Approaching Data Protection by Design in Connected Communal Spaces

A Case for Contextualised Participatory Design

Martin Kraemer, CDT16

There is a gap between person-centred data protection legislation and practices, and communal implications of internet-connected technology. Modern communal spaces – such as our homes – typically involve heterogeneous groupings of individuals with dynamic social structures, unattributed responsibilities, and varying levels of skill. Designing systems for use in these spaces requires taking into account communal factors, however data protection for communal spaces is not deeply understood. Studies to disentangle this complex problem space lie at the heart of my doctoral work. In this short article, I make the case for *Contextualised Participatory Design* which appears promising in accounting for heterogeneous social groups and their dynamics, complementing individual perspectives on data protection.

Introduction

Over the past 30 years, internet-connected technology has fundamentally changed the way we conduct our lives. Where, why, and how people make use of the internet has had long lasting impact: internet cafes emerged and disappeared; people started working from home and other places; and the newest wave of internet-connected smart home devices brings increasingly sophisticated and unobtrusive technology to our homes. Today, we use internet-connected technology ubiquitously: we are connected anywhere and everywhere we go, often without realising it. The resulting context collapses have been discussed at great length in the literature: portability of devices and ad hoc sharing of information between locations means that traditional physical, social, and institutional boundaries are blurred as people carry devices to different spaces.

Data Protection by Design is increasingly recognised by law- and policy makers.

Concerns of data protection are almost omnipresent in studies of internet-connected technology use, and legislators have taken on the challenge of regulating the collection and use of data. The focus of our work lies within the EU, whose General Data Protection Regulation (GDPR) is said to have had impact on technology globally [16]. The EU adapted existing privacy-by-design guidelines as data protection principles to codify rules for data collection and processing [4]. The GDPR requires that these principles are to be followed from the outset, by design and by default. They detail rules for data processing and use, and they highlight the importance of appropriate security measures.

The spirit of the GDPR is to protect individuals' right to privacy and, by implication, society as a whole ; however, it is unclear how its rather abstract data protection principles can be observed for the broad variety of connected communal spaces such as cafes or smart homes. For example, different skills, interests, and preferences in using internet-connected technology can cause friction; a security camera might capture several people at the same time, while only one of them set up and explicitly consented to its use.

Research on privacy beyond the individual in communal spaces is nascent.

In the academic literature, issues of data protection have been researched in context of informational or data privacy. Because privacy is "inherently socio-technical and situated", we need to use methods that "explore people and situations" in spaces "where the 'right' definition of privacy might not be known at the outset" [24]. Existing privacy theories highlight the importance of context for privacy and its interactional and interpersonal character [1,11,21]. Most empirical work assumes perspectives of individuals or of specific user groups [25,26], while few contributions have explicitly considered aspects of connected and communal privacy [2,23]. However, to apply data protection by design successfully to connected communal spaces a better understanding of how individuals and communities manage their privacy, both individually and as a diverse group, is required.

The literature on informational privacy reveals several different notions of privacy beyond the individual. Each being different in scope, they demonstrate the complexities of the problem space, emphasising the entanglement of privacy with social and cultural considerations. Between them, these contributions consider common goals, shared data (or shared inferred information), shared access to devices and accounts, a shared sense of community across online and offline spheres, physical proximity with other people, and feelings of responsibility for others.

However, the *use of technology in shared communal spaces* such as our homes has altered the way we conduct our lives. In these socially, physically, and temporally diverse settings, technology use is embedded in interpersonal relationships, follows perceived norms, roles, and hierarchies, and is continuously negotiated [6,8,9]. In the home, networks and devices are often shared between household members and used collectively. In contrast to 'third spaces', members of the household expect to share access to and distribute responsibilities for networks and devices, considering personal characteristics (attitude, aptitude, competence, and skill) when navigating individual and shared use of devices [5,10,14].

It is unclear how to comply by design with requirements of laws and regulations.

Data protection by design has mostly been approached by emerging practice and research in privacy engineering. The field has a strong policy and engineering focus, aiming to translate regulatory guidelines and requirements into engineering practice [13,54]. For example, [22] identified three different approaches including architecture, policy, and interaction; [7] proposed design strategies; and [15] linked engineering best practices with privacy impact assessment and privacy enhancing technologies to make privacy-by-design goals verifiable and measurable. These approaches have been criticised for their 'check-list' character [12], and chosen design perspectives were said to be narrow in their understanding of privacy as individual control over data [24].

Within the domain of informational privacy research, [24] argued for the application of design orientations such as Value Sensitive (e.g. [17]) and Participatory Design (e.g [18]). Communal aspects in particular have been considered by participatory design (PD) approaches (e.g. in workplace, in design environment, or in workshops) [19]. [26] employed participatory design to explore privacy perceptions and designs of smart home owners [25] and bystanders [26]. They suggest shifting the focus toward cooperative mechanisms and bystander-centric mechanisms to equally consider both perspectives by design, and they highlight the importance of considering privacy seeking behaviours, varying expectations, and contextual variations in understanding and contrasting privacy perceptions [26]. This illustrates how these orientations help to explore situations in which a clear definition of privacy might not be known from the outset.

To summarise, approaching data protection by design and by default in connected communal spaces needs to take into consideration: (1) the important impact of the use of connected technology in shared and communal spaces beyond the individual; (2) the complex and interrelated nature of data protection in such spaces, in that individual perspectives overlap with each other and a group perspective emerges; (3) context when designing for data protection in the form of social and cultural facets but also physical features of the environment in which a technology is used; and (4) shortcomings of existing approaches, in that methods from the related field of privacy engineering are not fit for this purpose.

A case for Contextualised Participatory Design

We propose contextual participatory design (PD) to address these challenges. Our proposal follows calls from previous contributions bridging the gap between privacy and design [20,24] and the successful application of participatory design (PD) working with specific user groups [25,26] and communities [3]. Known as the "third space in HCI" [19], PD reinforces the role of end users as stakeholders in the design process and can be instrumental in understanding their values and expertise [19,24]. Thereby, PD invites interpretation by users and focuses more on collectivism than individualism, with a heterogeneity of perspectives becoming the norm [19].

PD allows the interpersonal character of data protection in shared spaces to take centre stage in investigations, allowing participant designers to more fully exploring its contextual nature. Exploring data protection "through the eyes of stakeholders" [24] in this way allows us to investigate how stakeholders make sense of data protection in connected and shared spaces. A PD approach, then, appears promising for three reasons: (1) the lack of a clear approach definition of data protection in shared connected spaces; (2) PD allows the interpersonal character of data protection in shared spaces to take centre stage; and (3), thereby, PD is well suited to explore its contextuality.

A popular PD approach in the literature is the Future Workshop format. Stakeholders join researchers in *critiquing* the present, *envisioning* the future, and *implementing*—moving from the present to the future [19]. We suggest to adapt this format as follows:

> *Critiquing the present* – introduce the problem space in three steps: (1) task participants to explore shared spaces as context for the design exercise, i.e. the home and a coffee shop; (2) introduce participants to design challenges of data protection that are familiar to them and useful in discussing data protection goals, e.g. retaining control over data; and (3) provide guiding questions to jointly reflect on what data protection could mean in such spaces.
>
> *Envisioning the future* – posit a relatable design challenge, e.g. focused on a common activity so that the design activity can be facilitated through shared experiences. Assist with sketching and clarify technical questions where required, but leave it to the group to fill the design space given to them. Conclude the session with a presentation and short discussion of the design solution.
>
> *Implementing* – help participants with drawing more specific sketches of contextual use and mockups of the devices and interfaces so as to fully capture their ideas and understanding. If desired, prototype some of their ideas later and involve some of the initial participants in user testing.

This approach is well suited to approach data protection by design and by default in connected communal spaces for three main reasons: (1) it shifts focus to improving a familiar task/problem in (2) considering a familiar environment (e.g. home or a cafe) while (3) exploring a somewhat familiar design space (data protection). Based on our initial applications of this approach, the use of existing design techniques and artefacts appears promising in introducing stakeholders to a problem space without requiring them to be "conversationally familiar" from the outset. We believe a structured contextual exploration can benefits explorations of privacy: Firstly, in a multi-cultural society such as ours, a contextual exploration of data protection can foreground socio-cultural aspects; and secondly, the approach allows our participants to become familiar with each others' lived experiences.

Contributing towards reusable and relatable insights

Ultimately, we hope the described approach can help with much needed innovation towards achieving data protection by design internet-connected technologies. The design session becomes a melting pot for the needs and desires of privacy researchers, information technology experts, user experience designers, and user groups. What might result from these sessions – and our initial efforts would encourage everyone to pursue this stream of research – is the development of a common vocabulary. This vocabulary and insights on its usefulness are much needed to advance existing design techniques and artefacts so as to account for contextual aspects that matter to users and enable designers to more holistically consider data protection in communal spaces by design.

Acknowledgements

Ideas for large parts of this article stem from long discussions and joint research efforts with my supervisor Ivan Flechais and my fellow DPhil students Norbert Nthala, Paula Fiddi, and William Seymour.

References

1. I Altman. 1975. The environment and social behavior: privacy, personal space, territory, crowding. Brooks/Cole Pub. Co., Monterey, Calif. Retrieved from https://books.google.co.uk/books?id=GLBPAAAAMAAJ

2. Alison Burrows, David Coyle, and Rachael Gooberman-Hill. 2018. Privacy, boundaries and smart homes for health: An ethnographic study. Health & Place 50, May 2017: 112–118. https://doi.org/10.1016/j.healthplace.2018.01.006

3. Chhaya Chouhan, Christy M. LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. 2019. Co-designing for community oversight: Helping people make privacy and security decisions together. Proc. ACM Hum.-Comput. Interact. 3, CSCW. https://doi.org/10.1145/3359248

4. Council of the European Union. 2016. General Data Protection Regulation. OJ L 119. Retrieved from http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

5. Andy Crabtree, Richard Mortier, Tom Rodden, and Peter Tolmie. 2012. Unremarkable networking: the home network as a part of everyday life. Proceedings of the Designing Interactive Systems Conference. ACM.: 554–563. https://doi.org/10.1145/2317956.2318039

6. Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'Privacy' for a Networked World. Computer Supported Cooperative Work: CSCW: An International Journal 26, 4-6: 453–488. https://doi.org/10.1007/s10606-017-9276-y

7. George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tirtea, and Stefan Schiffner. 2015. Privacy and data protection by design - from policy to engineering.

8. Paul Dourish and Genevieve Bell. 2011. Rethinking privacy. In Divining a digital future: Mess and mythology in ubiquitous computing. The MIT Press, Cambridge, Mass., 137–160. https://doi.org/10.7551/mitpress/9780262015554.003.0069

9. Paul Dourish. 2006. Re-Space-ing Place : " Place " and " Space " Ten Years On. In Proceedings of the 2006 20th anniversary conference on computer supported cooperative work - cscw '06, 299—–308.

10. Radhika Garg and Christopher Moreno. 2019. Understanding Motivators , Constraints , and Practices of Sharing Internet of Things. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3, 2: 1–21. https://doi.org/10.1145/3328915

11. Erving Goffman. 1975. The presentation of self in everyday life. Life as theater: 173. https://doi.org/10.2307/258197

12. Seda Gürses and Jose M. Del Alamo. 2016. Privacy Engineering: Shaping an Emerging Field of Research and Practice. IEEE Security and Privacy 14, 2: 40–46. https://doi.org/10.1109/MSP.2016.37

13. Seda Gürses, Carmela Gradiant Troncoso, and Claudia Diaz. 2015. Engineering privacy by design reloaded. Amsterdam Privacy Conference: 1–21. Retrieved from https://iapp.org/resources/article/engineering-privacy-by-design-reloaded/

14. Martin J Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring communal technology use in the home. In Proceedings of the halfway to the future symposium 2019 (HTTF 2019). https://doi.org/10.1145/3363384.3363389

15. Inga Kroener and David Wright. 2014. A Strategy for Operationalizing Privacy by Design. The Information Society 30, 5: 355–365. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/01972243.2014.944730

16. He Li, Lu Yu, and Wu He. 2019. The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management 22, 1: 1–6. https://doi.org/10.1080/1097198X.2019.1569186