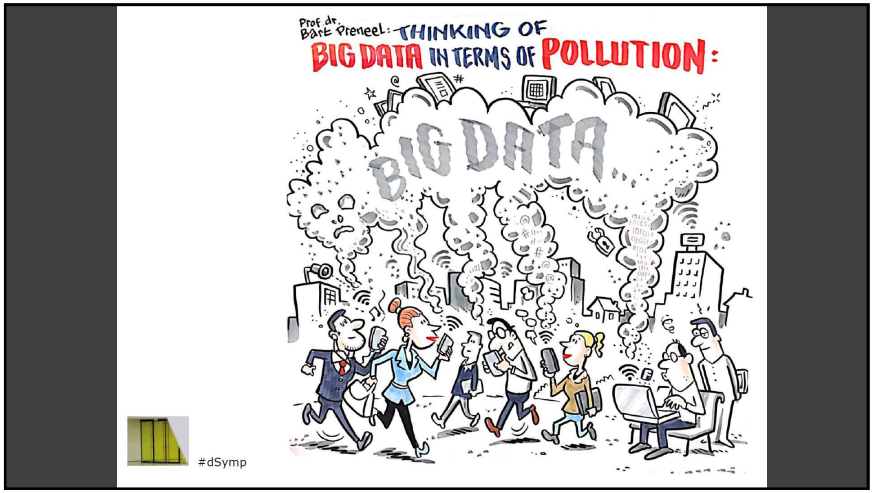
What about insurance companies?



28

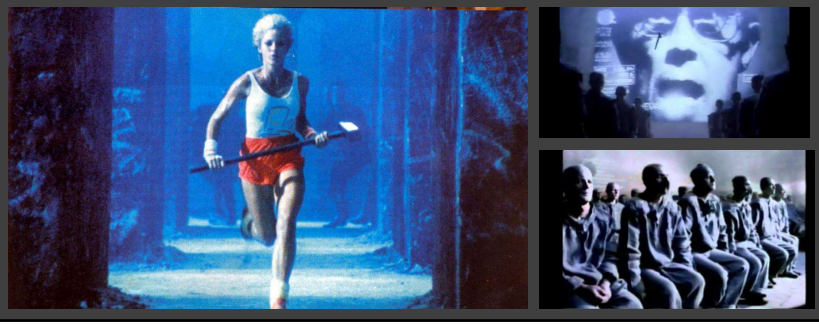
A metafor

Thinking of
Big Data in terms
of pollution



Trend 5: Big Data for mass surveillance

« Who knew in 1984…



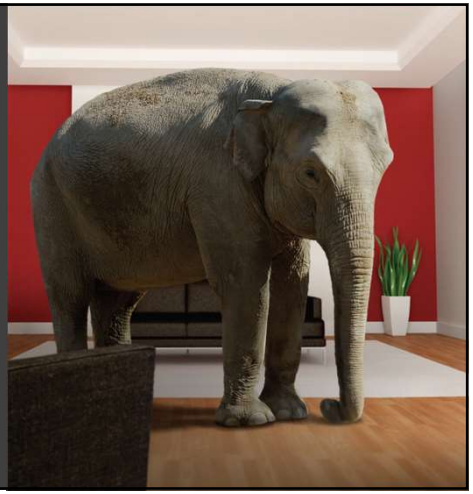
… and the Zombies would be paying customers ? »

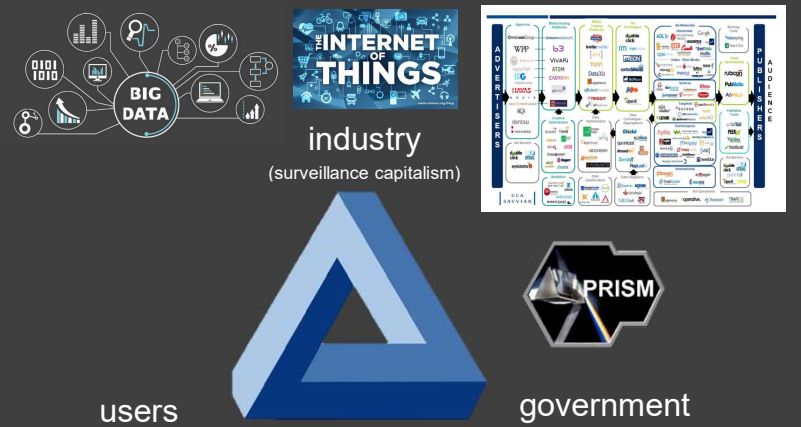
NSA calls the iPhone users public 'zombies' who pay for their own surveillance

It's the

metadata

stupid



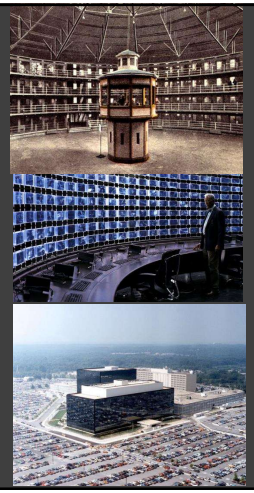


1945–1989 East Germany

Mass surveillance

panopticon
[Jeremy Bentham, 1791]

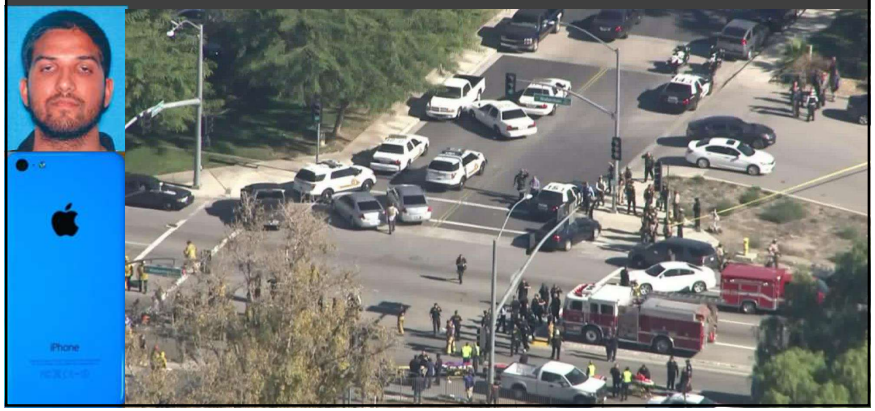
discrimination
fear
conformism - stifles dissent
oppression and abuse



Trend 6

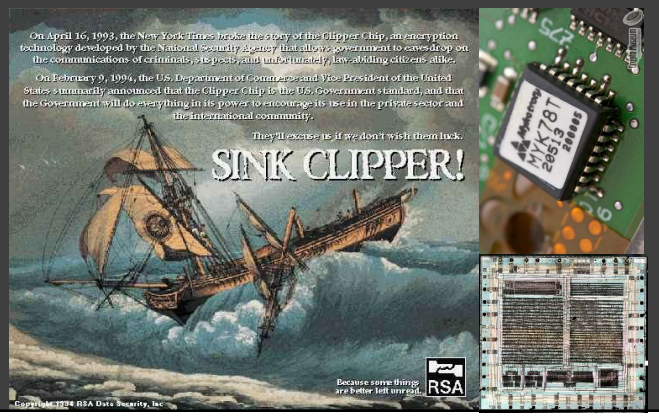
The Crypto Wars will ~~return~~ continue

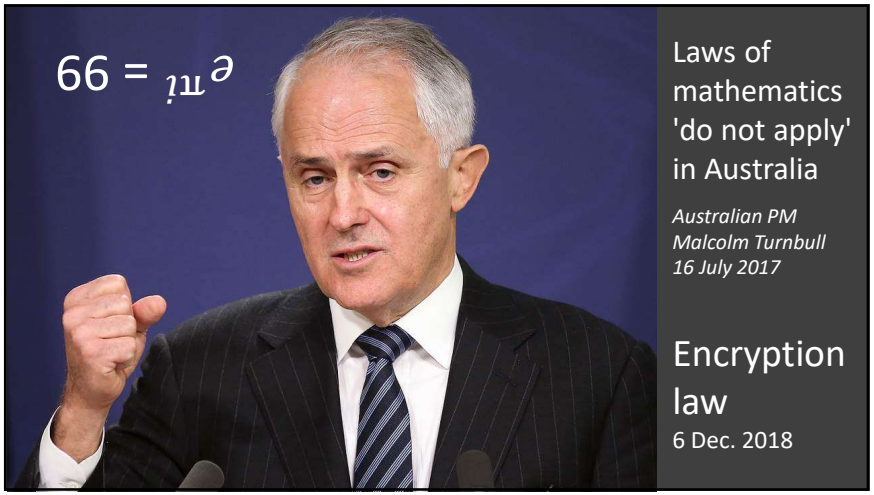
San Bernardino, CA, December 2, 2015



At the request of the FBI, based on an all writs order (1789), a U.S. federal magistrate judge has ordered Apple to break the security of the iPhone

It is an old battle



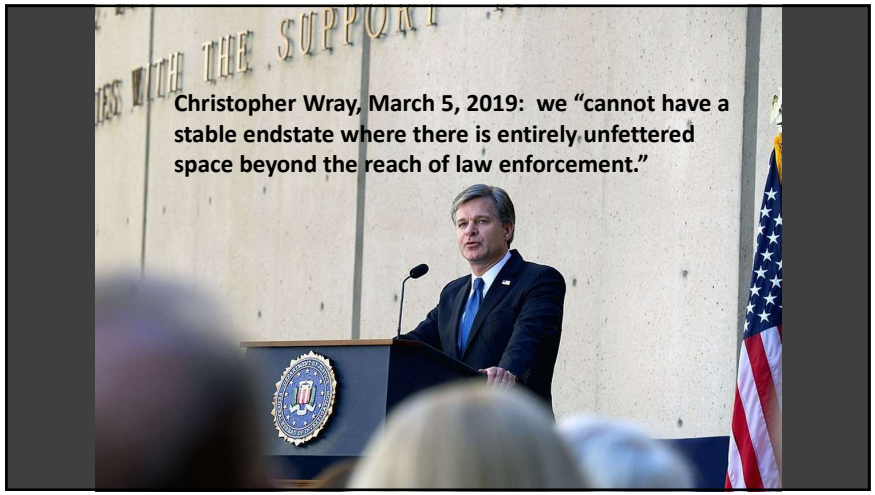


Laws of mathematics 'do not apply' in Australia

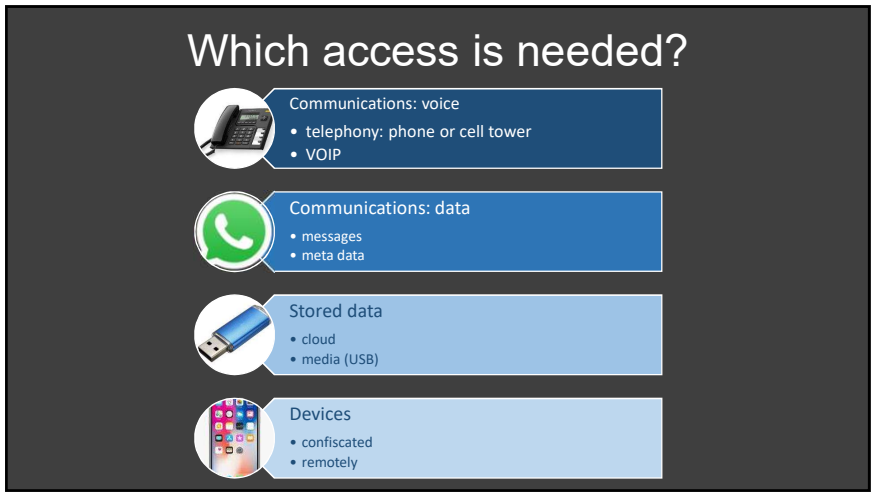
Australian PM Malcolm Turnbull 16 July 2017

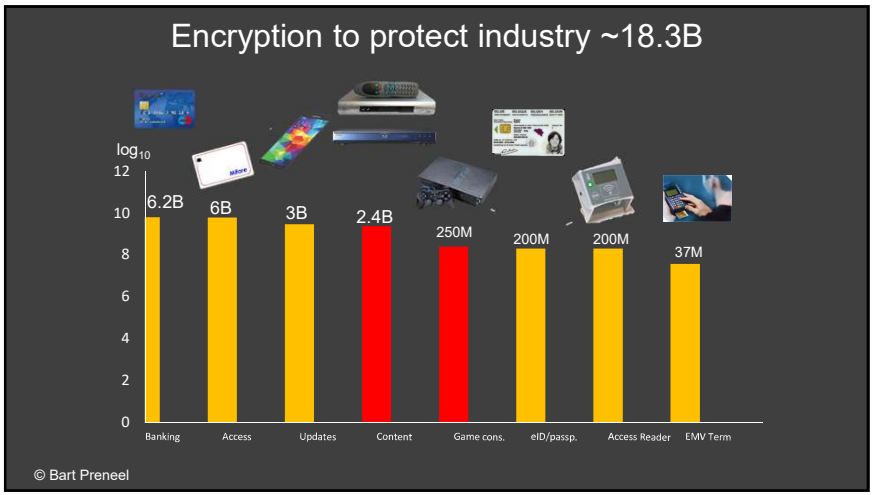
Encryption law

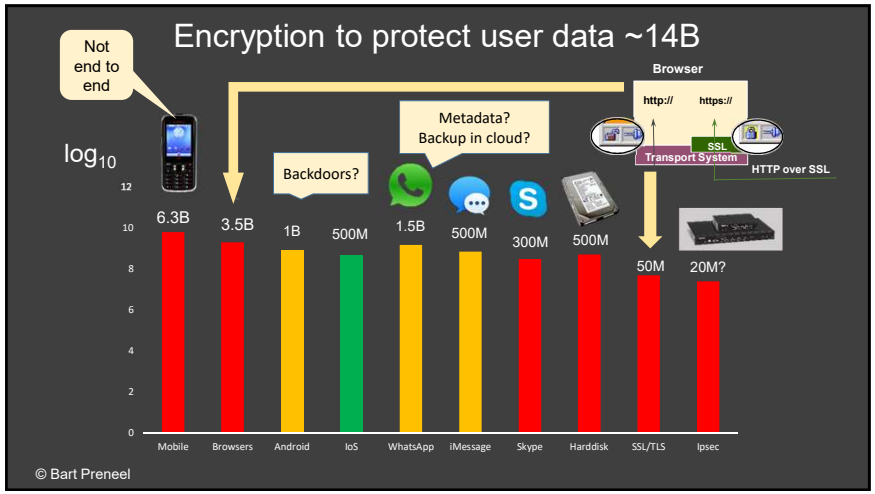
6 Dec. 2018


Christopher Wray, March 5, 2019: we "cannot have a stable endstate where there is entirely unfettered space beyond the reach of law enforcement."


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)
SECTION SUPPORTERS
HUAWEI
ADVERTISING
FOR A BETTER CONNECTED EUROPE

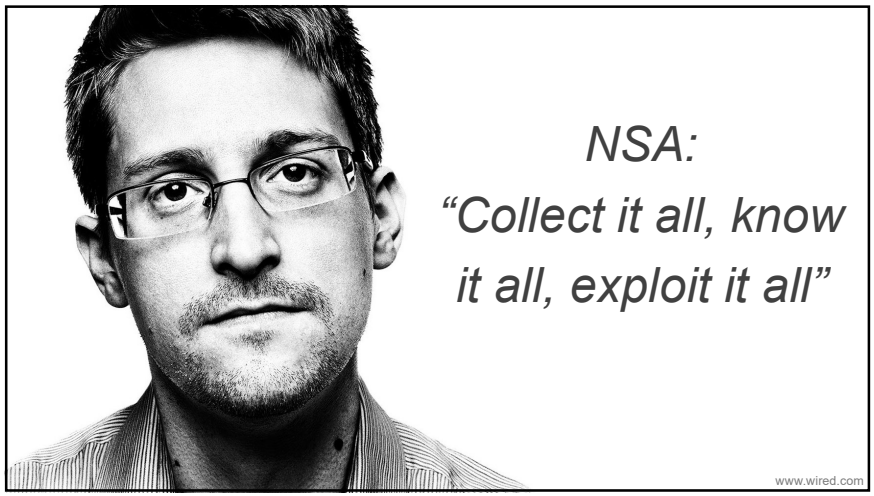

Which access is needed?
Communications: voice
• telephony: phone or cell tower
• VOIP
Communications: data
• messages
• meta data
Stored data
• cloud
• media (USB)
Devices
• confiscated
• remotely


Encryption to protect industry ~18.3B
log10
12
10
8
6
4
2
0
6.2B
6B
3B
2.4B
250M
200M
200M
37M
Banking
Access
Updates
Content
Game cons.
eID/passp.
Access Reader
EMV Term
© Bart Preneel


Encryption to protect user data ~14B
Not end to end
Browser
http://
https://
SSL
Transport System
HTTP over SSL
Metadata? Backup in cloud?
Backdoors?
log10
12
10
8
6
4
2
0
6.3B
3.5B
1B
500M
1.5B
500M
300M
500M
50M
20M?
Mobile
Browsers
Android
IoS
WhatsApp
iMessage
Skype
Harddisk
SSL/TLS
Ipsec
© Bart Preneel


Do we have secure communications in 2018?
09:41
A breach at any point in SS7 could potentially give a hacker access to any system user


Trend 7
Nation state hacking and cyber arms proliferation


NSA:
"Collect it all, know it all, exploit it all"
www.wired.com

(Part of) government seems to prefer offense over defense

How many 0-days do the NSA, FBI, and CIA have?

Are they revealed to vendors?

If so when?

0-days stolen by Shadow brokers from Equation Group resulting in Wannacry, Petya, not-Petya

US$ 250 M loss for Maersk

EU COM(2017)608

towards an effective and genuine Security Union

encryption will not be “prohibited, limited or weakened”

“measures should not have an impact on a larger or indiscriminate number of people”.

more collaboration

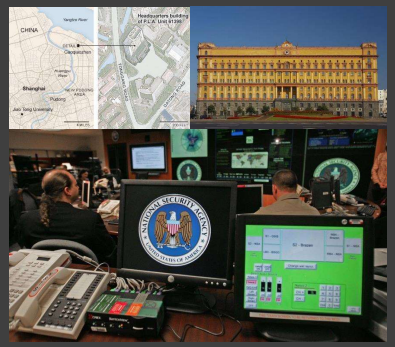
96 (or 24?) extra people for Europol

encourages the countries to collaborate in developing a toolbox with alternative investigation techniques

Key search machines? 0-days? Malware

Sed quis ipse custodiet custodes?

But who shall watch over the guards?



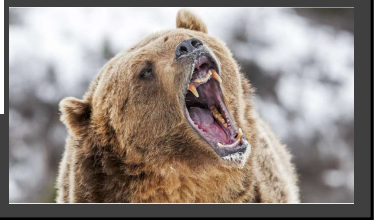
Just a recent example

MOTHERBOARD

RUSSIAN HACKERS | By Joseph Cox | Nov 9 2018, 10:04pm

The US Military Just Publicly Dumped Russian Government Malware Online

US Cyber Command, a part of the military tasked with hacking and cybersecurity operations, says it is releasing malware samples as an information sharing effort.



Architecture is politics [Mitch Kaipor'93]

Avoid single point of trust that becomes single point of failure

Regulatory Initiatives

California: Senate Bill 287 (Sept '18):

by Jan. 2020, any internet connected device must be equipped with reasonable security features, designed to prevent unauthorized access, modification or information disclosure

UK: Code of practice for consumer IoT security (Oct.'18)

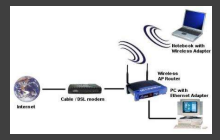
13 guidelines

EU cybersecurity Act (draft, Jun'18):

voluntary EU-wide certification driven by member states

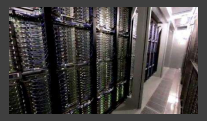
Changing role of cryptography

communications



storage

during computation

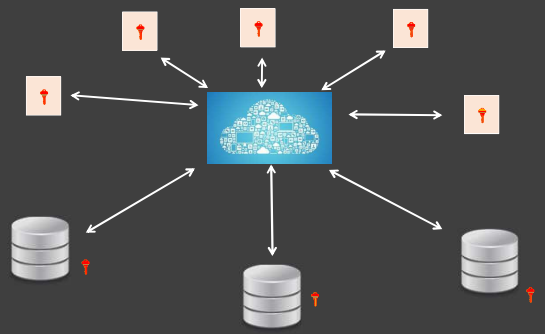


C. Bonte, E. Makri, A. Ardeshirdavani, J. Simm, Y. Moreau, F. Vercauteren, Towards Practical Privacy-Preserving Genome-Wide Association Study, 2017

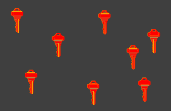
From Big Data to small local data

Data stays with users

From Big Data to encrypted data MPC (Multi-Party Computation)



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

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

We can take back control of our data

Industrial policy
Targeted surveillance
European sovereignty and values

Bart Preneel, COSIC, an imec lab at 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

68

More information (1)

Other presentations

- B. Preneel, IoT: regulatory approaches in the EU, December 2018, http://homes.esat.kuleuven.be/~preneel/preneel_legal_eu_nov18_v1.pdf
- B. Preneel, Lawful Interception and the Never-Ending Crypto Wars, October 2018, http://homes.esat.kuleuven.be/~preneel/preneel_crypto_wars_gba_v1.pdf
- Langere versie van deze presentatie: B. Preneel: Challenges for (Embedded) Security and Privacy, http://homes.esat.kuleuven.be/preneel_future_security_escar_nov18v1.pdf
- Korte versie van deze presentatie: https://www.youtube.com/watch?v=uYk6yN9eNfc

Documents and Links

https://www.enisa.europa.eu/
https://www.eff.org/nsa-spying/nsadocs
https://cjfe.org/snowden
http://www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20130923CDT71796#menuzone

More information (2)

Books

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

Whitfield Diffie, Susan Landau, Privacy on the Line. The Politics of Wiretapping and Encryption. Updated And Expanded Edition, MIT Press, 2010

Susan Landau, Surveillance or Security? The Risks Posed by New Wiretapping Technologies. MIT Press, 2013

Susan Landau, Listening In: Cybersecurity in an Insecure Age, Yale University Press, 2017

US National Academies, Decrypting the Encryption Debate, 2018, https://www.nap.edu/read/25010/chapter/1

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 (3)

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/