Privacy in a Mobile, Connected World

Research questions

Today's technologies allow for massive generation, storage and analysis of personal data, and many services we use daily rely on data-based functionalities. This data recording and use may challenge the users' privacy in different ways. In this seminar, we want to have a closer look at these challenges and explore different aspects of privacy relevant to the field of HCI.

1. Protecting privacy is a major challenge with regard to today’s technologies. What does the concept of privacy mean in the context of HCI research? Discuss resulting design implications using examples.

2. How does behavioural tracking affect the diffusion of private data? Discuss possible protection mechanisms and their advantages and disadvantages.

3. What are privacy nudges? How can privacy nudges improve information decision making? Present practical examples of systems using privacy nudges and discuss the effectiveness of privacy nudges in general.

4. Which privacy risks do people face when using mobile devices? Give an overview and discuss how (some of) these risks can be diminished by the help of technology.

5. What does “control” mean in the context of privacy? What role does control play with regard to privacy concerns and the willingness to share private information? Discuss the advantages and disadvantages of systems that help users control their privacy.
6. What is the privacy paradox? How do risk perception and trust influence the privacy paradox? Discuss possible explanations for the privacy paradox.

7. How much do people know about potential risks of data sharing and privacy management? How does educating users affect privacy attitudes? Discuss whether user education is a feasible approach for better privacy management.

8. Analytics strive for creating hyper-personalised user experiences by extracting individuals’ personal traits from their online behaviour. What are the effects of such personal profiling on people’s privacy perception? Discuss the resulting design implications for hyper-personal analytics systems.

9. Automatic context sensing is increasingly used by context-aware applications to provide personalised services. Privacy controls allow for individual privacy management, but setting and adapting privacy preferences increases user burden. How could privacy management be facilitated? Compare and discuss different approaches.

10. Data collection and tracking are common when using apps on mobile devices, and may leak personal data to third parties. How do users feel about data leakage and how does this affect their behaviour? Discuss the design implications for apps that result from these observations.

11. End User License Agreements should inform users about data collection practises and thus allow for informed privacy decision, for example, when installing an application or registering with a service. However, these notices often lack usability and are therefore simply ignored by most users. What are design challenges for privacy notices and best practices? Discuss these practices in the context of mobile applications.
12. Obfuscation can be used as a privacy-preserving mechanism, for example in web search. Explain the concept of obfuscation and discuss whether obfuscation is a valid approach to personal data protection.


13. Most applications and services (to a certain extent) allow for individually adapting privacy preferences and thus for defining personal privacy policies. How do users cope with this possibility? Discuss the advantages and disadvantages of personal privacy policies.


14. How do expectations about data collection influence users’ privacy concerns and their trust in an app or service? Discuss the influence of informing users about data collection practises and the resulting design implications for app developers and service providers.


15. What is the personalisation-privacy paradox? What are possible explanations for this paradox? Discuss implications for the design of personalised applications and services.


16. In order to be able to address users’ privacy concerns, it is important to quantify privacy attitudes. How can privacy concern and attitudes be measured? Compare different approaches and their advantages and disadvantages. Are there best practices?


17. Users of social networking sites often seem to be willing to expose a vast amount of personal and even sensitive information to mostly loosely defined acquaintances. What are the reasons for this behaviour? What are patterns of personal information revelation? Discuss the privacy implications of online social networking.

18. Does gender influence privacy attitudes and privacy concern with regard to online data collection and behavioural tracking? How do women and men react to increased privacy concern? Discuss how application designers and service providers can account for gender-specific differences related to privacy.


19. Research has observed that people are willing to disclose sensitive information for relatively small rewards. Do people care for their privacy after all? What value do they assign to privacy protection? Given these investigations, discuss whether letting people pay for privacy protection is a feasible approach.


20. Research on information privacy has resulted in a plethora of literature and a great variety in research methodology. Discuss and point out possible research gaps and new research directions.

Pavlou, Paul A. "State of the information privacy literature: where are we now and where should we go?." MIS quarterly 35.4 (2011): 977-988