

# The Future of Security and Privacy

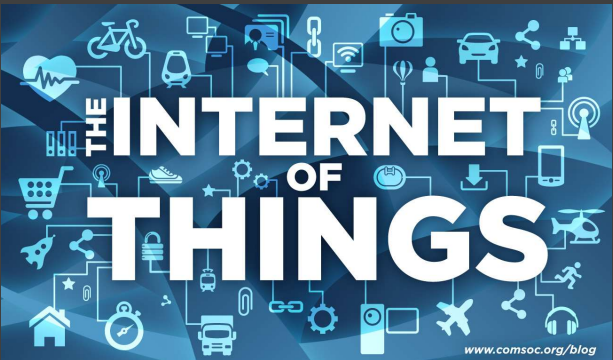
Bart Preneel  
COSIC KU Leuven and imec





## Trend 1

IoT makes IT more intrusive



www.comsoc.org/blog

## IoT markets (source: Intel)

### A SPECTRUM OF SMART STUFF


The IoT contains an enormous variety of connected objects, including:

**TINY STUFF**  
**SMART DUST**

Computers smaller than a grain of sand can be sprayed or injected almost anywhere -- to measure chemicals in the soil, or to diagnose problems in the human body.

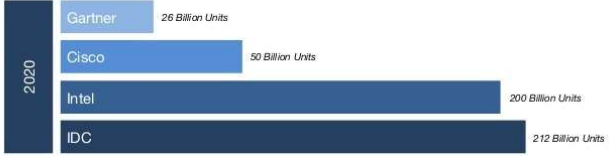
**ENORMOUS STUFF**  
**AN ENTIRE CITY**

Fixed and mobile sensors dispersed throughout the city of Dublin are already creating a real-time picture of what's happening, and will help the city react quickly in times of crisis.



## How fast will IoT grow?

### BY 2020, HOW MANY DEVICES WILL EXIST?



Source	2020 Projections (Billion Units)
Gartner	26
Cisco	50
Intel	200
IDC	212

Source:  
 [1] <http://www.gartner.com/newsroom/id/2684616>  
 [2] <http://www.intel.com/secure/it/ww/us/en/iot/internet-of-things/infographics/guide-to-iiot.html>  
 [3] <http://www.cisco.com/internet-of-things.html>  
 [4] <http://www.cdnet.com/article/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things/>

**THE INTERNET OF THINGS**

Intrusive  
unavOidable  
sTealthy

www.comsoc.org/blog

### IoT security risks

**DID IRAN HIJACK U.S. DRONE?** CNN  
Follow @Iran on Twitter: @Eombarrett

**NEW THIS MORNING**  
**DICK CHENEY FEARED ASSASSINATION**  
WORDED HEAVY CHENEY WOULD BE TARGETED

Mirai botnet, a DDoS nightmare turning Internet of Things into Botnet of things

### 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 Domains

- Information Security Systems Governance and Risk Management
- Ecosystem Management
- IT Security Architecture
- IT Security Administration
- Identity and Access Management
- IT Security Maintenance
- Physical and Environmental Security
- Intrusion Detection, Prevention and Logging
- Continuity Management
- Security Incident Management

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

## IoT Security and Privacy Recommendations

- Policies:** security and privacy by design, asset management, risk and threat management
- Organisation, people and process:** state of the art solutions, lifecycle support, 3<sup>rd</sup> party relationships, incident management, training and awareness
- Technology:** hardware and software security, AAA, secure communications and storage, monitoring and logging, [...]

ENISA Baseline Security Recommendations for IoT in the context for critical information infrastructures, 2017  
 ENISA Cyber Security and Resilience of smart cars, 2016

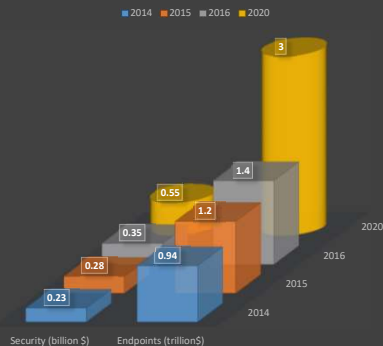
## IoT security risks

- 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>

## 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** (Dec'18):

voluntary EU-wide certification driven by member states

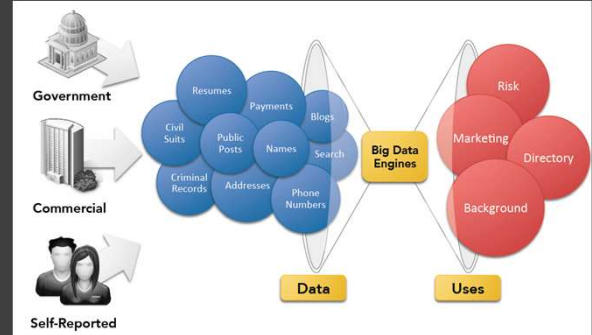






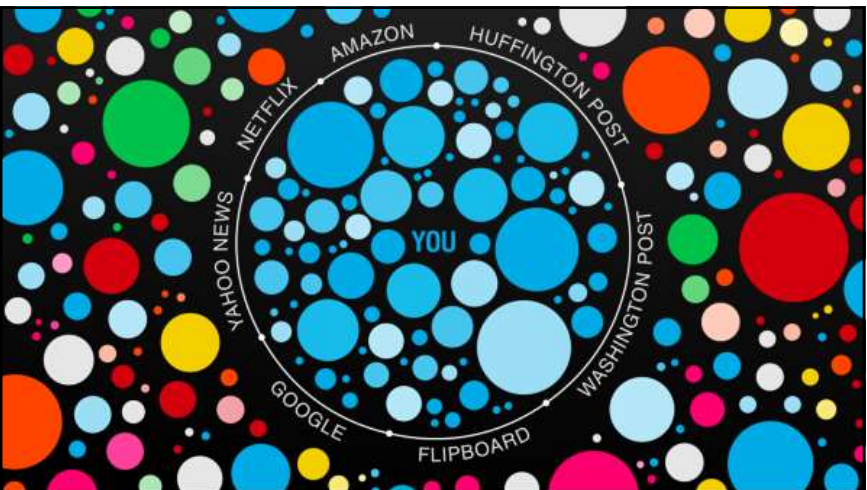
Big data is high **volume**, high **velocity**, and/or high **variety** information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization [Gartner 2010]

### The data supply chain [Jim Adler]



[https://www.usenix.org/sites/default/files/conference/protected-files/adler\\_sec13\\_slides.pdf](https://www.usenix.org/sites/default/files/conference/protected-files/adler_sec13_slides.pdf)

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)

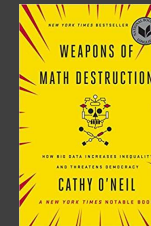
By applying analytics to incident data sets, we can **learn** how the bad guys behave and detect them even faster next time around

## AI and privacy

Leakage of training data

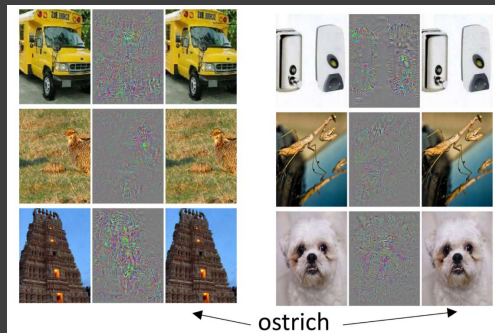
Leakage of models

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







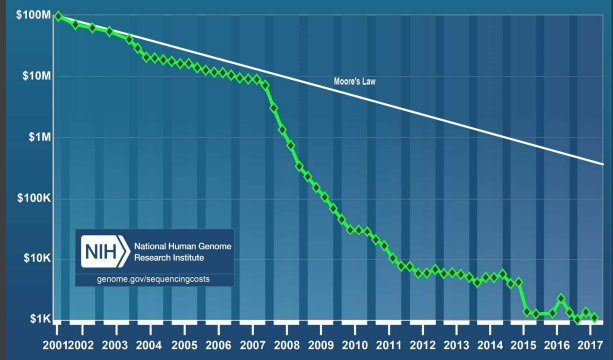
### World's biggest government data breaches

<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)

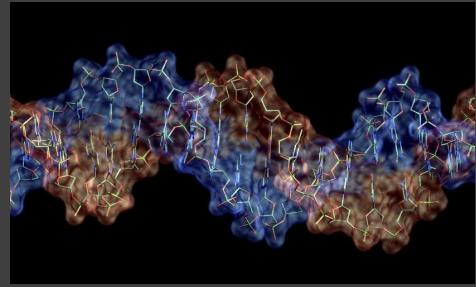
### Cost per Genome



NIH National Human Genome Research Institute  
genome.gov/sequencingcosts

### Your family DNA can be used against you

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



What about insurance companies?

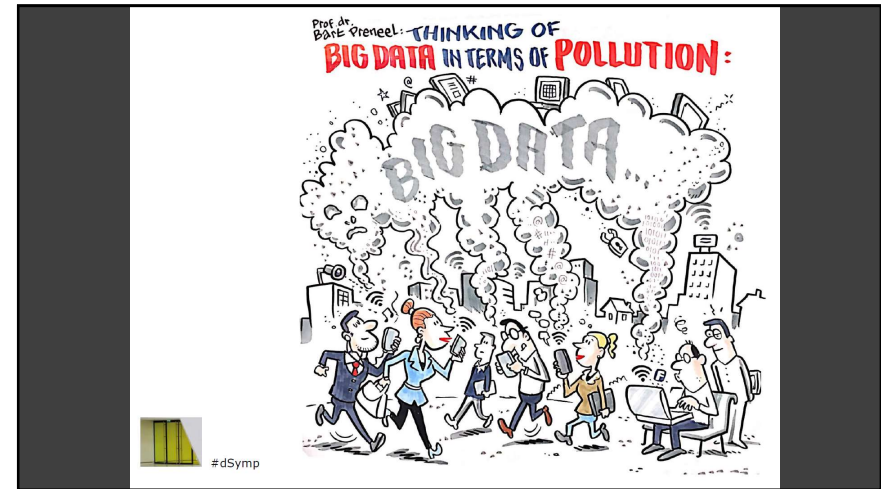
### Privacy is a security property





## 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

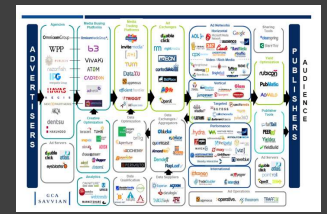


It's the metadata stupid



THE INTERNET OF THINGS

industry



users



government

### 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 Germany 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

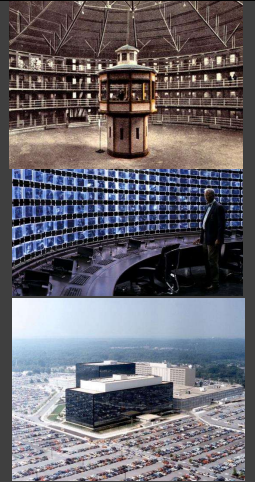
### 1945–1989 East Germany



### Mass surveillance

panopticon  
[Jeremy Bentham, 1791]

discrimination  
fear  
conformism - stifles dissent  
oppression and abuse



### Trend 6



The Crypto Wars will return continue







### 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

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

### Which access is needed?

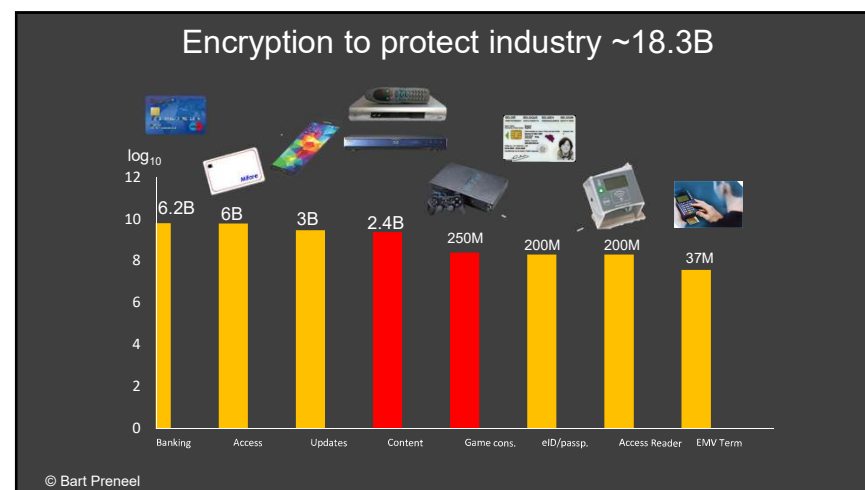
- 
**Communications: voice**
  - telephony: phone or cell tower
  - VOIP
- 
**Communications: data**
  - messages
  - meta data
- 
**Stored data**
  - cloud
  - media (USB)
- 
**Devices**
  - confiscated
  - remotely

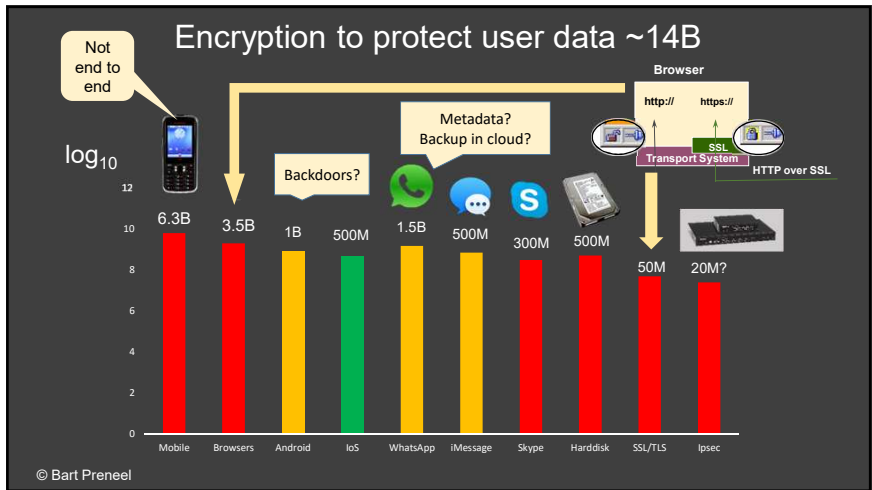
### Do we have secure communications in 2018?



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

### Names and definitions of leaked CIA hacking tools

Posted Mar 9, 2017 by Devin Coldewey

www.techcrunch.com

]HackingTeam[  
Rely on us.




Remote Control System

**THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION**

*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 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



Just a recent example

**MOTHERBOARD**

RUSSIAN HACKERS | By Joseph Cox | Nov 9 2016, 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.




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?



Optimism is a moral duty

*We need a  
Digital Geneva  
Convention*

Microsoft President  
Brad Smith:  
“Nation states are  
hacking civilians in  
peace time”

RSA  
Conference  
2017



Architecture is politics [Mitch Kaipor'93]

Avoid single point of **trust** that becomes single point of **failure**





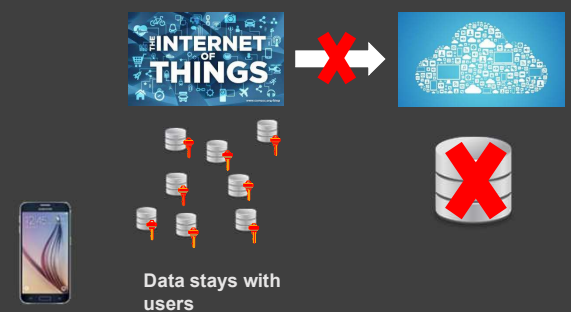
# Changing role of cryptography

communications      storage      during computation

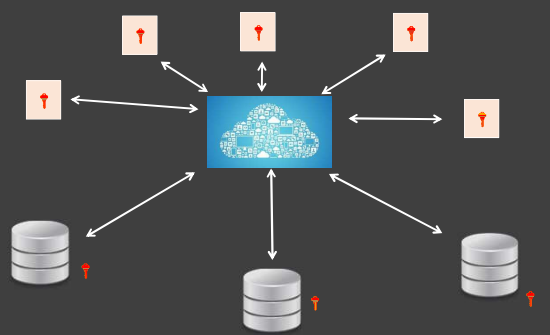


C. Bonte, E. Makri, A. Ardehshirdavani, J. Simm, Y. Moreau, F. Vercauteren, Towards Practical Privacy-Preserving Genome-Wide Association Study, 2017

# From Big Data to small local data



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



# Distributed solutions can work

Root keys of some CAs  
Skype (pre -2011)  
Cryptocurrencies



## Distributed systems with local data

Many services can be provided based on **local** information processing

- advertising
- proximity testing
- set intersection
- road pricing and insurance pricing

Cryptographic building blocks: ZK, OT, PIR, MPC, (s)FHE

Limited deployment:

- massive data collection allows for other uses and more control
- fraud detection may be harder
- lack of understanding and tools

## Centralization for small data

exceptional cases such as genomic analysis

- pseudonyms
- differential privacy
- searching and processing of encrypted data
- strong governance: access control, distributed logging

fascinating research topic but we should

favor local data

not oversell cryptographic solutions

## 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, imec-COSIC KU Leuven

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



75

## 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](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/](http://www.spiegel.de/international/topic/nsa_spying_scandal/)

Very short version of this presentation: <https://www.youtube.com/watch?v=uYk6YN9eNfc>