Hochschule Konstanz
Fakultät Informatik

Introduction to IT Security

WIN+AIN

Hanno Langweg

01b Goals and Principles - Privacy

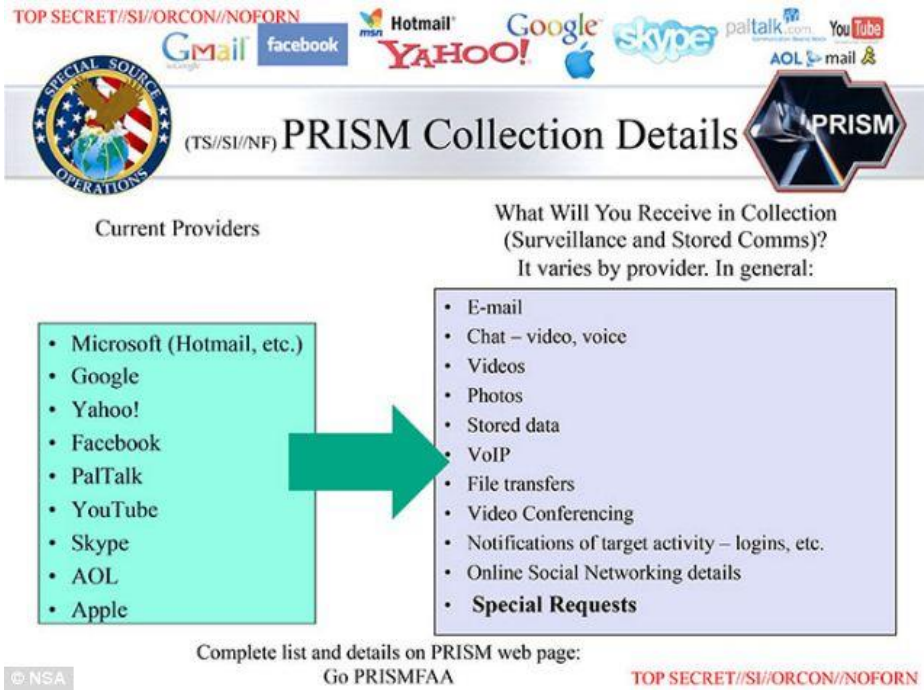
What is privacy?

- **Stakeholders**
  - Users, businesses, regulators, public authorities etc.
- **Context**
  - Usage (e.g. location, application, personal data)
  - Online experience and past privacy violations
  - Cultural background and privacy attitude
  - ...
- **Challenges** of individual protection
  - Requires effort, knowledge, understanding
  - Not directly rewarding
  - Hard to outsource and automate


Why all that fuzz about data privacy?
I've done nothing wrong!
(c) 2017 by Lothar Fritsch

Why privacy?

- Societal perspective
  - Foundation of democracy
  - Freedom of speech
- Individual perspective
  - Free personal development
  - Ownership pf personal data of any kind
- With reduced/no privacy
  - Being afraid of observation and consequences
  - Hesitance to develop personally



https://en.wikipedia.org/wiki/File:PRISM_Collection_Details.jpg
https://de.wikipedia.org/wiki/Elektronische_Gesundheitskarte#/media/File:Elektronische_Gesundheitskarte_2011.svg
https://de.wikipedia.org/wiki/ELENA-Verfahren#/media/File:Elena-schriftzug.svg
https://www.google.de

Privacy protection

- Data protection (by law)
- Privacy by design
- Technical data protection

"Data protection" (Datenschutz)

- Measures for the **protection of** stored and transferred **personal data** against manipulation or misuse
  BDSG in place in Germany since 1978 (+updates)
- Originally for protection of **citizens** against **governmental** institutions
- Businesses regulated with regard to some aspects of data protection (e.g. telecommunications, healthcare)
- **Increased need for regulation** owing to growing use of IT (+sufficient funding for implementation)

Data protection principles

- **Data minimisation**
  - The service should be offered with a **minimum** of needed data
- **Information** of data subject
  - The person whose data is being stored, **should know** what has been stored
- Acceptance with **consent**
  - The data subject is to be **asked in advance**

EU Privacy Directives

- Data Protection Directive (Directive 95/46/EC)
  - Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive on Privacy and Electronic Communications (Directive 2002/58)
  - Directive on Privacy and Electronic Communications with regard to data retention, spam and cookies
- Directives need to be implemented by national laws

https://europa.eu/european-union/sites/europaeu/files/docs/body/flag_yellow_low.jpg

EU General Data Protection Regulation

- EU regulation 2016/679 on protection of natural persons with regard to the processing of personal data
  - **Explicit** vs. assumed **consent** (Art. 6-8)
  - **Right to be forgotten** (demand that personal data be deleted if there are no grounds it be kept; art. 12,14,17)
  - **Easier access +** transfer to different provider (Art. 20)
  - **Privacy by design** and **by default** (Art. 25)
  - **Notification** about **data breaches** (Art. 33,34)
  - **Higher fines**, ≤ max(20 Mio. €, 4% turnover) (Art. 83)
- Effective since 2018, does not need to be implemented by member states
  (regulation vs. directive)

EU GDPR: Scope

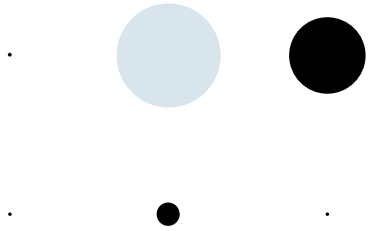
- **Processing of personal data** at least partly by automated means or as part of a filing system
  - Exemption for personal activity of natural persons
  - Exemption for authorities addressing criminal offences
- Establishment of controller/**processor in EU**
  - Even if processing takes place outside of EU
- **Data subject in the EU**
  - Even if processing takes place outside of EU, provided that goods/services are offered (regardless of payment) or behaviour is monitored

EU GDPR: Personal data

- Personal data: any information relating to an **identified** or **identifiable** natural person ("data subject")
  - Companies have no privacy
- Identifiable directly or indirectly by reference e.g.
  - Name
  - ID number
  - Location data
  - Online identifier
  - Physical, physiological, genetic, mental, economic, social identify

EU GDPR: Processing

- Processing: **any operation** on personal data
  - Collection
  - Recording, organisation, structuring, storage
  - Adaptation, alteration
  - Retrieval, disclosure
  - Restriction, erasure, destruction



EU GDPR: Privacy by design

- Art. 25 Data protection by design and by default
  - Implement measures (e.g. pseudonymisation) for **data minimisation**
  - Ensure that **by default** only necessary personal data is processed
  - Amount, storage period, accessibility

- Limited by state of the art, cost of implementation, context/purpose of processing

Privacy by design **principles**

1. **Proactive** not Reactive; **Preventative** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** into Design
4. Full Functionality – **Positive-Sum**, not Zero-Sum
5. End-to-End Security – **Full Lifecycle Protection**
6. **Visibility** and **Transparency** – Keep it **Open**
7. Respect for User Privacy – Keep it **User-Centric**

- https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Summary

- Privacy
  - Data minimisation, information, consent
  - EU GDPR
  - Privacy by design