The e-privacy proposal: legal consistency with other legal instruments; level playing field

Hearing on ePrivacy

"The proposed rules for the protection of personal data in the electronic communications in the EU"

European Parliament,
LIBE Committee

2017-04-11

Prof. Dr. Kai Rannenberg
Deutsche Telekom Chair of
Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Acknowledgements

- Associations involved in discussions
  - Council of European Professional Informatics Societies (CEPIS)
  - Trust in Digital Life (TDL)
- Examples of consulted sources
  - Article 29 DP Working Party
  - European Academy for Freedom of Information and Data Protection (EAID)
  - European Telecommunications Network Operator's Association (ETNO)
  - Individual experts and organisations
  - Colleagues at Goethe University Frankfurt
- The statement is personal.

Overview

- The paradox of (protected) electronic communication
- Electronic communication and the need for protection
- The OTT market and the need for a level playing field
  - Location data and OTT user profiles
  - Wifi/Bluetooth tracking
  - Privacy settings & security risks
  - Internet of Things

Addressing the paradox of (protected) electronic communication

- Electronic communication is more and more in need of protection of privacy and confidentiality.
- Offering properly protected communication is (often) not properly honored by the market:
  - Unprotected communication is offered for free.
  - Regulation so far covers only one market segment ("traditional" telcos).
  - No level playing field.

➢ Including Over-the-Top communications services (OTTs) into the scope of the regulation is essential for effective protection.

➢ It needs to be done thoroughly.

Electronic communication and the need of protection

- Privacy protected communication is not only an fundamental right (EU Charter Article 8) individual for the individual, but an essential prerequisite for a working democracy.
- Communication metadata are a well structured data sets, that can very easily be exploited by attackers with computing capabilities.
- Communication content needs to be transferred, often into another domain, so it is inherently at risk.

➢ GDPR would not be enough to cover this.

Communication services not a product on its own (anymore)

- Simple (unprotected) digital communication can technically be provided as a byproduct or free service especially if one considers user data as a resource.
  - OTTs offer “free” communication in exchange for personal data (WhatsApp, Facebook, Instagram, …).
  - Prices and margins for communication services go down (often to 0).
  - If there are no trust guarantees we end up with a “Lemons Market”, the loss of trust, and detrimental effects for democracy.
- Art. 3(1)(a) "irrespective of a payment" and (Art. 4(2) "ancillary feature") are important features to cover this development.
- But more is needed.

Aspects of the OTT market

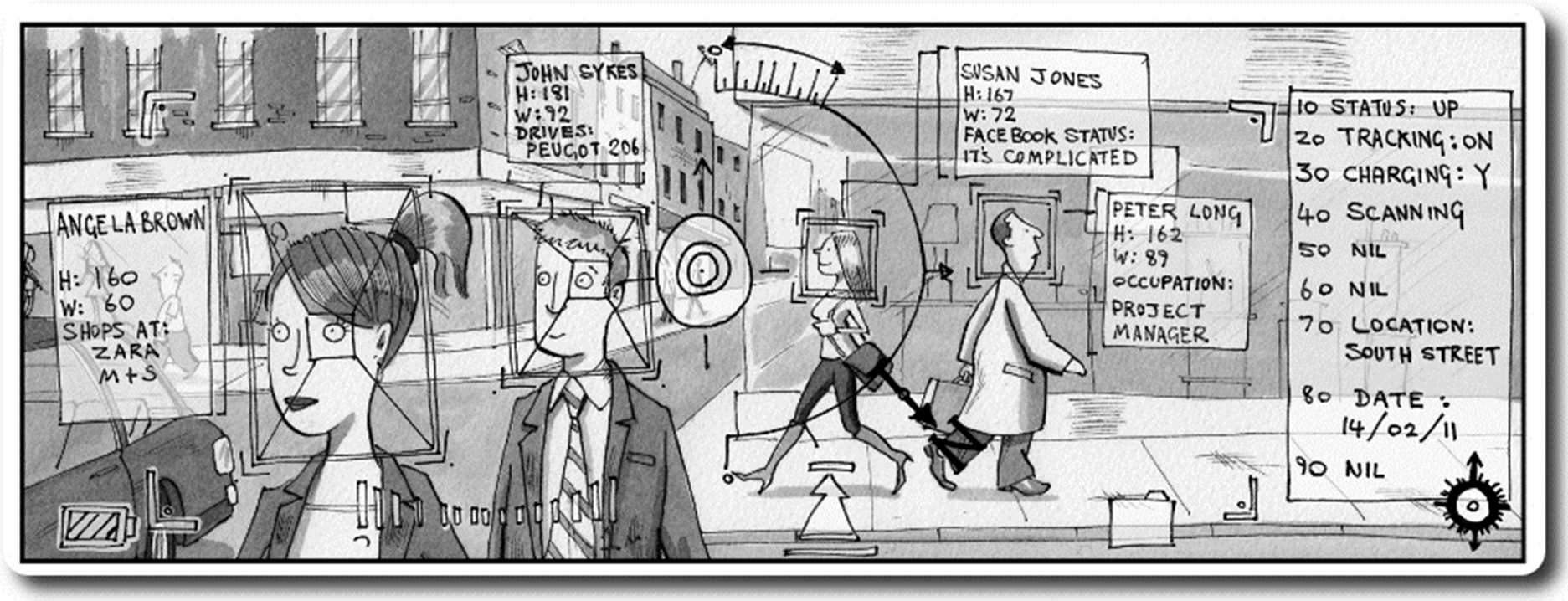
- Incentive (triggered by e.g. via venture investors) to quickly collect large numbers of registered "users" and their (movement) profiles (users = resources ≠ customers)
- Application segments not (yet) clearly defined, e.g.
  - Messaging part of social network (Facebook) experience?
  - Household management part of Google experience?
- Trend towards market domination by a single or very few players "owning" data (re)sources
- Is this situation a solid basis to protect constitutional values?

➢ Providers of better (protected) services need better protection to move towards a level playing field.

➢ OTTs need to be covered more comprehensively:

- ➢ Location data
- ➢ Web-tracking, offline-tracking (via Wifi or Bluetooth)

Location data tightly coupled with OTT user profiles



- Needs to be considered in
  - Art. 4(3)(c): Definition of "electronic communications metadata"
  - Art. 8(2)(b): Collection zones with Wifi/Bluetooth tracking

[www.thebigdatainsightgroup.com/site/article/big-data-talk-005-big-data-big-brother]

Location data Definition

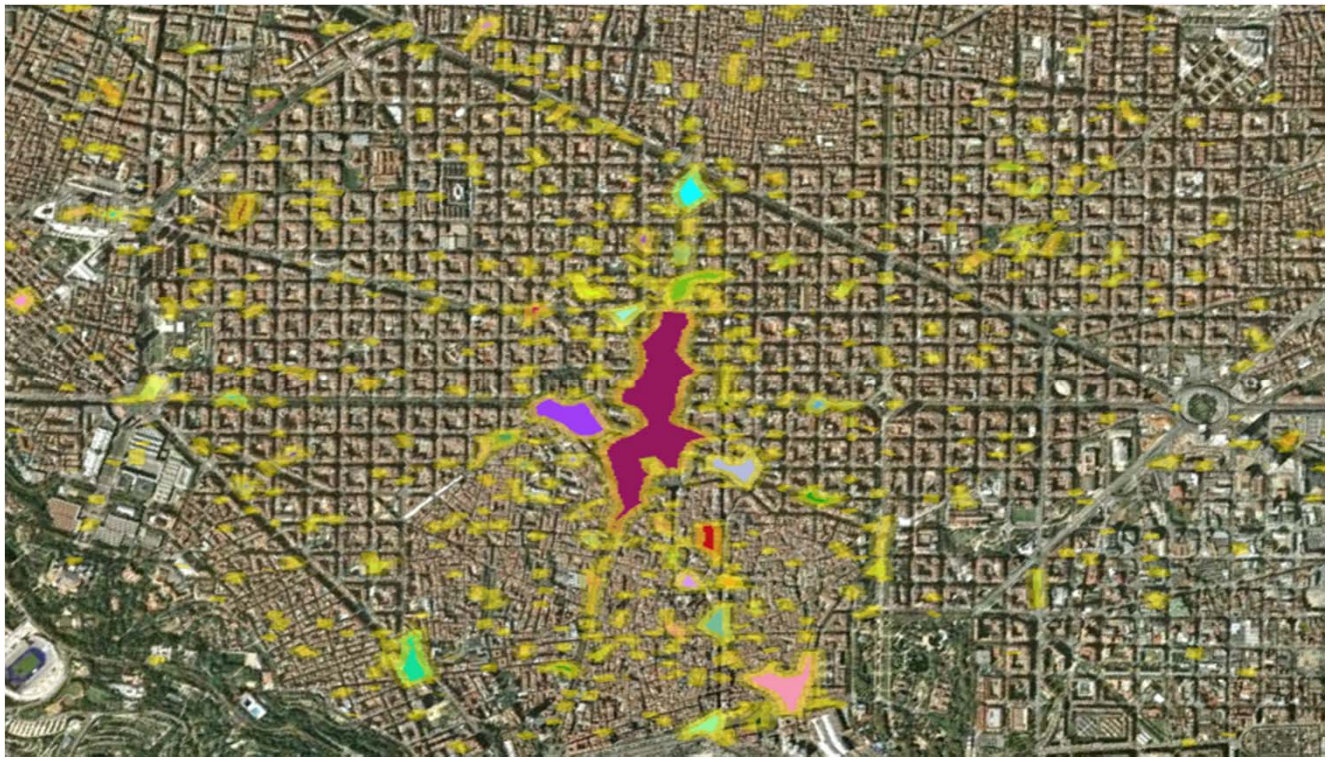
- Art. 4 (3)(c): " 'electronic communications metadata' means [...], including [...] **data on the location of the device generated in the context of providing electronic communications services**, [...]"
- Too narrow:
  - Telcos are covered.
  - OTTs are not covered!

➢ Only limited protection for users (and the borderline is hard to understand for users)

➢ Competitive disadvantage for telcos (European players)

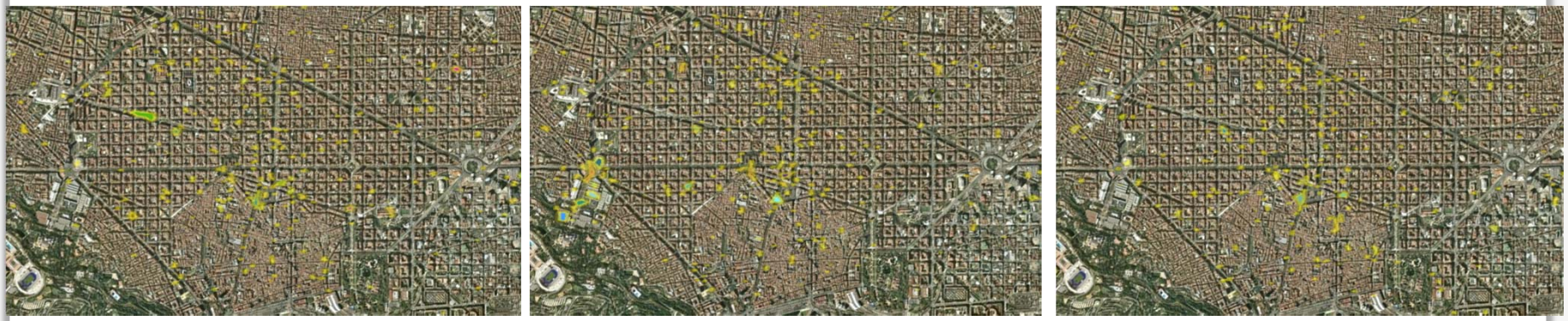
➢ **Delete the text in red.**

Location data, Recital (17)
Heatmaps (Geo-spatial Clustering)

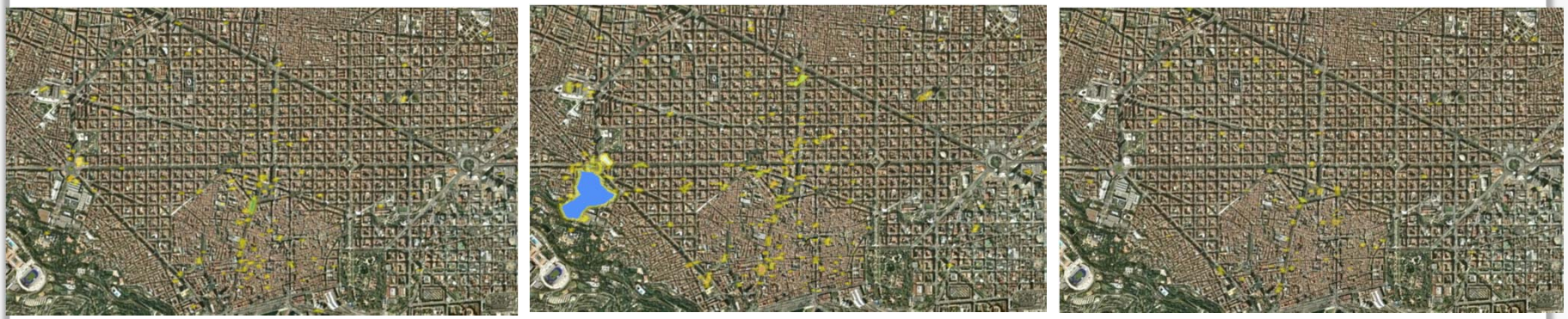


Location data, Recital (17)
Traffic Movements

Locals



Tourists



- Traffic movements can be shown with anonymous data also.
  - ➢ No (pseudonymous) identifier needed
  - ➢ Change Recital (17)

Art. 8(2)(b): Collection Zones with Wifi/Bluetooth tracking

- Person responsible for collection must indicate measures end-users may take to minimize or stop the collection.
- Gives the impression that organisations may collect information emitted by terminal equipment to track the physical movements of individuals (such as "Wifi/Bluetooth-tracking") without the consent of the individual concerned.
- The party collecting these data could apparently comply by means of a notice informing users to switch off their devices, when they do not want to be tracked.

➢ Contrary to a basic goal of the telecommunications policy of the European Commission to provide high-speed mobile internet connectivity with strong privacy protections at a low cost to all Europeans, across borders.

Covering the OTT market towards a more level playing field

? Level playing field with GDPR regulated players:

- ✓ Only DPAs as supervisors
- ✓ Consistency Mechanism
- ✓ EDPB
- – Art. 21(1) lacks link to Art. 80 GDPR (Representation of data subjects)
- – Art. 23:
  - – Art. 8 and 10 deserve higher fines
  - – Why dependencies from Member States provisions?

Articles 10 and 17
Privacy settings & security risks

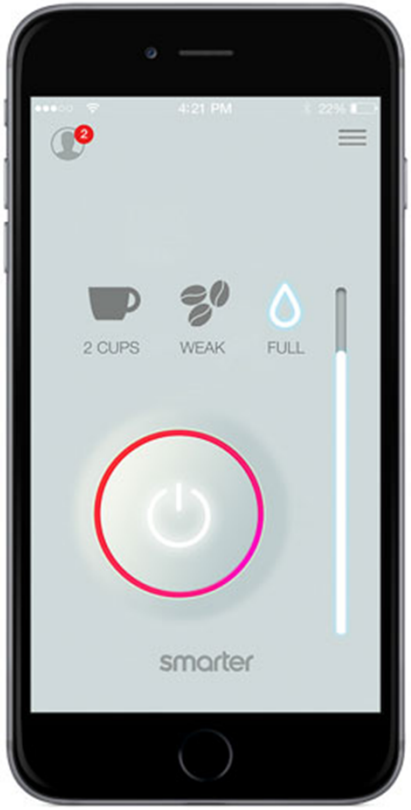
- Communicating (Internet of Things) devices go way beyond
  - (Smart) phones and tablets
  - Devices provided by a telco
- Recent web protocols (Bluetooth Web API) enable websites to search via Bluetooth for devices near the surfing device
  - Learn, what devices the surfing visitor has
  - Try to access them and check security settings
- ➢ Include Hardware and hardware providers in duties for
  - ➢ Offering privacy settings
  - ➢ Informing about security risks
- ➢ *Mandate app market operators and app providers to give information on
  - ➢ privacy properties of apps and
  - ➢ privacy risks of apps

*Additional point following a request in the discussion, cf. presentation in Annex 1

7.40 am – Making coffee

Information:

- Daily routines
- Coffee consumption

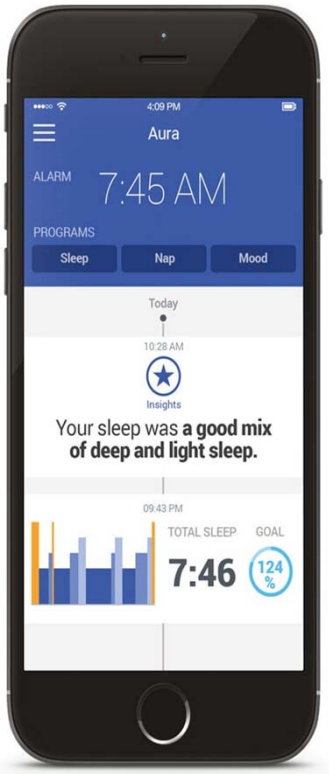


[Philipps / Saeco]

7.45 – Getting up

Information:

- Sleep rhythm
- Sleeping habits



[Withings]

7.50 – Shaving (foam running out)

Information:

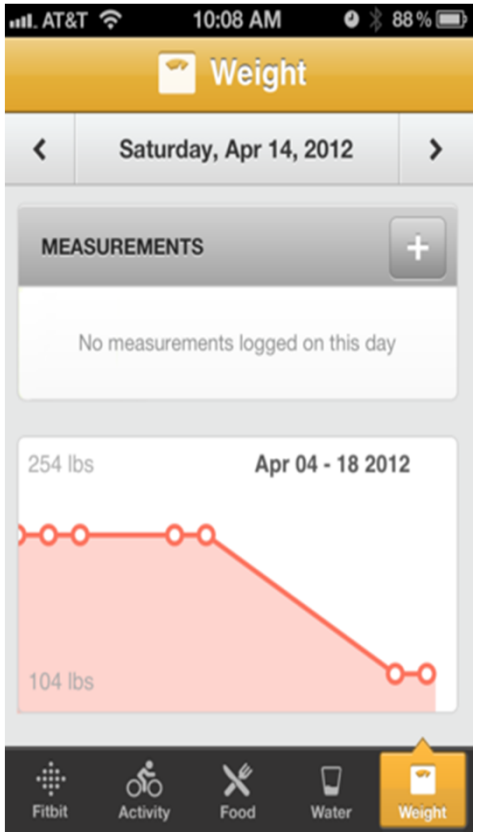
- Daily routine
- Preferred products

[Amazon]

7.52 – Weighing

Information:

- Daily routine
- Weight



[Fitbit]

7.55 – Cleaning teeth

Information:

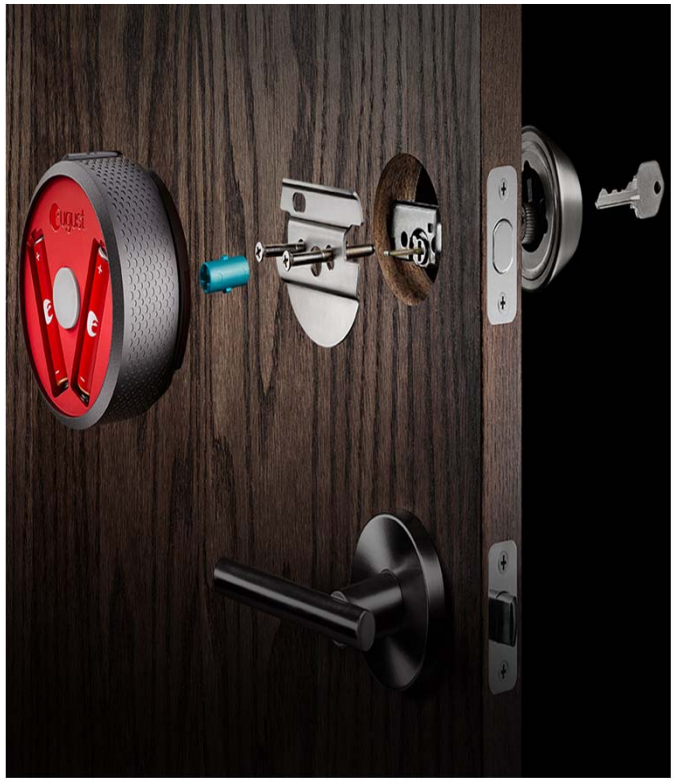
- Daily routine
- Dental health (care)

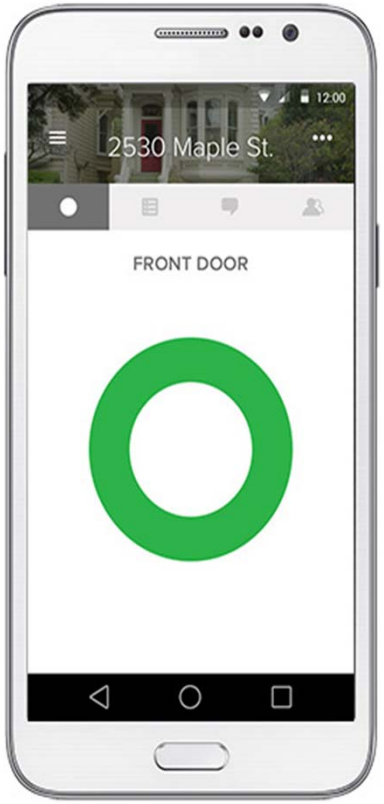
[Oral-B]

8.30 – Locking the door

Information:

- Daily routine
- Persons in household



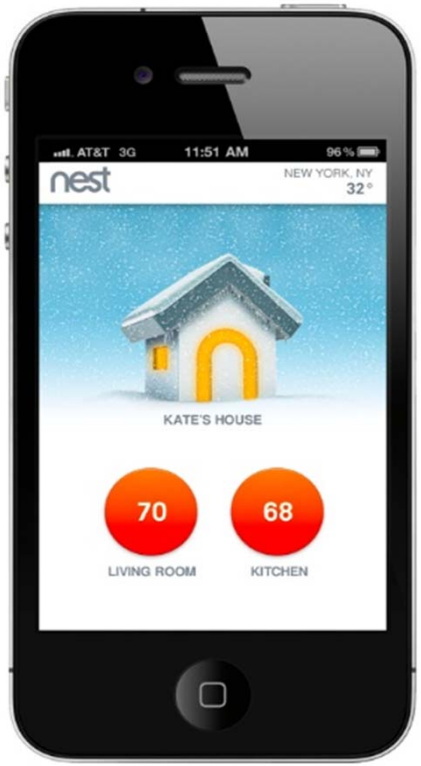


[August]

8.35 – Turning heating down

Information:

- Daily routine
- Persons in house

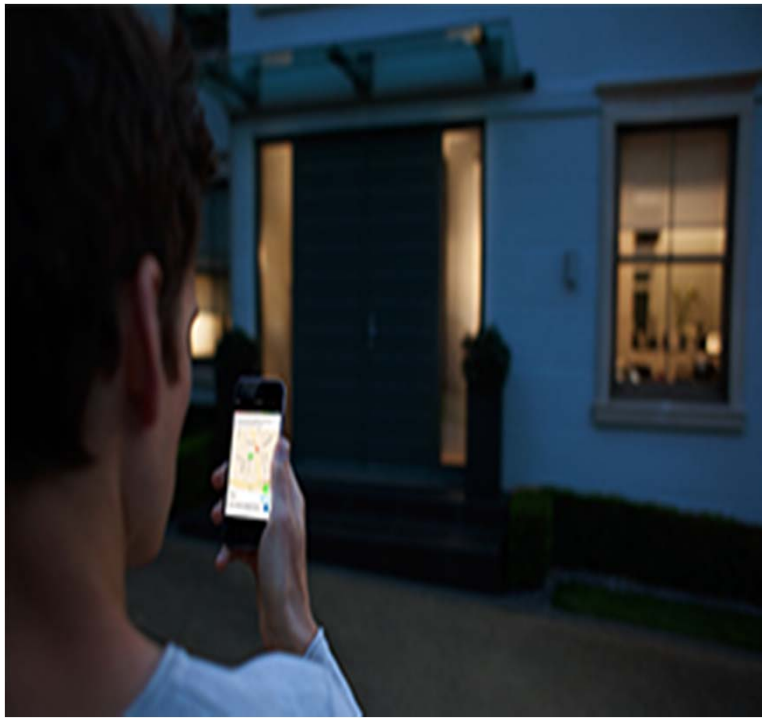


[Nest]

8.40 – Lights out?

Information:

- Daily routine
- Persons in house



[Philipps]

More devices

[Sony]

[Mattel]

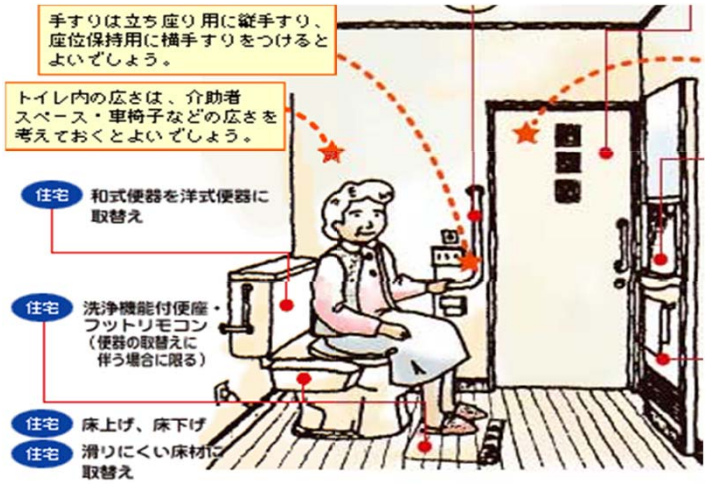
[LG]

[Beurer]

[Source: Discovergy]

The networked washlet

- … and in Japan, Matsushita has demonstrated a health-monitoring toilet that can analyze your stool and send the information online to your doctor. [www.asiaweek.com/asiaweek/technology/article/0,8707,130495,00.html, 2001-06-22]
- “ … sensors detect seven abnormal behavior patterns of the elderly in their living quarters and three abnormal patterns in the toilet area. Any abnormality that is sensed is automatically transmitted to the PHS terminals or pagers of the nursing staff. The care monitor system that uses these sensors will help provide safe and high quality nursing service.” [www.mew.co.jp/e-tecrepo/73e/main02.html]



[Hitachi, Matsuhita Electric Works Limited, Panasonic, Toto]

Annexes

1. **As a (requested) example for a Privacy provision, that the ePrivacy Regulation could mandate, please find the presentation:** User Control Mechanisms for Privacy Protection Should Go Hand in Hand with Privacy-Consequence Information: The Case of Smartphone Apps [**Bal, Rannenberg 2014]**
2. **References**

Annex 1

1. **As a (requested) example for a Privacy provision, that the ePrivacy Regulation could mandate, please find the presentation:** User Control Mechanisms for Privacy Protection Should Go Hand in Hand with Privacy-Consequence Information: The Case of Smartphone Apps [**Bal, Rannenberg 2014]**

User Control Mechanisms for Privacy Protection Should Go Hand in Hand with Privacy-Consequence Information: The Case of Smartphone Apps

W3C Workshop on Privacy and User–Centric Controls

20–21 November 2014, Berlin, Germany

Dipl.-Inf. Gökhan Bal, Prof. Dr. Kai Rannenberg
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

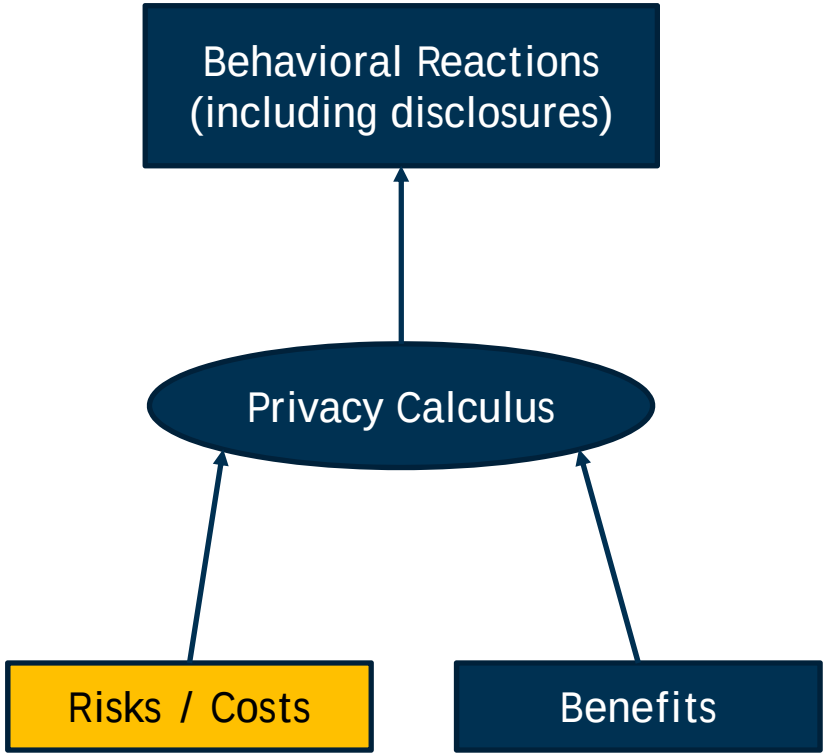
1 MOTIVATION

1. Motivation
Two Perspectives on Privacy Protection

Privacy Protection as a Process (Brunk 2005)

Risk awareness is key!

Decision-making as a calculus of risks and benefits (Culnan and Armstrong 1999)



1. Motivation
Problems

- Benefits are what drive users towards service use.
- Privacy thoughts most often are only a „supporting actor" in users' decision-making.
- More effective privacy-risk communication is needed to help users understand the consequences of behavior.
- **Call: integrate (privacy-)consequence information into user-control mechanisms.**

2 THE CASE OF SMARTPHONE APPS

2 The Case of Smartphone Apps
Privacy Risks of Smartphone App Usage

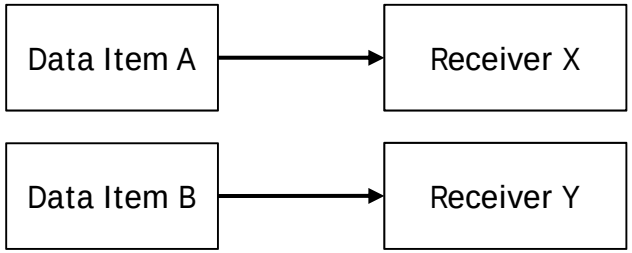
- Apps are useful and provide utility.
- APIs (e.g. geolocation API) as
  - …enabler of utility.
  - …threat to user privacy.
- Negative examples: „Path“ & „Brightest Flashlight“
- Lack of risk transparency and “hidden” information flows lead to a bias in users’ risk perceptions.
- Explicitness regarding consequences can help (Laughery et al. 1993).

2 The Case of Smartphone Apps
Privacy Risks of Smartphone App Usage

First-order privacy risk:

- apps can access a multiplicity of sensitive resources (enabled to provide utility).
- most apps have Internet access.
- information flows often without notice.

→ **risk: leakage of sensitive data[1].**

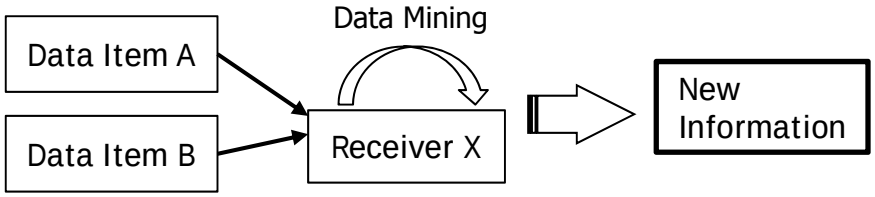


[1]e.g., Egele et al. 2011; Enck et al. 2010

Second-order privacy risk:

- Profiling: aggregated smartphone data can be used to generate meaningful information about the user (predict user traits, personality traits, movement patters)[2]

→ **risk: implicit revelations of private information due to data-aggregation potentials.**

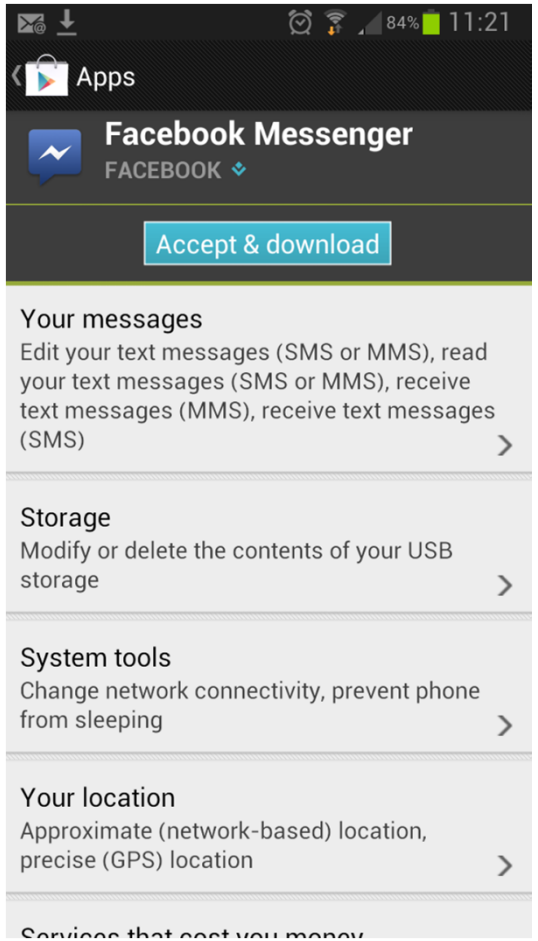


[2]e.g., Kwapisz et al. 2010; Weiss and Lockhart 2011; Chittaranjan et al. 2011; Min et al. 2013; González et al. 2008; Phithakkitnukoon et al. 2010.

2 The Case of Smartphone Apps
Current Privacy-Risk Communication

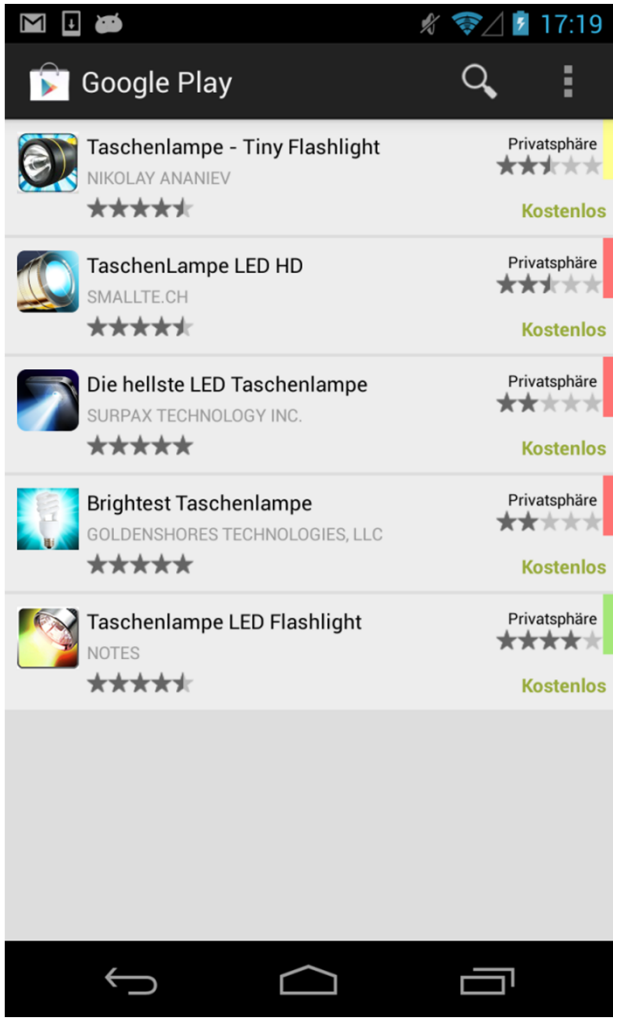
Current privacy risk information is…

- … static,
- … coarse-grained & technical,
- … timed inappropriately,
- … ignored largely,
- … does not support informed decision-making.



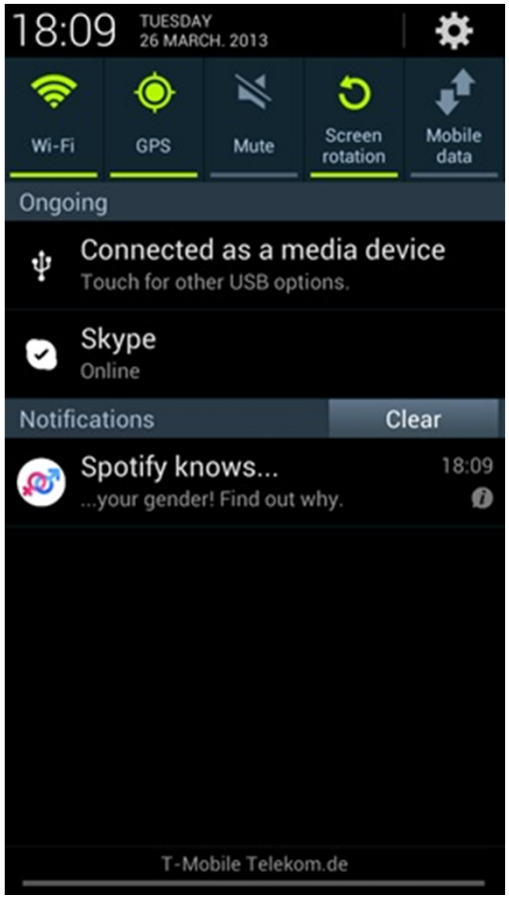
2 The Case of Smartphone Apps

Suggested New Approaches (1/2): Google Play Study



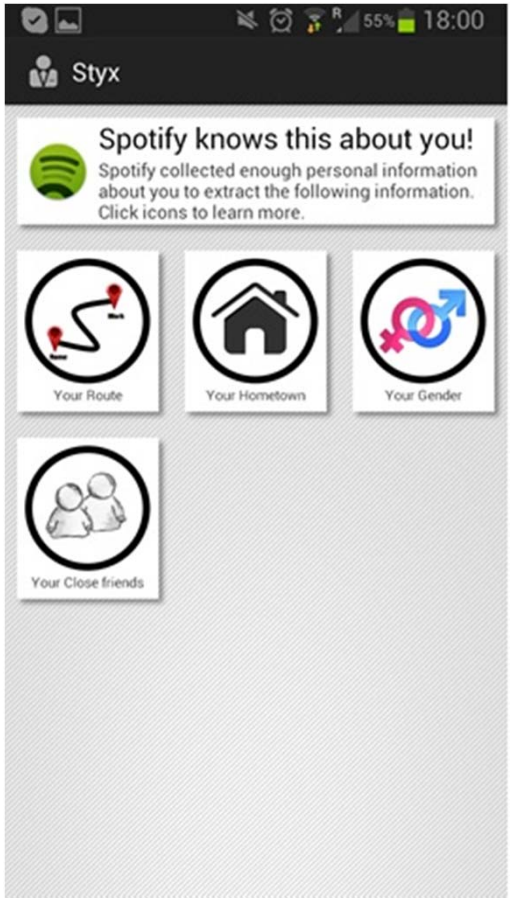
2 The Case of Smartphone Apps

Suggested New Approaches (2/2): Android Study



Styx Notification

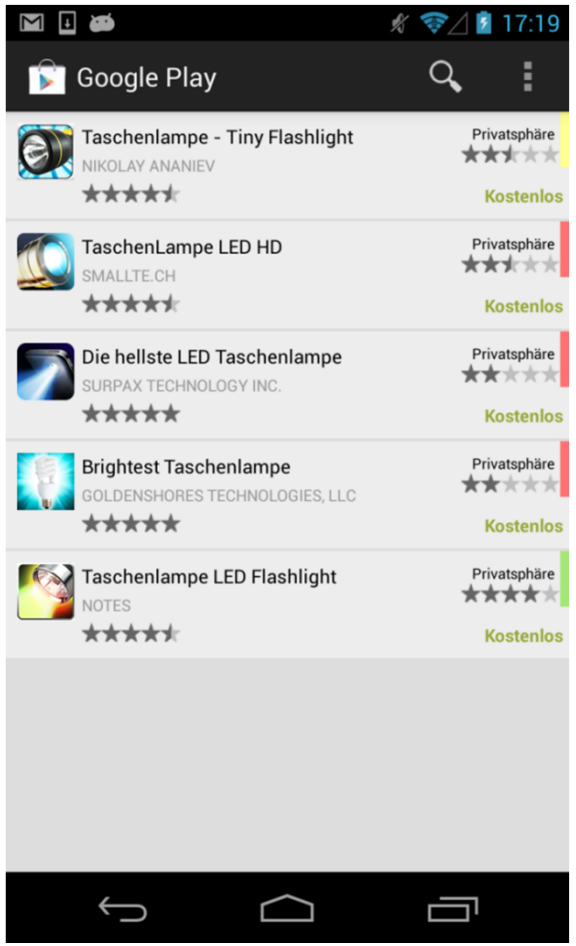
Styx Inference Screen



Styx Dashboard

2 The Case of Smartphone Apps
Results of Two User Studies (Summary)

- A consequence-based privacy-risk communication leads to:
  - increased privacy and risk awareness,
  - better comprehension of risks,
  - better comparison of apps,
  - privacy as a stronger decision factor,
  - safer app choices.



CHALLENGES & RECOMMENDATIONS

3 Challenges & Recommendations
Challenges

Challenge	Description
1. Conceptualization of Privacy Consequences	• Identification and conceptualization of consequences • Consideration of context, scenario, etc. • Positive vs. negative consequences
2. Consider functionality and context of data access	• Consideration of the purpose of an application (“demand level”) • Context of access (e.g. background information flows vs. active UI)
3. Monitor data-access behavior of apps	The actual data-access behavior of an app is significantly influencing the privacy intrusiveness of an app (what resources? how frequent? what combinations? interactions with other apps?); TaintDroid as an example (Enck et al. 2010).
4. Consider Privacy Transparency of App Providers	Privacy-related consequences also depend on how the app provider processes personal data; statements from the app provider such in a privacy policy could be used to determine consequences.
5. Automation	Automation of monitoring and risk assessments will positively influence efficiency, effectiveness, scalability, and costs.

3 Challenges & Recommendations
Recommendations

Who?	What?
Smartphone Platform Providers	Mechanisms to keep track of sensitive-information flows; reason about privacy intrusiveness of apps based on data-access behavior; communicate observed behavior to other potential users.
App Marketplaces	Add more useful privacy information about apps, especially about privacy consequences to support decision-making; add privacy rating for apps based on their data-access profiles and purpose of data access; provide developers with standardized ways to explain permission requests.
App Developers	Provide explanations for permission requests (e.g. core functionality, side functionality, advertisements, etc.).
W3C	Support app developers by standardizing transparency mechanisms in Device API use.

THANK YOU!

Gökhan Bal, Dipl.-Inf.
Institute of Business Informatics
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
Grüneburgplatz 1, 60629 Frankfurt am Main, Germany
Tel: +49(69) 798-34702, Fax: +49(69)798-35004
Web: http://www.m-chair.de

2. References

References 1

- ABC4Trust: www.abc4trust.eu
- ABC4Trust video: https://abc4trust.eu/index.php/press/2011-11-08-14-42-18
- Gökhan Bal, Kai Rannenberg: User Control Mechanisms for Privacy Protection Should Go Hand in Hand with Privacy-Consequence Information: The Case of Smartphone Apps", W3C Workshop on Privacy and User–Centric Controls, Berlin, 2014-11-20/21, https://m-chair.de/images/documents/publications/Position_Paper_W3C_WPUCC_Bal__Rannenberg.pdf
- Gökhan Bal, Kai Rannenberg, Jason Hong: Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns; Pp. 187-202 in Computers and Security, Volume 53, September 2015, doi:10.1016/j.cose.2015.04.004
- Kim Cameron, Reinhard Posch, Kai Rannenberg: Proposal for a common identity framework: A User-Centric Identity Metasystem; Pp. 477 – 500 in [Rannenberg, Royer, Deuker 2009]
- CEPIS (Council of European Professional Informatics Societies): Critical technological dependency requires a revised privacy policy of major service providers; www.cepis.org/index.jsp?p=942&n=963&a=5861&;
- CEPIS LSI (Legal & Security Issues Network): www.cepis.org/index.jsp?p=827&n=942
- Sebastian Clauß, Marit Köhntopp: Identity management and its support of multilateral security. Computer Networks, Volume 37, Issue 2, October 2001, Pages 205-219
- Deutsche Telekom Chair for Mobile Business & Multilateral Security; www.m-chair.de
- FIDIS: Future of Identity in the Information Society; www.fidis.net
- ISO/IEC JTC 1/SC 27/WG 5: Identity Management and Privacy Technologies; www.jtc1sc27.din.de

References 2

- Ioannis Krontiris, Herbert Leitold, Reinhard Posch, Kai Rannenberg: eID Interoperability; Pp. 167-186 in: Walter Fumy, Manfred Paeschke (Eds.): Handbook of eID Security – Concepts, Practical Experiences, Technologies, Publicis, ISBN 978-3-89578-379-1
- Sebastian Pape, Frank Wagner: IT-Sicherheit (und Datenschutz) im Internet der Dinge, 7. ERFA-Runde Datenschutz und IT-Sicherheit, Arbeitgeberverband Großhandel, Außenhandel, Dienstleistungen e.V., Dortmund; www.smjp.de/pages/career/research/talks.shtml
- PICOS: Privacy and Identity Management for Community Services; www.picos-project.eu
- PRIME: Privacy and Identity Management for Europe; www.prime-project.eu
- PrimeLife: Privacy and Identity Management for Life; www.primelife.eu
- Privacy&Us: Privacy & Us innovative training network; www.privacyus.eu
- Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3
- Kai Rannenberg: CamWebSim and Friends: Steps towards Personal Security Assistants; Pp. 173 - 176 in Viktor Seige et al.: The Trends and Challenges of Modern Financial Services – Proceedings of the Information Security Summit; May 29-30, 2002, Prague; Tate International; ISBN 80-902858-5-6

References 3

- Kai Rannenberg: Identity management in mobile cellular networks and related applications; Information Security Technical Report; Vol. 9, No. 1; 2004; pp. 77 – 85; ISSN 1363-4127
- Kai Rannenberg, Jan Camenisch, Ahmad Sabouri: Attribute-based Credentials for Trust – Identity in the Information Society, 2015, Springer, DOI 10.1007/978-3-319-14439-9
- Kai Rannenberg, Denis Royer, Andre Deuker: The Future of Identity in the Information Society – Opportunities and Challenges; Springer 2009, ISBN 978-3-540-88480-4
- TDL (Trust in Digital Life): Working Group "Personal Data"; https://trustindigitallife.eu/what-we-do/working-groups/personal-data/
- Markus Tschersich, Christian Kahl, Stephan Heim, Stephen Crane, Katja Böttcher, Ioannis Krontiris, Kai Rannenberg: Towards Privacy-enhanced Mobile Communities - Architecture, Concepts and User Trials, Pp. 1947-1960 in Journal of Systems and Software, Special Issue: Mobile Applications Volume 84, Issue 11, November 2011
- Daniel Villatoro, Jetzabel Serna, Víctor Rodríguez, Marc Torrent-Moreno: The TweetBeat of the City: Microblogging Used for Discovering Behavioural Patterns during the MWC2012; pP. 43-56 in: Jordi Nin, Daniel Villatoro: Citizen in Sensor Networks; LFirst International Workshop, CitiSens 2012, Montpellier, France, August 27, 2012, Revised Selected Papers, Lecture Notes in Computer Science, Volume 7685,2013
- Jan Zibuschka, Lothar Fritsch, Mike Radmacher, Tobias Scherner, Kai Rannenberg: Enabling Privacy of Real-Life LBS: A Platform for Flexible Mobile Service Provisioning; in Proceedings of the 22nd IFIP TC-11 International Information Security Conference 2007; 14-16 May 2007, Sandton, South Africa; Springer AICT IFIP Series

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Prof. Dr. Kai Rannenberg
Goethe University Frankfurt
Theodor-Adorno-Platz 4
60629 Frankfurt, Germany
WWW www.m-chair.de
E-Mail info@m-chair.de
Phone +49 (0)69 798 34701
Fax +49 (0)69 798 35004