ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

Information Security and Privacy (COM-402)

Introduction to Privacy

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

Some slides/ideas adapted from: George Danezis, Bart Preneel, Claudia Diaz, Seda Guerses, JP Hubaux, Bryan Ford

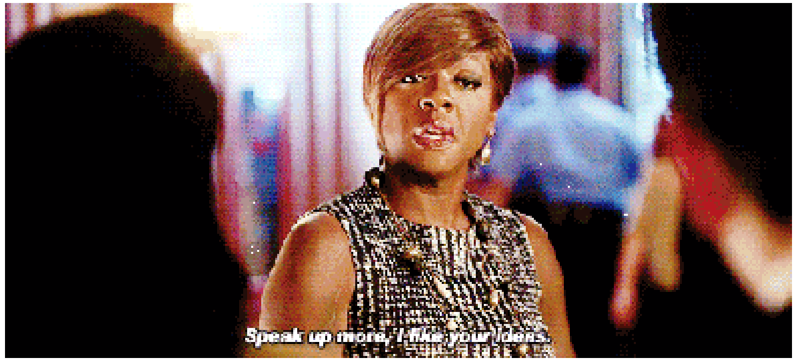
We will be using SpeakUp

- Channel 209902
- http://web.speakup.info/ng/room/5c828712a377bdbd5e9bf025

We will be using SpeakUp

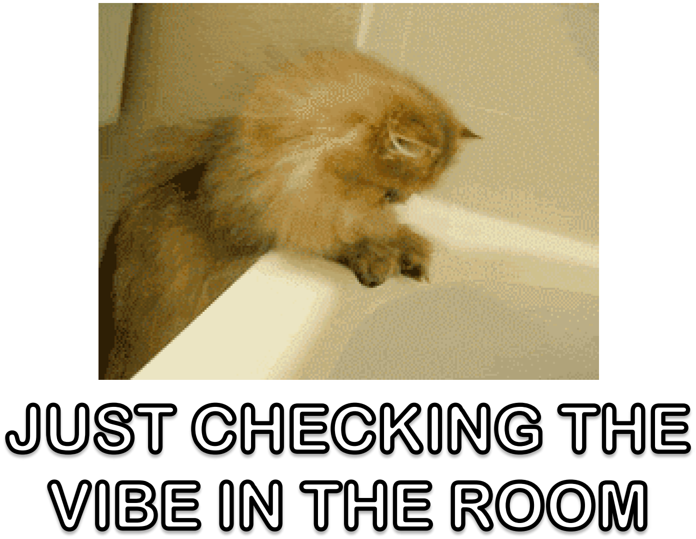
- Channel 209902
- http://web.speakup.info/ng/room/5c828712a377bdbd5e9bf025

And sometimes also speaking up 😱



Warming up!

Privacy is about



A. Hiding information

B. Controlling where information goes

C. Controlling how the information is used

D. Privacy is not important, I have nothing to hide

Warming up!

Privacy in the DIGITAL world is important

A. For individuals

B. Beyond individuals (society)

C. I told you, stop asking: I have nothing to hide

D. Privacy is over (Facebook, Google, etc) why even bother…

Warming up!

Encryption is enough to solve privacy problems

A. Yes

B. No

Goals of the next three lectures

- Understanding that privacy is not only an individual-oriented problem.
  - Privacy is a security property
  - Privacy is key to maintain democratic societies
  - Privacy crosses individuals' boundaries

- There are different conceptions of privacy depending
  - on the privacy paradigm: what does it mean to protect privacy
  - on the adversary model: recognizing and modeling privacy adversaries

- Learning examples of Privacy Enhancing Technologies suitable for each adversary model
  - some of them with Prof. Hubaux
  - more in CS-523!

- Privacy requires protecting information beyond content: The need to protect meta-data
  - Inference attacks based on meta-data

Information Security and Privacy (COM-402)

Part 1: Why we need Privacy

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

Some slides/ideas adapted from: George Danezis, Bart Preneel, Claudia Diaz, Seda Guerses, JP Hubaux, Bryan Ford

The context: Availability of data

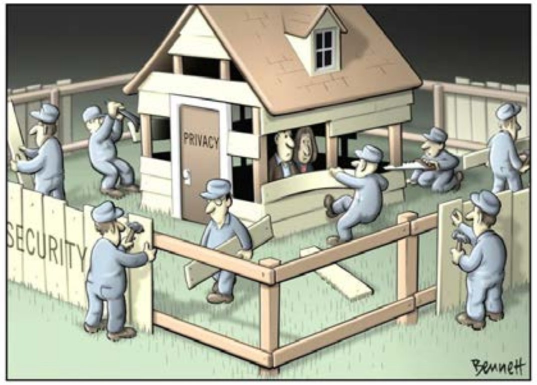
Intelligent data-based applications

- Recommendation systems
  - Movies (Netflix)
  - Products (Amazon)
  - Friends (Social networks)
  - Music (Spotify, iTunes)
- Location based services
  - Friend finders
  - Maps
  - Points of interest
- Health monitoring
- Children/Elderly trackers
- Smart metering
- Intelligent buildings

Individual applications are legitimate

Together they become a cheap
SURVEILLANCE INFRASTRUCTURE

We need privacy!



But what about security!!?!?!?!

What do you think?

Are privacy and security contradictory?

A. Yes

B. No

Common belief:
we need to tradeoff security for privacy!

"For National Security surveillance is good and privacy is bad"

(Surveillance == Security) == True ??

Surveillance may be not **effective**: smart adversaries evade surveillance

criminals use Telegram, Threema, Signal,...
… but we do not!!

Surveillance tools can be **abused**: lack of transparency and safeguards

Snowden revelations: NSA spying on Americans, companies, ...
Spanish Interior ministry spying independentist politicians

Surveillance tools can be **subverted** for crime / terrorism

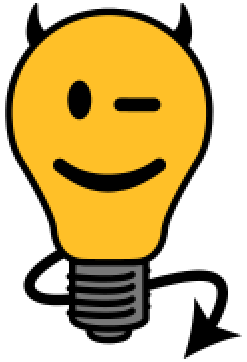
Greek Vodafone scandal (2006): "someone" used the legal interception functionalities (backdoors) to monitor 106 key people: Greek PM, ministers, senior military, diplomats, journalists...

And any system can become a surveillance system

(aka the risk of function creep)

Function creep: expansion of a process or system where data collected for one specific purpose is subsequently used for another unintended or unauthorized purpose.

"We will create a new system to improve X"



"We have this data, why don't we use it for Y"

A recurrent function creep example: identity systems

Aadhaar - India's “optional” Unique Identity identification number scheme

12-digit identity number based on their biometric information and demographic data

>1 billion people stored in the database

Goal “*promoted as providing the poor with an identity*”

It became:

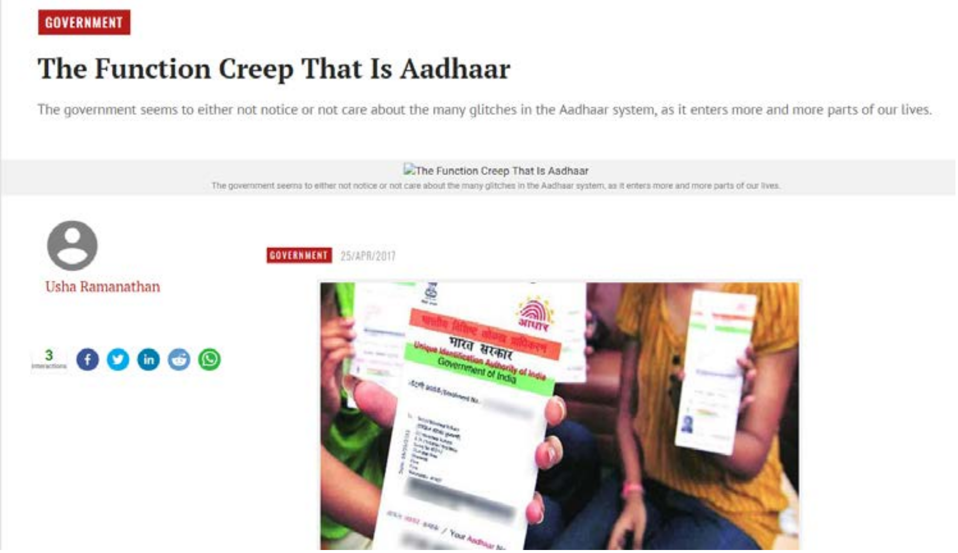
mandatory for benefits system (distribution of food rations and fuel subsidies)

mandatory for buying a SIM card

mandatory for opening a bank account

pay taxes

no education without UID



GOVERNMENT

The Function Creep That Is Aadhaar

The government seems to either not notice or not care about the many glitches in the Aadhaar system, as it enters more and more parts of our lives.

The Function Creep That Is Aadhaar

The government seems to either not notice or not care about the many glitches in the Aadhaar system, as it enters more and more parts of our lives.

Usha Ramanathan

3 interactions

GOVERNMENT 25/APR/2017

Women rescued from prostitution are to put their numbers on the database to get rehabilitated!!

https://privacyinternational.org/feature/2299/initial-analysis-indian-supreme-court-decision-aadhaar

https://thewire.in/government/aadhaar-function-creep-uid

A recurrent function creep example: identity systems

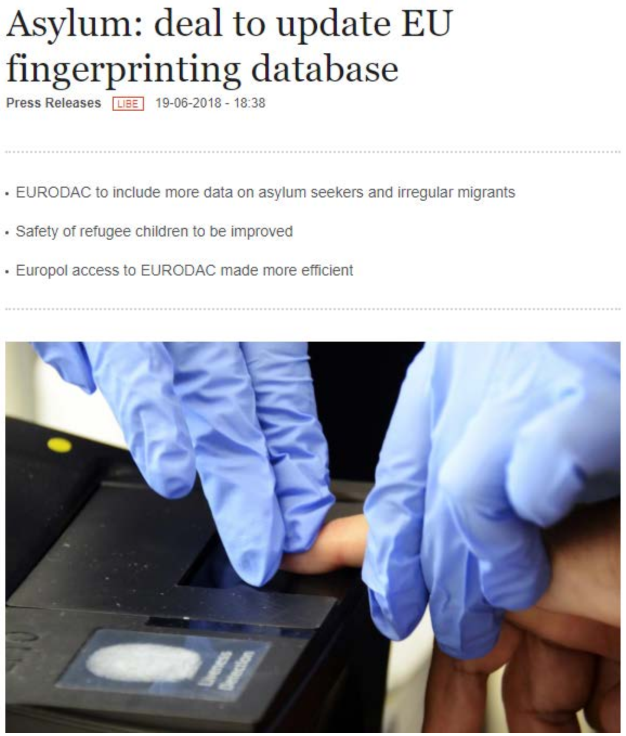
EURODAC - fingerprint database for asylum seekers

Goal: store fingerprints from all people who cross the border into a European country without permission – asylum seekers as well as irregular migrants to help immigration and asylum authorities to better control irregular immigration to the EU, detect secondary movements (migrants moving from the country in which they first arrived to seek protection elsewhere) and facilitate their readmission and return to their countries of origin.

It became:

database for police and public prosecutors, such as Europol.

More data: in addition to fingerprints, the facial images and alphanumerical data (name, ID or passport number) of asylum seekers and irregular migrants will also be stored. Fingerprints from 6 years old.



Asylum: deal to update EU fingerprinting database

Press Releases LIBE 19-06-2018 - 18:38

- EURODAC to include more data on asylum seekers and irregular migrants
- Safety of refugee children to be improved
- Europol access to EURODAC made more efficient

https://www.euractiv.com/section/justice-home-affairs/news/eurodac-fingerprint-database-under-fire-by-human-rights-activists/
http://www.europarl.europa.eu/news/en/press-room/20180618IPR06025/asylum-deal-to-update-eu-fingerprinting-database

Privacy **IS** a security property

For individuals

protection against crime / identity theft, control over one's information, protection against profiling and manipulation.

MAY BECOME

ONE RING TO RULE THEM ALL

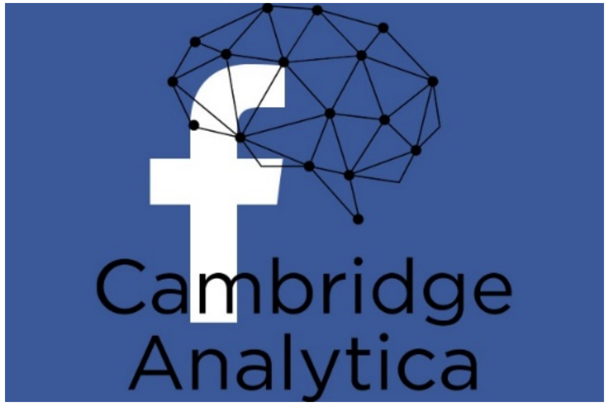
Cambridge Analytica

For companies

protection of trade secrets, business strategy, internal operations, access to patents

For governments / military

protection of national secrets, confidentiality of law enforcement investigations, diplomatic activities, political negotiations



100K users installed CA Facebook App

enabled **COLLECTING PERSONAL DATA** of 87+ million

public profile, page likes, birthday and current city

creation of **PROFILES** of the subjects of the data

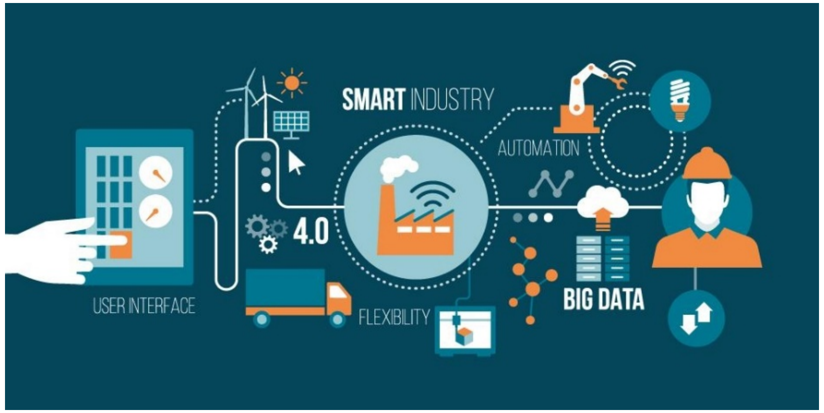
TARGETED ADVERTISEMENTS influenced the US elections

Privacy **IS** a security property

Denying privacy to some is denying privacy to all!!

INFRASTRUCTURE IS SHA

Individuals, Industry, and Governments use the same applications.



Directly
(Cloud-based services, Industry 4.0, Blockchain)

Indirectly
(employers are users)

Privacy **IS** a security property

For individuals

protection against crime / identity theft, control over one’s information, protection against profiling and manipulation.

For companies

protection of trade secrets, business strategy, internal operations, access to patents

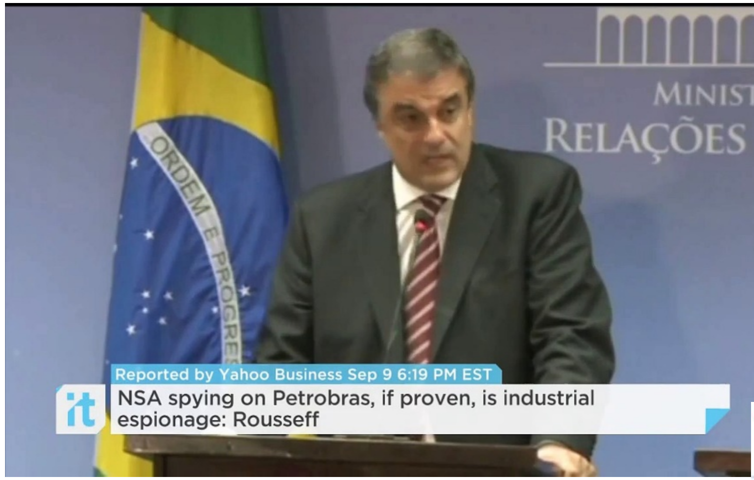
MAY BECOME

ONE RING TO RULE THEM ALL

For governments / military

protection of national secrets, confidentiality of law enforcement investigations, diplomatic activities, political negotiations

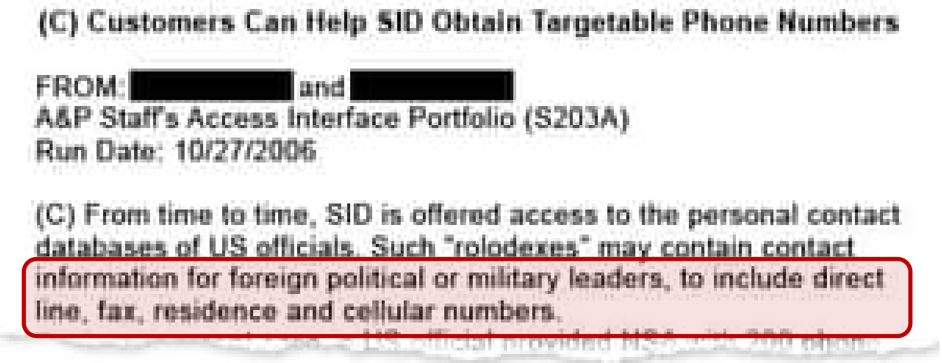
For companies



Reported by Yahoo Business Sep 9 6:19 PM EST

NSA spying on Petrobras, if proven, is industrial espionage: Rousseff

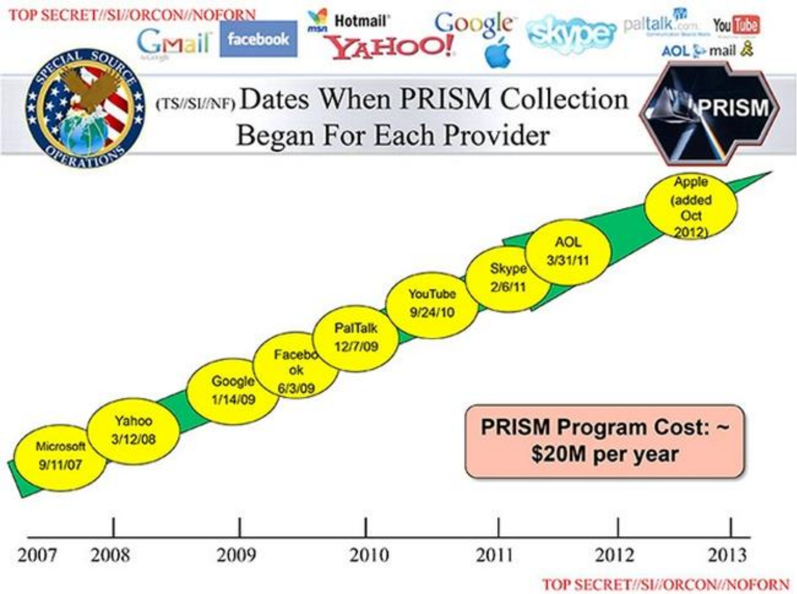
For governments



(C) Customers Can Help SID Obtain Targetable Phone Numbers

FROM: [redacted] and [redacted]
A&P Staff's Access Interface Portfolio (S203A)
Run Date: 10/27/2006

(C) From time to time, SID is offered access to the personal contact databases of US officials. Such "rolodexes" may contain contact information for foreign political or military leaders, to include direct line, fax, residence and cellular numbers.



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

PRISM Program Cost: ~ $20M per year

and Privacy is important for society

Daniel Solove,
Prof. of Law

“Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. **A society without privacy protection would be suffocation**”

Not so much Orwell’s “Big Brother” as Kafka’s “The Trial”:

> “...a bureaucracy with inscrutable purposes that uses people’s information to make important decisions about them, yet denies the people the ability to participate in how their information is used”
>
> “The problems captured by the Kafka metaphor are of a different sort than the problems caused by surveillance. They often do not result in inhibition or chilling. Instead, they are problems of information processing—the storage, use, or analysis of data—rather than information collection.”
>
> “...not only frustrate the individual by creating a sense of helplessness and powerlessness, but they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives.”

MAY
BECOME

ONE RING TO RULE THEM ALL

Takeaways

Digital identities are very powerful

but enable cheap “surveillance”

Privacy is of course is about sensitive individuals’ information

but also needed for safeguard societal and democratic values

Privacy **IS** a security property

the need for a tradeoff is a fallacy