Karlsruhe Institute of Technology

Privatsphäre und Freiheit oder Überwachung und Zensur in Web und Mobile Apps?

Thorsten Strufe – Von Hamburg bis Karlsruhe (mit kleinen Umwegen)

Competence Center for Applied Security Technology


TECHNISCHE
UNIVERSITÄT
Cluster of Excellence
CeTI
Centre for Tactile Internet
with Human-in-the-Loop
CeTI
CfaED
CENTER FOR
ADVANCING
ELECTRONICS
DRESDEN
5G Lab
GERMANY
TED
IDEASWORTHSPREADING
HAEC
ROSI


CeTI


Benchmarking
Peer-to-Peer Systems


EURECOM


Karlsruhe Institute of Technology
...angekommen!

- Und was treibt den

Lehrstuhl für IT-Sicherheit mit
Schwerpunkt auf praktischen
Sicherheitsmethoden und –systemen

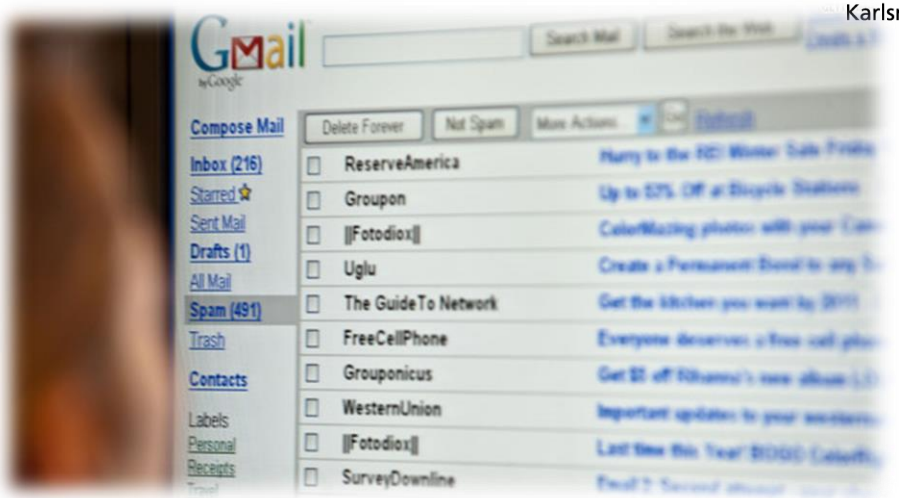
am KIT nun eigentlich an?

Post und Telekommunikation

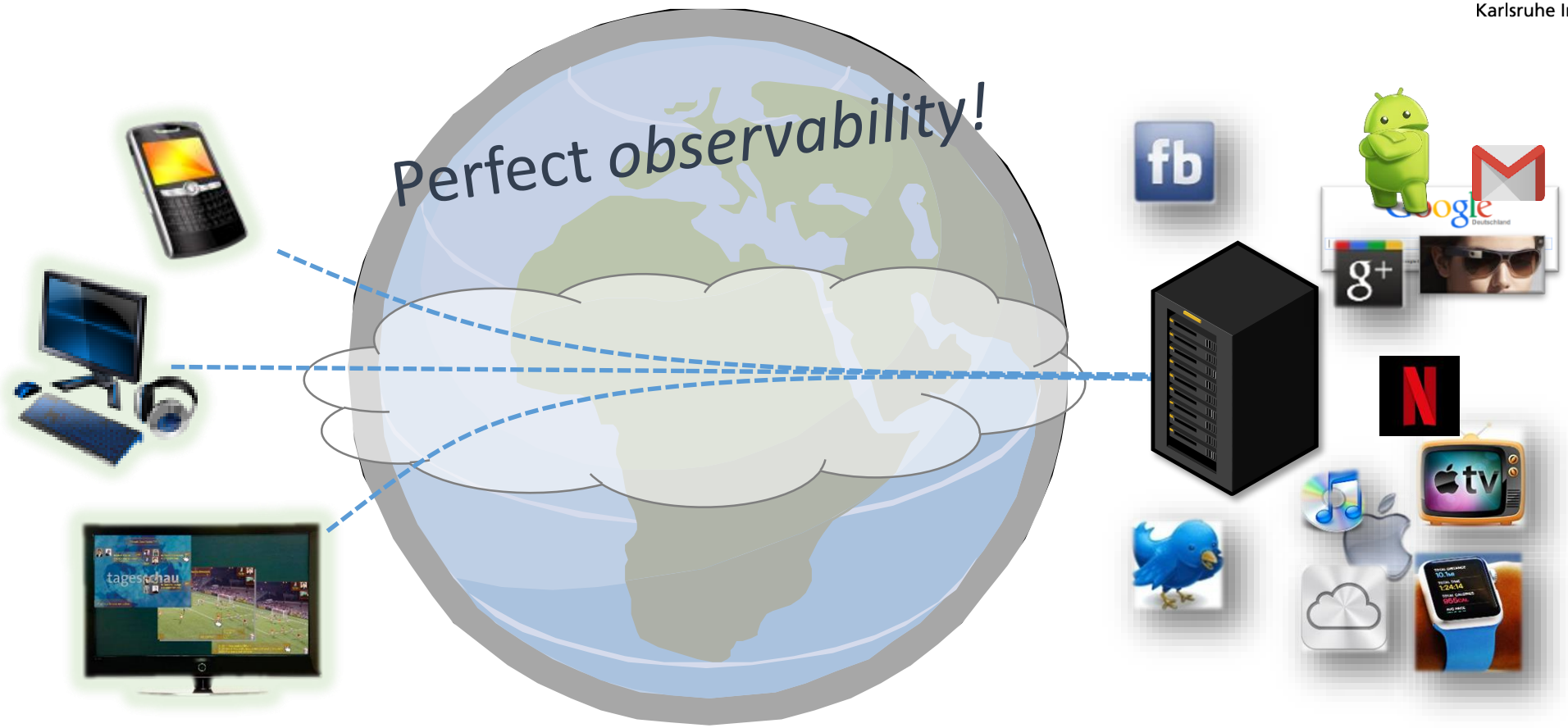
Informationsbeschaffung und Verbreitung

Zugang: Art und Reichweite

Willkommen im neuen Millenium!



Zugang: Art und Reichweite Heute



1: Zentrale globaler Dienstanbieter
2: Globaler Zugang über das Internet

Konvergenz und Segmentierung

- Web-Anfragen konvergieren auf die Seiten von 6 Firmen
  - Erfolg basierend auf starker Personalisierung
- Meinungsbildung konvergiert auf große Anbieter
  - Facebook: 1.94 Mrd Nutzer
  - Twitter, Google+, reddit
- Transparente Einbindung Dritter
  - Hosting, Clouds
  - Content Delivery Networks
  - Analytics

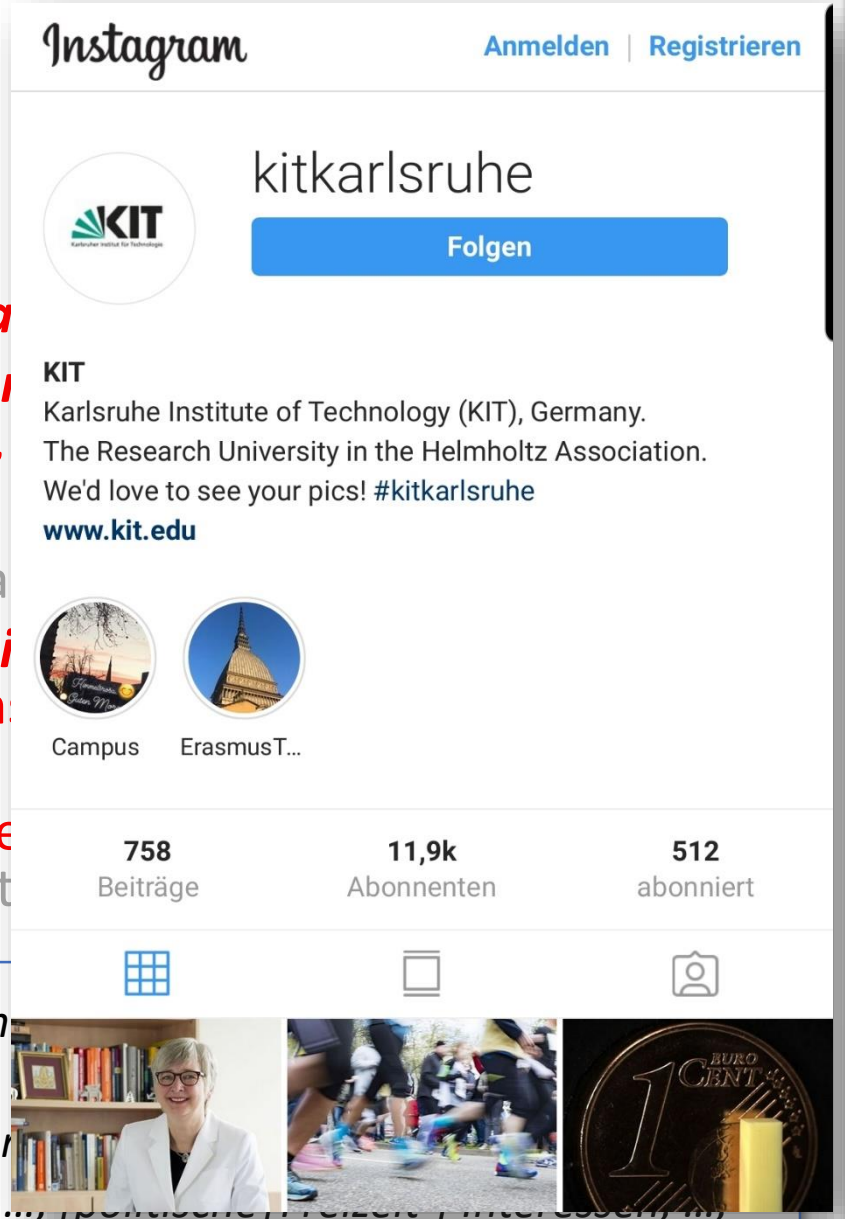
[Nielsen]
[Datanyze]

Beobacht- und Ableitbare Informationen

- Angegeben, explizit
  - Erstellte Inhalte
  - Kommentare
  - Strukturelle Interaktion (Kontakte, +1)

- Extrahiert
  - Präferenz– und
  - Gesichtserkennungsmodelle
  - Private Details

- Metadaten
  - ***Sitzungsa***
  - ***Interesse*** Gruppen,
  - ***Einfluss***
  - Clickstrea
  - ***Kommuni*** Art, Inten Ausmaß)
  - ***Ort*** (IP; ge Koordinat

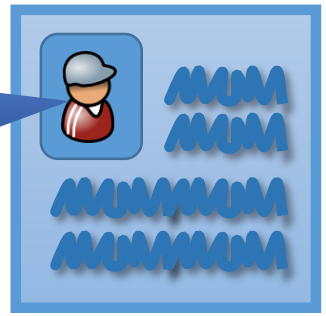


Soziodemograph
Geschlecht, Alter,
…, Bildungsgr
Haushaltsgröße, …, [politische | Freizeit-] Interessen, …)
persönlicher Besitz, …, Versicherungen, Investments,…
[AGOF]

Bedroht: Beobacht- und Ableitbare Informationen

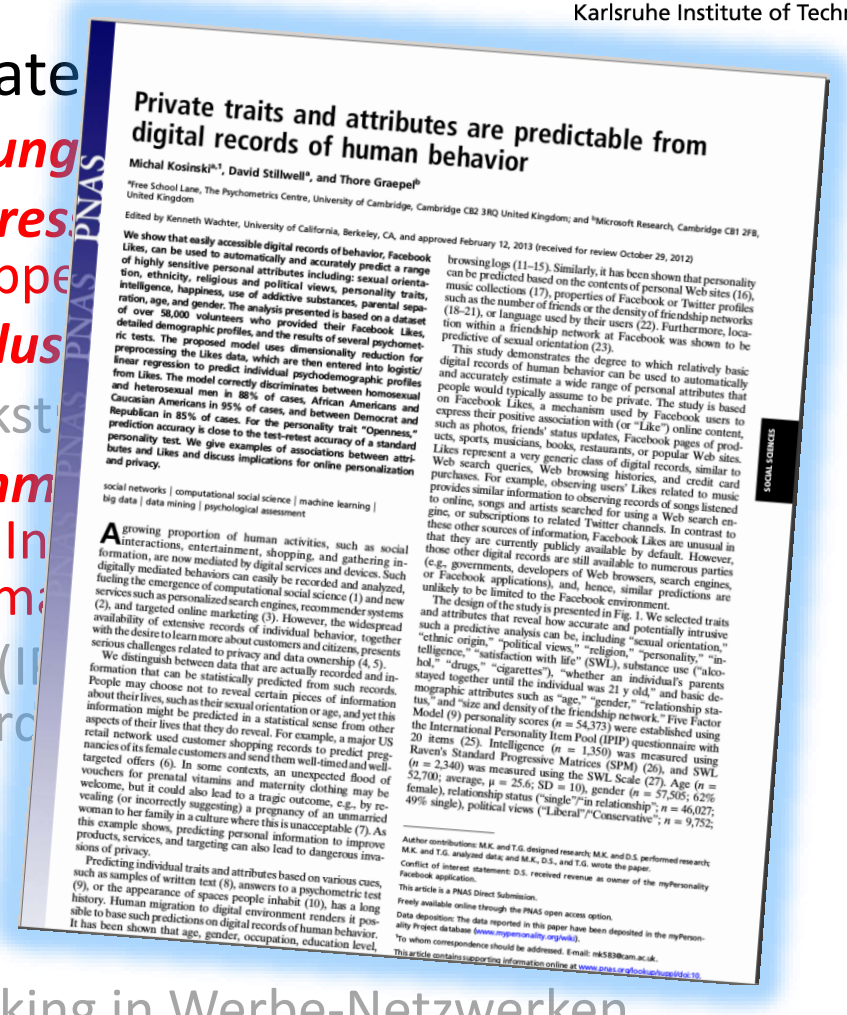
- Angegeben, explizit
  - Erstellte Inhalte
  - Kommentare
  - Strukturelle Interaktion (Kontakte, +1)

Wir haben doch nichts zu verbergen…!?



- Extrahiert
  - Präferenz– und
  - Gesichtserkennungsmodelle
  - Private Details

- Metadate
  - ***Sitzung***
  - ***Interes***
    Gruppe
  - ***Einflus***
  - Clickst
  - ***Komm***
    Art, In
    Ausm
  - ***Ort*** (I
    Koorc



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 such as the number of friends or the density of friendship networks (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, μ = 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.

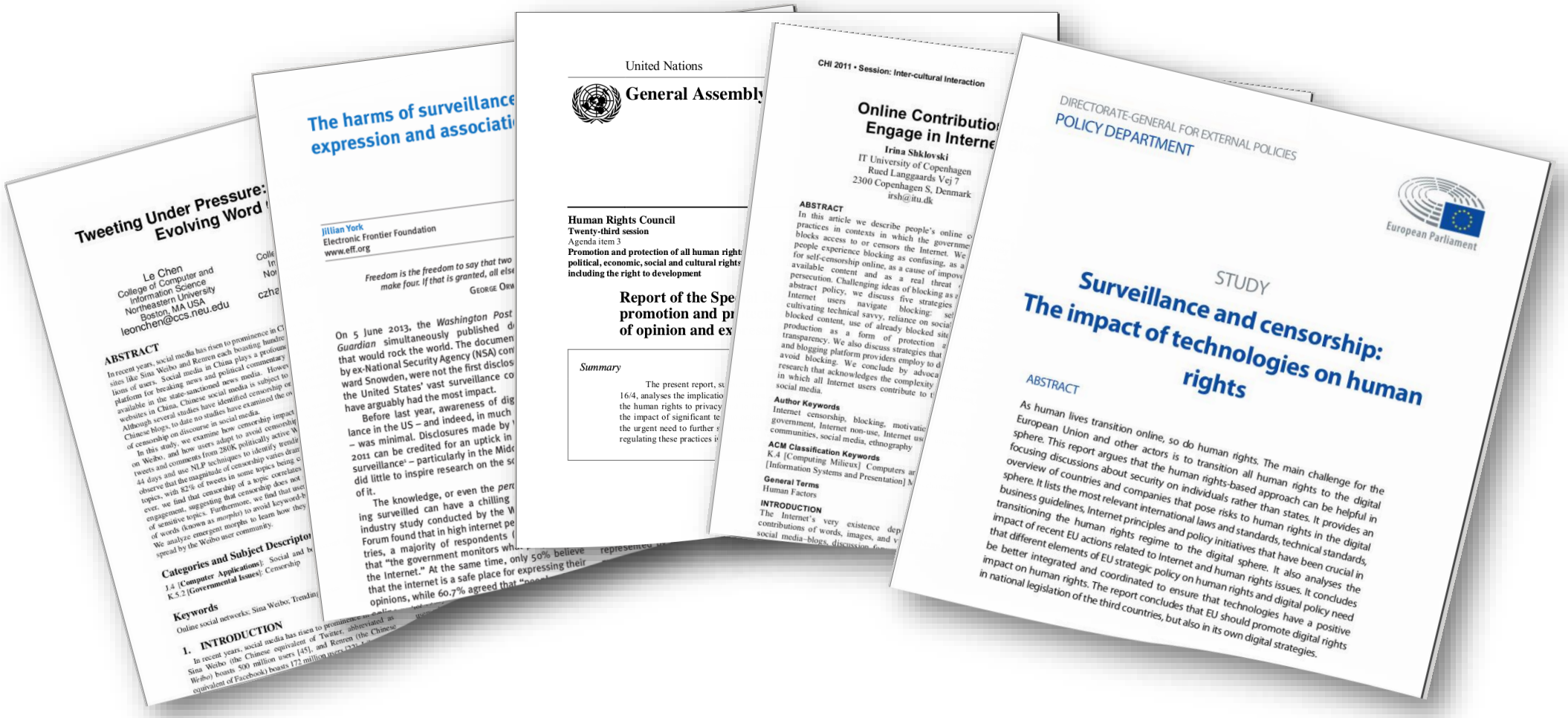
Data deposition: The data reported in this paper have been deposited in the myPersonality Project database (www.mypersonality.org/wiki).

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

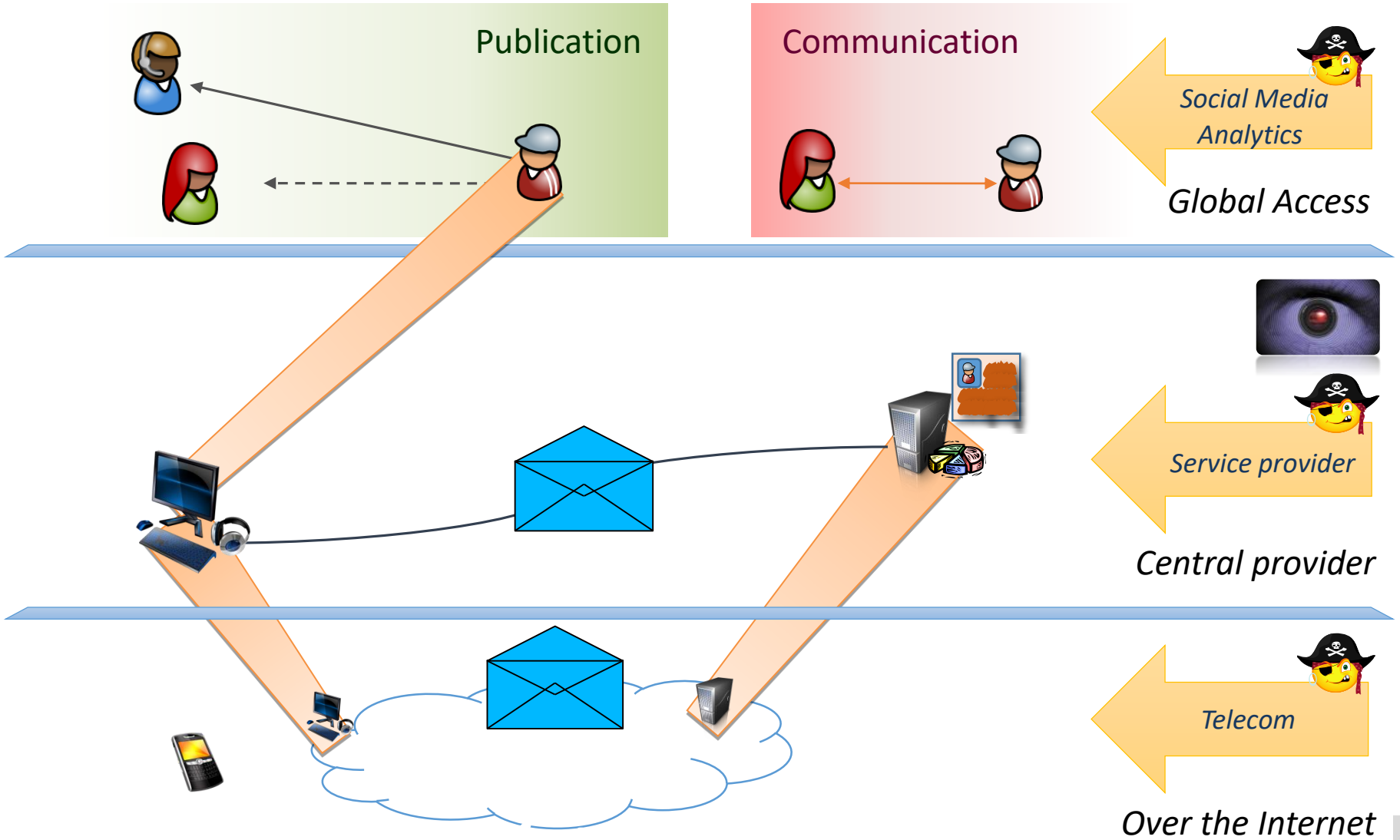
This article contains supporting information online at www.pnas.org/lookup/suppl/doi:10.

- Extern
  - Tracking in Werbe-Netzwerken

[4] TI '11
[5] ht '15
[A]


Tweeting Under Pressure:
Evolving Word
Le Chen
College of Computer and Information Science
Northeastern University
Boston, MA USA
leonchen@ccs.neu.edu
ABSTRACT
Categories and Subject Descriptors
Keywords
Online social networks; Sina Weibo; Trending
1. INTRODUCTION
The harms of surveillance
expression and associati
Jillian York
Electronic Frontier Foundation
www.eff.org
Freedom is the freedom to say that two
make four. If that is granted, all else
George Orw
On 5 June 2013, the Washington Post
Guardian simultaneously published d
that would rock the world. The documen
by ex-National Security Agency (NSA) con
ward Snowden, were not the first disclos
the United States' vast surveillance co
have arguably had the most impact.
Before last year, awareness of dig
lance in the US – and indeed, in much
– was minimal. Disclosures made by
2011 can be credited for an uptick in
surveillance[2] – particularly in the Mid
did little to inspire research on the sc
of it.
The knowledge, or even the perc
ing surveilled can have a chilling
industry conducted by the W
Forum found that in high internet pe
tries, a majority of respondents (
that "the government monitors wh
the Internet." At the same time, only 50% believe
that the internet is a safe place for expressing their
opinions, while 60.7% agreed that
United Nations
General Assembly
Human Rights Council
Twenty-third session
Agenda item 3
Promotion and protection of all human rights
political, economic, social and cultural rights
including the right to development
Report of the Spe
promotion and pr
of opinion and ex
Summary
The present report, su
16/4, analyses the implicatio
the human rights to privacy
the impact of significant te
the urgent need to further s
regulating these practices it
CHI 2011 • Session: Inter-cultural Interaction
Online Contributio
Engage in Interne
Irina Shklovski
IT University of Copenhagen
Rued Langgaards Vej 7
2300 Copenhagen S, Denmark
irsh@itu.dk
ABSTRACT
Author Keywords
ACM Classification Keywords
General Terms
Human Factors
INTRODUCTION
DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT
European Parliament
STUDY
Surveillance and censorship:
The impact of technologies on human rights
ABSTRACT
As human lives transition online, so do human rights. The main challenge for the European Union and other actors is to transition all human rights to the digital sphere. This report argues that the human rights-based approach can be helpful in focusing discussions about security on individuals rather than states. It provides an overview of countries and companies that pose risks to human rights in the digital sphere. It lists the most relevant international laws and standards, technical standards, business guidelines, Internet principles and policy initiatives that have been crucial in transitioning the human rights regime to the digital sphere. It also analyses the impact of recent EU actions related to Internet and human rights issues. It concludes that different elements of EU strategic policy on human rights and digital policy need be better integrated and coordinated to ensure that technologies have a positive impact on human rights. The report concludes that EU should promote digital rights in national legislation of the third countries, but also in its own digital strategies.

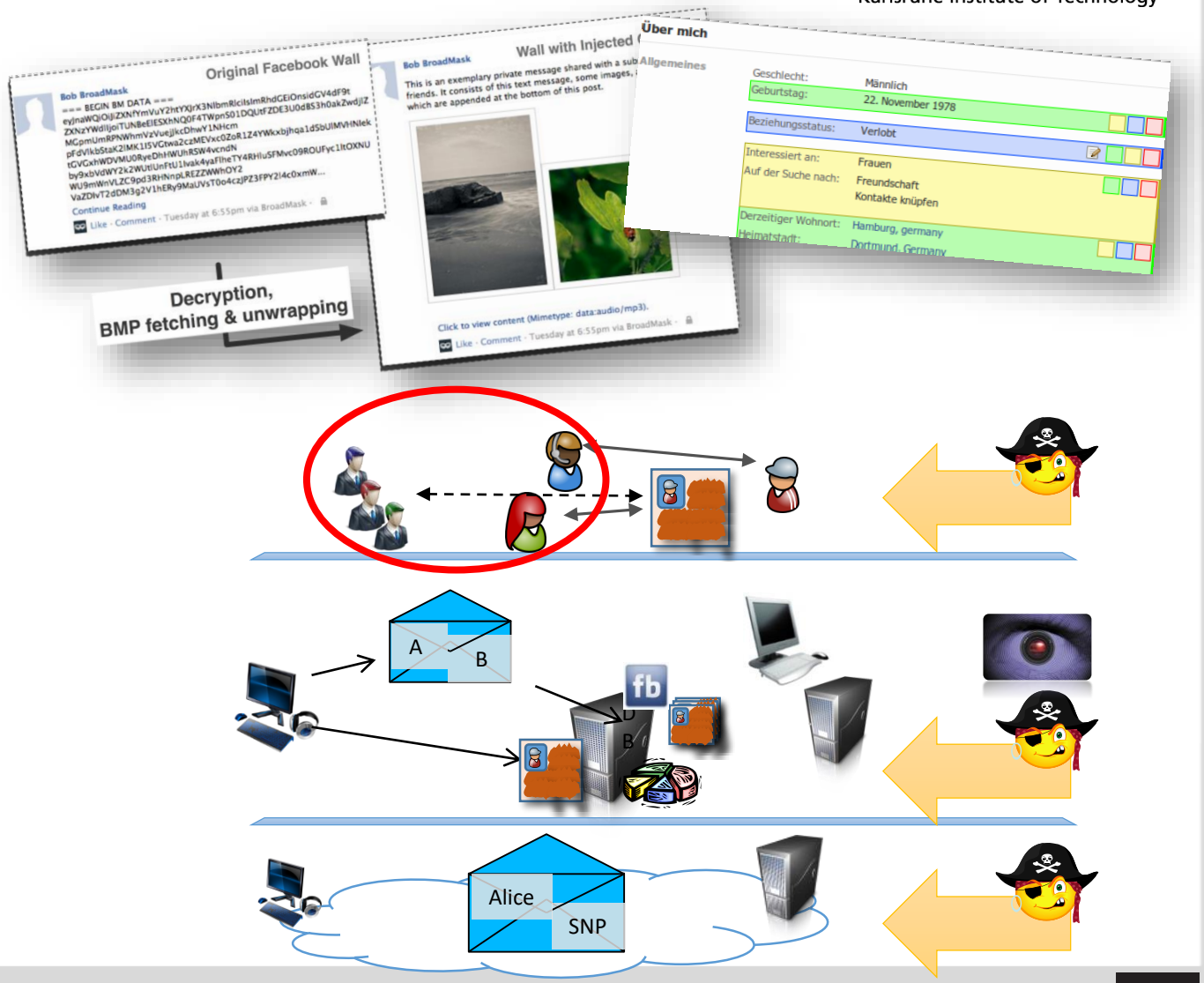
Modellierung und Akteure



Source: T. Cutillo

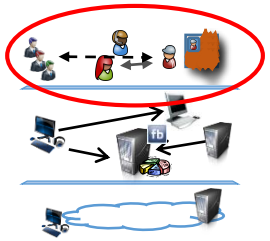
Lösungsklassen und Beiträge des Lehrstuhls

- ***Verständnis der Benutzung***
  - Intentions-Erkennung
  - Benutzer-Unterstützung
  - Privacy-Analysen



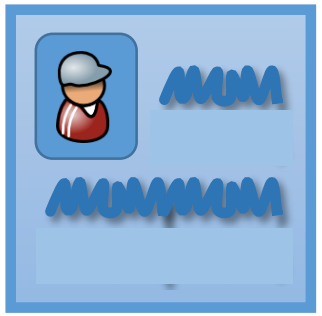
[7] FC '11
[8] WWW '12

Inhalt Geschützt, also: „Nur Meta-Daten“



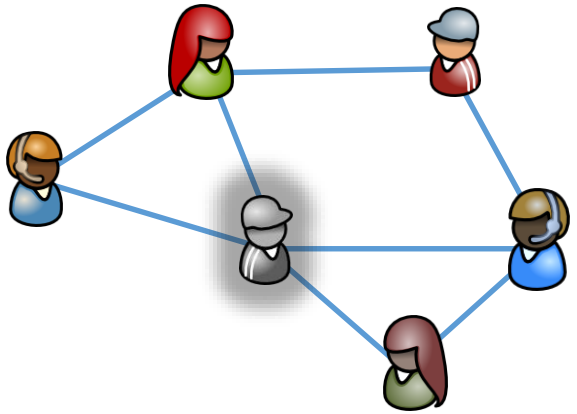
„Facebook Mining“ Angriffe

- Vorlesung 5/7 Semester (Studenten ohne ML-Erfahrung)



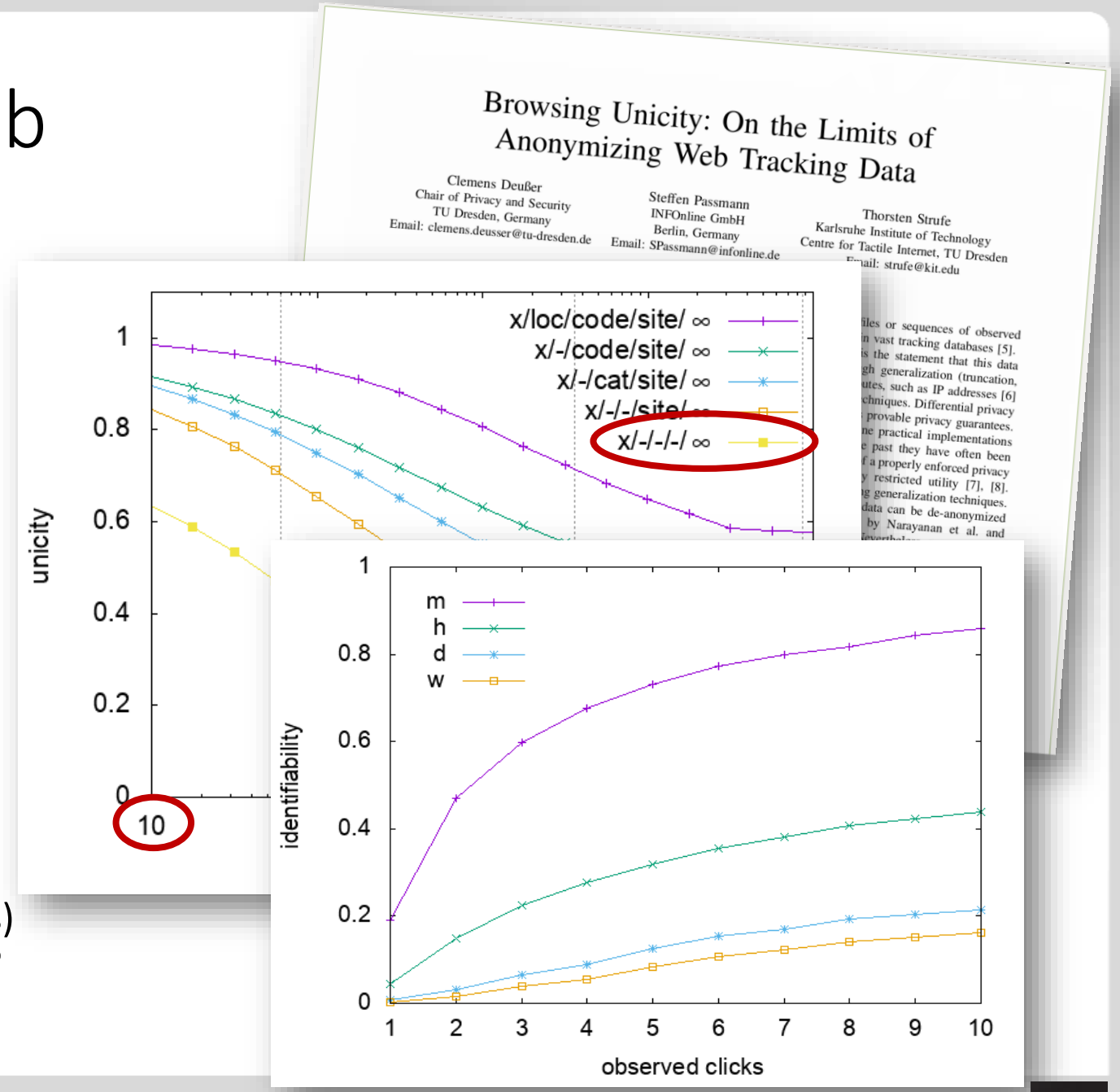
- Eingabedaten:
  - Teilprofile
  - Nachbarschaft

- Mit hoher Genauigkeit inferiert:
  - Geschlecht
  - Alter
  - Bildungsstand
  - Arbeitgeber-Treue
  - Sexuelle Präferenzen
  - Politische Einstellungen



Identifizierbarkeit im Web

- Web-Tracking ist allgegenwärtig
- Situation:
  - Tracker behaupten Anonymisierung
  - „Oktett löschen“: Generalisierung
  - DS-GVO: Pseudonym ≠ Anonym
- Studie
  - Kooperation mit Industriepartner
  - Umfassende Datenbanken (deutscher Web-Markt, 2-3 Mrd Besuche pro Tag)
  - Fragen:
    - Entstehen pseudonyme Daten (Ausmaß)
    - Wie schnell ist ein Trace identifizierbar?

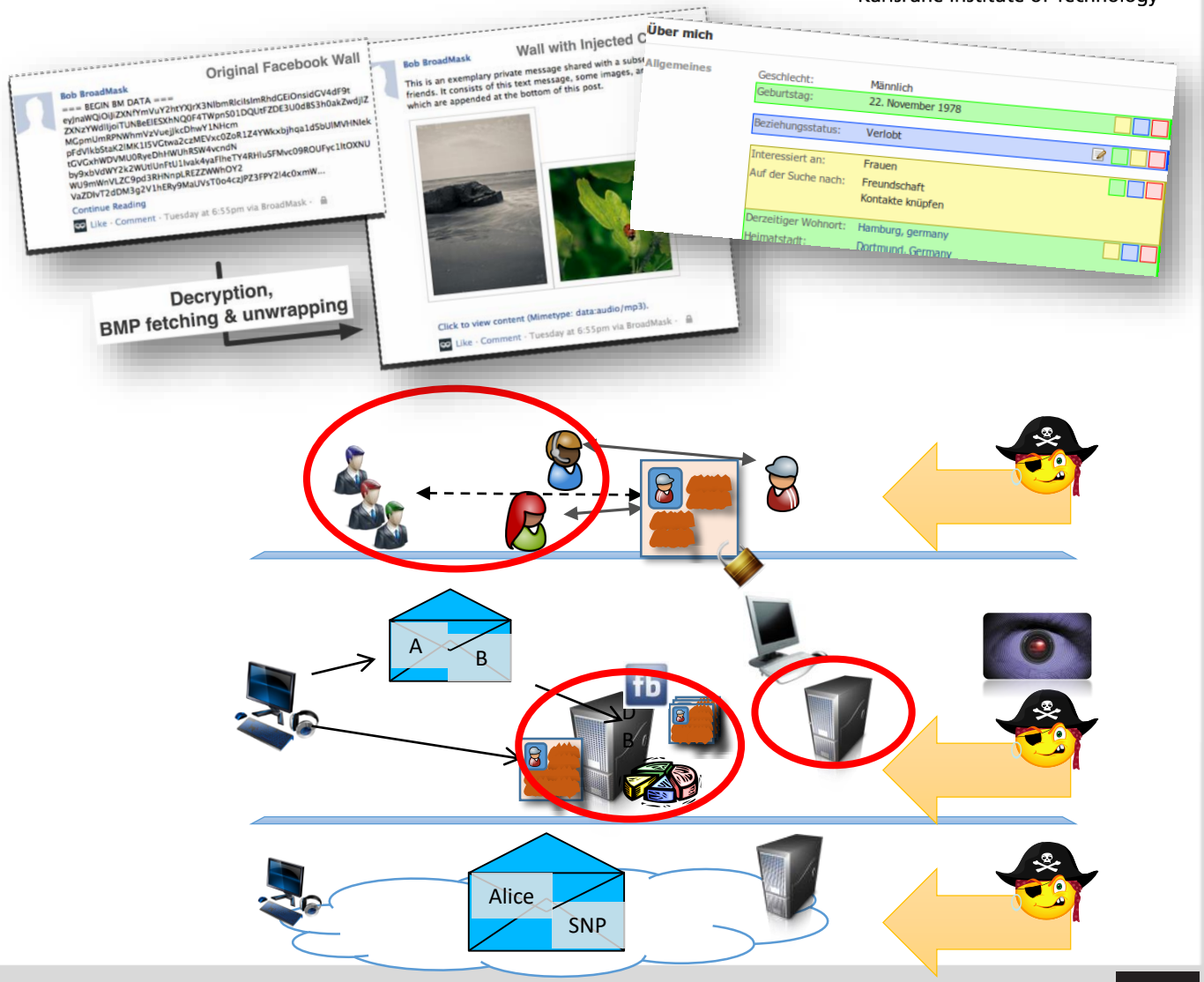


[9] IEEE S&P ’20

Lösungsklassen und Beiträge des Lehrstuhls

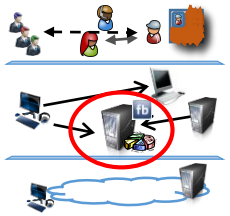
- ***Verständnis der Benutzung***
  - Intentions-Erkennung
  - Benutzer-Unterstützung
  - Privacy-Analysen

- ***Privacy-Enhancing Technologies***
  - Anonymitäts-Metriken/Analysen
  - Anonyme Kommunikation
  - Anonyme Dienste (F2F/Web)



PETs: Verteilung von Daten und Kontrolle

Karlsruhe Institute of Technology



- ***Dezentralisierung der Dienste***

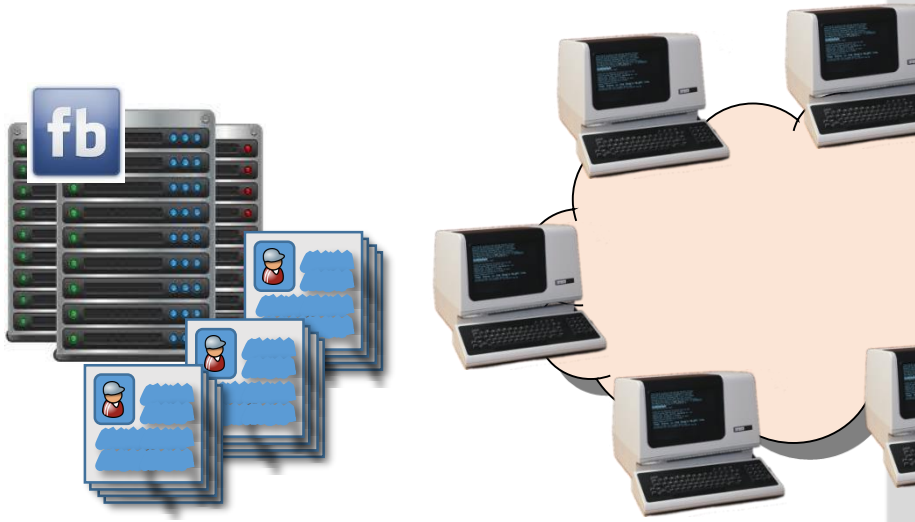
- Federated SNS

diaspora*

- DOSN

Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND

Deutscher Bundestag



- Social overlays/“darknets“

TED
IDEASWORTHSPREADING

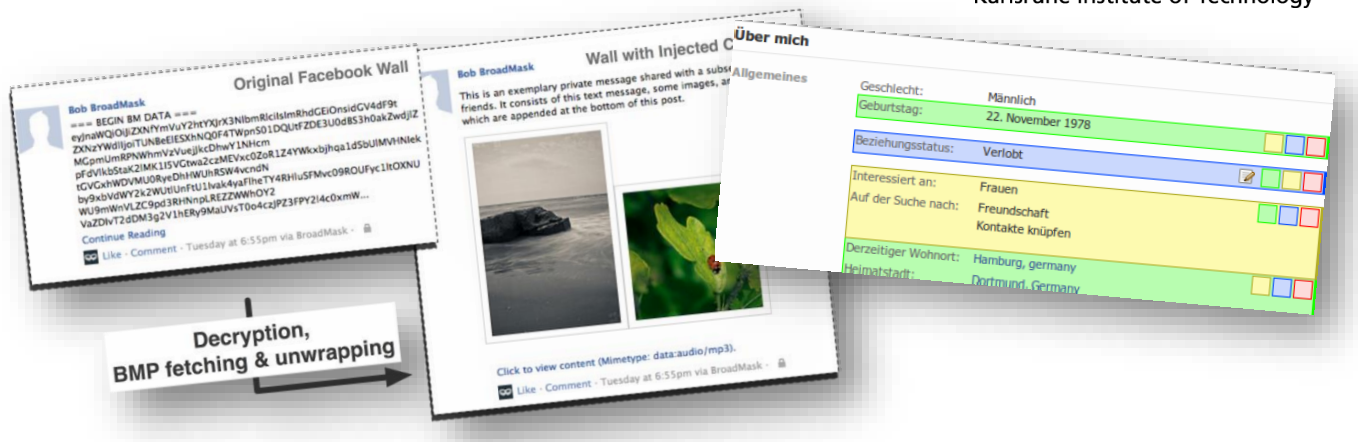
[10] ICC ’13
[11] Comm.Mag
[12] INFOCOM ’13
[13] INFOCOM ‘15
[14] INFOCOM ‘16
[15] INFOCOM ’17
[16] PETS ‘14

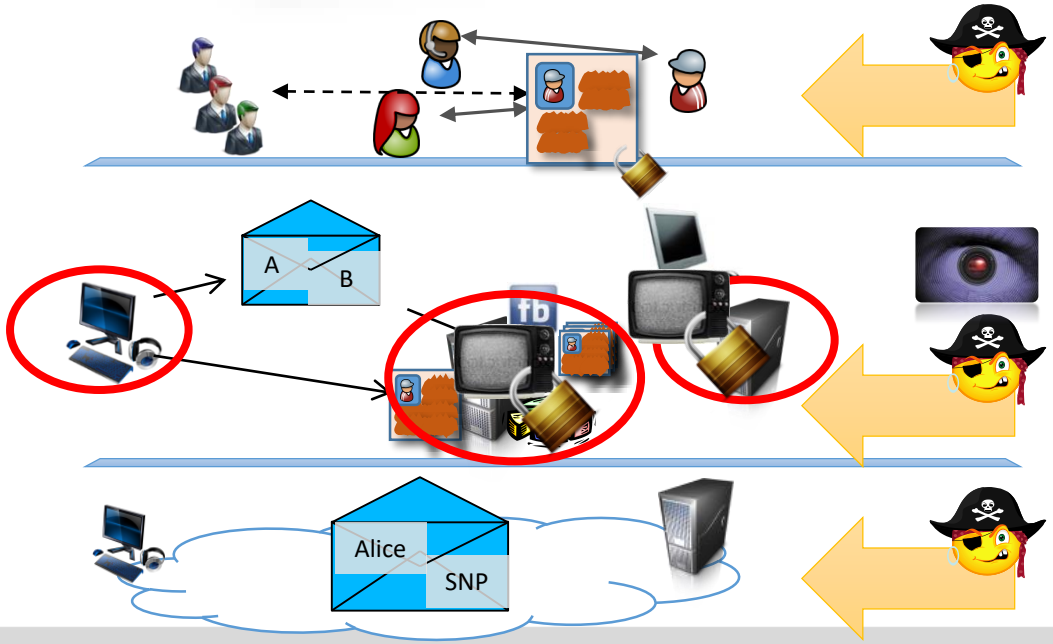
KASTEL

Lösungsklassen und Beiträge des Lehrstuhls

- ***Verständnis der Benutzung***
  - Intentions-Erkennung
  - Benutzer-Unterstützung
  - Privacy-Analysen

- ***Privacy-Enhancing Technologies***
  - Anonymitäts-Metriken/Analysen
  - Anonyme Kommunikation
  - Anonyme Dienste (F2F/Web)

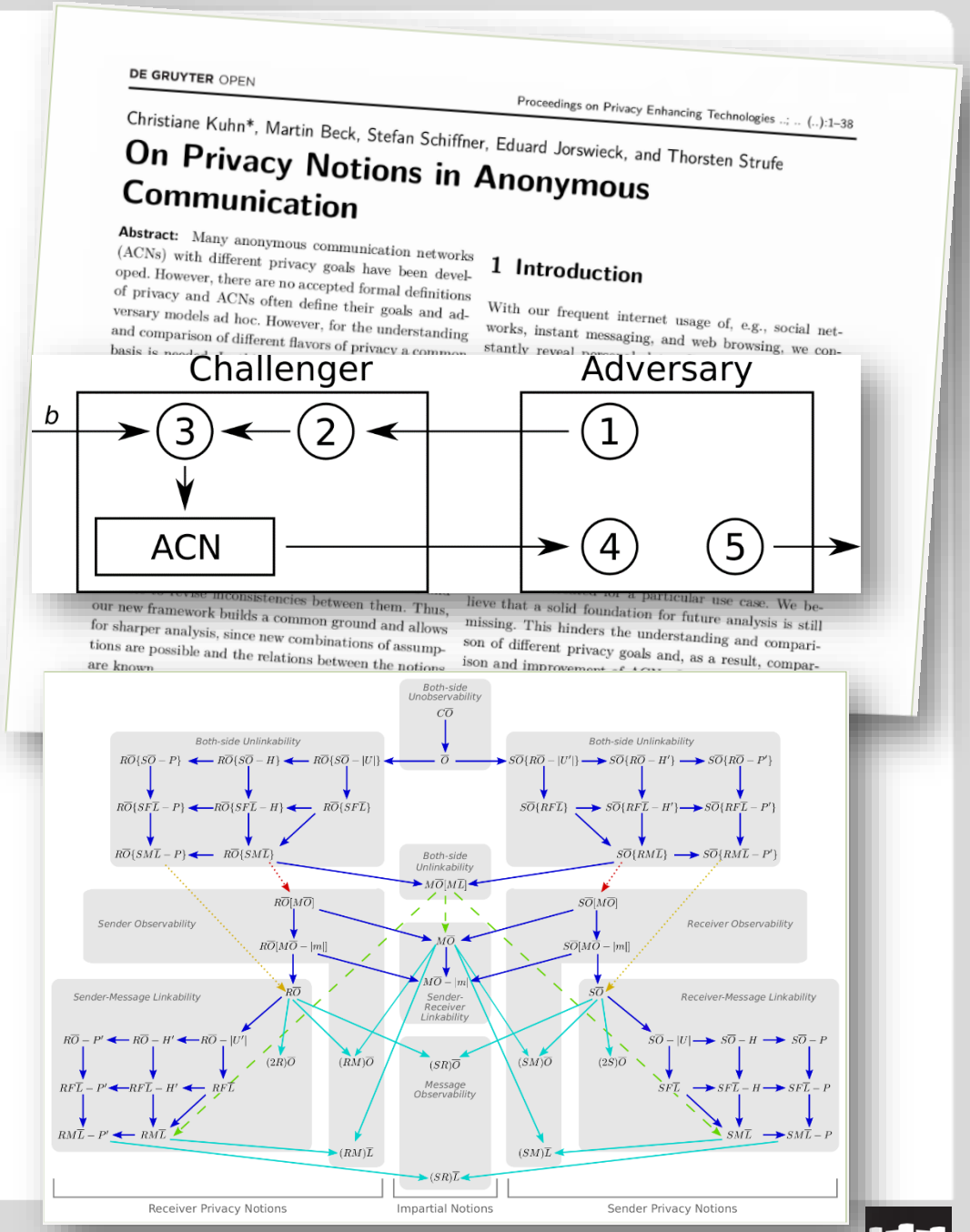




Bewertung der Anonymisierung

- Vielzahl an Anonymisierungsnetzen
  - *TOR, AN.ON, DC, HORNET, Loopix, ZCash,…*
  - Viele behaupten *„Sender-Anonymität“*, einige *„Empfänger-Anonymität“*, einige *„Transaktions-Vertraulichkeit“*
  - Literatur kennt *„Unlinkability“*, *„Unobservability“*, *„Pseudonymity“*, *„*-Anonymity“*, *„Anonymity Sets“*, *„Indistinguishability“*
  - Was bedeutet das nun alles?

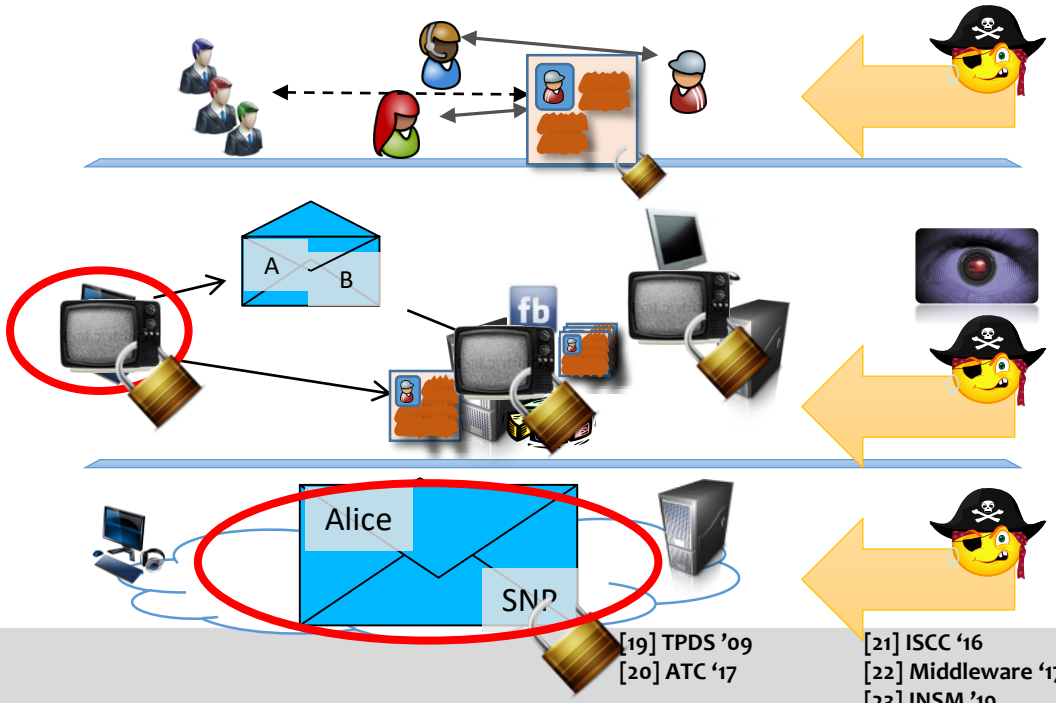
- Studie
  - Formalisierung von Anonymität im Netz basierend auf Spielen
  - Berücksichtigung beobachtbarer Kommunikationseigenschaften
  - Definition und Analyse unterschiedlicher Privacy-Notions, sowie ihrer Abhängigkeiten



[17] PETS ’19
[18] S&P ‘20

Lösungsklassen und Beiträge des Lehrstuhls

- ***Verständnis der Benutzung***
  - Intentions-Erkennung
  - Benutzer-Unterstützung
  - Privacy-Analysen
- ***Privacy-Enhancing Technologies***
  - Anonymitäts-Metriken/Analysen
  - Anonyme Kommunikation
  - Anonyme Dienste (F2F/Web)
- ***Praktische/Netzsicherheit***
  - SDN/NFV-Absicherung
  - Netzisolation/VPN-Sicherung
  - Denial-of-Service Resistenz



[19] TPDS '09
[20] ATC '17
[21] ISCC '16
[22] Middleware '17
[23] INSM '19

Zukunft bei KIT/IT-Sec

- Vernetzung nimmt zu und kulturelle Praktiken ändern sich rasant
- Wir wollen
- Die ***Sicherheit von Netzen*** und vernetzten Geräten erhöhen
- Systeme ***dezentralisieren*** und Komponenten ***isolieren***
- Die ***Privatsphäre*** schützen helfen und Beeinträchtigungen verhindern
- ***Benutzer-Intentionen*** verstehen, Hilfen anbieten, ***Missbrauch unterbinden***
- Privacy messbar machen, Systematik für Analyse und Entwicklung anbieten

References

[1] Thorsten Strufe. Ein Peer-to-Peer-basierter Ansatz für Live Multimedia-Streaming. PhD Thesis. 2007

[2] Wolfgang Effelsberg, Ralf Steinmetz, and Thorsten Strufe (Eds.): "Benchmarking Peer-to-Peer Systems - Understanding Quality of Service in Large-Scale Distributed Systems.", LNCS State of the Art Surveys, 7847, Springer, Heidelberg, 2013

[3] Timo Richter, Stefan Escher, Dagmar Schönfeld, and Thorsten Strufe. Forensic analysis and anonymisation of printed documents. ACM Information Hiding and Multimedia Security. 2018

[4] Thomas Paul, Sonja Buchegger, and Thorsten Strufe. Decentralized social networking services. Trustworthy Internet, 187-199. 2011

[5] Axel Schulz, Benedikt Schmidt, and Thorsten Strufe. Small-scale incident detection based on microposts. ACM Hypertext & Social Media, 3-12. 2015 (best paper award)

[6] Leucio-Antonio Cutillo, Mark Manulis, and Thorsten Strufe. Security and privacy in online social networks. Handbook of Social Network Technologies and Applications, 497-522. 2010

[7] Felix Günther, Mark Manulis, and Thorsten Strufe. Cryptographic treatment of private user profiles. International Conference on Financial Cryptography and Data Security, 40-54. 2011

[8] Thomas Paul, Martin Stopczynski, Daniel Puscher, Melanie Volkamer, and Thorsten Strufe. C4ps: colors for privacy settings. Proceedings of the 21st International Conference on World Wide Web, 585-586. 2012

[9] Clemens Deußer, Steffen Passmann, and Thorsten Strufe. Browsing Unicity: On the limits of anonymizing web tracking data Inproceedings. IEEE Symposium on Security and Privacy (S&P), 2020

[10] Stefan Schulz, and Thorsten Strufe. d^2 Deleting Diaspora: Practical attacks for profile discovery and deletion. IEEE International Conference on Communications (ICC), 2042-2046. 2013

[11] Leucio-Antonio Cutillo, Refik Molva, and Thorsten Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. IEEE Communications Magazine 47 (12), 94-101. 2009

[12] Stefanie Roos and Thorsten Strufe. A contribution to analyzing and enhancing darknet routing. IEEE INFOCOM, 615-619. 2013

[13] Stefanie Roos and Thorsten Strufe. On the impossibility of efficient self-stabilization in virtual overlays with churn. IEEE INFOCOM, pages 298 – 306, 2015

[14] Stefanie Roos, Martin Beck, and Thorsten Strufe. Anonymous Addresses for Efficient and Resilient Routing in F2F Overlays. IEEE INFOCOM, 2016

[15] Stefanie Roos, Martin Byrenheid, Clemens Deusser, and Thorsten Strufe. BD-CAT: Balanced Dynamic Content Addressing in Trees. IEEE INFOCOM, 2017

[16] Stefanie Roos, Benjamin Schiller, Stefan Hacker, and Thorsten Strufe. Measuring freenet in the wild: Censorship-resilience under observation. Privacy Enhancing Technologies Symposium, 263-282, 2014

[17] Christiane Kuhn and Martin Beck and Stefan Schiffner and Eduard Jorswieck and Thorsten Strufe. On privacy notions in anonymous communication. Proceedings on Privacy Enhancing Technologies (2), 105-125. 2019

[18] Christiane Kuhn, Martin Beck, and Thorsten Strufe. Breaking and (partially) fixing provably secure onion routing. IEEE Symposium on Security and Privacy (S&P), 2020

[19] Michael Brinkmeier, Günter Schäfer, and Thorsten Strufe Optimally dos resistant p2p topologies for live multimedia streaming. IEEE Transactions on Parallel and Distributed Systems 20 (6), 831-844. 2009

[20] Martin Beck, Pramod Bhatotia, Rui-Chuan Chen, Christof Fetzer, and Thorsten Strufe. PrivApprox: privacy-preserving stream analytics. USENIX ATC, 659-672. 2017

[21] Hani Salah, and Thorsten Strufe. Evaluating and mitigating a collusive version of the interest flooding attack in NDN. IEEE ISCC, 938-945. 2016

[22] Do Le Quoc, Rui-Chuan Chen, Pramod Bhatotia, Chirstof Fetzer, Volker Hilt, and Thorsten Strufe. StreamApprox: approximate computing for stream analytics. ACM/IFIP/USENIX Middleware, 185-197. 2017

[23] Tao Li, Hani Salah, Xin Ding, Thorsten Strufe, FHP Fitzek, Silvia Santini. INFAS: In-Network Flow mAnagement Scheme for SDN Control Plane Protection IFIP/IEEE Symposium on Integrated Network and Service Management. 2019

[A] Kosinski, Michal & Stillwell, David & Graepel, Thore. Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences of the United States of America. 2013

[B] Le Chen, Chi Zhang, and Christo Wilson. Tweeting under pressure: analyzing trending topics and evolving word choice on sina weibo. ACM conference on Online social networks. 2013

[C] Jillian York. The harms of surveillance to privacy, expression and association. Global Information Society Watch. 2013

[D] Frank La Rue. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. UN Human Rights Council. 2013

[E] Shklovski, Irina & Kotamraju, Nalini. Online contribution practices in countries that engage in internet blocking and censorship. Conference on Human Factors in Computing Systems. 2011

[F] Ben Wagner, Joanna Bronowicka, Cathleen Berger, and Thomas Behrndt. Surveillance and censorship:The impact of technologies on humanrights. Report of the Directorate General for External Policies of the European Parliament. 2015