Course Description

Privacy

Contents

The Big Idea

This course deals with the ongoing technical and social development, which leads to more and more privacy-related concerns in everyday life, often observable in web-based interactive systems.

Privacy as a human right, even though its origin goes way back in time, is widely considered highly jeopardized. Following daily news, privacy concerns are being discussed in various contexts: So-called "anti terror laws" lead to massive privacy restrictions for entire societies, e.g. extension of CCTV. In addition also advocacy groups and companies try to influence politics and legislation – possibly to establish their businesses? – and quite often does it result in further drawbacks for people's privacy, e.g. the new German passport includes an RFID tag with questionable advantages. In the public debate examples like these raise questions about an increasing number of privacy violations and how to achieve both privacy and security within our society. At the same time people give up their privacy all by themselves by publishing personal information on the web and share it with an unknown audience on purpose. Being familiar with the ongoing public debate about privacy, it sounds like a paradox.

Privacy issues often arise with technical progress and the web is a source of completely new kinds of problems, because of its huge number of participants, because of its ease of use – and also because of its international nature, its poor legal regulations and possibilities to actually

protect people's rights, and because of its technical complexity, which makes it very hard for people to assess and understand consequences of their behavior.

In this course the term "Privacy" will be deconstructed first into its different dimensions, meanings and notions and then applied to various contexts: In everyday life privacy is a common concept which affects all people living together in communities and societies. The understanding and exercise of privacy is thereby tightly coupled with the term and concept of society. Although in societies privacy is widely seen as a valuable right, it's susceptible to attacks from different parties, whose motivations need to be understood and discussed. The web context requires the common notion of privacy to be adjusted. Transferring the concept from a local society to a global community reveals completely new challenges regarding both privacy abuse and privacy protection. Besides technical origins of those problems, there might also exist a lack of domain knowledge among web users and therefore an unawareness of risks regarding own actions, that needs to be questioned. However, instead of seeing the constant decrease of privacy as potentially harmful, one can also see new opportunities coming with it and postulate the beginning of a new era, called "Post-privacy". Post-privacy activists try to accept the fact that with ongoing technical progress ultimate personal privacy can't be achieved forever. Nevertheless, this doesn't mean to make every piece of information public for anyone. Post-privacy expresses a willingness to face the fact that today no information can actually be protected effectively and that living in such a society may actually be possible, albeit different. In the context of web science these different perspectives on Privacy are considered crucial, when designing web based systems that should be used by people within communities and societies. This course aims for a multi-dimensional discussion of the term privacy.

Intended Learning Outcomes

The students

- develop a big picture of privacy, know basic terms and are able to argue using a professional jargon,
- have basic knowledge about the origin of privacy and its legal manifestation within the European Union
- are familiar with the different dimensions (legal, social, cultural, political, psychological, philosophical) and facets (locational, informational, decisional) of privacy and can apply them to case studies
- are familiar with the different notions of communities vs. societies and the relation between privacy and transparency within communities and societies
- know the notion of privacy in the web context, have knowledge about risks that arise with privacy loss and are able to create and critically discuss solutions to protect privacy within that context
- know the Post-privacy approach as an alternative way of thinking about current privacy concerns and are able to create design solutions for web based systems in Post-privacy scenarios
- can join and lead a discussion about privacy-related design solutions in the development of web based systems

Structure of the Course

Fundamentals – Origin and notions of Privacy

The course starts with a brief history on privacy concepts: Where does the term privacy come from and which similar concepts have existed in human history? Subsequently the current concept of privacy will be deconstructed in its various dimensions (legal, social, cultural, political, psychological, philosophical) and different facets (at least locational, informational, decisional) using real-life examples. The concepts of community and society as presuppositions for privacy will be introduced and its interplay with privacy illustrated. Having understood the broad nature of privacy, the question of responsibility will be in focus: What does "being in control of one's privacy" really mean and who is responsible to protect people's privacy? The role of government, state and also the role of the European Convention on Human Rights will be discussed.

Everyday Life, Everyday Privacy

This part of the course covers everyday privacy assaults apart from web-related scenarios, e.g governmental CCTV, RFID implementations, anti-terrorism activities, work of advocacy groups and companies for profit reasons, and typical arguments from the public debate. Real-world examples raise questions like: How does privacy relate to the wish for more security? How are the concepts of freedom of speech and transparency related to privacy questions in this context? If there's a general fear of loosing even more privacy, how is this consistent with the request for more governmental transparency in order to control the state and politicians better? A discussion about the distribution of power within a society finishes this part of the course.

Privacy and the Web

Having understood privacy with all its presuppositions and dependencies, the concept shall now be transferred to the web domain. Of course, this won't go without adjustments of the already known characteristics. The lecture will cover topics such as the presence and (at a later time) explosion of private data online and the potential of abuse that arise from it, early ways of keeping online privacy (use of anonymity and pseudonymity) and how the web 2.0 lead to significant changes in the usage of the web. Assaults, and threats will be discussed using real-world examples (e.g. location-based services, Google StreetView, recent activities of the hacker group "Anonymous"), along with motivations (e.g. criminal, public protest, state security) and dimensions (e.g. self-imposed, legal, illegal). However, the web has also introduced new qualities of privacy problems that haven't existed in such a manner before, e.g. in terms of identity theft. The lecture closes with an examination of such abuse potentials and an elaboration of current efforts to increase privacy on a technical web level with privacy-enhancing technologies, e.g. P3P.

Post-Privacy

"Privacy is dead, get over it.", said Scott McNealy, CEO of Sun MicroSystems, and he's not alone with this idea. In fact it's not a cynic prediction of a dark future, Post-privacy advocates rather try to find concepts for living in a society in which no information can be assumed to stay private:

Technological progress will sacrifice privacy, no matter what. So, if we don't want to stop technological progress, isn't it time to start thinking about ways to get along with the consequences? If all created and collected information must be considered potentially harmful, if revealed and misused, data reduction and data economy can be first strategies to avoid unnecessary information in the first place. Post-privacy is about entering a dialogue and questioning current concepts of data-driven web based systems. Furthermore it's an invitation to discuss utopian ideas and to foresee the upcoming social and technical development of the web.

Didactic Concept, Schedule and Assignments

Introductory lecture on site

The introductory meeting deals with organizational course details and a short lecture to introduce basic definitions and concepts of privacy, its origin, its current legal foundation and how the notions of privacy relate to web science. The students are encouraged to form small groups (up to three participants) and to choose appropriate case studies (real or fictional), which will be used in the following workshops to explore new meanings and facets of privacy, and to find solutions to deal with them. The case studies should include privacy-related situations the students have experienced themselves, with at least one case study chosen from the web domain.

1st Online Workshop

This workshop consists of two phases: The first part is held in a seminarial form. The course subject (Everyday Life, Everyday Privacy) is presented in a highly interactive matter, open questions are discussed with the lecturer and among the students. For the second phase students will work in groups to specify the notion of privacy their case study deals with, the risks and potentials for misuse of disclosed personal information and ideas that could help to prevent information misuse and personal harm in future similar situations. Group presentations and a concluding discussion will complete this session.

2nd Online Workshop

The second workshop is based on basic readings regarding the topic "Privacy and the Web" and again structured as a seminarial and a group work phase. After being familiar with basic notions of privacy from the first workshop, these concepts now get applied to the web (science) context. In the second group work phase students are asked to find answers regarding their web-related use cases and questions like: How are privacy concerns different, when the assault context changes from offline life to the web? How is privacy protection different on the web and how does it relate to discomfort of use? Who is responsible for privacy protection in the web context? Technical and societal solutions to increase privacy protection for certain case studies should be outlined and discussed. Group presentations and a concluding discussion will complete this session.

3rd Online Workshop

The third workshop starts with a presentation of the lecturer, introducing the Post-privacy approach of dealing with contemporary technical and societal changes as a drastically different perspective (without being cynic). Based on their case studies in a group work phase the students should develop a utopia "5 years from now" and elaborate on their case studies again in this new context. Which social development have they chosen as a basis for their utopia and why? How could web scientists help steering this development? Findings are discussed in a concluding plenary session.

Wrap-up Session On Site

This on-site workshop is dedicated to clarify open questions of the students concerning all course issues and to summarize workshop content.

The wrap-up session is also used to complete the written examination (45 minutes).

Examination

The participants receive a detailed scenario with a list of questions, covering the range of course core topics. The students have to debate this scenario in terms of the given questions.

References

Fundamentals and Everyday Privacy

DeCew, J., "Privacy", The Stanford Encyclopedia of Philosophy (Fall 2012 Edition), Edward N. Zalta (ed.), <http://plato.stanford.edu/archives/fall2012/entries/privacy/>.

Wacks, R. (2010). Privacy: A Very Short Introduction. Oxford University Press.

Sofsky, W., Rendall, S. (2008). Privacy: A Manifesto. Princeton University Press. <http://press.princeton.edu/titles/8725.html>.

Privacy and the Web

Trepte, S., Reinecke, L. (2011). Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web. Springer. <http://books.google.de/books?id=ru2aU0r7sM0C>

Pollach, I. (2007). What's wrong with online privacy policies? Communications of the ACM, 50(9). <http://dl.acm.org/citation.cfm?id=1284627>.

Cranor, L. (2002). Web Privacy with P3P. O'Reilly Media. <http://books.google.de/books?id=KVEV7c7gghEC>.

Post-privacy

Heller, C. (2008). Embracing Post-Privacy. 25th Chaos Communication Congress. <http://events.ccc.de/congress/2008/Fahrplan/events/2979.en.html>. Video recording: <http://www.youtube.com/watch?v=2WGw2xWCyn0> Slides: <http://www.slideshare.net/plomlompom/embracing-postprivacy-optimism-towards-a-future-where-there-is-nothing-to-hide-presentation>.

Grimmelmann, J. (2009). Saving Facebook. Iowa Law Review 94. <http://works.bepress.com/james_grimmelmann/20>.

Brin, D. (1996). The Transparent Society. Wired (CondéNet). <http://www.wired.com/wired/archive/4.12/fftransparent.html>.

Schneier, B. (2008). The Myth of the 'Transparent Society'. Wired News (CondéNet). <http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0306>.

Schneier, B. (2006). The Eternal Value of Privacy. Wired News (CondéNet). <http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886>.

27.02.2019