weizenbaum
institut

Privacy Icons Project (PIP)
Expert Workshop at the Weizenbaum Institute for the Networked Society
Research Group 4 – Data as a Means of Payment
27th February 2019

The Research Group "Data as a Means of Payment" invited around 20 experts to discuss several aspects of its ongoing research project on privacy icons (PIP). The goal of the project is to develop a tool for improving the decision-making process of users in consent situations by conveying *via* icons relevant information about data processing aspects that might entail risks to the interests of users.

Presentation of the PIP at the Weizenbaum Institute

The Research Group opened by presenting the current stage of its project. The introduction highlighted the power of symbols in representing and conveying information, followed by a theoretical and legal overview on concepts of autonomy, informational self-determination and informed consent as well as on the way in which they interrelate. Despite the critique on consent as a legal institution that legitimises data processing, the approach followed is that some of the problematic aspects of consent can be alleviated through visual elements, and specifically, *via* privacy icons. An important methodological component of the project is developing a broad risk-based approach, which is more user-oriented rather than purely controller-oriented. The idea is to identify data processing aspects that entail an inherent risk to the interests of users. The intention thereby is to enhance these aspects through visual means in order to increase *inter alia* user awareness and possibly influence the decision-making process in the context of granting or denying consent. Based on the text of the GDPR, the Group compiled a risk catalogue that lists the legal provisions dealing with this concept, which the GDPR does not specifically define, in order to better understand and incorporate it in later study and analysis.

The presentation proceeded by describing psychological processes and phenomena in connection with users' behaviour, including the so-called "information privacy paradox". It mentioned different levers that can be pulled to address this issue and the way in which visualisation could contribute to enhance user motivation, attention and awareness while reducing cognitive effort with regard to privacy decisions. The risk attributed to various aspects of data processing provides a selection criterion that informs the decision of choosing which data processing aspects to visualise and include in the icons set. The presentation was concluded by discussing some design choices and enforcement options for achieving a broad acceptance of privacy icons in conjunction with transparency obligations under the GDPR.

Experts Presentations

Prof. **Louisa Specht-Riemenschneider** (Professor for Civil Law, Information Law and Data Law at the Friedrich-Wilhelms-University in Bonn) held a presentation on the future of consent in data protection law. She explained the relevance of consent for the principles of data protection law and mentioned that effective consent indeed must be informed, but in reality, users hardly ever read the information provided, especially in the context of online services. Prof. Specht-Riemenschneider named several solution approaches while noting the advantages of visualisation of information in combination with consent assistants and technical data protection. Regarding feasibility and compatibility of such a solution under the legal framework of the GDPR, it was noted that not all the information obligations under Arts. 13, 14 GDPR can be visualised: A text level remains necessary, and therefore, a layers model should be preferred.

Dr. **Yoan Hermstrüwer** identified three types of challenges regarding consent: (1) The decision problem, i.e., that users make bad or uninformed choices; (2) the institutional problem in the sense that those choices result from the interaction with others, for instance, in the context of network effects; and (3) the personality problem, meaning that bad choices are idiosyncratic. He discussed two contradicting approaches to these challenges. The first is "pushing decisions" which would carry an element of paternalism as it intervenes with individual choices to prevent self-inflicted harm. The second approach is enabling decisions and is associated with the concept of autonomy. Here, the decision to grant or withhold consent would have to be free and informed; thus, personal

Fraunhofer FOKUS · Freie Universität Berlin · Humboldt-Universität zu Berlin · Technische Universität Berlin · Universität Potsdam · Universität der Künste Berlin · WZB · Gefördert vom Bundesministerium für Bildung und Forschung

will and knowledge are basic conditions for consent. Alongside these approaches, also market perspectives play a role, such as market failures, information asymmetries, negative externalities involved in privacy decisions and the public goods problem. Dr. Hermstrüwer highlighted some of the challenges involved in visualisation of data processing risks while emphasising the impact of uncertainty regarding future impacts of a consent decision. He advocated for a regulative approach that focuses on the procedure of data processing, with information about this procedure to be given using a simple visualisation through privacy information, labels, or icons. At the same time, such an approach is susceptible to undesired effects of icons that one should be aware of, such as habituation and overemphasis on the average user.

Yannic Meier (Research Assistant at Chair for Social Psychology – Media and Communication at the University of Duisburg) presented some results of his group's current study involving the protection motivation theory (PMT), which states that fear can be effective in motivating people to behave privacy-protective. He noted that fear is an affective state that can protect a person from a threat and went on explaining some of the cognitive mediating processes of the PMT. The motivation to protect one's privacy is affected by the threat appraisal and the coping appraisal. Their current study investigated whether fear appeals by a tool can influence Facebook users' privacy-protective behaviour. Among others, they examined the impact of perceived efficacy of the tool and fear of consequences on privacy protection intention. The results showed *inter alia* that participants who believed in their ability to protect themselves judged the privacy-enhancing tool to be more effective; people who thought there was not much they could do to protect their privacy found the tool more effective when it induced fear. The result of the study (subject to limitations) is that inducing fear leads to a slightly stronger link between response-efficacy and self-withdrawal and to an increased self-withdrawal intention among people who desire more privacy protection. It does not, however, lead to an increased relationship between fear and self-withdrawal. Nevertheless, fear seems to be a good predictor of privacy protection motivation, regardless of additional fear induction. Connecting this to privacy icons, Mr. Meier suggested that icons should be accompanied by easily understandable descriptions of how to achieve better protection.

Arianna Rossi (Postdoc Researcher at SnT. Université du Luxembourg) presented the set of icons developed by CIRSFID during her time at the University of Bologna and the methodology used. One important question is how existing technologies can be used to create machine-readable visual structure and visualisations. A multi-layered architecture for the management of legal information is a well-established paradigm: Machine-readable specifications can be added (legal XMLs and ontologies) to the document's content and leveraged to obtain a user-friendly presentation. PrOnto (=Privacy Ontology) is an ontology of the GDPR: Its modules formalizing rights of the data subjects, actors, processing operations, processing purposes and legal bases have been visualised to create the icon set.

Icons have idiosyncratic features in comparison to other forms of visualisations. Contrary to what is commonly believed, depending on these characteristics, icons can be easily or hardily interpreted: To make icons understandable, a shared visual vocabulary should be used. The DaPIS project designed a methodology to create such icons. Several open questions were addressed regarding the precise goals of the icons. They could be used as information markers in privacy policies in order to give salience to information that would otherwise be lost when people skim through the text. Additionally, icons can serve as clear indicators for the presence or absence of data processing aspects. They can further fulfil a warning function. Icons can be used in different interfaces, contexts and ecosystems (e.g., privacy policies, consent management, privacy identity management). Some symbols are clearer and more instinctively understandable than others. The level of clarity depends on what is visualised and on how much of it is already part of the "visual library" of the user. Obviously, different user groups react differently to icons, posing a challenge to standard graphical symbols' evaluation methods. However, icons might be universally used and recognised across the EU if they are sufficiently standardised and if the data subjects know their meaning: Expectations about the potentials of icons to solve many of the problems of transparency and consent must remain realistic.

A lively discussion followed, and in conclusion, the large majority of the participants agreed that the idea of privacy icons was promising and that further research should be conducted on the topic.