# Crafting Privacy: Two Case Studies Integrating Cross-Disciplinary Perspectives on Privacy in Design

Maaike Harbers[1], Mortaza S. Bargh[1,2], Florian Cramer[1], Sunil Choenni[1,2], Jeannette Nijkamp[1] and Anne Nigten[3]

[1] Rotterdam University of Applied Sciences, Rotterdam, The Netherlands
[2] Ministry of Justice and Security, The Hague, The Netherlands
[3] The Patching Zone, Rotterdam, The Netherlands
m.harbers@hr.nl

**Abstract.** Privacy by design is a widely acknowledged necessity, yet its practice is still in its infancy. Many scholars have argued that privacy by design requires a cross-disciplinary approach in which privacy perspectives from different disciplines need to be integrated from the beginning of the design process. This paper investigates the potentials and shortcomings of a workshop format, used in the early stages of a (re)design process, to integrate viewpoints of multiple stakeholders from different disciplines. The workshop is used in two cases involving privacy issues, in the healthcare and in the insurance domain. The results show that different stakeholders, representing social, technological, ethical, legal, domain and user perspectives, identified different problems. Together, they thus provided a more complete view on the issues at stake, forming a better starting point to account for privacy in the design process. Based on the results, the paper suggests a number of research directions for combining diverse views from multiple stakeholders.

**Keywords:** Privacy by design, cross-disciplinary, information technology, human computer interaction, IT, HCI.

## 1 Introduction

The ubiquitous presence of technology creates ever more urgency to account for privacy issues [13]. Considering and accounting for privacy during the design of information systems is often referred to as ‘privacy by design’ [1,10,12,16]. Privacy by design has become particularly prominent due to the European Union’s General Data Protection Regulation (GDPR), that has gone into effect in May 2018, which requires meeting the principles of privacy by design when processing personal data [6].

One of the best-known works on privacy by design is by Cavoukian [1], introducing seven design principles to enable individuals to gain personal control over their information and to enable organizations to gain a sustainable competitive advantage. Cavoukian’s principles are high-level guidelines that still need to be translated to actual system designs and engineering practices [8]. Currently, there exist no well-established approaches for translating the high-level privacy by design principles to practice [8,19,23].

One of the major challenges in applying privacy by design is that it requires the integration of perspectives from multiple stakeholders (user, designer, developer, etc.) and disciplines (HCI, software engineering, law, etc.) [4,5,8,15]. In the area of requirement engineering, a number of methods have been proposed that integrate multiple perspectives to elicit privacy-related system requirements, e.g. by using multiple information sources [15], questionnaires and scenarios [7], and workshops with multiple stakeholders [2,3,5,17].

Although the above works aim at taking into account multiple perspectives in eliciting privacy requirements, they do not elaborate upon how well the applied methods integrate these perspectives in practice. In this paper, we therefore investigate the potentials and shortcomings of using a workshop with multiple stakeholders as a method to surface privacy-related problems from multiple perspectives, by applying it to two design cases.

## 2 Case studies

The workshop we use is suitable for the initial phase of a systematic privacy by design approach, aiming to identify privacy issues and trade-offs from multiple perspectives related to the (re-)design of an information system. A diverse participant group is key to the approach, as the participants represent multiple perspectives on privacy. The workshop centers around a timeline, which serves as a boundary object to bridge the participants' domains of expertise [21,22]. This timeline is used to capture the flow of data in the system to be (re-)designed. The use of a timeline with data is inspired by mappings as known from IT and HCI/UX, such as a customer journey map [11,14], threat modelling [18], and a typical data lifecycle (e.g., as considered by various spheres in [20]).

To gain practical experience with the workshop format, we organized two sessions with 6 stakeholders: a problem owner (domain expert), an end-user, and four privacy experts with a social, ethical, technical and legal perspective, respectively. The workshops were led by a moderator (a designer). The roles of moderator and privacy experts were fulfilled by researchers at Rotterdam University of Applied Sciences (RUAS), and those of problem owner and end-user by people outside of RUAS, associated to the respective domains. In an iterative design fashion, the results of the first session were used to inform the second.

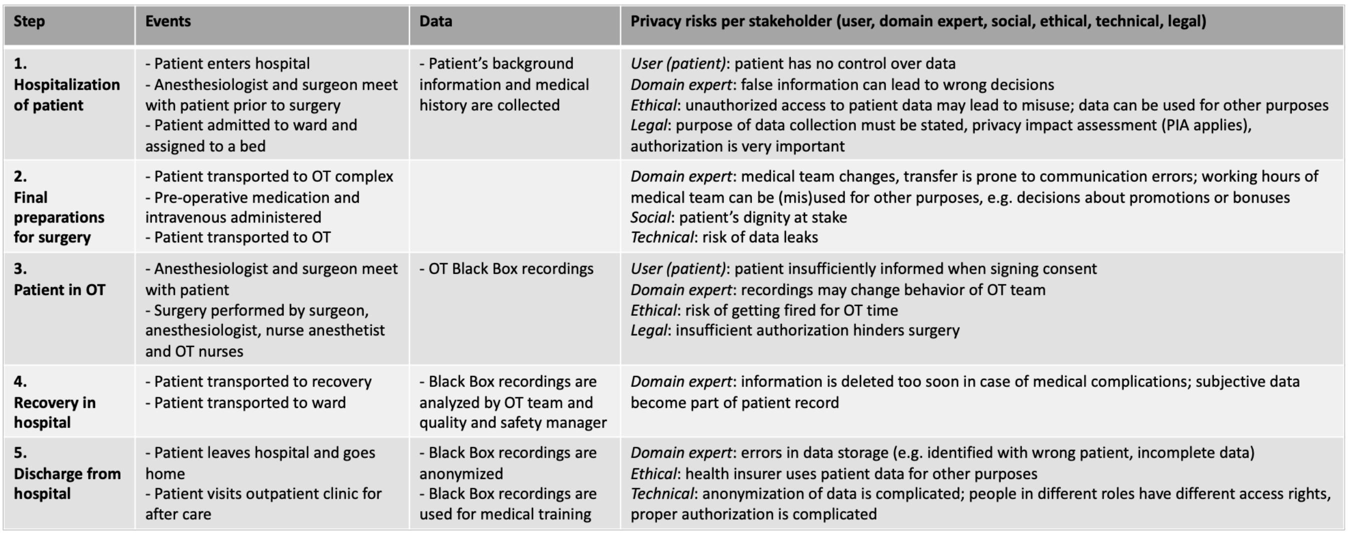
### 2.1 Case 1: The OT black box

The first case deals with the design of recording surgeries in the Operation Theater (OT) in a so-called OT Black Box. Data stored in this OT Black Box contain video and audio recordings of the OT, featuring the patient and the OT team, typically consisting of surgeons, anesthesiologists, nurse anesthetists and OT nurses. These recordings are later used by the OT-team to analyze and evaluate their performance, and by a quality and safety manager to detect potential safety issues and improve the OT procedure if possible. After two days, the recordings are anonymized (patient and OT-team are no longer identifiable) and used for medical training purposes. Recordings are then no longer available for the patient who underwent the surgery.

Before the workshop, the moderator and problem owner prepared a timeline consisting of five steps (see Figure 1). For each step, a large (A0-sized) paper was put on the wall, on which the other workshop participants could write and add sticky notes. Each participant was provided with markers and sticky notes of a unique color, so that the contributions on the poster could be traced back to the different perspectives.

The four-hour workshop session consisted of five activities. First, the design case was introduced by the problem owner, explaining what happens in each timeline step. Second, data assets per timeline step were identified by the workshop participants (first individually, then in a group discussion), and added to the posters. Third, privacy violation risks per timeline step were identified (first individually, then in a group discussion), and added to the posters. Fourth, opportunities and risks of the information system as a whole were determined and trade-offs were identified (in a group discussion). Fifth, the workshop participants agreed on a set of design constraints, based on the identified trade-offs (in a group discussion).

Figure 1 shows some of the ‘data’ and ‘privacy risks’ that were identified per timeline step. The overview is not exhaustive but intends to provide a gist of the contributions from different participants. The results show that they bring in different perspectives. For instance, the social privacy expert mentions that the patient’s dignity may be at stake, whereas the legal privacy expert points at the application of a privacy impact assessment.



| Step | Events | Data | Privacy risks per stakeholder (user, domain expert, social, ethical, technical, legal) |
|---|---|---|---|
| **1. Hospitalization of patient** | - Patient enters hospital<br>- Anesthesiologist and surgeon meet with patient prior to surgery<br>- Patient admitted to ward and assigned to a bed | - Patient’s background information and medical history are collected | *User (patient)*: patient has no control over data<br>*Domain expert*: false information can lead to wrong decisions<br>*Ethical*: unauthorized access to patient data may lead to misuse; data can be used for other purposes<br>*Legal*: purpose of data collection must be stated, privacy impact assessment (PIA applies), authorization is very important |
| **2. Final preparations for surgery** | - Patient transported to OT complex<br>- Pre-operative medication and intravenous administered<br>- Patient transported to OT | | *Domain expert*: medical team changes, transfer is prone to communication errors; working hours of medical team can be (mis)used for other purposes, e.g. decisions about promotions or bonuses<br>*Social*: patient’s dignity at stake<br>*Technical*: risk of data leaks |
| **3. Patient in OT** | - Anesthesiologist and surgeon meet with patient<br>- Surgery performed by surgeon, anesthesiologist, nurse anesthetist and OT nurses | - OT Black Box recordings | *User (patient)*: patient insufficiently informed when signing consent<br>*Domain expert*: recordings may change behavior of OT team<br>*Ethical*: risk of getting fired for OT time<br>*Legal*: insufficient authorization hinders surgery |
| **4. Recovery in hospital** | - Patient transported to recovery<br>- Patient transported to ward | - Black Box recordings are analyzed by OT team and quality and safety manager | *Domain expert*: information is deleted too soon in case of medical complications; subjective data become part of patient record |
| **5. Discharge from hospital** | - Patient leaves hospital and goes home<br>- Patient visits outpatient clinic for after care | - Black Box recordings are anonymized<br>- Black Box recordings are used for medical training | *Domain expert*: errors in data storage (e.g. identified with wrong patient, incomplete data)<br>*Ethical*: health insurer uses patient data for other purposes<br>*Technical*: anonymization of data is complicated; people in different roles have different access rights, proper authorization is complicated |

**Fig. 1.** Data and privacy risks identified by workshop participants for case 1 (OT Black Box).

After identifying privacy risks, participants agreed that the most important trade-off was improved healthcare versus deteriorated privacy, i.e., recordings by the OT Black Box can enhance the quality of healthcare, but they introduce privacy violation risks for both the patient and the OT team. There was little time left to perform the last activity, identifying design constraints. Participants stressed that data should only be used for the purpose they were collected for.

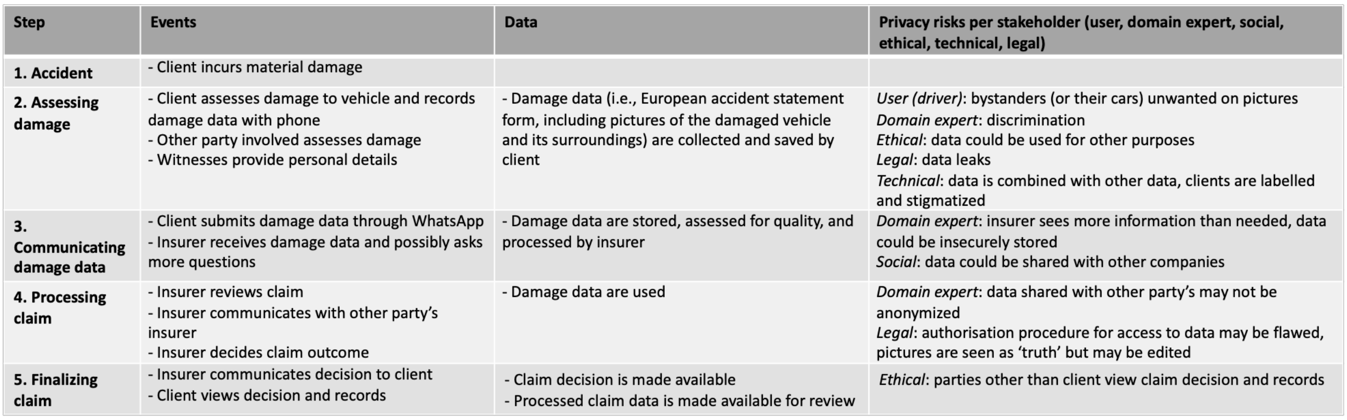
### 2.2 Case 2: WhatsApp damage claims

The second design case involves the use of the mobile application WhatsApp for damage claims to an insurance company. The insurance company offers its customers the possibility to send text and pictures of car damage (including pictures of the location) via WhatsApp, when claiming the damage to the insurance company. These messages and pictures are encrypted by WhatsApp.

Although detailing the ‘data’ of all timeline steps in the first workshop brought forward deeply engaged participants, it also led to discussions in which domain-specific details were explored by non-experts. Moreover, it led to time shortage later on in the session. We therefore asked the problem owner in the second workshop to detail the data in each timeline step beforehand (Figure 2, 3rd column). The other workshop activities remained the same.

Figure 2 shows the results of the second workshop session. Again, these results are not exhaustive, yet indicative. Similar to case 1, privacy issues related to ownership, faulty data and function creeps were identified. In the discussions, a lot of attention was paid to the trustworthiness of the photos sent for a damage claim via WhatsApp, as they could easily be manipulated or uploaded from the internet. Thanks to the new setup of the workshop, it was possible to complete all workshop activities this time.

Participants identified a trade-off between ease of use and privacy. Using WhatsApp for reporting damage increases ease of use for customers but introduces privacy risks due to relying on a 3rd party service provider. Other trade-offs identified were



| Step | Events | Data | Privacy risks per stakeholder (user, domain expert, social, ethical, technical, legal) |
|---|---|---|---|
| 1. Accident | - Client incurs material damage | | |
| 2. Assessing damage | - Client assesses damage to vehicle and records damage data with phone<br>- Other party involved assesses damage<br>- Witnesses provide personal details | - Damage data (i.e., European accident statement form, including pictures of the damaged vehicle and its surroundings) are collected and saved by client | *User (driver)*: bystanders (or their cars) unwanted on pictures<br>*Domain expert*: discrimination<br>*Ethical*: data could be used for other purposes<br>*Legal*: data leaks<br>*Technical*: data is combined with other data, clients are labelled and stigmatized |
| 3. Communicating damage data | - Client submits damage data through WhatsApp<br>- Insurer receives damage data and possibly asks more questions | - Damage data are stored, assessed for quality, and processed by insurer | *Domain expert*: insurer sees more information than needed, data could be insecurely stored<br>*Social*: data could be shared with other companies |
| 4. Processing claim | - Insurer reviews claim<br>- Insurer communicates with other party’s insurer<br>- Insurer decides claim outcome | - Damage data are used | *Domain expert*: data shared with other party’s may not be anonymized<br>*Legal*: authorisation procedure for access to data may be flawed, pictures are seen as ‘truth’ but may be edited |
| 5. Finalizing claim | - Insurer communicates decision to client<br>- Client views decision and records | - Claim decision is made available<br>- Processed claim data is made available for review | *Ethical*: parties other than client view claim decision and records |

**Fig. 2.** Data and privacy risks identified by workshop participants for case 2 (WhatsApp for damage claims).

knowledge versus privacy (collecting and storing information increases insurers' knowledge, but introduces privacy risks), costs versus privacy (building an in-house application protects customers' privacy, but increases costs), ease of use versus security (as the ease of using WhatsApp creates security risks due to relying on a 3rd party service provider).

The workshop participants identified the following design constraints and recommendations: 1) insurance companies should develop their own application rather than relying on  3rd parties such as WhatsApp, this should be done according to privacy by design principles, 2) customers should always be able to choose whether they want to make use of WhatsApp, 3) customers should be informed about their options and the implications of their choices, 4) as least data as possible should be collected, data should not be collected if they will not be used, 5) customers should be able to access their personal data stored by the insurance company, and 6) authorization of data access should be implemented carefully in the insurance company in order to avoid function creeps.

## 3 Discussion and conclusion

In both design sessions, stakeholders from different disciplines identified different (privacy) problems and high-level requirements. For instance, the technical expert focused on issues related to the processing of data, such as data leaks and de-anonymization of data, whereas the social expert brought up the issue of human dignity and the legal expert identified issues related to authorization of access. The number of identified issues of all stakeholders was larger than any of the individual stakeholders' contributions. Having multiple perspectives represented thus provided a richer view on the design case at hand. Besides helping the privacy by design of IT systems, the workshops were increasing awareness about privacy and its complexity among the participants, i.e., they learned from each other and gained more insight in the complexity of privacy by design.

A number of issues should be considered when combining perspectives of multiple stakeholders in a workshop in general, and in this workshop in particular. First, in a multiple stakeholder workshop, there is a risk that some perspectives are more dominant in the discussion than others. This could be countered by stricter time management by the moderator, making sure that all participants receive an equal amount of speaking time. Second, different perspectives, objectives and/or identified risks may not be of equal importance. In future work, guiding principles for weighing different perspectives should be developed. Third, the boundary object of a multi-stakeholder workshop, in our case the timeline, steers the discussion in the workshop. In future research, developing guidelines for preparing the timeline could help avoiding too directive descriptions. Fourth, in our workshops, a number of well-known tradeoffs did not surface (e.g., data-subject/user control versus central/system control, prevention versus mitigation, and technical versus procedural). This could be explained by a lack of expertise of the participants. Yet, the likelihood of overseeing important trade-offs can be lowered by providing more structure for discussing design trade-offs and providing design recommendations, for example by systematically holding design tradeoffs along various dimensions (e.g., data usage vs data privacy, data-subject control vs central control, prevention vs mitigation, and technical vs procedural).

In future work, we will take up the issues mentioned in this discussion and work on the subsequent steps of a privacy by (re)design approach. We foresee the need of developing a method that systematically translates the current workshop outcomes (i.e., design recommendations and constraints) into software requirements, e.g. by using bridging concepts such as value stories [9], turning privacy by design into privacy engineering. For giving more structure to the design thinking process, we foresee organizing the design discussions along three directions of security related aspects, users-being-in-control related aspects and data-minimalization related aspects. The outcome of these sessions should deliver a number of promising design options, which can be prototyped and improved in a number of iterations.

## Acknowledgements

The authors thank all the workshop participants for sharing their expertise and for their valuable contributions.

## References

1. Cavoukian, A. (2009). Foundational Principles-Privacy by design. URL: http://www. Privacybydesign. Ca/index. Php/about-pbd/7-foundamental-principles.
2. Choenni, S. & Leertouwer, E. (2010). Public safety mashups to support policy makers. In Proceedings of Int. Conf. on Electronic Government and the Information Systems Perspective (EGOVIS), Springer-Verlag, Germany, pp. 234-248.
3. Choenni, S., van Dijk, J. & Leeuw, F. (2010). Preserving privacy whilst integrating data: applied to criminal justice. Information Polity, Int. J. of Government & Democracy in the Information Age, 15(1-2), pp. 125-138, IOS Press.
4. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design-from policy to engineering.
5. Degeling, M., Lentzsch, C., Nolte, A., Herrmann, T., & Loser, K. U. (2016). Privacy by Socio-Technical Design: A Collaborative Approach for Privacy Friendly System Design. In Proc. of Collaboration and Internet Computing (CIC), pp. 502-505, IEEE.
6. European Commission (2016). Reform of EU data protection rules. Url: http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
7. Gharib, M., Salnitri, M., Paja, E., Giorgini, P., Mouratidis, H., Pavlidis, M., & Della Siria, A. (2016). Privacy requirements: Findings and lessons learned in developing a privacy platform. In Proc. International Requirements Engineering Conference, pp. 256-265.
8. Gürses, S., & del Alamo, J. M. (2016). Privacy Engineering: Shaping an Emerging Field of Research and Practice. In Proceedings of IEEE Security & Privacy, 14(2), 40-46.
9. Harbers, M., Detweiler, C., & Neerincx, M. A. (2015). Embedding stakeholder values in the requirements engineering process. In Proc. of Conference on Requirements Engineering: Foundation for Software Quality, pp. 318-332, Springer.
10. Hoepman, J. H. (2014). Privacy design strategies. In IFIP International Information Security Conference, pp. 446-459, Springer Berlin Heidelberg.

11. Lee, J.H., Kim, M.J., & Kim, S.W. (2015). A Study Customer Journey Map for User Experience Analysis of Information and Communications Technology Service, Springer International Publishing.
12. Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In International conference on Ubiquitous Computing, 273-291. Springer Berlin Heidelberg.
13. Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
14. Norton, D. W., & Pine, B. J. (2013). Using the customer journey to road test and refine the business model. Strategy & Leadership, 41(2), 12-17.
15. Notario, N., Crespo, A., Martín, Y. S., Del Alamo, J. M., Le Métayer, D., Antignac, T., Kung, A., Kroener, I. & Wright, D. (2015). PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. Proc. of Security and Privacy Workshops (SPW), 151-158, IEEE.
16. Schaar, P. (2010). Privacy by design. Identity in the Information Society, 3(2), 267-274.
17. Schikhof, Y., Mulder, I. & Choenni, S. (2010). Who will watch (over) me? Humane monitoring in dementia care, Int. J. of Human-Computer Studies, 68(6), pp. 410-422, Elsevier.
18. Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.
19. Spiekermann, S. (2012). The challenges of privacy by design. Communications of the ACM, 55(7), 38-40.
20. Spiekermann, S. & Cranor, L.F. (2009). Engineering privacy. IEEE Transactions on software engineering, 35(1), 67-82.
21. Star, S. L. (2010). This is not a boundary object: Reflections on the origin of a concept. Science, Technology, & Human Values, 35, 601–617.
22. Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, “translations” and boundary objects: Amateurs and professionals in Berkeley’s Museum of Vertebrate Zoology, 1907–39. Social Studies of Science, 19, 387–420.
23. Stark, L., King, J., Page, X., Lampinen, A., Vitak, J., Wisniewski, P. & Good, N. (2016). Bridging the gap between privacy by design and privacy in practice. Proc. of the CHI Conference on Human Factors in Computing Systems, pp. 3415-3422. ACM.