TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

# Betriebssysteme und ***Sicherheit***

Thorsten Strufe

*Modul 1: Einleitung*

*Disclaimer: Inhalte übernommen aus Materialien von **Winfried Kühnhauser**, Günter Schäfer, Mitarbeitern des Lehrstuhls*

Dresden, WS 16/17

# Überblick

Wer sind wir und wofür interessieren wir uns

Überblick des Sicherheitsteils von BuS

Einige Grundlagen zur IT-Sicherheit

# Wer wir sind

Professur „Datenschutz und Datensicherheit“

Für diese Vorlesung:


- Thorsten Strufe
  - INF 3070 / +49 351 463 38247
  - thorsten.strufe [at] tu-dresden.de


https://dud.inf.tu-dresden.de

# Wofür wir uns interessieren..

- Können wir Überwachung verhindern und Datenschutz sichern?
- Wie können Kommunikationsinfrastrukturen gesichert werden?
- (Wie) kann vertraulich kommuniziert werden?
- Kann es konkurrenzfähige Online-Dienste ohne Datenschutz-Probleme geben?
  - *Social Networking?*
  - *Recommendation Systems?*
  - *Data Mining auf privaten Daten (medizinisch!)?*
- Wie können wir solche Systeme entwickeln – und überhaupt deren Kontext verstehen?
- Always on: wie können wir das nächste große Data-Loss-Desaster vermeiden?

[1] [2] [3] [4]

TECHNISCHE UNIVERSITÄT DRESDEN

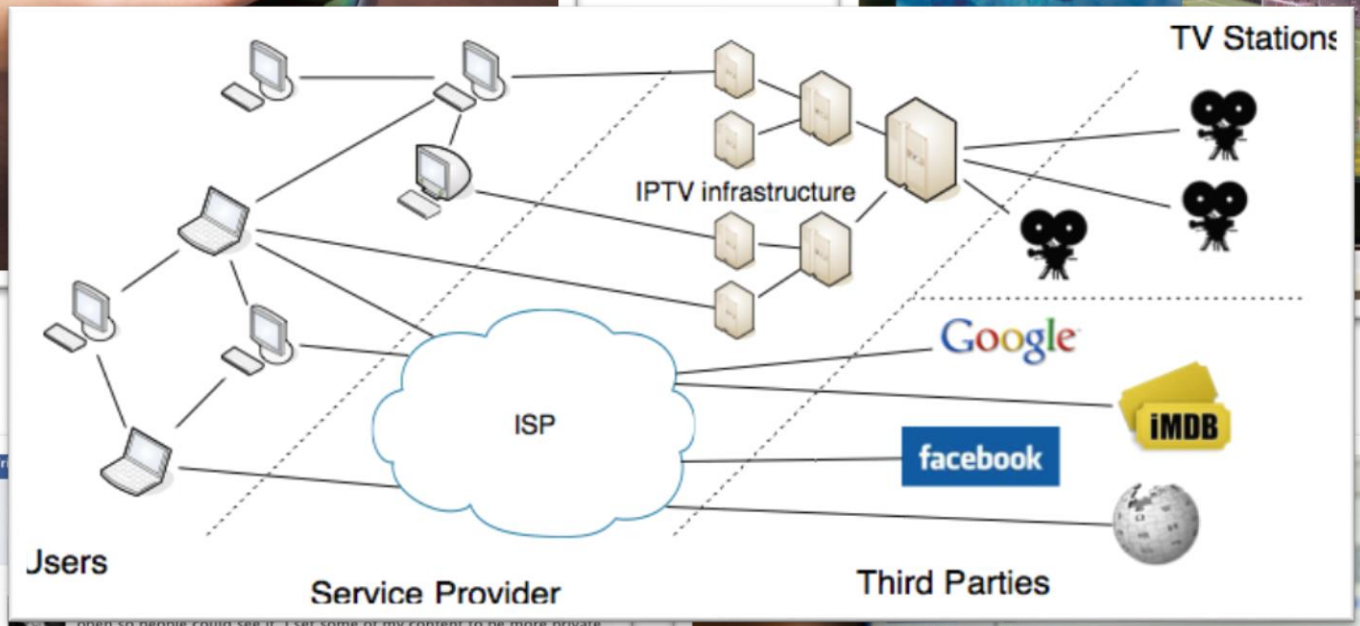
# Aber wo ist das Problem?




TECHNISCHE UNIVERSITÄT DRESDEN

# ...goes online.



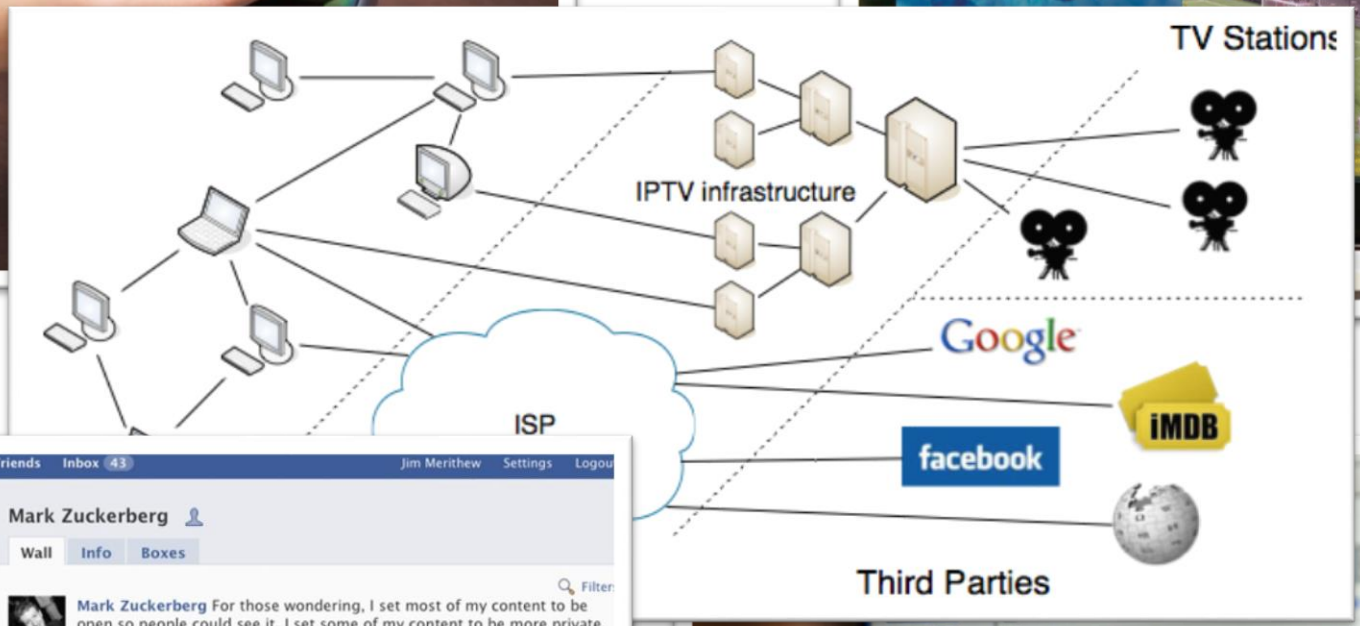




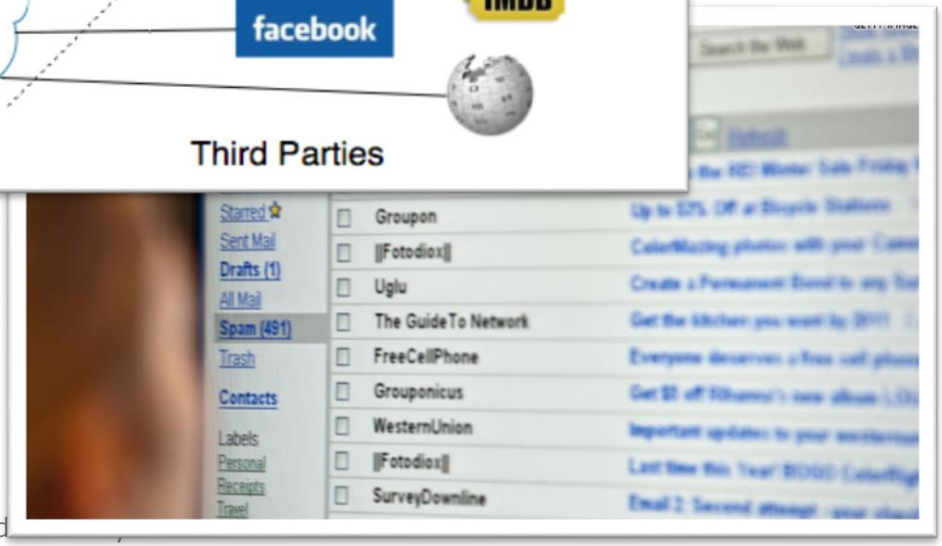
TECHNISCHE UNIVERSITÄT DRESDEN

# ...goes online.









# Datenschutz in Social Media

## Internet-Nutzung konzentriert auf 6 Unternehmen

- Personalisierung führt zur Attraktivität
- Datensparsamkeitsgebot steht Geschäftsmodell entgegen

## Konvergenz der Kommunikation und Meinungsäußerung

- Facebook integrierte Kommunikationsplattform mit 1.6Mrd. Benutzern
- Google, g+: 350 Mio Benutzer
- Eindeutige Identifikation

## Zunahme mobiler Benutzung

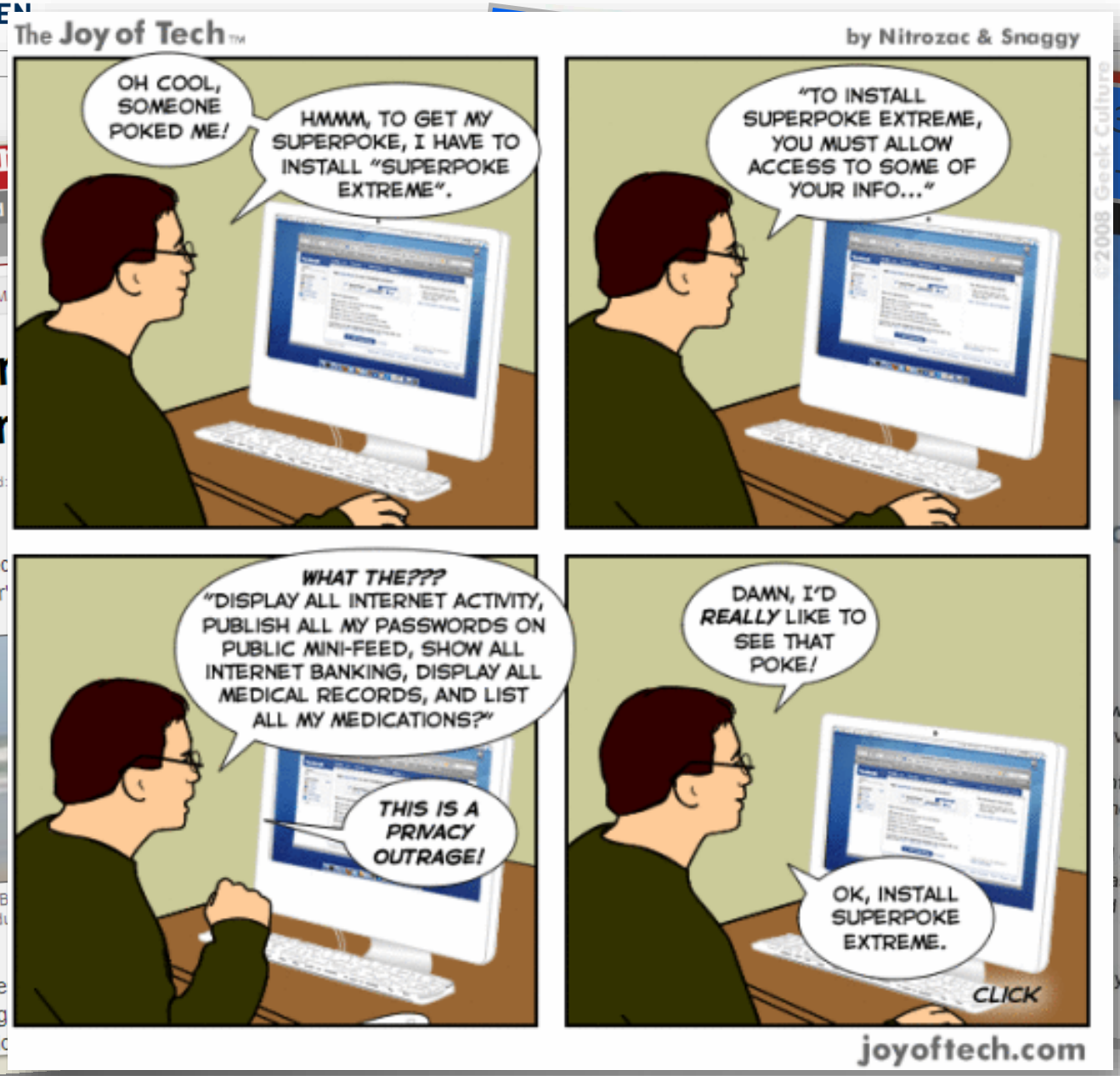
- Identifiziert, jederzeit zu lokalisieren
- Konfiguration schwieriger

TOP 10 WEB BRANDS BY UNIQUE AUDIENCE (U.S. TOTAL)

| Rank | Brand | Unique Audience | Time Per |
|---|---|---|---|
| 1 | Google | 170,629,000 | 2:05:30 |
| 2 | Facebook | 145,297,000 | 6:41:44 |
| 3 | Yahoo! | 135,100,000 | 2:32:52 |
| 4 | YouTube | 124,073,000 | 1:57:28 |
| 5 | MSN/WindowsLive/Bing | 123,133,000 | 1:15:40 |
| 6 | Microsoft | 86,986,000 | 0:47:26 |
| 7 | Amazon | 84,735,000 | 0:38:14 |
| 8 | AOL Media Network | 83,826,000 | 2:09:36 |
| 9 | Wikipedia | 76,310,000 | 0:24:25 |
| 10 | Ask Network | 69,447,000 | 0:12:30 |

**[Nielsen]**

# ...with calculated side effects...



# Beobacht- und Ableitbare Information

## Explizit

- Created content
- Comments
- Structural interaction (contacts, likes)

## „Metadaten“

- ***Session artifacts*** (time of actions)
- ***interest*** (retrieved profiles; membership in groups/participation in discussions)
- ***influence***

Clickstreams, ad preferences

***communication*** (end points, type, intensity, frequency, extent)

***location*** (IP; shared; gps coordinates)

## Abgeleitet

- Preference– and
- Image recognition models

## Extern verkettet

- Observation in ad networks

# Akteure bei Social Networking Services

## Subscribers

## Provider


## Partner

Advertisers

zynga Extending Partner

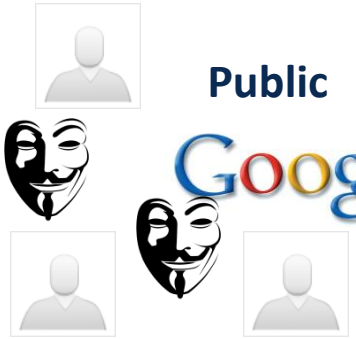
## Cloud/CDN Provider

CLOUDFLARE

Akamai

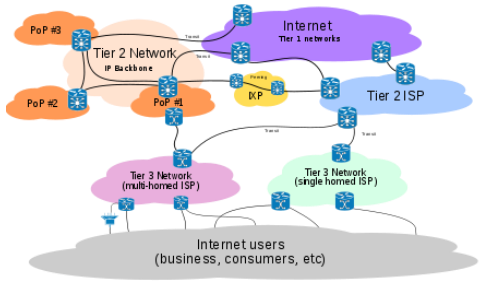
## Institutions


## Public

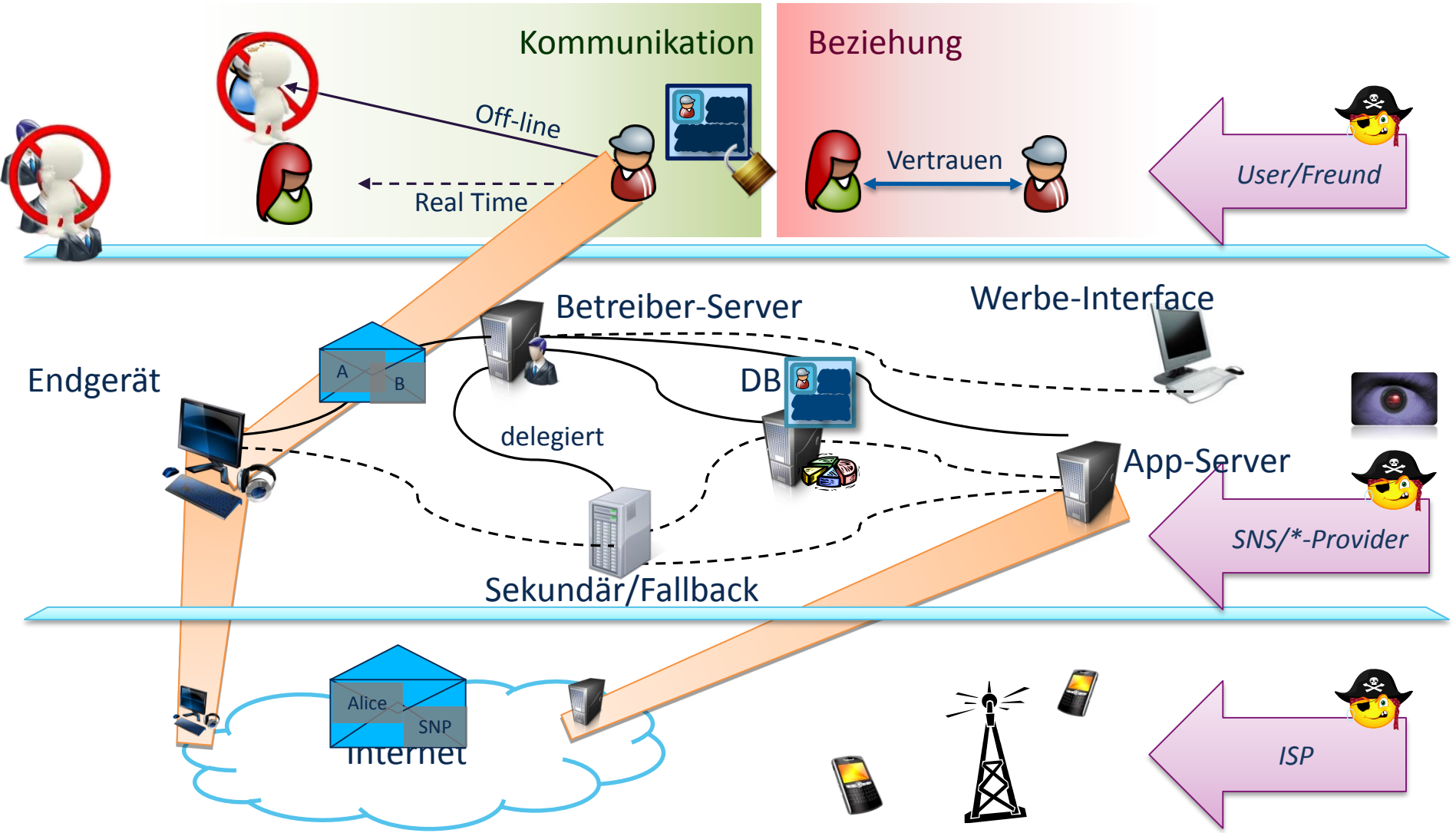


Google

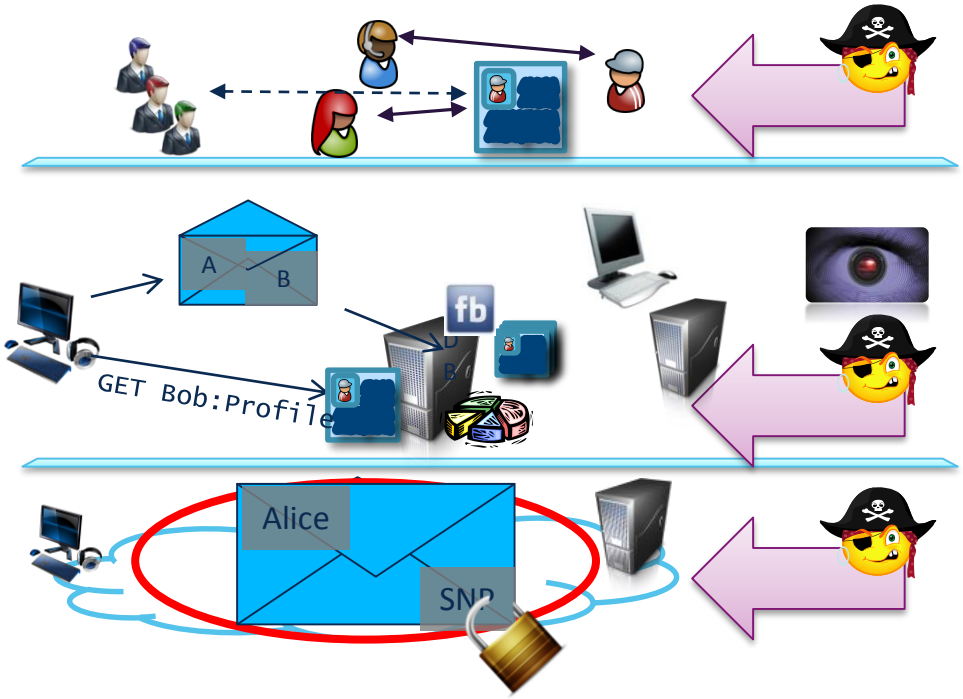
## Network Provider



# Schichtenmodell und Angreifer



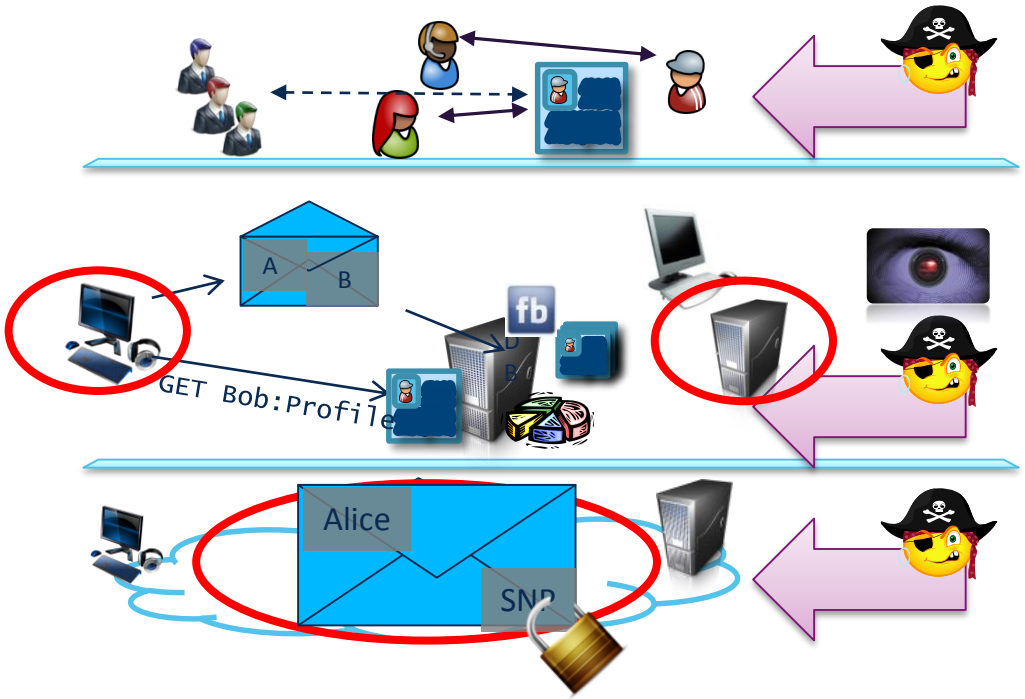
- ***Netzwerk-Sicherheit***
  - Schutz der übertragenen Daten
  - Schutz des Netzwerkes



# DuD Forschungscluster

- ***Netzwerk-Sicherheit***
  - Schutz der übertragenen Daten
  - Schutz des Netzwerkes

- ***Privacy-enhancing Techs***
  - Netzwerk-Anonymisierung
  - Anonymisierte Dienste



# Dezentralisierung gegen Zensur

## *Vollständige Verteilung*

- *Dezentralisiere Dienste*
- *Nur explizites Vertrauen*


## System-Klassen

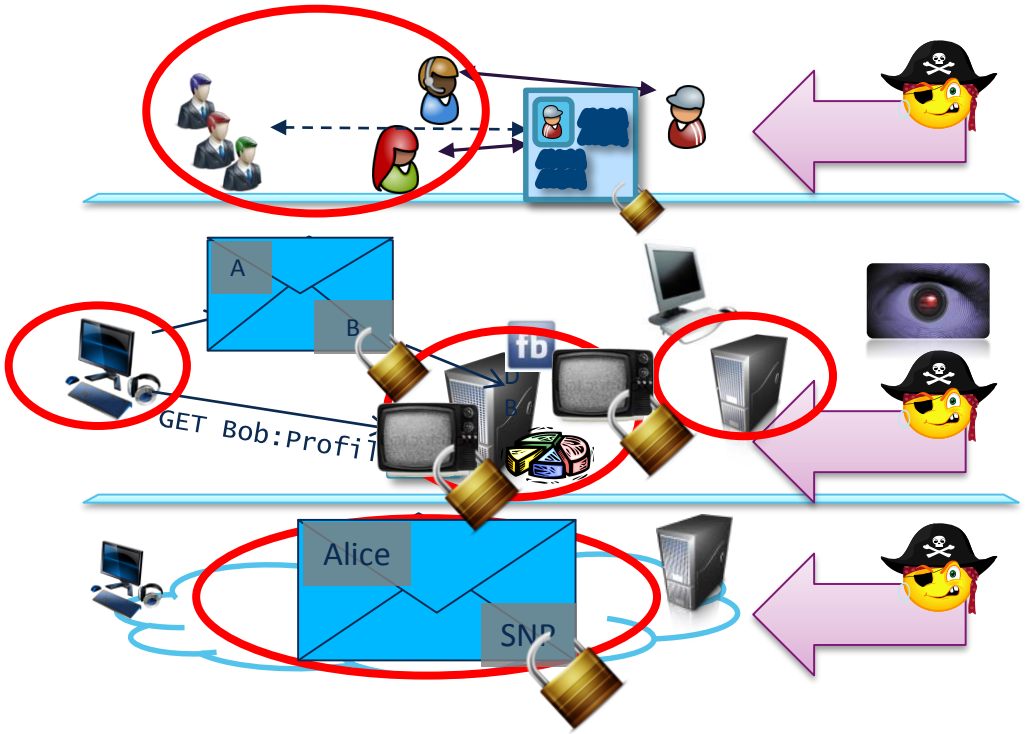
- Federated SNS
- P2P / D-OSN
- Social Overlays and Darknets

diaspora*

PeerSoN

# Solution Classes / Research Clusters

- ***Netzwerk-Sicherheit***
  - Protecting the transmission
  - Protecting the network
- ***User/System Understanding***
  - Bewertung der Privatheit
  - Intention recognition
  - Unterstütznug & Bedienbarkeit
- ***Privacy-enhancing Techs***
  - Netzwerk-Anonymisierung
  - Anonymisierte Dienste
- ***Schutz der Inhalte***
  - Secure Computation



# DuD in der Lehre

| FS | Wintersemester | FS | Sommersemester |
|---|---|---|---|
| 1 | | 2 | Informations- und Kodierungstheorie |
| 3 | Betriebssysteme & Sicherheit | 4 | *Forschungslinie* |
| 5 | **BAS-4** *SaC-1* / Kanalkodierung | 6 | **BAS-4** *SaC-2/Crypto* |
| 7 | | 8 | **Vert-4,** ANW/AFT, Beleg *SaC-2/Crypto/Resilient Networking* |
| 9 | **Vert-4**, ANW/AFT *FB-Mining*/Kanalkodierung | 10 | Diplom/Masterarbeit |

**BAS-4**:

- **S**ecurity **& C**rypto 1
- **S&C** 2 (PETs)
- Crypto
- Kanalkodierung

**Vert-4:**

- S&C 1&2
- Crypto
- Resilient Networking
- Mining Facebook
- Kanalkodierung

**B-510/B-520**:

- **S**ecurity **& C**rypto 1
- **S&C 2** (PETs)
- Kanalkodierung
- Seminare/Praktika

| FS | Wintersemester | FS | Sommersemester |
|---|---|---|---|
| B1 | | B2 | Informations- und Kodierungstheorie |
| B3 | | B4 | |
| B5 | **B-510** Betriebssysteme & Sicherheit | B6 | **B-520** Bachelor-Thesis |
| M1 | **BAS-4** | M2 | **BAS-4, VERT-4, ANW** |
| M3 | **Vert-4, FPA** | M4 | Master-Thesis |

Aber nun zu

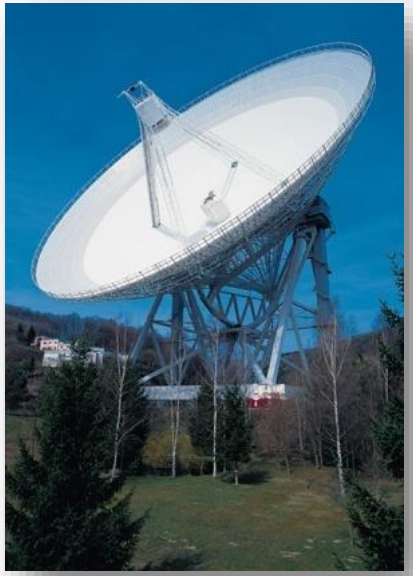
Betriebssysteme und Sicherheit!

# Risikoszenarien

## Informationssysteme

- Sicherheit
- Korrektheit
- Verfügbarkeit
- Echtzeitfähigkeit
- Skalierbarkeit
- Offenheit

# Kommunikationssysteme

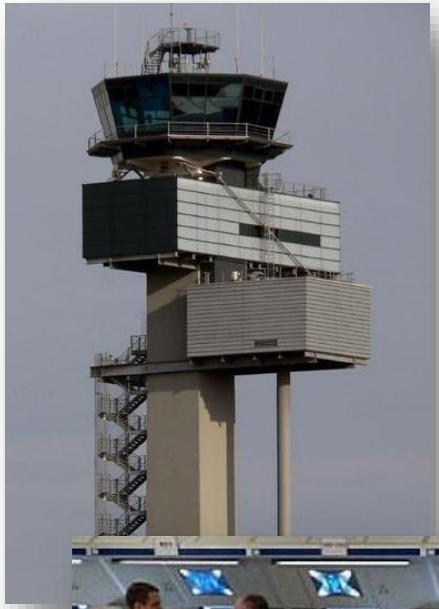



- Sicherheit
- Korrektheit
- Verfügbarkeit
- Echtzeitfähigkeit
- Skalierbarkeit
- Offenheit

# Energiemanagement

- Sicherheit
- Korrektheit
- Verfügbarkeit
- Echtzeitfähigkeit
- Skalierbarkeit
- Offenheit

# Verkehrsmanagement




- Sicherheit
- Korrektheit
- Verfügbarkeit
- Echtzeitfähigkeit
- Skalierbarkeit
- Offenheit

# Spektrum sicherer IT-Anwendungen

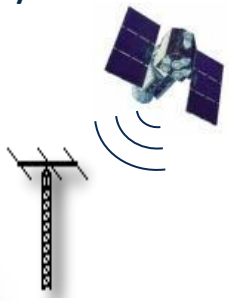
Sichere IT-Systeme

SmartCards

Informationssysteme

Infrastruktur-management

Kommunikations-systeme



# Safety und Security

## (Funktions-)Sicherheit (*safety*)

Ziel: Schutz vor Schäden durch Fehlfunktionen von IT-Systemen

technisches Versagen; Alterung, Stromausfall, Schmutz

menschliches Versagen; Dummheit, mangelnde Ausbildung, Fahrlässigkeit

höhere Gewalt; Feuer, Blitzschlag, Erdbeben

→ Schutz vor einem IT-System, bedroht durch Fehler, Ausfälle

## (IT-)Sicherheit (*security*)

Ziel: Schutz vor Schäden durch zielgerichtete Angriffe auf IT-Systeme

Wirtschaftsspionage, Betrug, Erpressung, Kundendaten aus Lichtenstein …

Terrorismus, Vandalismus

→ Schutz des IT-Systems, bedroht durch strategische Angreifer

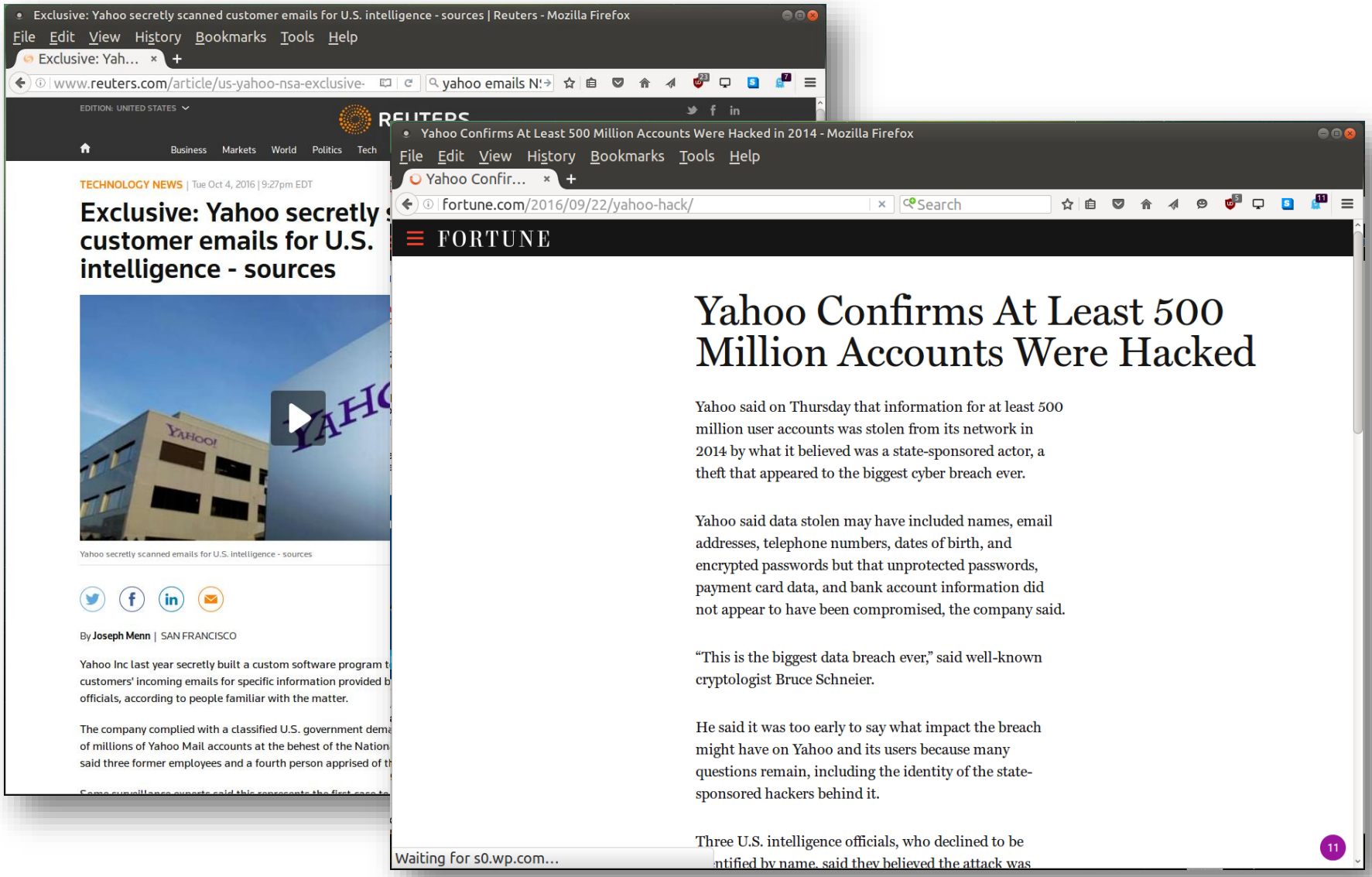
# Und was war das mit Datenschutz?

***Sicherheit*** schützt Daten (und Services/Systeme)

***Privacy*** ist der Schutz von Individuen ***vor*** Daten

- Kontrolle über Benutzung der Daten durch andere (Institutionen)
- Geben und entziehen von Einwilligung zur Nutzung
- Setzt voraus:
  - Transparenz von Datensammlung und -verarbeitung
  - … mögliche Auswirkungen (***informierte*** Einwilligung)
  - Datenminimierung *(hilft auch für die Sicherheit!)*

# Wealth of Data: „Datenreichtum“



# „Anyways, nobody cares, we'll be rich!"

Advocate to pay $5.5 million over data breach: record HIPAA settlement - Chicago Tribune - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Advocate to p... ×

www.chicagotribune.com/business/ct-advocate

SECTIONS SEARCH Chicago Tribune

TUESDAY SEP. 27, 2016 BREAKING SPORTS TRENDING OPINION SUBURBS ENTERTAIN

Advocate to pay $5.5 m
data breach: record HIP
settlement


Advocate Condell Medical Center in Libertyville. (Rick Kambic / Pioneer Press)

By Lisa Schencker · Contact Reporter
Chicago Tribune

AUGUST 5, 2016, 7:20 AM

Report: Verizon wants $1 billion discount after Yahoo privacy concerns | TechCrunch - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Report: Verizo... ×

https://techcrunch.com/2016/10/06/report-verizon-wants-

Got a tip? Let us know. Follow Us

News Video Events CrunchBase Message Us Search

STARTUP BATTLEFIELD Just one day left to apply to the Startup Battlefield at Disrupt London! Apply now!

security
acquisition
Yahoo
Verizon
Finance
Popular Posts

## Report: Verizon wants $1 billion discount after Yahoo privacy concerns

Posted Oct 6, 2016 by Katie Roof (@Katie_Roof), Kate Conger (@kateconger)

Next Story


It's bad news for Yahoo. The company is in the midst of finalizing its sale to Verizon, but recent revelations about hacking and spying may be costing them a pretty penny.

A story from the New York Post alleges that Verizon is now asking Yahoo for a hefty $1 billion discount to finalize what was supposed to be a $4.8 billion deal. (Full disclosure: TechCrunch is owned by Verizon, although we do not have any inside knowledge about this).

CrunchBase

Verizon Communications

FOUNDED 1983

OVERVIEW
Verizon Communications is a broadband and telecommunications company operating 4G LTE network, 3G network, and information and entertainment services. It is a Dow 30 company that employs a diverse workforce of more than 180,000 dedicated employees around the world. It serves mass market, business, government, and wholesale customers by delivering broadband and other wireline and wireless communication ...

LOCATION
New York, NY

CATEGORIES
Mobile, Information Technology, Communications Infrastructure

WEBSITE
http://www.verizon.com/

Full profile for Verizon Communications

Yahoo! +

# „We're different, we'll manage, don't worry"

***„Most engineers have never properly learned to develop software" – Rombach, Fraunhofer, 2014***

***„Most computer scientists have never properly learned to develop SECURE software" – Any security professor on earth, 2016***

DATA CENTRE SOFTWARE NETWORKS SECURITY TRANSFORMATION DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

Security

**Bungling Microsoft singlehandedly proves that golden backdoor keys are a terrible idea**

Redmond races to revoke Secure Boot policy

10 Aug 2016 at 06:56, Chris Williams 580

**Updated** Microsoft leaked the golden keys that unlock Windows-powered tablets, phones and other devices sealed by Secure Boot – and is now scrambling to undo the blunder.

These skeleton keys can be used to install non-Redmond operating systems on locked-down computers. In other words, on devices that do not allow you to disable Secure Boot even if you have administrator rights – such as ARM-based Windows RT tablets – it is now possible to sidestep this block and run, say, GNU/Linux or Android

More like this

Microsoft Windows

Most read

High rear end winds cause F-35A ground engine fire

Google rushes in where Akamai fears to tread, shields Krebs after world's-worst DDoS

Heathrow airport and stock exchange throw mystery BSODs

Unimpressed with Ubuntu 16.10? Yakkety Yak... don't talk back

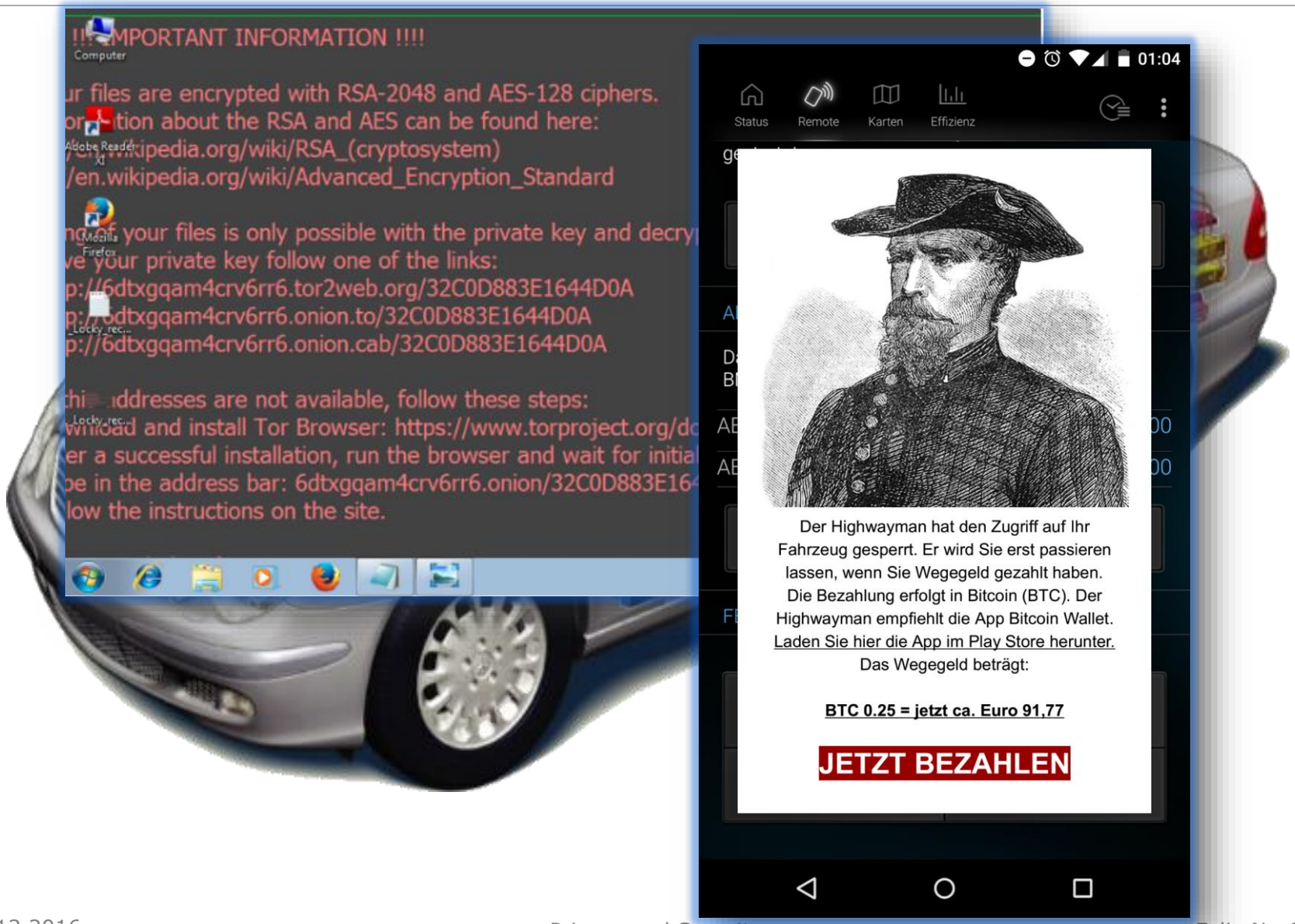
Silicon Valley's top exorcist rushed off his feet as Demons infest California

Spotlight

The Register uses cookies. Find out more. Close

# And the Dirty Reality…

# IT – Cars – Security



# Ziele der IT-Sicherheit

Etwas allgemeiner, die Aufgaben der IT-Sicherheit:

**Reduktion operationeller Risiken von IT-Systemen**

- Modellierung von System und Umwelt
- Erhebung und Spezifikation von Sicherheitsanforderungen
- Bedrohungsanalysen
- Risiko-Einschätzungen
- Design, Konstruktion und Umsetzung von Schutzmechanismen

# Übersicht des Ablaufs

Sicherheitsanforderungen

Bedrohungen
Schwachstellen
Risiken

Sicherheitspolitiken
Modellierung und Spezifikation

ZSLs, HRU, RBAC, ABAC, MLS;
Skippy, XACML, SELinux SPSL

Sicherheitsmechanismen

Authentisierung
Zugriffssteuerung
kryptographische Funktionen

Sicherheitsarchitekturen

TCBs, Referenzmonitore,
Nizza, SELinux, Kerberos

# Wie machen wir Systeme sicher?

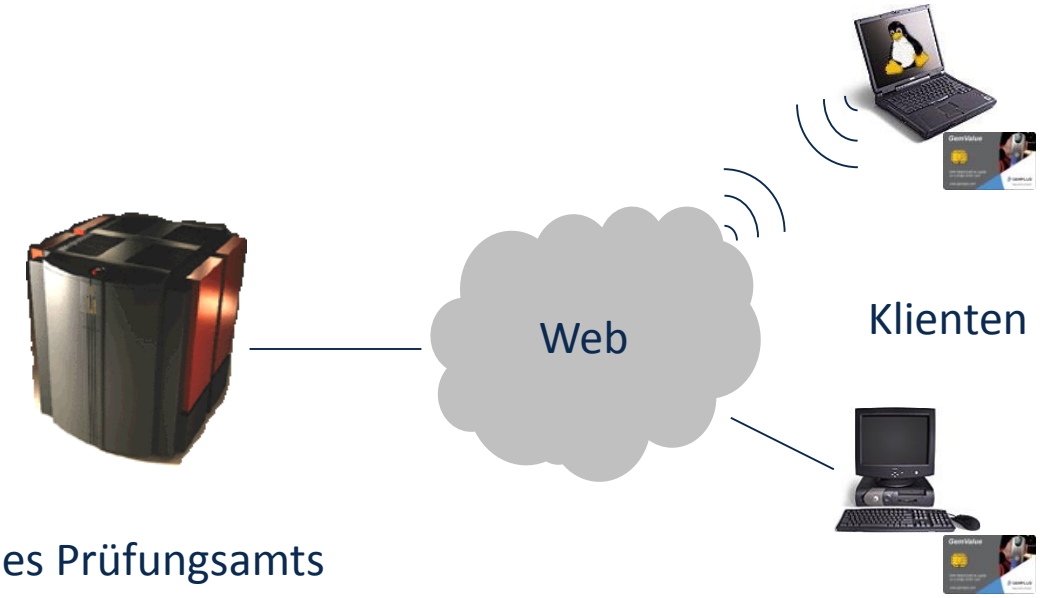
## Beispielszenario: webbasiertes Prüfungsmanagementsystem

Dienste

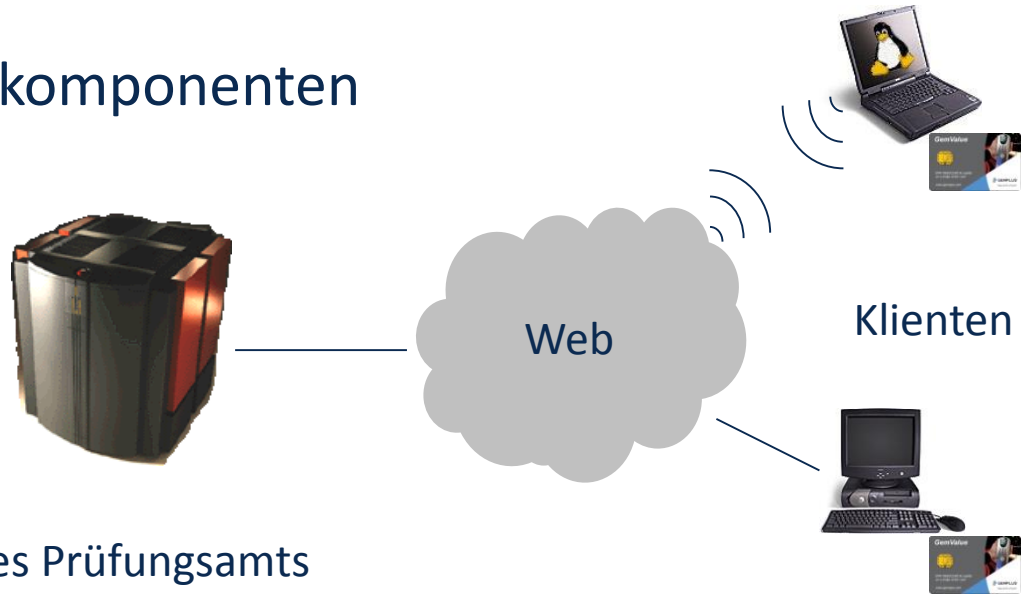
- Prüfungsan- und -abmeldung
- Noteneingabe und -abfrage
- Auskünfte, Bescheinigungen

für

- Studierende
- Lehrende
- Prüfungsamt



# SW-Architekturkomponenten




Server

- jExam/SLM: Datenbank mit Studierenden, Noten, Prüfungsordnung
- Webserver-Frontend
- Authentisierungsserver
- Betriebssystem
- Sicherheitspolitik

Klienten

- Webbrowser mit Authentisierungs-Plugin (Chipkartenleser), Mobile Apps
- Betriebssystem

# Operationelle Risiken

Integrität:

- Noten
- Prüfungsanmeldungen

Vertraulichkeit

- Persönliche Daten
- Noten

(Rechts-)Verbindlichkeit

- Noten
- Bescheinigungen (Zeugnisse)

Verfügbarkeit

- Prüfungsabmeldungen
- Anmeldungen zu Sportkursen

# Reduktion operationeller Risiken: Modellierung von Regeln, Sicherheitseigenschaften

identitätsbasierte Regeln
- der Professor als Prüfer darf …

rollenbasierte Regeln
- alle Prüfer dürfen …
- alle PA-Mitarbeiter dürfen …
- alle Studierenden dürfen …

zeitbasierte Regeln
- bis zu 4 Tage vor einer Prüfung kann …
- innerhalb 6 Wochen nach einer Prüfung muss …

attributbasierte Regeln
- als vertraulich klassifizierte Dokumente müssen ...

→ definiert durch Regelsysteme (Sicherheitspolitiken)

# Terminologie: Datenschutz & Datensicherheit

## *Datenschutz*

- alle Vorkehrungen zur Verhinderung unerwünschter (Folgen der) Datenverarbeitung für die Betroffenen *(Persönlichkeitsrecht)*, rechtliche und technische Aspekte
- Beschränkung auf juristische Vorkehrungen →
  - Technisch-organisatorischer Datenschutz: technische und organisatorische Ziele und Maßnahmen, die zur Durchsetzung der juristischen Ziele notwendig sind

## *Datensicherung*

- Maßnahmen, Vorkehrungen und Einrichtungen zum Schutz von „Daten“

## *Datensicherheit (IT-Sicherheit)*

- ***Ziel:*** Sicherung der Funktion und Eigenschaften eines IT-Systems trotz unerwünschter Ereignisse (verbleibende Risiken tragbar)

# Datenschutz: Risiken

Risiken für den Datenschutz durch IKT

- Schnelle Erfassung und Auswertung von Daten möglich
- Möglichkeit der unbemerkten Datenerhebung
- Kontrolle schwierig

→ Notwendigkeit des Datenschutzes

Datenschutz

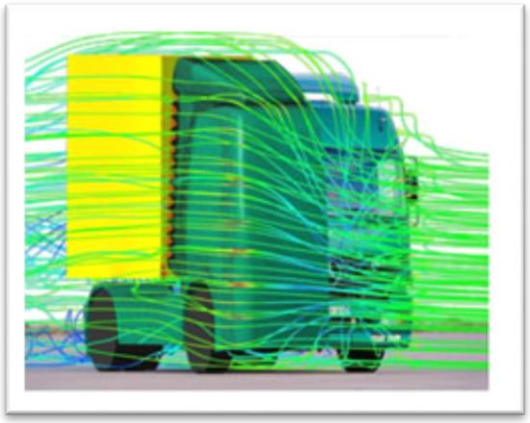
= Schutz der Privatsphäre

= Schutz vor Daten + Schutz ***der*** Daten (vor „Verlust“)

# Aber welche Daten denn?

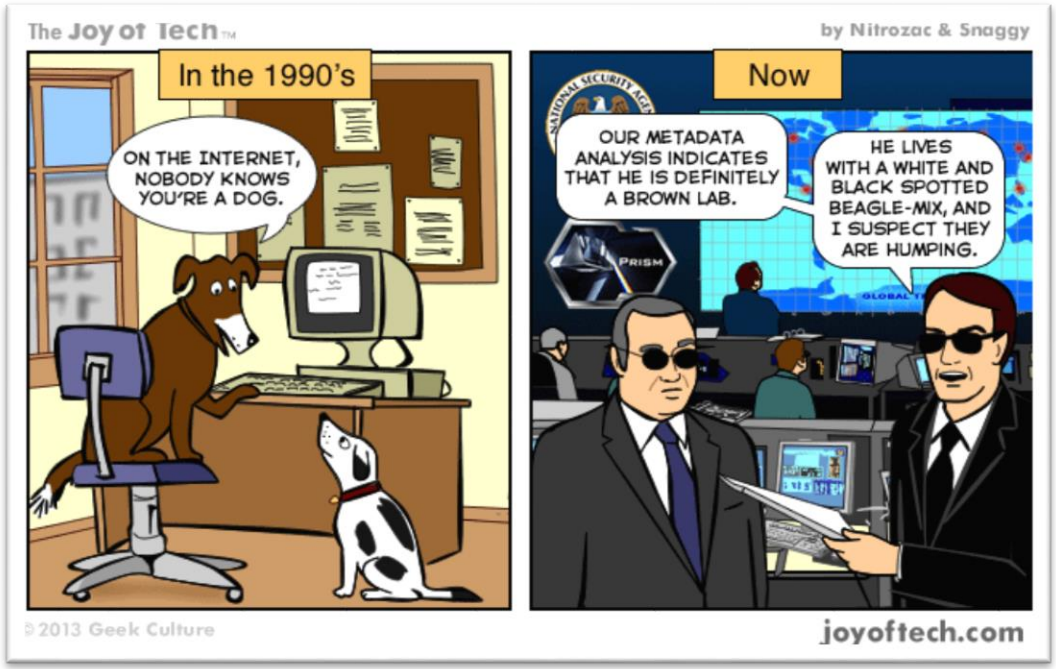
Daten ohne ***Personenbezug***

- Simulationsdaten
- Messungen in Experimenten



Daten ***mit Personenbezug***

- Arten
  - Inhalte
  - Verkehrsdaten
- Veröffentlichung
  - Bewusst
  - Unbewusst



# Einschub: „Es geht nur um Verkehrsdaten“

***Verkehrsdaten-Brisanz***

Teilnehmer kontrollierter Studie

- *Riefen Familie,…*
- *… Gentlemen Establishments,*
- *… Waffenladen,*
- *… Headshop und Baumarkt,*
- *…Medizinische Spezialisten,*
- *…Familienplanung, Eltern, Frauenarzt*

[1] https://cyberlaw.stanford.edu/blog/2013/11/what%27s-in-your-metadata

***Infere***

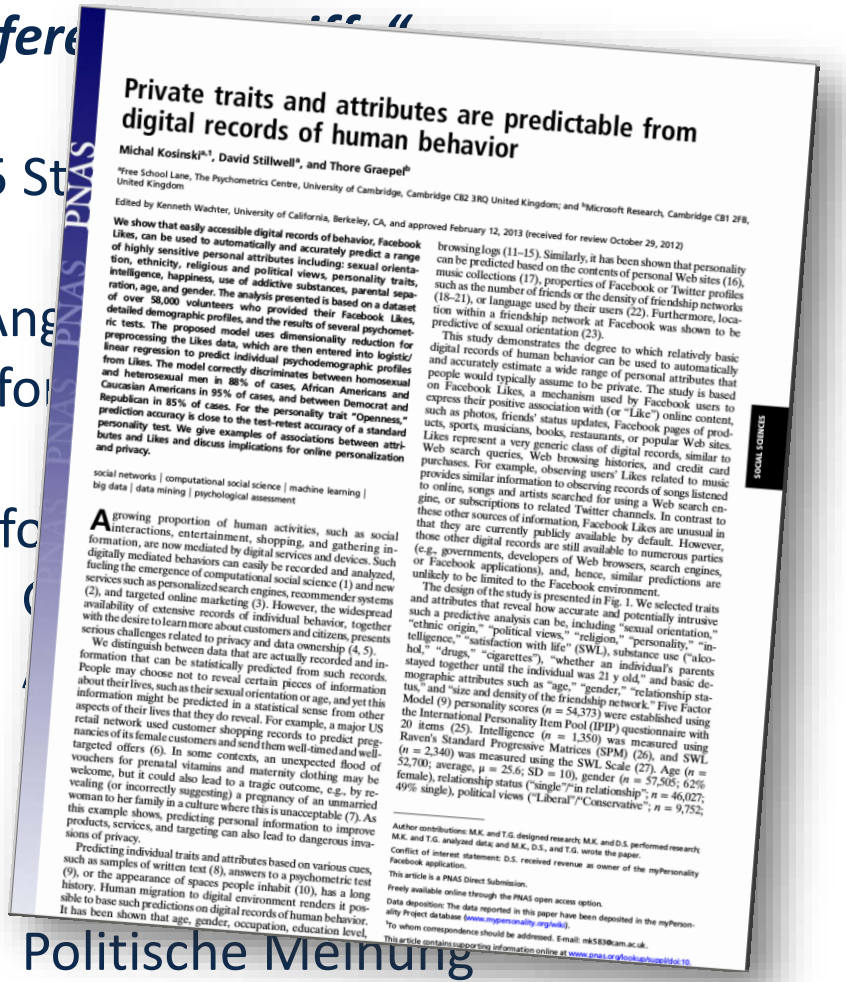
15 St

„Ang

Info

Erfo

- (
- /
- 
- 
- 
- Politische Meinung



Private traits and attributes are predictable from digital records of human behavior

Michal Kosinski[a,1], David Stillwell[a], and Thore Graepel[b]

[a]Free School Lane, The Psychometrics Centre, University of Cambridge, Cambridge CB2 3RQ United Kingdom; and [b]Microsoft Research, Cambridge CB1 2FB, United Kingdom

Edited by Kenneth Wachter, University of California, Berkeley, CA, and approved February 12, 2013 (received for review October 29, 2012)

We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The analysis presented is based on a dataset of over 58,000 volunteers who provided their Facebook Likes, detailed demographic profiles, and the results of several psychometric tests. The proposed model uses dimensionality reduction for preprocessing the Likes data, which are then entered into logistic/linear regression to predict individual psychodemographic profiles from Likes. The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases. For the personality trait "Openness," prediction accuracy is close to the test–retest accuracy of a standard personality test. We give examples of associations between attributes and Likes and discuss implications for online personalization and privacy.

social networks | computational social science | machine learning | big data | data mining | psychological assessment

A growing proportion of human activities, such as social interactions, entertainment, shopping, and gathering information, are now mediated by digital services and devices. Such digitally mediated behaviors can easily be recorded and analyzed, fueling the emergence of computational social science (1) and new services such as personalized search engines, recommender systems (2), and targeted online marketing (3). However, the widespread availability of extensive records of individual behavior, together with the desire to learn more about customers and citizens, presents serious challenges related to privacy and data ownership (4, 5).

We distinguish between data that are actually recorded and information that can be statistically predicted from such records. People may choose not to reveal certain pieces of information about their lives, such as their sexual orientation or age, and yet this information might be predicted in a statistical sense from other aspects of their lives that they do reveal. For example, a major US retail network used customer shopping records to predict pregnancies of its female customers and send them well-timed and well-targeted offers (6). In some contexts, an unexpected flood of vouchers for prenatal vitamins and maternity clothing may be welcome, but it could also lead to a tragic outcome, e.g., by revealing (or incorrectly suggesting) a pregnancy of an unmarried woman to her family in a culture where this is unacceptable (7). As this example shows, predicting personal information to improve products, services, and targeting can also lead to dangerous invasions of privacy.

Predicting individual traits and attributes based on various cues, such as samples of written text (8), answers to a psychometric test (9), or the appearance of spaces people inhabit (10), has a long history. Human migration to digital environment renders it possible to base such predictions on digital records of human behavior. It has been shown that age, gender, occupation, education level, browsing logs (11–15). Similarly, it has been shown that personality can be predicted based on the contents of personal Web sites (16), music collections (17), properties of Facebook or Twitter profiles (18–21), or language used by their users (22). Furthermore, location within a friendship network at Facebook was shown to be predictive of sexual orientation (23).

This study demonstrates the degree to which relatively basic digital records of human behavior can be used to automatically and accurately estimate a wide range of personal attributes that people would typically assume to be private. The study is based on Facebook Likes, a mechanism used by Facebook users to express their positive association with (or "Like") online content, such as photos, friends' status updates, Facebook pages of products, sports, musicians, books, restaurants, or popular Web sites. Likes represent a very generic class of digital records, similar to Web search queries, Web browsing histories, and credit card purchases. For example, observing users' Likes related to music provides similar information to observing records of songs listened to online, songs and artists searched for using a Web search engine, or subscriptions to related Twitter channels. In contrast to these other sources of information, Facebook Likes are unusual in that they are currently publicly available by default. However, those other digital records are still available to numerous parties (e.g., governments, developers of Web browsers, search engines, or Facebook applications), and, hence, similar predictions are unlikely to be limited to the Facebook environment.

The design of the study is presented in Fig. 1. We selected traits and attributes that reveal how accurate and potentially intrusive such a predictive analysis can be, including "sexual orientation," "ethnic origin," "political views," "religion," "personality," "intelligence," "satisfaction with life" (SWL), substance use ("alcohol," "drugs," "cigarettes"), "whether an individual's parents stayed together until the individual was 21 y old," and basic demographic attributes such as "age," "gender," "relationship status," and "size and density of the friendship network." Five Factor Model (9) personality scores ($n$ = 54,373) were established using the International Personality Item Pool (IPIP) questionnaire with 20 items (25). Intelligence ($n$ = 1,350) was measured using Raven's Standard Progressive Matrices (SPM) (26), and SWL ($n$ = 2,340) was measured using the SWL Scale (27). Age ($n$ = 52,700; average, $\mu$ = 25.6; SD = 10), gender ($n$ = 57,505; 62% female), relationship status ("single"/"in relationship"; $n$ = 46,027; 49% single), political views ("Liberal"/"Conservative"; $n$ = 9,752;

Author contributions: M.K. and T.G. designed research; M.K. and D.S. performed research; M.K. and T.G. analyzed data; and M.K., D.S., and T.G. wrote the paper.

Conflict of interest statement: D.S. received revenue as owner of the myPersonality Facebook application.

This article is a PNAS Direct Submission.

Freely available online through the PNAS open access option.

Data deposition: The data reported in this paper have been deposited in the myPersonality Project database (www.mypersonality.org/wiki).

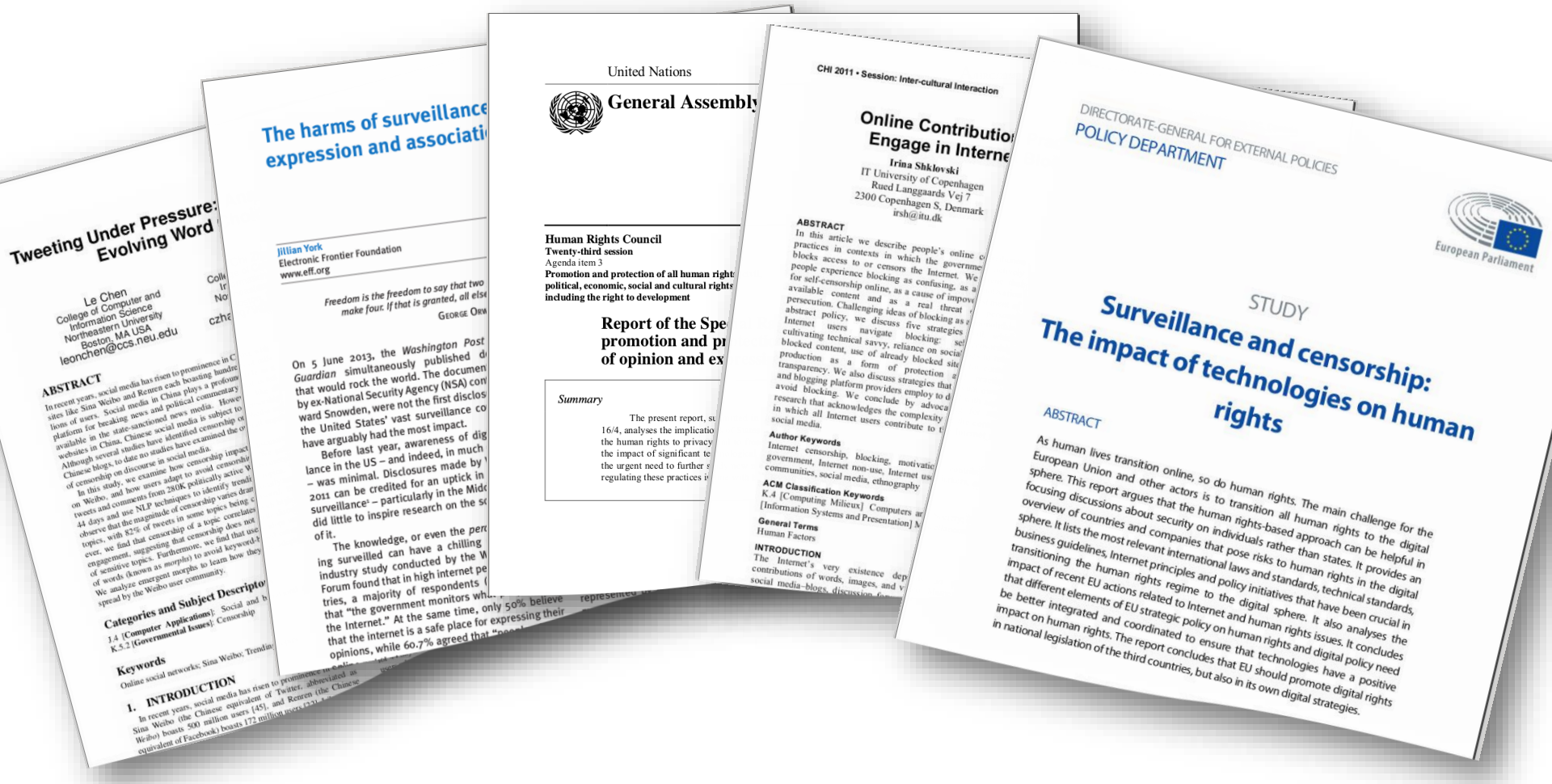
[1]To whom correspondence should be addressed. E-mail: mk583@cam.ac.uk.

This article contains supporting information online at www.pnas.org/lookup/suppl/doi:10.

PNAS PNAS PNAS

SOCIAL SCIENCES

# „Ich hab nichts zu verbergen“



# Privatheitsverständnis: Right to be let alone

Samuel Warren, ***Louis Brandeis***: "**The Right to Privacy**", Harvard Law Review, Vol. IV, No. 5, 15th December **1890**

**Grund:** "snapshot photography" (technische Neuerung)

- Ermöglichte Zeitungen Bilder von Personen ohne deren Einwilligung zu veröffentliche
- Privatpersonen wurden in ihrer Individualität verletzt
- Befürchtung, dass "moralische Standards" in Gefahr seien

**Überlegung:**

- Grundprinzip des Gewohnheitsrechts: Schutz von Person und Besitz des Individuums
- *"it has been found necessary from time to time to define anew the exact nature and extent of such protection"*
- *"Political, social, and economic changes entail the recognition of new rights"*

**Schlussfolgerung:**

- "**right to be let alone**"
- Konsequenz: Opt-out

# Vs.: Informationelle Selbstbestimmung

Europäisches Grundverständnis (Volkszählungsurteil 1983, BRD)

Vorletzter Zensus in Deutschland (1981 geplant, stark verzögert)

Starke öffentliche Opposition

- Angst vor der Überwachungsgesellschaft
- Diskussion des „gläsernen Menschen“
- Öffentliche Aufforderungen zum zivilen Ungehorsam
- Durchgeführt 1987
- Resultat war Anfangsfehler von 25%

…*für die Preisgabe minimaler Informationen, dem **Staat** gegenüber*

**Grundidee der Kontrolle des Individuums über die es betreffenden Daten**

Konsequenz: Opt-in und anschließende Kontrolle

# Ihr Recht auf Datenschutz

*„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.“* (Art 8, Eur. Menschenrechtskonvention)

Recht auf informationelle Selbstbestimmung im BDSG:

> *„Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.“*

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt:

***Verbot mit Erlaubnisvorbehalt***

Erforderlich: rechtliche Grundlage durch

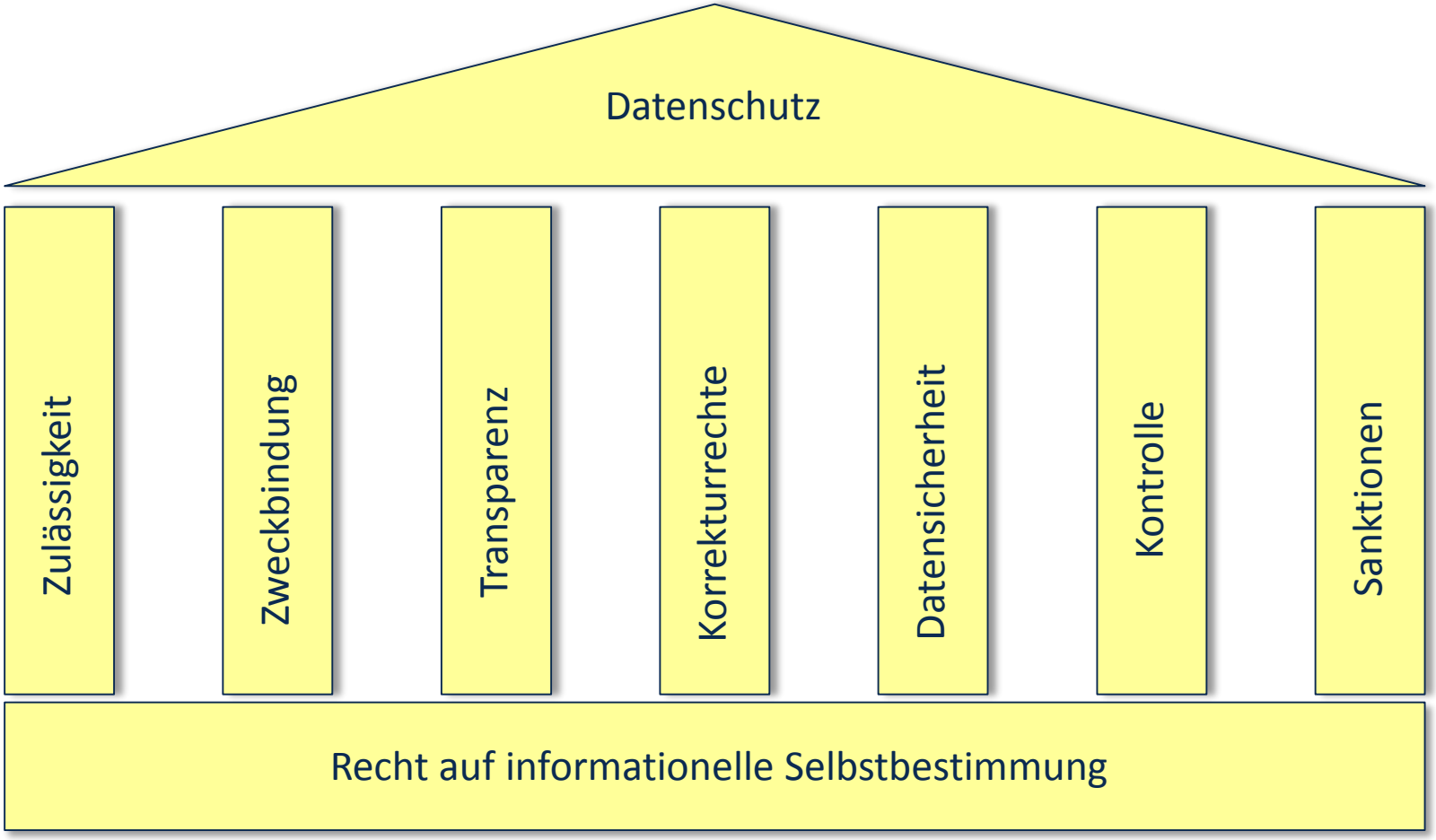
- Gesetzliche Grundlage (BDSG) oder
- andere Rechtsvorschrift (z.B. Betriebsvereinbarung)
- Einwilligung des Betroffenen
  - Ausreichende Information
  - Freiwilligkeit
  - Widerruflichkeit

# Was ist Personen-beziehbar?

Legal: ***P***ersonally ***I***dentifiable ***I***nformation / ***PII***

- ***US:*** *Name, address (Phone, Email), national identifiers (tax, passports), IP address, driving (vehicle registration, drivers licence), biometrics (face, fingerprints), credit card numbers, date/place of birth (age, login name(s), gender, "race", grades, salary, criminal records)*
- ***EU:*** *'personal data' shall mean any informa or identifiable natural person ('data subject one who can be identified, directly or indire reference to an identification number or to to his physical, physiological, mental, econo identity* [EU directive 95/46/EC]

# 7 Säulen des Datenschutzes



# Datenschutz – Zweckbindung

Verwendungszweck muss bei Erhebung festgelegt sein

Information der Betroffenen notwendig

Zweckänderung erfordert gesonderte Legitimation

Datensparsamkeit:

- Begrenzung auf die für den jeweiligen Zweck ***notwendigen*** Daten
- Möglichkeiten der Anonymisierung bzw. Pseudonymisierung
- Löschen nicht mehr benötigter Daten (bzw. Sperren)

# Datenschutz – Transparenz

***Informationspflicht***: verantwortliche Stelle muss aktiv werden

***Auskunftsanspruch:*** von Betroffen geltend zu machen

Erhebung erfolgt grundsätzlich beim Betroffenen

→ Unterrichtung des Betroffenen durch verantwortliche Stelle über

- Identität der verantwortlichen Stelle
- Zweck der Erhebung, Verarbeitung und Nutzung
- Kategorien von Empfängern

Auskunftsanspruch: zusätzlich Art und Umfang gespeicherter Daten, Herkunft und Empfänger

Auskunft (grundsätzlich) unentgeltlich

# Datenschutz – Korrektur, Kontrolle, Sanktion

## Korrekturrechte

- Berichtigung
- Löschen bzw. Sperren
- Widerspruch

## Kontrolle

- Intern: betrieblicher Datenschutzbeauftragter
- Extern: Aufsichtsbehörde

## Sanktionen

- Bußgeld, Strafe, Schadensersatz

# Datenschutz und Datensicherheit

Datenschutz ist sinnvoll, denn man sollte wissen, wer welche personenbezogenen Daten zu welchem Zweck speichert und nutzt.

Man muß sich darüber klar sein, welche Daten man preisgeben will.

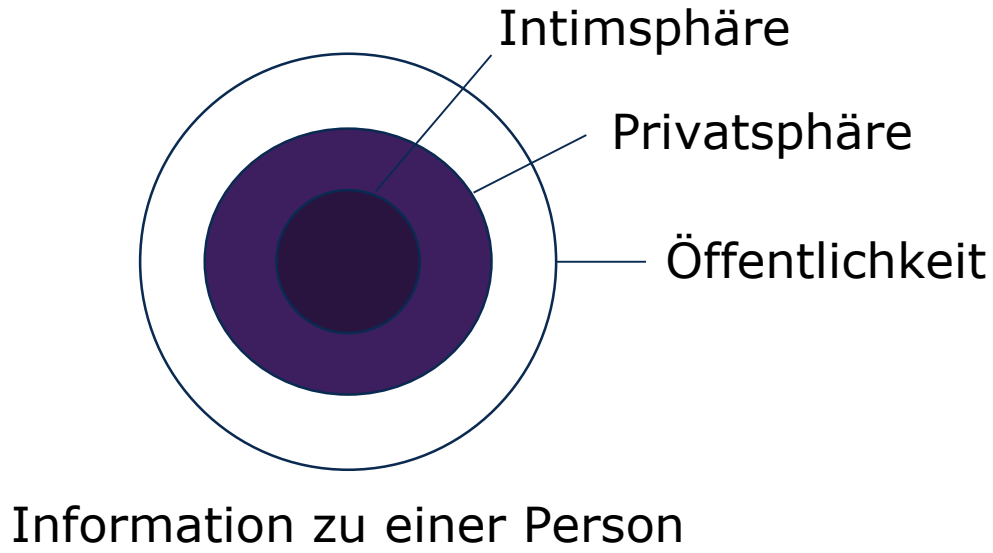
Man sollte nur das für den jeweiligen Zweck erforderliche Minimum an personenbezogenen Daten preisgeben.

*Wie sicher sind Ihre Daten, haben Sie darüber Kontrolle?*

*Google play? App Store anybody?*

# Datenschutz: Sphärenmodell

Bereiche unterschiedlicher Schutzwürdigkeit durch konzentrische Kreise (z.B. 3) dargestellt, nach außen hin abnehmende Schutzwürdigkeit




Zuordnung der Daten zu den Sphären individuell

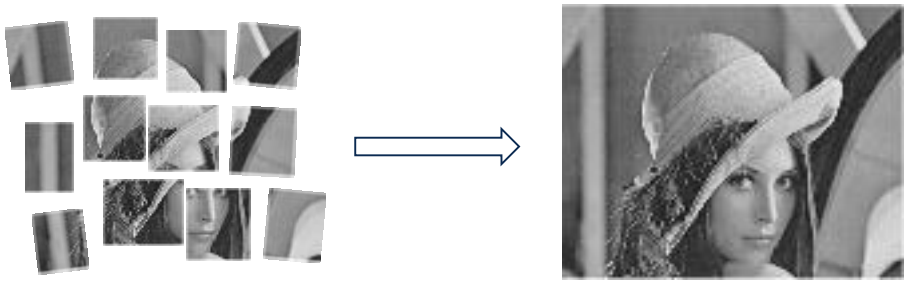
Zuordnung auch abhängig von Situation

# Datenschutz: Mosaikmodell

***Idee:***

Informationen über Menschen lassen sich in Teile zerlegen

Zusammenfügen von Einzelteilen ergibt präzises Gesamtbild



- Mosaikmodell berücksichtigt auch Schutz von Daten, die laut *Sphärenmodell* nicht zum absolut schützenswerten Bereich gehören
- Zugriff auf einzelnen Teile nicht dargestellt
- Überprüfung, welche Verknüpfungen kritisch sind, ist schwierig
- Nicht nur Datenerfassung, auch Datenverarbeitung berücksichtigen!

# Datenschutz: Rollenmodell

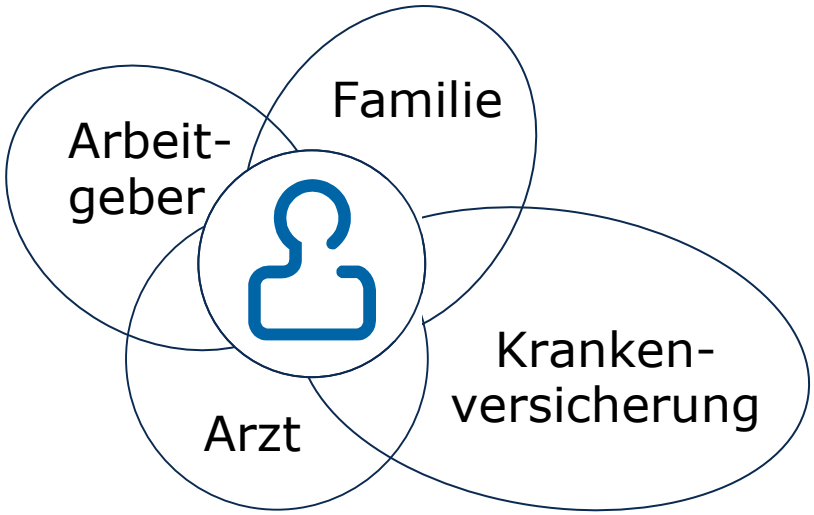
***Idee:***

Menschen agieren in Rollen

Darlegung aller Informationen nicht notwendig zu deren Erfüllung

Statt Trennung der Daten in Bereiche verschiedener Sensibilität:

Erzeugung von Einzelbildern




Beibehaltung der Trennung der Einzelbilder

Selbstbestimmung der Datenweitergabe nur bedingt (problematisch z.B. gegenüber öffentlichen Behörden)

# References


Stefan Katzenbeisser, „Einführung in Trusted Systems“, teaching materials, TU Darmstadt, 2015
Mark Manulis, „Introduction to Cryptography“, teaching materials, TU Darmstadt, 2011
Winfried Kühnhauser, „Systemsicherheit“, teaching materials, TU Ilmenau, 2014
Elke Franz, „Datensicherheit“, teaching materials, TU Dresden, 2014

---

Frederik Armknecht and Thorsten Strufe. “An Efficient Distributed Privacy-preserving Recommendation System”. In IEEE Med-Hoc-Net, 2011.

Sonja Buchegger et al. "PeerSoN: P2P social networking: early experiences and insights." In: Second ACM EuroSys Workshop on Social Network Systems. ACM, 2009

Leucio-Antonio Cutillo, et al. „Handbook of Social Network Technologies and Applications“, chapter „Security and Privacy in Online Social Networks“. Springer, 2010.

Chen, Le, Chi Zhang, and Christo Wilson. "Tweeting under pressure: analyzing trending topics and evolving word choice on sina weibo." In ACM COSN, 2013

Clarke, Ian, et al. „Freenet : A distributed anonymous information storage and retrieval system." Designing Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2001

La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression " (2011).

Köpsell, Stefan, et al. "Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes." Datenschutz und Datensicherheit: DuD 27.3 (2003): 139-142.

Michal Kosinski, et al. “Private traits and attributes are predictable from digital records of human behavior” PNAS 2013 110 (15) 5802-5805

Thomas Paul, et al. „Exploring Decentralization Dimensions of Social Networking Services: Adversaries and Availability“. In SIGKDD/HotSocial, 2012.

Thomas Paul, et al. “C4PS – Helping Facebookers Manage their Privacy Settings”. In SocInfo, 2012.

Shklovski, Irina, and Nalini Kotamraju. "Online contribution practices in countries that engage in internet blocking and censorship." In IGCHI Conference on Human Factors in Computing Systems. ACM, 201

Benjamin Schiller, et al. „Resilient tree-based live streaming for mobile scenarios.“ In IEEE PerCom Workshops, March 2014

Daniel Schreiber, et al., “Social IPTV: a Survey on Chances and User-Acceptance.” In International Workshop on Personalization and Recommendation on the Web and Beyond, 2010

Schulz, Stephan, and Thorsten Strufe. „$d^2$ Deleting Diaspora: Practical attacks for profile discovery and deletion." IEEE ICC, 2013

Wagner, Ben, et al. “Surveillance and censorship : The impact of technologies on human rights”, EP/EXPO/B/DROI/FWC/2013 08/Lot8/02

Warren, Samuel, Brandeis, Louis. “The Right to Privacy”, Harvard Law Review, Vol. IV, No. 5, 1890

York, Gillian “The harms of surveillance to privacy, expression and association”, in “Communications surveillance in the digital age”, 2014


---

*All images credit wikimedia, unless otherwise stated*