A UX Approach to Privacy and Security: the Impact of User, Contextual and System-Related Factors

Verena Distler
University of Luxembourg
Esch-sur-Alzette, Luxembourg
verena.distler@uni.lu

Carine Lallemand
University of Luxembourg
Esch-sur-Alzette, Luxembourg
carine.lallemand@uni.lu

Vincent Koenig
University of Luxembourg
Esch-sur-Alzette, Luxembourg
vincent.koenig@uni.lu

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org. CHI 2018, April 21–26, 2018, Montréal, QC, Canada. Copyright is held by the owner/author(s). Publication rights licensed to ACM ACM.

Abstract
This position paper lays out current and future studies which we conduct on the UX aspects of security and privacy, our goal being to understand which factors influence privacy-related decision-making. We advocate using UX design methods in order to study interindividual differences, system-related and contextual factors involved in privacy and security attitudes and behaviors. These results will contribute to user-tailored and personalized privacy initiatives and guide the design of future technologies.

Author Keywords
Privacy; Socio-technical security; User Experience Design; Technology acceptance.

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous;

Introduction
Technologies nowadays perform increasingly complex and security-relevant tasks and play an important role in almost all areas of our everyday lives. While the technology's performance and security might be critical in these situations, the relevance and scope of security

and privacy challenges thereby increase. Privacy can be defined as the ability of individuals to maintain control of their personal information [16], with the goal of enhancing autonomy and/or minimize vulnerability [8]. In the field of information technology, security can be defined as the limited effects of an attacker trying to make a system fail, meaning the system's tamper-resistance [11]. In UX Design, perceived security is defined as feeling safe and in control of your life, rather than feeling uncertain and threatened by your circumstances [5].

On these grounds, various actors undertake efforts to improve privacy and security. However, these endeavors often take a techno-centered approach, which frequently leads to poorly designed systems. Security breaches caused by "human error" are therefore common. Reducing the security problem to a technical question and blaming users to be "the weakest links" when a security breach occurs is a frequent and bad practice [14]. We consider that these breaches can often be blamed on badly designed systems, which do not take human characteristics into account during the design phase. As [4] state, if users are left to be weak points in a system's functioning, the system interfaces with its users in an insecure way, violating basic principles of psychology and security economics. In order to improve users' privacy and security when using technologies, it is therefore imperative to take a human-centered approach when designing and improving these systems. User Experience (UX) design allows for understanding user, contextual and system-related factors impacting security and privacy decision-making. Individual factors also include one's awareness and knowledge of privacy matters. On the one hand, some users might not perceive any threat, or might not realize the value of their personal data, potentially leading to unwilling consequences. On the other hand, users' decision-making processes in the context of security and privacy might also be based on tradeoffs, as studied for example by [19, 12]. Users are regularly confronted with situations where they need to evaluate the potential benefits of using a technology in exchange for its possible drawbacks. This problem should also be seen through the lens of voluntariness of use, as choice is not always given to the users (e.g., in a professional context). Recent research has revealed that privacy concerns differ between individuals and that systems should be tailored to these different privacy profiles [17, 18, 9]. Privacy concerns are for instance influenced by demographic differences, privacy attitudes, cultural dimensions and contextual/situational factors [7]. In line with this research, we hypothesize that there are individual differences in the accepted tradeoffs. Moreover, we consider that the accepted compromises are context- and system dependent. The overarching objective of our studies will be to understand people's awareness of privacy and the underlying decision-making processes in order to guide the design of future technologies.

Current studies

Privacy and technology acceptance

PARTICIPANTS. In a first study, eight focus groups (4 face-to-face and 4 online) involving 32 participants (17 men, 15 women) from different cultural backgrounds and socioeconomic characteristics served as a basis for an ongoing survey on users' perception of privacy. The focus groups were comprised of 4 to 5 participants. Our goal is to represent a large spectrum of users in the focus groups. We created two expert groups with professionals of the digital field, two student groups

with non-IT related majors, and four groups of the general population. We invited participants with a multitude of nationalities, including France, Luxembourg, Macedonia, Croatia, China, Russia, Poland, Italy, Belgium, Spain, Canada, India, Kenya, Mauritius. The average age of our participants was 33.1 years (Min=19, Max=55). At the educational level, one (3%) participant had no high school diploma, seven (22%) had completed high school level education, 11 (35%) had completed an undergraduate or Bachelor's degree, 10 (31%) had completed a Master's degree, and three (9%) hold a PhD.

METHODOLOGY. In these studies, we present participants with a selection of technology use scenarios derived from a previous study by [12]. Each scenario presents a potential situation where a technology could provide various benefits in exchange for different kinds of user data: 1/ office surveillance cameras, enhancing employees' security against a potential risk of surveillance and performance management. In the second scenario, 2/ sharing health information, the scheduling of doctors' appointments can be done online in return for allowing the doctor to upload medical data onto an online platform. The third scenario offers the advantage of potential savings using a 3/ smart thermostat, which however also provides information on the movements in the house. And the fourth scenario, 4/ free social media, would allow people to reconnect with peers in exchange for being shown targeted ads. Participants are invited to comment on each scenario by arguing why the situations described seem acceptable or not. A discussion on the acceptability and acceptance of these technologies follows.

First insights might suggest differences of perception based on cultural dimensions, such as individualism - collectivism: while all but one participants from countries with a highly individualistic culture (according to [6]) found the installation of surveillance cameras at their workplace inacceptable, 3 participants out of the four who found it acceptable come from countries with a highly collectivist culture (where people act in the interests of the group before individual concerns) namely Russia, China and Kenya. The fourth person stated that it is her previous experiences working in shops with cameras which influenced the acceptance. Similar individual differences in privacy were observed in all of the scenarios, emphasizing that a one-size fits all approach is not adequate in the context of privacy and security. Ongoing studies include an online questionnaire replicating a part of the study by [12] with the objective of reaching a more international audience. Beyond the scenarios, the survey will include privacy fatigue items [2], technology acceptance items (adapted from [15]), and questions exploring people's actual knowledge about privacy and their actual behavior. This will enable us to understand which types of users exist with relation to privacy-tradeoffs, potentially allowing us to create context-based "privacy personas". We expect this mixed methods protocol to inform us on individual differences in privacy perceptions, more specifically on the tradeoffs and factors impacting perceived risk and willingness to give away personal data. Contextual factors are of course of primary importance and are therefore included as variables in our studies. We intend to analyse how compliant our results are with established technology acceptance models [15] in the context of privacy.

Privacy and security in the context of eVoting

In a second study, we investigated privacy and security concerns in the context of eVoting. For this study, we conducted four focus groups with a total of 16

participants (8 men, 8 women). Two groups were recruited at the university (students and UX professionals) and two groups were recruited outside of the university. The average age was 34.7 (Min=21, Max=55). One (6%) participant had no high school diploma, four (25%) a high school diploma, five (31%) a bachelor's degree or equivalent, four (25%) a master's degree or equivalent and two (13%) hold a PhD. Amongst 16 participants, ten nationalities were represented, mainly from Europe but also from Russia and Asia.

We strived to understand to which extent people are aware of potential risks and threats regarding eVoting. We also explored factors that give participants a feeling of security and privacy in the context of eVoting and potential tradeoffs between usability and security. Again, participants stemmed from different cultural and socio-economic backgrounds, while also having different voting experiences and behaviours. Contextual factors, such as the type of elections at stake, the country of residence, type of devices used or technical aspects of IT security were discussed by the groups as impacting their attitudes. A particular characteristic of the groups we have formed is their international composition (several nationalities represented in each group), thereby allowing participants to debate around varied voting experiences, expectations and concerns. One of the groups for instance involved participants from Russia, China, Poland and Luxembourg. The topic of trust in governments and political systems in place appeared as a relevant factor strongly impacting people's perception of the pros and cons of eVoting.

As discrepancies between user attitude and their actual behavior exist, the so-called privacy paradox [10], we plan to experimentally study eVoting experience through user testing of a highly secure eVoting platform, Selene [13]. Previous studies of similar voting systems [1] have pointed out important usability issues, leading to a high number of invalid or erroneous votes and acceptance issues. Beyond usability, we will take a broader, context-based UX approach in order to understand how the design of the eVoting platform Selene can inspire security, confidence and a feeling of privacy. To address this objective, several variations of the eVoting platform Selene will be prototyped and tested, e.g. through different levels of user feedback, levels of transparency of complex cryptographic processes. As we consider interdisciplinarity as a key condition of success in privacy and socio-technical security research, members of our team have complementary backgrounds in user experience, information architecture, psychology, cryptography, and network security.

Conclusion

Our research follows a user-centered approach, defined as a way to "understand people's actions, and aspects of experience that people will find relevant when interacting with a product" [3, p. 262]. Using UX design methods and processes, we therefore advocate studying interindividual differences, along with system-related and contextual factors involved in privacy and security attitudes and behaviors. The overarching goal for our current and future studies will be to understand which factors influence privacy-decision making. We thereby hope to contribute to well informed, user-tailored and personalized privacy initiatives. At a larger level, we strive to contribute to the development of a user-centered and personalized approach to socio-technical security.

References

1. Acemyan, C. Z., Kortum, P., Byrne, M. D., & Wallach, D. S. (2014). Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. The USENIX Journal of Election Technology and Systems, 2(3), 26–56.
2. Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–51.
3. Forlizzi, J., & Battarbee, K. (2004). Understanding experience in interactive systems. Proceedings of DIS' 2004, 261-267.
4. Gollmann, D., Herley, C., Koenig, V., Pieters, W., & Sasse, M. A. (2015). Socio-Technical Security Metrics (Dagstuhl Seminar 14491). Dagstuhl Reports, 4(12), 28.
5. Hassenzahl, M., Eckoldt, K., Diefenbach, S., Laschke, M., Len, E., & Kim, J. (2013). Designing moments of meaning and pleasure. Experience design and happiness. International Journal of Design, 7(3).
6. Hofstede, G. Asia Pacific J Manage (1984) 1: 81.
7. Li, Y., Kobsa, A., Knijnenburg, B. P., & Nguyen, C. (2017). Cross-Cultural Privacy Prediction. Proceedings on Privacy Enhancing Technologies, 2017(2), 113–132.
8. Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. Journal of Social Issues, 59(2), 243–261.
9. Morton, A., & Sasse, M. A. (2014). Desperately seeking assurances: Segmenting users by their information-seeking preferences. In Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on (pp. 102–111). IEEE.
10. Norberg, P.A., Horne, D.R., Horne, D.A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors, Journal of Consumer Affairs, 41(1), 100–126.
11. Pieters, W. (2006). Acceptance of voting technology: between confidence and trust. In K. Stølen et al. (Eds.) iTrust 2006, LNCS 3986 (pp. 283–297). Berlin-Heidelberg: Springer-Verlag.
12. Rainie, L., & Duggan, M. (2015). Privacy and Information Sharing. Pew Research Center.
13. Ryan, P. Y., Rønne, P. B., & Iovino, V. (2016). Selene: Voting with transparent verifiability and coercion-mitigation. In International Conference on Financial Cryptography and Data Security (pp. 176–192). Springer.
14. Schneier, B. (2000) Secrets & Lies: Digital Security in a Networked World. John Wiley & Sons, Inc., New York, NY, USA, 1st edition.
15. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425–478.
16. Westin, A. F. (1968). Privacy and freedom. Washington and Lee Law Review, 25(1), 166.
17. Wilkinson, D., Sivakumar, S., Cherry, D., Knijnenburg, B. P., Raybourn, E., Wisniewski, P., & Sloan, H. (2017). User-Tailored Privacy by Design. Internet Society.
18. Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. International Journal of Human-Computer Studies, 98, 95–108. doi: 10.1016/j.ijhcs.2016.09.006
19. Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. Decision Support Systems, 106, 44–52.