Privacy in New Technologies
Seminar kick-off

4 May 2020

seminar@m-chair.de

Chair of Mobile Business & Multilateral Security

Goethe University Frankfurt

Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
3. Presentation of topics
4. Questions

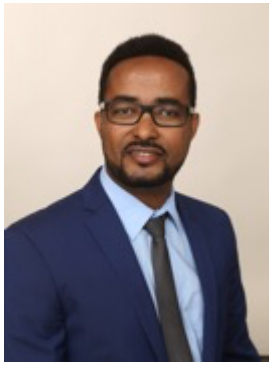
Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
3. Presentation of topics
4. Questions

Supervisors

Majid Hatamian
M.Sc.

Ann-Kristin Lieberknecht
M.Sc.



Welderufael B. Tesfay
Dr.

Chair of Business Administration, especially Business Informatics, Mobile Business and Multilateral Security

Chair of Mobile Business & Multilateral Security

Theodor-W.-Adorno-Platz 4
Campus Westend
RuW, 2nd Floor

Phone: +49 69 798 34701
Fax: +49 69 798 35004
eMail: info@m-chair.de

www.m-chair.de

Seminar grade

- This seminar consists of two administrative parts:

- Paper
- Presentation

- Participation in all parts is **required** for the successful completion of the seminar.
- The work is evaluated on an individual basis (but can be done in groups of 2).

Important dates

Date	What	Where/When/How
4th May 2020	Kick-off	Vidyo
5th May 2020 (by midnight)	Submission of preferred topics	Email to: seminar@m-chair.de
7th May 2020	Distribution of Topics	Via email
26th June 2020 (by midnight)	Paper submission	MS-word/OpenOffice template AND PDF to: seminar@m-chair.de
2nd July 2020 (by midnight)	Presentation submission	Email to: seminar@m-chair.de
3rd July 2020	Presentations – day 1	RuW 2.202 – 10:00 to 18:00
6th July 2020	Presentations – day 2	RuW 2.202 – 10:00 to 18:00

- Agenda will be sent to all participants prior to the presentation days.
- Possibly one of the presentation days will be cancelled!

Formal requirements for papers

- For the paper, the formal requirements of the chair apply.
  - Please use the provided word template
  - Use the APA (American Psychology Association) or AMS (American Mathematical Society) style for citations
  - At least 10 pages are recommended (excluding cover, table of contents, references, etc.)

Paper submission

- Seminar papers must be submitted in **electronic form** in the following formats:
  - MS-Word or OpenOffice
  - Adobe PDF

  via E-Mail to: seminar@m-chair.de

- The PDF file should include the statutory declaration with your **scanned signature.**

Formal requirements for presentations

- Seminar presentation:
  - Duration: 15 min. at most
  - Following discussion: 15 min.

- Submission until 02.07.2020
  - Powerpoint format or PDF
  - E-mail to seminar@m-chair.de

Contact

In case of any questions or problems arise during the seminar you can contact: seminar@m-chair.de

For comprehensive questions please make an appointment with the supervisor of your topic:

- welderufael.tesfay@m-chair.d
- majid.hatamian@m-chair.de

Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
3. Presentation of topics
4. Questions

Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
   - Introduction
   - Legal aspects
   - Technical aspects
   - User aspects
3. Presentation of topics
4. Questions

Data Protection and Privacy

- Both terms are related but not synonymous and *have many definitions*.
- 2 popular ones:
  - Data protection is the protection from harmful and unsolicited usage of data linked to the personal sphere of a person.
  - Privacy is the right to be left alone, e.g. to be unwatched or anonymous [WaBr1890]

Introduction I

- Early day definitions: "The right to be left alone" Warren and Brandeis, 1890, Harvard Law Review: "The right to privacy" [WaBr1890]
- Beginning of information age: "The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Westin, 1967.

- Westin's index
  - Privacy fundamentalists
  - Privacy pragmatists
  - Privacy unconcerned

Source: https://pixabay.com/es/de-distancia-junction-direcci%C3%B3n-1020088/

Introduction II

- Contemporary: **It is complex.**
  - "The ability of the individual to protect information about himself" Goldberg et. al 1997

- Personal information: "Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly "

Source: https://pixabay.com/es/icono-la-cabeza-ver-el-perfil-1247948/

Privacyinternational.org

- https://www.youtube.com/watch?v=zsboDBMq6vo&list=PLz3h0TjXz7gVaaQ75qBEYXcYziZZ3Jmv6&index=2&t=0s

Dimensions of Privacy Protection

- Legal aspects of privacy
  - Supportive legal frameworks (e.g., right to be forgotten, safe harbor/privacy shield)
- Technical aspects of privacy
  - Privacy engineering, and PETs
- User aspects of privacy
  - User awareness, and usability

Source: https://pixabay.com/es/cl%C3%A1usula-correo-electr%C3%B3nico-en-1462968/

Source: https://pixabay.com/es/sistema-red-noticias-conexi%C3%B3n-954972/

Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
   - Introduction
   - Legal aspects
   - Technical aspects
   - User aspects
3. Presentation of topics
4. Questions

General Data Protection Regulation (GDPR)

- Entered into force on 24 May 2016 and applies since 25 May 2018.

- The European Commission says that the recently approved regulation “puts the citizens back in control of their data, notably through”:
  - A right to be forgotten - Users will have the right to demand that data about them be deleted if there are no "legitimate grounds" for it to be kept.
  - Privacy by design and by default – privacy friendly default settings to be the norm.

General Data Protection Regulation (GDPR)

eIDAS Regulation

- REGULATION on electronic identification and trust services for electronic transactions in the internet market.
- One of the objectives is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services.
- Authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online.

[Electronic identification and trust services (eIDAS): regulatory environment and beyond, ec.europa.eu]

Law Alone is not Sufficient

- Data protection / Privacy law alone not sufficient
  - Not all processing can be controlled (e.g. every network node).
  - Deliberate breaking and bending of law (different legislations on the internet)
  - Economic pressure can force customers to give consent to almost any kind of ‘privacy’ policy (e.g. selling privacy for “peanuts”).

[Reagle1998, SelfReg1999, Bell2001, Hoofnagle2005]

Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
   - Introduction
   - Legal aspects
   - Technical aspects
   - User aspects
3. Presentation of topics
4. Questions

Technical Aspects of Privacy

A. Privacy by design
B. Privacy engineering
C. Privacy enhancing technologies

Source: https://pixabay.com/es/humanos-siluetas-redes-internet-1157116/

A. Privacy by design

- Refers to the notion of embedding privacy directly into the design of ITs and systems
- Adopted as one essential principle in the GDPR.

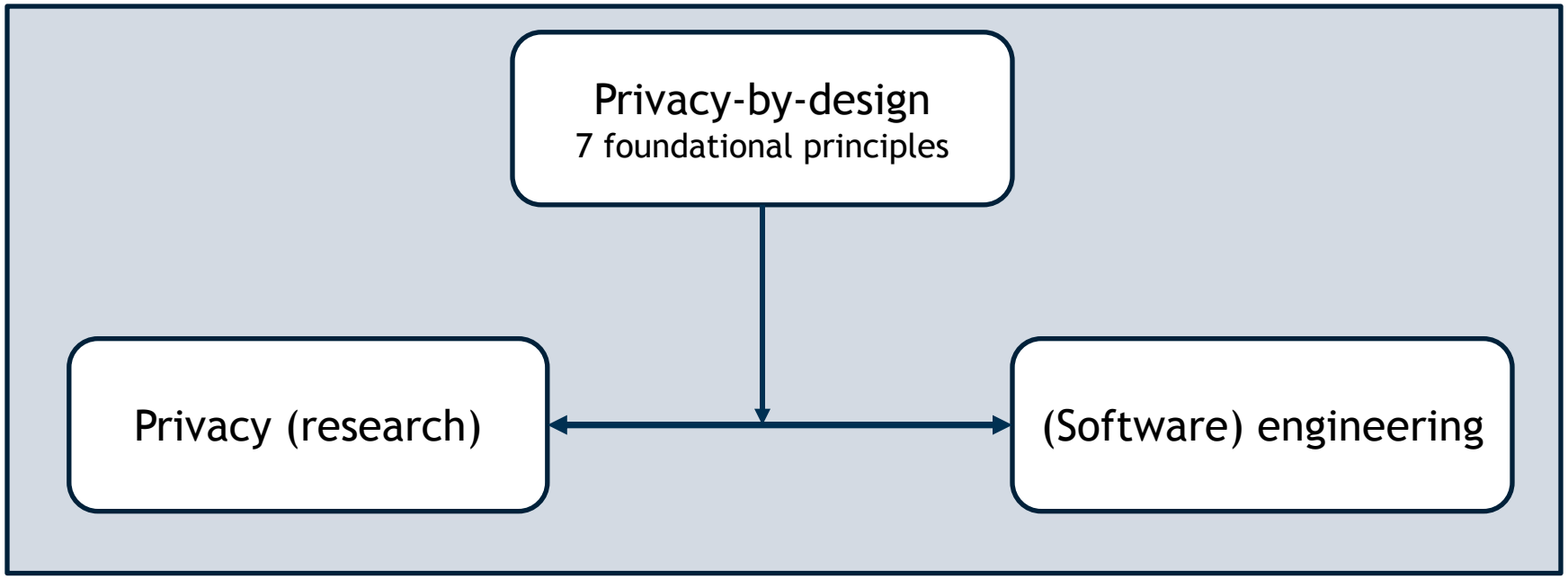
[Cavoukian2010]

7 foundational principles

- Proactive not reactive
- Privacy as the Default setting
- Privacy Embedded into the Design
- Full Functionality
- End-to-End Security
- Visibility and Transparency
- Respect for User Privacy

B. Privacy engineering I

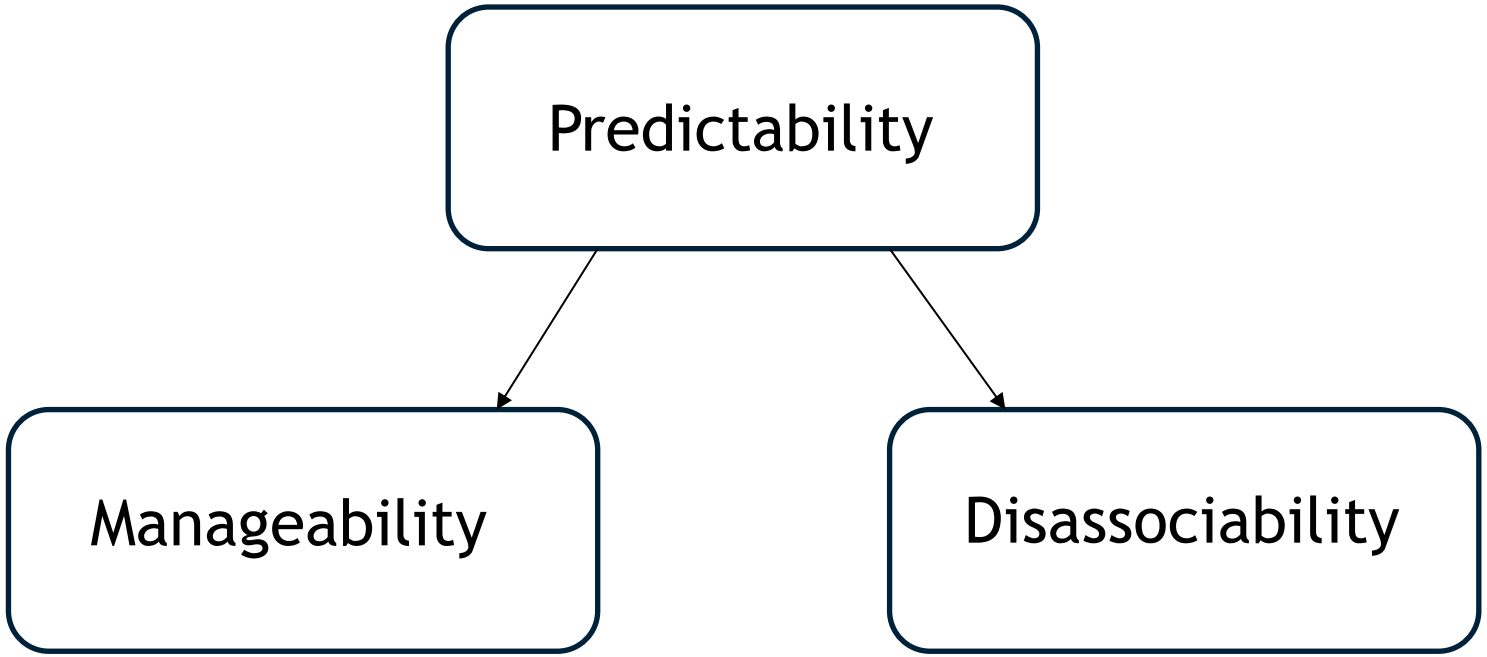
- Connection between research and practice (privacy and software engineering)



[Gürses2016]

B. Privacy engineering II

- Three main goals:



[NIST2014]

C. Privacy enhancing technologies

- Privacy Enhancing Technologies (PETs)
  - It refers to the category of technologies that minimise the processing of personal data
- Examples
  - Automatic anonymisation (e.g. Anonymizer, iPrivacy)
  - Encryption tools (e.g. SSL)
  - Policy Tools (e.g., P3P, TRUSTe)

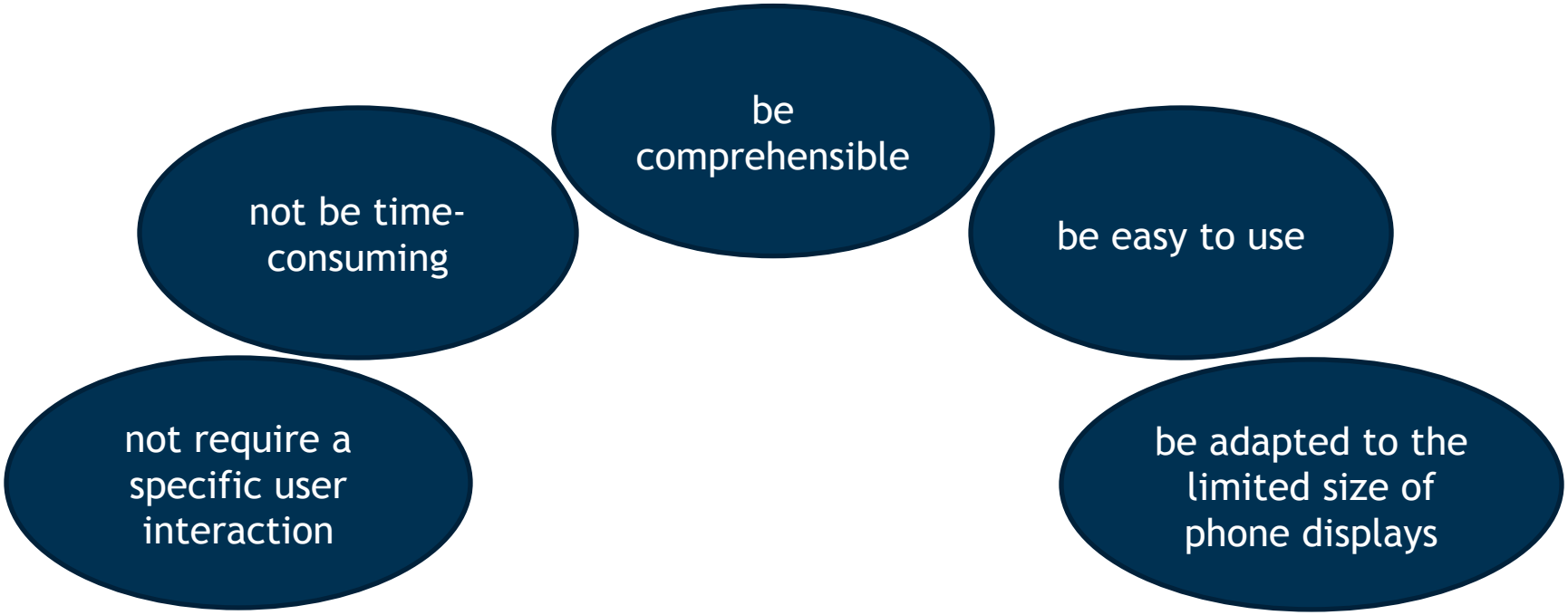
[Danezis2014]

Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
   - Introduction
   - Legal aspects
   - Technical aspects
   - User aspects
3. Presentation of topics
4. Questions

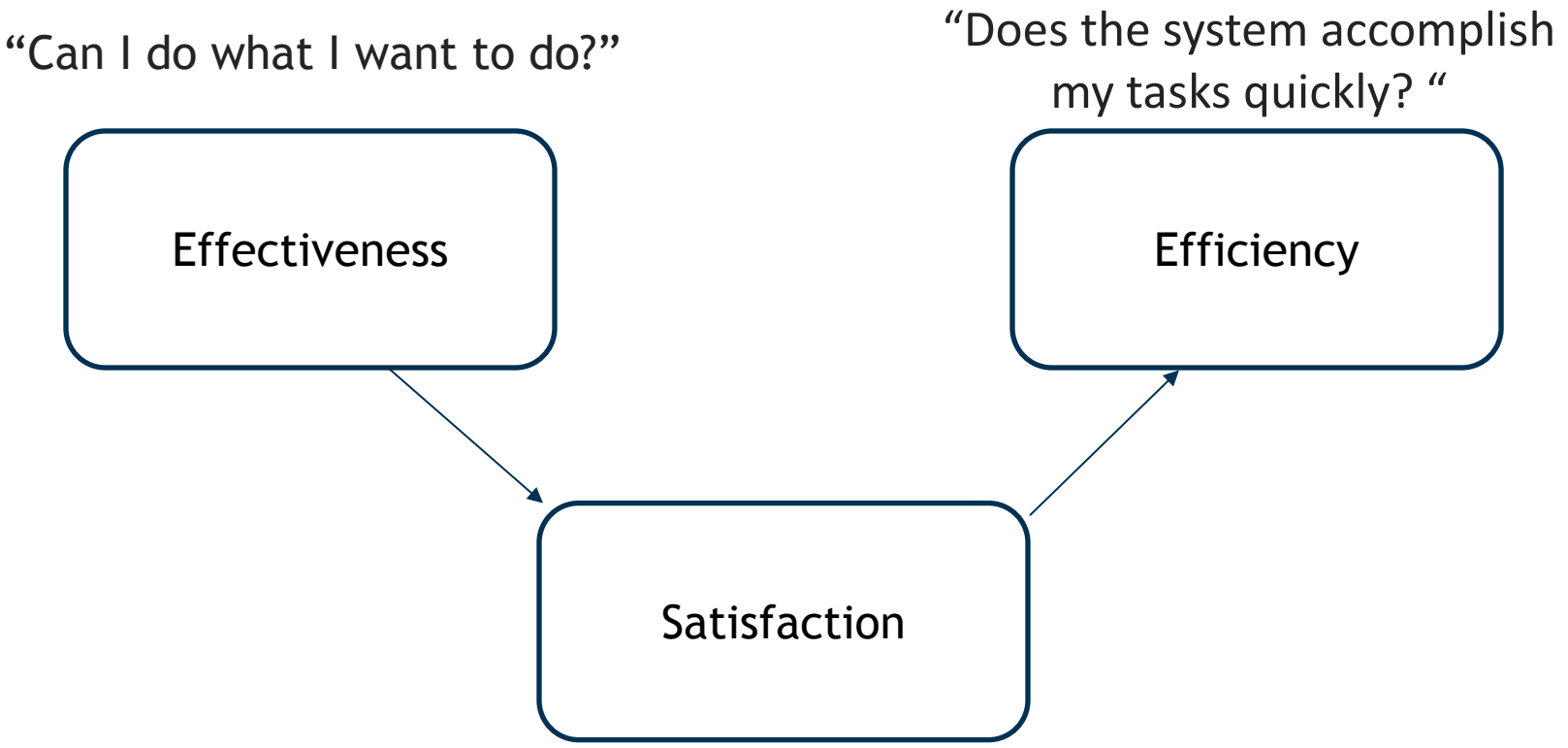
User awareness

- User awareness (transparency)
- Solution should:



[Danezis2014]

Usability



[National Academy2010]

Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
3. Presentation of topics
4. Questions

Topic 1: A survey on tools for achieving usable privacy in smartphone ecosystems

- Smartphones apps collect lots of information from sensors.
- Users are often unaware of what information is being collected, how often, for which purpose?
- **Privacy Enhancing Technologies (PETs)** can support users in privacy and data protection to ensure unnecessary or unwanted processing of personal data.

Topic 1: A survey on tools for achieving usable privacy in smartphone ecosystems

- Expected results:
  - A structured view on existing PETs in smartphone ecosystems.
  - Based on intensive literature review, the most recent works should be collected, categorised, and examined.
  - A detailed comparison enabling the understanding of strengths/weaknesses of each reviewed category and its respective examined tools.

Topic 1: A survey on tools for achieving usable privacy in smartphone ecosystems

- Relevant literature:

- Enck, W., P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth (2010), Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones, in the Proceedings of the the 9th ACM USENIX Conference on Operating Systems Design and Implementation, Vancouver, BC, Canada, pp. 393–407.
- Enck, W., D. Octeau, P. McDaniel, and S. Chaudhuri (2011), A study of android application security, in the Proceedings of the the 20th USENIX Conference on Security, San Francisco, CA, USA, pp. 21–21.
- Gilbert, P., B. G. Chun, L. Cox, and J. Jung (2011), Automating privacy testing of smartphone applications, Tech. Rep. CS-2011-02, Duke University.
- Goldberg, I., D. Wagner, and E. Brewer (1997), Privacy-enhancing technologies for the internet, in Proceedings of the 42Nd IEEE International Computer Conference, COMPCON '97, pp. 103–, IEEE Computer Society, Washington, DC, USA.
- Harris, K. D. (2013), Privacy on the go: Recommendations for the mobile ecosystem, California Department of Justice.
- Hatamian, M., J. Serna, K. Rannenberg, and B. Igler (2017), Fair: Fuzzy alarming index rule for privacy analysis in smartphone apps, in the Proceedings of the 14th International Conference on Trust and Privacy in Digital Business (TrustBus), Lyon, France, pp. 3–18.

Topic 2: A survey on tools for achieving usable transparency in smartphone ecosystems

- Smartphone users (oftentimes) cannot decide what data about them is accessed, collected, processed, or transferred.
- However, app providers can (almost) collect, process, and use any kind of users' data.
- Such a relationship is usually specified by ‘information asymmetry’.
- **Transparency-Enhancing Tools (TETs)** are supposed to minimise such information asymmetry by helping users to understand how their data is used.

Topic 2: A survey on tools for achieving usable transparency in smartphone ecosystems

- Expected results:
  - A structured view on existing TETs in smartphone ecosystems.
  - Based on intensive literature review, the most recent works should be collected, categorised, and examined.
  - A detailed comparison enabling the understanding of strengths/weaknesses of each reviewed category and its respective examined tools should be done.

Topic 2: A survey on tools for achieving usable transparency in smartphone ecosystems

- Relevant literature:

- Pulls, T. (2012), Privacy-Preserving Transparency-Enhancing Tools, Licentiate thesis, Karlstad University.
- Murmann, P., et al. (2017), D4.1 user interface requirements, Deliverable, USECON, Privacy&Us.
- Guidelines on transparency under regulation 2016/679, Data Protection Working Party
- Liccardi, I., J. Pato, and D. J. Weitzner (2013), Improving mobile app selection through transparency and better permission analysis, Journal of Privacy and Confidentiality, 5(2), 1–55
- P. Murmann and S. Fischer-Hübner. *Tools for Achieving Usable Ex Post Transparency: A Survey.* IEEE Access, Vol. 5, 2017.
- J. P. Janic, P. Wijbenga, and T. Veugen, "Transparency enhancing tools(TETs): An overview," in Proc. 3rd Workshop Socio-Tech. Aspects Secur. Trust, Jun. 2013, pp. 18–25.
- H. Hedbom, "A survey on transparency tools for enhancing privacy," in The Future of Identity in the Information Society, Berlin, Germany: Springer, 2009, pp. 67–82.
- S. Patrick and S. Kenny, "From privacy legislation to interface design: Implementing information privacy in human-computer interactions," in Proc. Int. Workshop Privacy Enhancing Technol., 2003, pp. 107–124.
- P. Murmann and S. Fischer-Hübner, "Usable transparency enhancing tools: A literature review," Dept. Math. Comput. Sci., Karlstad Univ., Karlstad, Sweden, Tech. Rep., Jul. 2017.

Topic 3: Integrating privacy into smartphone app markets

- Current app markets offer a set of criteria by which users can choose and install an app.
- These criteria are mostly about functionality/usefulness of apps.
- Privacy-by-design mandates that privacy must be embedded into the design of IT products.
- However, users have no choice to compare apps in terms of privacy aspects when deciding downloading an app.

Topic 3: Integrating privacy into smartphone app markets

- Expected results:
  - Finding relevant elements in users' decision making process when it comes to downloading an app (in terms of privacy).
  - Designing an imaginary app market and embed those elements which were found in the previous step (following best usability practices).
  - Providing an understandable privacy performance/visualisation (in the form of numbers, diagram, risk levels, etc.) to users.
  - Investigating the importance of the proposed visualisation techniques on users' decision-making process by conducting a quantitative user study.

Topic 3: Integrating privacy into smartphone app markets

- Relevant literature:

- Bal, G., K. Rannenberg, and J. Hong (2015), Styx: Privacy risk communication for the android smartphone platform based on apps' data-access behaviour patterns, Computers & Security, 53, 187–202.
- M. Hatamian, N. Momen, L. Fritsch, and K. Rannenberg. A Multilateral Privacy Impact Analysis Method for Android Apps. Annual Privacy Forum 2019. Rome, Italy, June 2019
- N. Momen, Towards Measuring Apps' Privacy-Friendliness, Karlstad University, Faculty of Health, Science and Technology.
- P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions demystified. In Proceedings of the 18th ACM conference on Computer and communications security, pages 627–638. ACM, 2011.
- P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 3393–3402. ACM, 2013.
- A. Mylonas, M. Theoharidou, and D. Gritzalis. Assessing privacy risks in android: A user-centric approach. InInternational Workshop on Risk Assessment and Risk-driven Testing, pages 21–37. Springer, 2013.

Topic 4: Privacy perception of smartphone app users

- Apps can request a certain number of permissions which allows them to access device resources such as camera, location, etc.
- These permission requests are sometimes ignored by users even though they might appear irrelevant to the real functionality of the app:
  - Users do not understand the technical and ambiguous definitions of permissions;
  - users value the use of apps more than their personal data, despite the fact that the apps collect data for various purposes ranging from functionality to empowering their ads mechanisms.

Topic 4: Privacy perception of smartphone app users

- Expected results:
  - Analysing smartphone users' perception towards permission requests with respect to potential privacy threats (e.g. a malicious apps might turn the microphone on and record everything).
  - Analysing the privacy awareness and self-protective behaviour of smartphone users towards privacy threats in previous step.
  - Proposing remedies based on findings from previous step to adjust and improve privacy and security of smartphone ecosystems.

Topic 4: Privacy perception of smartphone app users

- Relevant literature:

- W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie. PScout: analysing the Android permission specification. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 217–228. ACM,2012.
- Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen. Little brothers watching you: Raising awareness of data leaks on smartphones. In Proceedings of the Ninth Symposium on Usable Privacy and Security, page 12.ACM, 2013.
- Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing, pages 501–510. ACM, 2012.
- Patil and J. Lai. Who gets to know what when: configuring privacy permissions in an awareness application. In Proceedings of the SIGCHI conference on Human factors in computing systems, pages 101–110. ACM,2005.
- I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 2347–2356. ACM, 2014.
- Felt, A. P., S. Egelman, and D. Wagner (2012), I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns, in the Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'12), New York, NY, USA, pp. 33–44.

Topic 5: Privacy in Infection Control Smartphone Apps

- Smartphone apps have the potential to the fight against infections diseases, such as Covid-19
- Since the Covid-19 pandemic started, governments have been using contact tracing apps to control the spread of the virus.
- However, others claim that there are severe privacy consequences of such apps which essentially turn citizens into sensing agents.

Topic 5: Privacy in Infection Control Smartphone Apps

- Expected results:
  - Analysing the context of the current use of smartphone apps in infectious disease control
  - Analysing the privacy consequences of such apps to ordinary users
  - Propose a structured framework to analyse these consequences, as well as suggest possible remedies.

Topic 5: Privacy in Infection Control Smartphone Apps

- Relevant literature:

- Yasaka, T. M., Lehrich, B. M., & Sahyouni, R. (2020). Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App. *JMIR mHealth and uHealth*, *8*(4), e18936.
- Fawaz, K., & Shin, K. G. (2014, November). Location privacy protection for smartphone users. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 239-250).
- Bell, J., Butler, D., Hicks, C., & Crowcroft, J. (2020). Tracesecure: Towards privacy preserving contact tracing. *arXiv preprint arXiv:2004.04059*.
- Cho, H., Ippolito, D., & Yu, Y. W. (2020). Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511*.

- Weblinks
  - https://www.ccc.de/en/updates/2020/contact-tracing-requirements
  - https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2
  - https://fs0c131y.com/covid19-tracker-apps/
  - https://www.securityweek.com/security-privacy-issues-found-government-covid-19-mobile-apps

Topic 6: Survey on Privacy Sensitive Information Detection Approaches in Textual Data

- With the fast proliferation of Internet services and always connected smart devices, users continue to (un)intentionally share large amount of personal data.
- Negative implications to user's privacy due to personal data sharing
- Privacy implications are more serious when users share Privacy Sensitive Information (PSI) online
- Detecting PSI disclosure is an important step towards tackling the privacy consequences of divulging such information

Topic 6: Survey on Privacy Sensitive Information Detection Approaches in Textual Data

- Expected results:
  - Analyse the existing work in PSI detection in user generated unstructured textual data
  - Propose a structured framework to analyse the state of the art in PSI detection approaches.
  - Identify the research gap and recommend future works.

Topic 6: Survey on Privacy Sensitive Information Detection Approaches in Textual Data

- Relevant literature:

- Tesfay, W. B., Serna, J., & Rannenberg, K. (2019, October). PrivacyBot: detecting privacy sensitive information in unstructured texts. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 53-60). IEEE.
- Bier, C., & Prior, J. (2014, June). Detection and labeling of personal identifiable information in e-mails. In *IFIP International Information Security Conference* (pp. 351-358). Springer, Berlin, Heidelberg.
- Castillo, S. R. M., & Chen, Z. (2016, November). Using transfer learning to identify privacy leaks in tweets. In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)* (pp. 506-513). IEEE.
- Jindal, P., Gunter, C. A., & Roth, D. (2014, September). Detecting privacy-sensitive events in medical text. In *Proceedings of the 5th ACM Conference on Bioinformatics, Computational Biology, and Health Informatics* (pp. 617-620).

Topic 7: Survey on Ethical Considerations in Machine Learning

- In recent years, the field of artificial intelligence specifically of machine learning has advanced a lot.
- It has become an integral, if not the main part of many data-driven problem-solving approaches and decisions.
- However, many researchers also question the ethical considerations in this approach.

Topic 7: Survey on Ethical Considerations in Machine Learning

- Expected results:
  - The objective of this seminar paper is to analyse the status of ethical consideration in machine learning based systems.
  - Propose a structured framework of the state of the art to analyse the ethical considerations
  - Identify missing ethical considerations, and propose integration mechanisms

Topic 7: Survey on Ethical Considerations in Machine Learning

- Relevant literature:

- Nath, R., & Sahu, V. (2020). The problem of machine ethics in artificial intelligence. *AI & SOCIETY*, *35*(1), 103-111.
- Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care—addressing ethical challenges. *The New England journal of medicine*, *378*(11), 981.
- Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. *The Cambridge handbook of artificial intelligence*, *1*, 316-334.
- LaChat, M. R. (1986). Artificial intelligence and ethics: an exercise in the moral imagination. *Ai Magazine*, *7*(2), 70-70.

- WebLinks

- https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Distribution of Topics

- Please send a mail to seminar@m-chair.de by 5 May 2020 (midnight) with
  - a list of your three preferred topics
  - a brief explanation why you want to cover them
  - Whether you are open to collaborating with somebody else (possibly already who).
- Based on this, we will make a distribution and let you know by 7 May 2020.

Agenda

1. Organisational information
2. Introduction to Privacy and Data Protection
3. Presentation of topics
4. Questions

Questions

Source: Pixabay released under Creative Commons CC0:
https://pixabay.com/es/pregunta-imagen-plaza-556104/

References

- [Cavoukian2010]: Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, 2010.
- [Gürses2016]: Privacy Engineering: Shaping an Emerging Field of Research and Practice IEEE Security and Privacy, 14:2, pp. 40-46, 2016.
- [NIST2014]: NIST Privacy Engineering Objectives and Risk Model Discussion Draft. Introduction, 2014.
- [Danezis2014]: Privacy and Data Protection by Design – from policy to engineering, 2014.
- [National Academy2010]: Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop
- [EC-Prot-2014] European Commission: Protection of personal data: http://ec.europa.eu/justice/data-protection/index_en.htm
- [WaBr1890] Samuel D. Warren, Louis D. Brandeis: The Right to Privacy, Harvard Law Review; Vol. IV; December 15, 1890, No. 5; http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Chair of Mobile Business & Multilateral Security

Goethe University Frankfurt
E-Mail: seminar@m-chair.de
WWW: www.m-chair.de