Needs and priorities considering privacy in the consumer space

Cybersecurity Standardization Conference 2021
Panel 6: Vision of the future
2021-02-04

online

Prof. Dr. Kai Rannenberg
Convenor ISO/IEC JTC 1/SC 27/WG 5
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Many devices/services are insecure and not privacy friendly

mobile business

- **Devices, especially smartphones**
  - Emit much more data than needed, e.g. flashlight apps transfer location data to app developer
  - Can be manipulated externally
- **Provider communication often unclear, e.g.**
  - App markets don't inform about app data flows
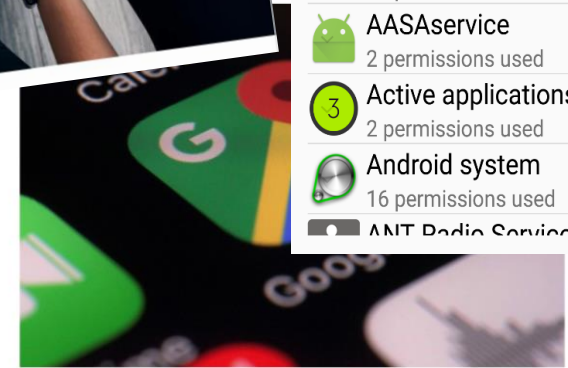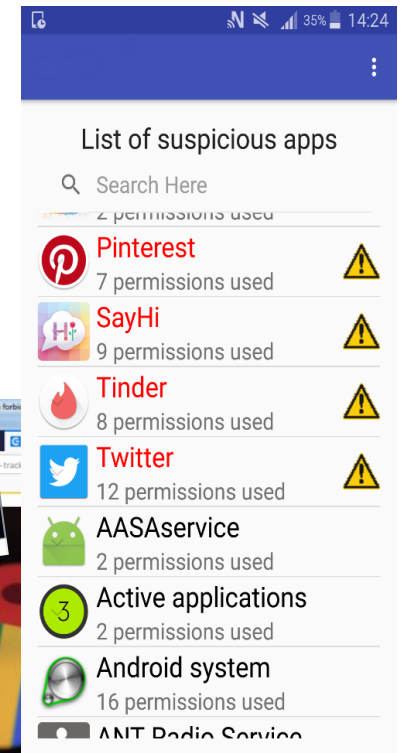 - Lack of information on tracking case
  - …

DAGENS NYHETER. Nyheter Ekonomi Kultur Sthlm Gbg Sport Ledare DN Debatt Insändare ≡ Me

Hälsa

Ny studie: träningsappar samlar känslig persondata

UPPDATERAD 2019-07-16 PUBLICERAD 2019-07-03

Foto: Shutterstock

Connected toys violate European consumer law - Forbruke

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras

Connected toys violate Europe ×

https://www.forbruke

FORBRUKERRÅDET

Forside > Siste Nytt > Connected toys violate European consumer law

Connected toys violate European consumer law

6. desember, 2016

The internet-connected toys My Friend Cayla and i-Que fail miserably when it comes to safeguarding basic consumer rights, security, and privacy.

Finn Myrstad

List of suspicious apps

🔍 Search Here

~~2 permissions used~~

Pinterest ⚠️
7 permissions used

SayHi ⚠️
9 permissions used

Tinder ⚠️
8 permissions used

Twitter ⚠️
12 permissions used

AASAservice
2 permissions used

Active applications
2 permissions used

Android system
16 permissions used

ANT Radio Service

APPS & SOFTWARE

Report says Google tracks your location on iPhone and Android even when you forbid it

Andy Meek @aemeek
August 13th, 2018 at 2:30 PM

(Sony)

(Beurer)

(Genesis)

(August)

(Amazon)

(Discovergy)
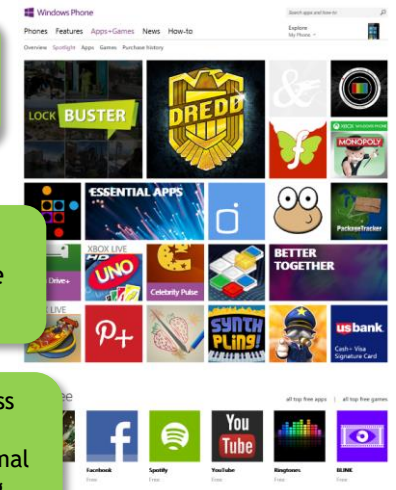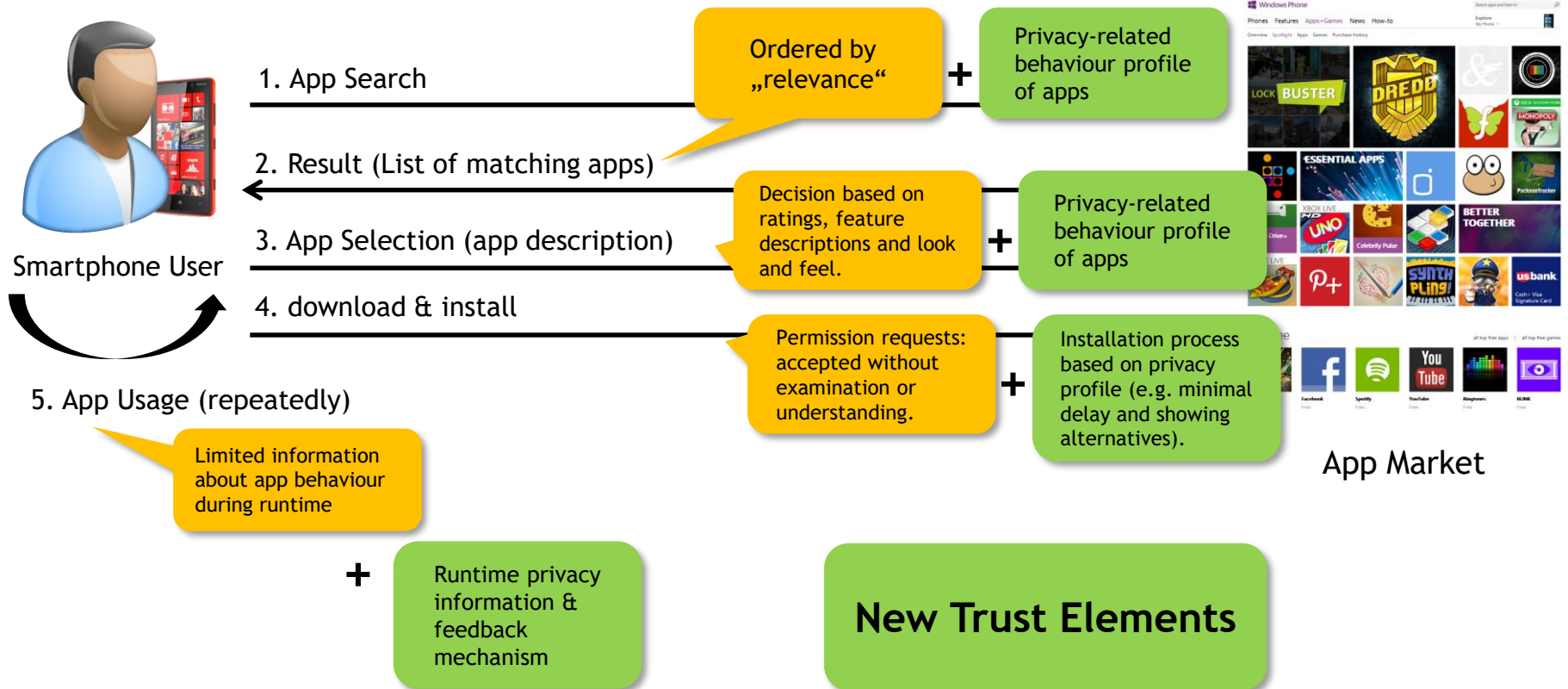
Improvements are needed on all levels

- Trustworthy devices
- Robust operating systems
- Privacy-friendly apps giving users control
- Better app markets informing users better about the apps
- Protection throughout the whole lifecycle
- Impartial evaluation of relevant system and service properties
- Trustworthy certification
- …

Smartphone User

1. App Search

Ordered by „relevance" + **Privacy-related behaviour profile of apps**

2. Result (List of matching apps)

3. App Selection (app description)

Decision based on ratings, feature descriptions and look and feel. + **Privacy-related behaviour profile of apps**

4. download & install

Permission requests: accepted without examination or understanding. + **Installation process based on privacy profile (e.g. minimal delay and showing alternatives).**

5. App Usage (repeatedly)

Limited information about app behaviour during runtime

+ **Runtime privacy information & feedback mechanism**

App Market

New Trust Elements

- Privacy framework (ISO/IEC 29100:2011; Amendment 1:2018, EN ISO/IEC 29100:2020)
- A framework for identity management (ISO/IEC 24760 (Parts 1-3), IS:2011, IS:2015, IS:2016)
- Online privacy notice and consent (ISO/IEC 29184:2020)
- Privacy by design for consumer goods and services (ISO/AWI 31700)
- Data protection and privacy by design and by default (prEN 17529)
- Privacy impact assessment – methodology (ISO/IEC 29134:2017, EN ISO/IEC 29134:2020)
- Privacy engineering for system life cycle processes (ISO/IEC TR 27550:2019)
- Privacy guidelines for Smart Cities (ISO/IEC TS 27570:2021)
- Privacy enhancing data de-identification terminology and classification of techniques (ISO/IEC 20889:2018)
- …

➢ Good standards (partially in the making)
➢ Needed especially
  ➢ More implementation
  ➢ More European pick-up

- Within 24 pages
  - "Privacy" is mentioned only once (in relation to AI).
  - "Data Protection" is mentioned 6 times (mostly when other initiatives are cited).
- Rather comprehensive on a very abstract level
+ ***Secure development lifecycle*** considered for ICT
  + Products,
  + Services,
  + Processes

- Support smaller players in standardisation, especially during the pandemic and its aftermath, and in the long run.
- Encourage more reliable products/services/processes by e.g. special provisions for consumer products/services:
  - Clear requirements,
  - Product liability as an underpinning.
- A certification system
  - Supported by an infrastructure (people, not just ICT),
  - Helping consumers to make use of certification results.
- Consider
  - App markets (to give more guidance to users)
  - Household goods and toys
  - Consumer services

Chair of Mobile Business & Multilateral Security

Prof. Dr. Kai Rannenberg

Goethe University Frankfurt
Theodor-Adorno-Platz 4
60629 Frankfurt, Germany

Phone +49 (0)69 798 34701
Fax +49 (0)69 798 35004

E-Mail: info@m-chair.de
WWW: www.m-chair.de

mobile
business

GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

- 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
- Chair for Mobile Business & Multilateral Security; www.m-chair.de
- Miro Enev, Sidhant Gupta, Tadayoshi Kohno, Shwetak N. Patel: Televisions, video privacy, and powerline electromagnetic interference; Pp. 537-550 in Proceedings of the 18th ACM conference on Computer and communications security (CCS '11). ACM, New York, NY, USA,. DOI=http://dx.doi.org/10.1145/2046707.2046770
- FIDIS: Future of Identity in the Information Society; www.fidis.net
- Ulrich Greveler, Benjamin Justus, Dennis Löhr: Multimedia Content Identification Through Smart Meter Power Usage Profiles; Proceedings of the International Conference on Information and Knowledge Engineering IKE'12, Las Vegas. ISBN 978-1-60132-222-4
- Majid Hatamian, Nurul Momen, Lothar Fritsch and Kai Rannenberg: A Multilateral Privacy Impact Analysis Method for Android Apps; 7th Annual Privacy Forum 2019, Rome, Italy, June 2019; In: Maurizio Naldi, Giuseppe F. Italiano, Kai Rannenberg, Manel Medina, Athena Bourka (eds): Privacy Technologies and Policy. APF 2019. Lecture Notes in Computer Science, Vol. 11498. Springer, Cham
- Majid Hatamian, Sebastian Pape, Kai Rannenberg: ESARA: A Framework for Enterprise Smartphone Apps Risk Assessment", in: G. Dhillon et al. (Eds.): ICT Systems Security and Privacy Protection, IFIP Sec 2019, IFIP AICT 562, https://doi.org/10.1007/978-3-030-22312-0_12
- Majid Hatamian, Jetzabel Serna, Kai Rannenberg, Bodo Igler: "FAIR: Fuzzy Alarming Index Rule for Privacy Analysis in Smartphone Apps". TrustBus 2017
- ISO/IEC 24760-1:2019 "A framework for identity management -- Part 1: Terminology and concepts"; http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
- ISO/IEC JTC 1/SC 27/WG 5: Identity Management and Privacy Technologies; www.jtc1sc27.din.de

- Georgios Kalogridis, C. Efthymiou, T. Lewis, S. Denic, R. Cepeda: Privacy for smart meters: Towards undetectable appliance load signatures; Pp. 232-237 in Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), IEEE, 2010

- Georgios Kalogridis, R. Cepeda, S. Z. Denic, T. A. Lewis, C. Efthymiou: Elecprivacy: Evaluating the privacy protection of electricity management algorithms; Pp. 750-758 in IEEE Trans. Smart Grid, 2(4), 2011

- 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

- Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, David Irwin: Private memoirs of a smart meter; Pp. 61-66 in Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building (BuildSys '10). 2010. ACM, New York, NY, DOI=http://dx.doi.org/10.1145/1878431.1878446

- Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel: Unique in the Crowd: The privacy bounds of human mobility; Scientific Reports 3, Article number: 1376 (2013); DOI:10.1038/srep01376

- Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex "Sandy" Pentland: Unique in the shopping mall: On the reidentifiability of credit card metadata; Science 30 January 2015: vol. 347 no. 6221 pp. 536-539; DOI: 10.1126/science.1256297

- 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

- 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

- Latanya Sweeney: k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570

- Welderufael B. Tesfay, Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, Jetzabel Serna. 2018. PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation. In IWSPA'18: 4th ACM International Workshop on Security And Privacy Analytics, March 19–21, 2018, Tempe, AZ, USA. ACM, New York, NY, USA. https://doi.org/10.1145/3180445.3180447

- Welderufael B. Tesfay, Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, Jetzabel Serna. 2018. I Read but Don't Agree: Privacy Policy Benchmarking using Machine Learning and the EU GDPR. In WWW '18 Companion: The 2018 Web Conference Companion, April 23–27, 2018, Lyon, France. ACM, New York, NY, USA. https://doi.org/10.1145/3184558.3186969

- Carmela Troncoso, E. Costa-Montenegro, C. Diaz, S. Schiffner, "On the difficulty of achieving anonymity for Vehicle-2-X communication"; Computer Networks 55(14), pp. 3199-3210, 2011

- 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