Towards Empowering the Human for Privacy Online

Kovila Coopamootoo

Towards Empowering the Human for Privacy Online

Kovila P.L. Coopamootoo

Newcastle University,
Newcastle upon Tyne, United Kingdom
{kovila.coopamootoo@newcastle.ac.uk

Abstract. While it is often claimed that users are more and more empowered via online technologies [4,16,17,31], the counterpart of privacy *dis*-empowerment is more than a suspicion [27]. From a human-computer interaction perspective, the following have previously been observed (1) users still fail to use privacy technologies on a large scale; (2) a number of human-computer interaction mismatches exist that impact the use of privacy technologies [32,22,5,15,6,1]; and (3) the user affect dimension of privacy is fear focused [14].
This paper reports on a experts' perspectives on empowering users towards privacy. We facilitated a workshop with $N = 12$ inter-disciplinary privacy experts to gather opinions and discuss empowering case-studies We reviewed literature focusing on the empowering versus dis-empowering impact of online technologies, and looked into psychological empowerment and usable privacy research.
The workshop participants pointed to a state of privacy *dis*-empowerment online, with human-computer interaction and business models as major themes. While it was clear that there is no clear-cut solution, supporting clearer communication channels was key to experts' mental models of empowered privacy online. They recommended enabling user understanding, not only for privacy threats but also in using privacy technologies and building user skills. To facilitate user interaction with complex secure communication tools, they suggested a transparency enhancing tool as a bridge between the user and encryption technology.
The outcome of the workshop and our review support the need for an approach that enables the human user, as well as their interactions and their active participation. For that we postulate the application of psychological empowerment [33]. To our knowledge, this paper provides the first known discussion among inter-disciplinary privacy experts on the topic of privacy *dis*-empowerment online, as well as the first categorisation of HCI mismatches impacting the use of privacy technologies.

1 Introduction

The internet is often seen as an empowering environment for consumers impacting personal, interpersonal, group and citizen-wide dynamics [4,16], and enabling consumer influence on product design, choice and decisions [17] and

co-creation [31]. However, the indiscriminate amount of information collected for this purpose is also seen to come with privacy-, identity- and empowerment-related issues [25]. In literature, the potential for privacy empowerment has been linked with awareness of threats [26], confidence in behaviour [7], and perception of control on distribution and use of personal information [23].

While Human-Computer Interaction (HCI) research in the area of Privacy has seen great progress under the flagship of Usable Privacy, enabling large-scale use of privacy enhancing technologies (PETs) still remains a challenge. Given the need for an approach that caters for the individual, their HCI interaction and their engagement online, we postulate the need for discussions on the concept and practice of 'empowering users online' from an HCI perspective. So far empowerment literature has focused on the workplace and has mainly come from organisational research and with a psychology angle [29,33].

Workshop. We facilitated a workshop entitled "Empowering the Human for Privacy Online" at IFIP Identity & Privacy Management Summerschool 2018, in Vienna. The workshop was organised with a presentation and an interactive component.

Contributions. To our knowledge, we provide the first known inter-disciplinary discussion on the topic of privacy empowerment. Our workshop points towards themes of HCI and skills, business models and trust, and choice and legal contexts. We also categorise and summarise HCI barriers to adoption of PETs under mismatches that need research attention.

2 Unpacking *Dis*-Empowerment Online

Definition. The Oxford dictionary defines empowerment as the
"authority or power given to someone to do something" which includes

"The process of becoming stronger and more confident, especially in controlling one's life and claiming one's rights".

2.1 Empowerment via Online Technology

Empowerment via the internet has been referred to as *e-empowerment* or *consumer empowerment*. Amichai et al. [4] proposed a conceptualization of ways the internet is used as an empowering tool, coining *e-empowerment*, and referring to four levels, namely personal, interpersonal, group and citizenship, while Fuglsang [16] showed how IT and the internet can be used in social experiments to enable active citizenship for seniors.

For their part, Fuller et al. [17] proposed the concept of consumer empowerment to describe consumers' perceived influence on product design and decision-making. They investigated perceived empowerment through internet-based co-creation activities. They observed that consumers engaging in co-creation felt more or less empowered, depending on the design of the virtual interaction tool, the related enjoyment, participants' task involvement as well as their creativity.

This is in line with Wathieu et al.'s suggestion that consumer empowerment is facilitated by consumers' ability to shape the composition of their choice set, where progress cues and information about other consumers are likely to enhance the experience [31]. Finally, Pires et al. argue that ICT is shifting market power from suppliers to consumers, with the ensuing consumer empowerment as unintended consequence of marketing [28].

2.2 Privacy Trade-Off

However, scholars have observed that mediated connections are more and more part of the infrastructure of people's lives in the internet age, where Pierson [27] argues that individuals' vulnerability is changing in relation to online consumer privacy when engaging with new network technologies, in particular those of mass self-communication. He posits greater external vulnerability for individuals induced by scalable systems, data replicability, persistence and searchability, and difficulties coping with internal vulnerability due to the increased complexity of the online environment.

In terms of trading privacy, O'Hara et al. discussed that while lifelogging, the indiscriminate collection of information concerning one's life and behaviour could be valuable in empowering the individual by providing a new locus for the construction of an online identity, it can also present some privacy, identity and empowerment-related issues [25].

In addition, literature also suggests that the potential for privacy empowerment includes awareness of threats [26], confidence in behaviour [7], and perception of control on distribution and use of personal information [23]. We find that perception of threats and risks [22] are often not accurate, confidence in behaviour is impacted by the fear dimension of privacy [8] and perception of control and use of personal information is often missing.

2.3 Why Privacy Empowerment?

Although privacy is implicit within human behaviour offline, in the online environment, it is mediated by technology and its human-computer interaction and thereby introduces a number of behavioural challenges not necessarily obvious and seamless to the human and to designers [9,12].

Bellotti & Sellen point to the problems of disembodiment (the actors are invisible in actions) and dissociation (actions are invisible to actors), both leading to visibility issues in privacy and security [5]. dePaula et al. examined the interaction problem of facilitating the understanding and effective use of PETs, by turning away from expression and enforcement and towards explication and engagement. These human-centred strategies towards enabling effective use of PETs, dubbed "user empowerment", have previously been raised by Wang & Kobsa [30], in particular with regards to empowering users in their privacy decisions.

3 Psychological Empowerment

We identify and review two main approaches of theorising about psychological empowerment in literature:(1) a cognitive model based on task assessments that impact intrinsic task motivation [29]; and (2) a nomological network including intrapersonal, interactional and behavioural components that also distinguish between empowerment processes and outcomes [33].

3.1 Cognitive Model

Thomas & Velthouse [29] defined *Psychological Empowerment* as increased intrinsic task motivation and proposed a theoretical model with four or cognitions or task assessments, namely *sense of impact*, *competence*, *meaningfulness*, and *choice* [29] that produce the motivation. The model captures individuals' interpretive processes via which they arrive at the task assessments. Psychological empowerment here focuses on intrinsic motivation and not on the managerial practices used to increase individuals' level of power.

Intrinsic Task Motivation involves positively valued experiences that individuals derive directly from a task. The core of the model therefore involves identifying these cognitions called task assessments (sense of impact, competence, meaningfulness, and choice [29]). These occur within the person and refer to the task itself, rather than the context of the task or rewards/punishments mediated by others. A task includes both **activities** and a **purpose**. The intrinsic value of goal or purpose accomplishment is produced by the articulation of a meaningful vision or mission.

3.2 Nomological Network

Zimmerman's nomological network extends the focus from intrapersonal aspects of the cognitive model to also include interactional and behavioural components [33].

In particular, the three components merge to form a picture of a person who believes that he or she has the capability to influence a context, understands how the system works in that context and engages in behaviours to exert control in that context. The intrapersonal aspect refers to how people think about themselves and includes domain-specific perceived control and self-efficacy, motivation to control, perceived competence, and mastery. The interactional aspect suggests that people are aware of their behavioural options, and includes critical awareness, understanding of causal agents, skill development, skill transfer and resource mobilisation. The behavioural aspect refers to actions taken to directly influence outcomes, including community involvement and participation and coping behaviours.

4 Usable Privacy

There has been roughly 19 years of research into approaches for aligning research in Human Computer Interaction with Computer Security, colloquially

under *usable privacy and security*. This body of research was established to investigate the usability issues that explain why established security and privacy mechanisms are barely used in practice.

State-of-the-art research in usable privacy has mainly spread across (1) usability of website privacy policy, platform for privacy preferences, and behavioural advertising, (2) policy specification and interaction, (3) mobile privacy and security, and (4) social-media privacy [18].

4.1 Human-Computer Mismatches

A key goal of Usable Privacy research has been to bridge the gap between human users and technology [18], where a number of HCI challenges have been identified that act as obstacles to adoption of privacy technologies. We refer to them as mismatches between the Human and the Computer system. These include:

- user needs vs structure of tools [32];
- user mental models vs conceptual models of tools [1];
- user perceptions of system risks vs actual risks [22];
- visible disclosure vs invisible threats [5];
- visible security and privacy action vs invisible impact [15];
- skills needed vs actual user skills [6].

In addition, recent work found that perceived anonymity and trust were strong determinants of behavioural intentions and actual use behaviour [19]. Yet another challenge to the adoption of privacy technologies, that relates to usable privacy, is the distinction in the cognitive and affective components of privacy and sharing attitudes [14], such that human-computer designs that induces cognitive aspects of close connections and joy affect may be incongruent with privacy appraisal online and subsequent protective behaviour.

4.2 Assisting the User

There have been endeavours to address certain mismatches in specific context. For example, for invisible privacy threats, Ackerman & Cranor [2] proposed privacy critics, that are semi-autonomous agents that can monitor users' actions, warn them about privacy threats and suggest suitable countermeasures.

To address skills development, Brodies et al. proposed allowing users to create privacy policies suitable to their skills and background and to visualise the policies they have created [6].

To aid user comprehension and assessment of actions, dePaula et al. deliberately proposed dynamic real time visualisation of system state [15] for integration of configuration and action (aid flexible and effective control), for peer to peer file sharing application.

In addition, various strategies have been proposed, in particular those designed to counter decision-making hurdles [3].

4.3 Towards Empowering the User

The first step to successfully protecting one's privacy online is effectively using privacy technologies. We however note that privacy technologies have not yet reached large scale nor mainstream use.

We perceive that human factors of privacy research has progressed within distinct components of the nomological network of psychological empowerment, and identified or addressed the intrapersonal, interactional or behavioural components separately. In addition, while the mismatches point to the interactional aspects of the network only, we position that to enable and sustain effective use of PETs on a large scale, addressing one mismatch at a time does not ensure use of PETs. For example supporting user understanding of privacy threats only and not building skills in how to use the PET is futile, as threat appraisal may accentuate fear and helplessness with regards to privacy and impact protection motivation [14,8].

We also postulate supporting users throughout their lifetime, that is, to not only investigate intrapersonal aspects of attitudes [14], concerns [21], affect [24], cogniton [12,11,13,10] and confidence in competency [8], but also (1) to investigate how the HCI enables the evaluation of risks in interaction, the gathering of skills and resources, and the awareness of the impact other agents online, as well as (2) to promote users' active contributions privacy protection online.

5 Workshop

We conduct a workshop at the *IFIP Summerschool in Privacy and Identity Management 2018*, in Vienna. The workshop was facilitated with both a presentation component and an interactive component.

5.1 Aim

To enable a discussion on privacy *(dis)*-empowerment online and how psychological empowerment may enable the use of privacy technologies.

5.2 Workshop Method

Procedure We first elicited participants' awareness of usable privacy, of supporting and enabling the user for privacy online, as well as their opinions on the state of *dis*-empowerment online. In particular we asked:

- What are your privacy research area/interests?
- What does Usable Privacy mean to you?
- What do you already know of ways to support and enable the user for privacy online?
- Do you think online users are currently empowered or dis-empowered wrt privacy? Why is this the case?
- What would empowered privacy online look like?

Second, we gave a presentation covering the history of usable privacy research and a review of state-of-the-art research. We introduced the concept of empowerment and made a case for privacy dis-empowerment online via literature and previous studies. We summarised the human-computer mismatches identified within Usable Privacy research.

Third we facilitated a discussion on ways to empower users online.

Fourth, we facilitated a longer discussion, with participants divided into 2 groups of 6 participants. The topics of the group exercise and discussion included to

- select a context between either the social web with transparency enhancing technologies (TETs) or anonymous communications which can use more traditional privacy enhancing technologies (PETs) or a combination of PETs and TETs;
- select PETs and TETs applicable to chosen context based on a list provided and add others if needed;
- discuss how an empowered privacy preserving and privacy enabling human-computer interaction may look like, and what are the environmental requirements;
- use the psychological empowerment models presented to create requirements, and identify empowered processes and outcomes.

Participants $N = 12$ participants joined the workshop, with a mix of male and female PhD researchers and academics. We did not elicit demographic data, as it is not relevant to the workshop aim. Instead we asked participants about their privacy research interests and their opinions on usable privacy and privacy *dis*-empowerment online (as described above).

Participants' research area and/or interests were spanned follows: we had 2 participants with connections to fairness (fairness in general and in relation to machine learning); 2 participants connected to privacy decision-making and risks; 3 participants either connected to the legal aspects of privacy or mapping legal requirements to human-computer requirements or into mechanisms implementation; 2 participants related to IoT and smarthome privacy; and the 3 others involved in areas of anonymity from a systems angle, trust building artificial intelligence and information security. These were gathered at the start of the workshop.

5.3 Opinions on Usable Privacy and Dis-/Empowerment Online

We provided a questionnaire at the beginning of the workshop with the questions as provided in Section 5.2 above. We report on the responses elicited which consitute participants' individual opinions. We refer to participant 1 as P1, participant 2 as P2 and so on till P12.

Usable Privacy Participants were queried on their perception of usable privacy.

According to 5 participants, usable privacy refers to *understandable methods of interacting with users*. They referred to communicating with users via ways that are not cognitively demanding (P2), enabling stakeholders to make decisions with full understanding of tradeoffs (P6), providing privacy technologies that are easy to understand and use (P7), as well as understandable data treatment and legal contexts (P11).

3 participants connected usable privacy with *ease of use*. These included P1 "interactive and easy to use", P7 "Privacy enhancing technologies (PETs) that are easy to use ... by users" and P8 "ease of navigation of settings and controlling these". In addition P10 referred to striking the best possible tradeiff between user experience and level of security.

2 participants referred to *efficiency* and/or *effectiveness* to explain usable privacy, with P1 "efficient way to exercise rights" and P9 "privacy that is effective and efficient for the user".

2 participants made a link between *the user and legal aspects*, with P5 "combine legal compliance with usability" and P11 "... explain legal contexts in a simpler way".

1 participant perceived usable privacy as related to *trust*, with P5 "making PETs trustworthy and deployable".

Ways to support and enable the user for privacy online We queried participants' awareness of ways to support and enable the user online.

3 participants responded with *human-computer interaction methods*, with P2 referring to "online nudges" and "feedback mechanisms", P7 refering to "transparency enhancing technologies can help users to understand the impact of using or not using PETs" and P5 "HCI challenges and requirements".

3 participants made a connection with *legal requirements of privacy*, with P2 "... providing opt-in choices (not opt-out)", P8 "currently most privacy is 'hidden' or non-existing although that is starting to change with GDPR" and P11 "GDPR and ... privacy protection code".

3 participants referred to *specific technological solutions*, such as P3 "VPN, proxy, TOR", P5 "PETs & TETs" and P10 "Auth protocols (e.g. SSO, OAuth, OpenID Connect) and their deployment in different technological scenarios (mobile, desktop, cloud), access control policies (specification and enforcement)".

In addition, 2 participants expressed a *lack of accessible methods*, with P9 "the existing ways are usually supporting and enabling users that are specially interested in their privacy and will put some considerate effort into maintaining it", or P8 "currently most privacy is 'hidden' or non-existing ... ".

Dis/Empowerment with respect to privacy online We asked participants if they felt users are currently empowered or dis-empowered with respect to their privacy online and to explain why they thought so. 11 participants responded while 1 did not provide an answer. The 11 pointed to users currently being dis-empowered with respect to their privacy online.

8 of the 11 participants pointed clearly towards dis-empowerment. 2 participants explained their verdict with a *lack of choice*, for example P11 said "... many times the user does not have a choice with respect to her privacy if she wants to use the online service". 2 participants pointed to the *complexity*, with P1 "... data processes are too complex" and P7 "they do/can not understand what people can do with lots of data". 3 participants supported their answer by referring to *business models*, with P2 "power dynamic favors business/state [who] favor profits", P3 "due to business benefits specially for large companies" and P10 "... due to business models ... and more in general companies [are] in the data monetization business". In addition, P6 explained linked dis-empowered online users with "mistrust and all its consequences".

3 of the 11 participants hinted towards *empowering possibilities*, with P5 explaining that "in theory there are many tools, but usability is indeed a problem", P9 making a distinction by the type of users, with "the lay users are currently feeling they have no power over their privacy anymore", and P12 hinting to a potential change in the future, with "generally dis-empowered maybe better with GDPR?".

Mental Models of empowered privacy online We elicited participants' mental model of empowered privacy online by asking them to describe how empowered privacy may look like.

6 participants' mental models included aspects of human-computer interaction, with 4 pointing towards clarity of communication and understandability, 2 pointing to intuitiveness, 1 pointing to having a choice to react and 2 towards control.

For *clarity of communication and understandability*, P1 depicted empowered privacy online with "provide adequate ... in clear and understandable manner", P2 referred to "clear un-conditional controls, clear online communication", P7 offered "users understand problems with respect to online privacy and have a choice, can re-act" and P3 "I can decide what data of mine to be shared in a more intuitive and straight-forward way".

For *intuitiveness*, P5 listed "intuitive, privacy by default, adapting to user needs" and P3 responded as above.

Choice was mentioned by P7 as above, while *control* was elicited from P2's response as above and P8 "ease of navigation of settings and controlling these".

In addition, 5 could not provide a response with P4, P9 and P11 not responding and P10 expressing "hard question, difficult to answer because of many contradicting interests from stakeholders" and P12 "not sure".

5.4 Empowered Privacy Human-Computer Interaction

We facilitated a 20 minutes group discussion, where participants gathered in two groups of 6 each. They were guided by the questions in the fifth part of the procedure described in Section 5.2. We report on the two empowering design solutions created by the two groups. Group 1 selected an anonymous communications case-study whereas Group 2 selected a social web case-study.

Anonymous Communication Group 1 participants chose a mix of privacy and transparency enhancing technologies to facilitate anonymous communications, in particular AN.ON and Privacy Score. AN.ON [1] is an anonymity service that ensures anonymity/un-trace-ability of the users machine via a series of intermediaries on a network of mixes. "Instead of connecting directly to a webserver, users take a detour, connecting with encryption through several intermediaries, so-called Mixes. The sequence of linked mixes is called a Mix Cascade. Users can choose between different mix cascades. Since many users use these intermediaries at the same time, the internet connection of any one single user is hidden among the connections of all the other users. No one, not anyone from outside, not any of the other users, not even the provider of the intermediary service can determine which connection belongs to which user."

PrivacyScore [2] is a browser add-on that acts as an automated website scanner to investigate websites for security and privacy issues [20]. The beta version reports on whether the website is tracking the user or allowing others to do so, whether the webserver offers HTTPS connections and the security of their configurations, whether the website has obvious security flaws, and whether the mail servers of the website support state-of-the-art encryption.

Participants discussed their choice for anonymous communication to target users who "care about their privacy", and for users who "trust the tools [sic] and want to pay for them [sic]". They observed that with AN.ON, human-computer interaction is a concern, in particular for users on the network and that currently the service is for "users who [sic] understand privacy". They therefore proposed PrivacyScore as TET to enhance users' trust in efficacy of AN.ON and facilitate adoption. They proposed "Privacy by Default" because they assessed that AN.ON was "are quite technical". Hence having PrivacyScore as TET would "show that a privacy-enhancing technology is working", and support average skills users. They also added that the anonymous communication setup of AN.ON with PrivacyScore may not work (another word) in all environments such for an employee in a work context, therefore highlighting the question of how individuals' right to privacy apply in a work context.

Social Web Group 2 participants chose Google Dashboard [3] as transparency enhancing technology (TET) for the social web. The TET supports awareness of data collection by allowing users to see some of the personal data that Google stores about them, linking to settings where users can influence the storage and visibility of data. However, note that with Google logging all user activities, user behaviour prediction and manipulation is a privacy issue while hacking is a cyber security risk with potentially huge impact.

As empowered privacy HCI, participants explained the need for users to be informed. They mentioned (a) awareness of policies, (b) sign up for data uses

[1] https://anon.inf.tu-dresden.de/index_en.html
[2] https://privacyscore.org/
[3] https://myaccount.google.com/dashboard

information, (c) data portability: move from provider to provider, (d) what's going on: who's looking at their data, (e) wider implications of data storage.

They also spoke about choice on data use by others.

6 Discussion

The outcomes of the workshop depict the complexity of the problem of enabling effective use of PETs on a large scale.

6.1 HCI & Skills

Workshop participants expressed the importance of the human-computer interaction in meeting the users, such as through clarity of communication and understandability to aid decisions (P1, P2, P3), feedback mechanisms (P2) for visible impact and ease of use of PETs (P1, P7, P8). In addition, complexity of interaction with PETs were also explicitly pointed out (P2, P7) as well as the current need of specialist skills and effort if one were to use PETs (P9). As example, the in the case-study discussion, Group 1 participants offered facilitating interaction between users and anonymous communication technology via TETs.

Workshop participants stressed on the need for more user understanding throughout the workshop, well beyond just understanding the threats of data usage (P1, P7) but also understanding how to use PETs and ease of use (P7), as well as understanding of legal contexts (P11).

These link directly with the incongruency observed via the HCI mismatches of Section 4.1. While the set of HCI mismatches point to the hard problem of enabling privacy online and sustaining use of privacy technologies, we postulate that the HCI complexity and enabling the individual user can be met by the three components of the nomological network of psychological empowerment [33].

6.2 Choice & Legal Requirements

While participants pointed to a (perceived) lack of choice with regards to privacy if users wanted to use online services (P11), the skills challenge, and poor awareness of resources can also be thought to contribute to a lack of choice. In addition, the intrapersonal aspect of psychological empowerment of confidence in competency or skills also constitute an impact on privacy motivation [8] and therefore a lack of choice.

Participants also postulated that enabling and supporting user privacy online requires provision of legal requirements, where there was hope that there would be more visible privacy solutions with the GDPR (P8, P9).

6.3 Business Models & Mistrust

Similar to previous research pointing to a general culture of fear with regards to privacy online, mainly associated with mistrusting the actions of businesses and

governments [14], workshop participants pointed to power dynamics favoring state and business profits (P2), benefits for large companies (P3) and business models based on data monetisation (P10) and mistrust (P6).

The power balance could be shifted if PETs design addressed the HCI mismatches for example, via better congruency with user needs, skills development, better perception of risks. On their part, participants postulated the need to make PETs more trustworthy and deployable (P5), as well as giving users a share of the profits (P6).

7 Conclusion

While it was clear from workshop participants that there currently exists a problem of privacy *dis*-empowerment online, there were no obvious solution on how to tackle the problem. There was a clear reliance on bridging the gap between users and complex privacy technologies via enhanced human-computer interaction. While power dynamics emerging from business models of data monetisation was found to be a major hassle, there was a sense of hope with the advent of the GDPR.

By enabling a discussion among inter-disciplinary privacy experts on the topic of privacy *dis*-empowerment online, as well as providing the first categorisation summary of HCI mismatches impacting the use of privacy technologies, this paper highlights avenues for future investigations in the area of human factors of privacy. For instance, investigating aspects of HCI that promote privacy empowerment as detailed in this paper and finding ways to promote large scale adoption of privacy technologies.

References

1. R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. Obstacles to the adoption of secure communication tools. In *Security and Privacy (SP), 2017 IEEE Symposium on*, pages 137–153. IEEE, 2017.
2. M. S. Ackerman, L. F. Cranor, and J. Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce*, pages 1–8. ACM, 1999.
3. A. Acquisti and al. Nudges for privacy and security: Understanding and assisting users' choices online. 2017.
4. Y. Amichai-Hamburger, K. Y. McKenna, and S.-A. Tal. E-empowerment: Empowerment by the internet. *Computers in Human Behavior*, 24(5):1776–1789, 2008.
5. V. Bellotti and A. Sellen. Design for privacy in ubiquitous computing environments. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93*, pages 77–92. Springer, 1993.
6. C. Brodie, C.-M. Karat, J. Karat, and J. Feng. Usable security and privacy: a case study of developing privacy management tools. In *Proceedings of the 2005 symposium on Usable privacy and security*, pages 35–43. ACM, 2005.
7. L. Church, J. Anderson, J. Bonneau, and F. Stajano. Privacy stories: confidence in privacy behaviors through end user programming. In *SOUPS*, 2009.

8. K. P. Coopamootoo. Work in progress: Fearful users' privacy intentions - an empirical investigation. In *7th International Workshop on Socio-Technical Aspects in Security and Trust*. ACM, New York, 2017.
9. K. P. Coopamootoo and D. Ashenden. Designing usable online privacy mechanisms: What can we learn from real world behaviour? In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, pages 311–324. Springer, 2010.
10. K. P. Coopamootoo and T. Groß. Mental models: An approach to identify privacy concern and behavior. At SOUPS 2014 workshop on Privacy Personas and Segmentation, 2014.
11. K. P. Coopamootoo and T. Groß. Cognitive effort in privacy decision-making vs. 3 x 4: Evaluation of a pilot experiment design. In LASER 2014 Workshop, 2014.
12. K. P. Coopamootoo and T. Groß. Mental models for usable privacy: A position paper. In T.Tryfonas and I.Askoxylakis, editors, *HAS 2014*, volume 8533 of *LNCS*, pages 410–421. Springer Int, 2014.
13. K. P. Coopamootoo and T. Groß. Mental models of online privacy: Structural properties and cognitive maps. In *British HCI 2014*, 2014.
14. K. P. Coopamootoo and T. Groß. Why privacy is all but forgotten - an empirical study of privacy and sharing attitude. *Proceedings on Privacy Enhancing Technologies*, 4:39–60, 2017.
15. R. De Paula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. F. Redmiles, J. Ren, J. A. Rode, and R. Silva Filho. In the eye of the beholder: a visualization-based approach to information system security. *International Journal of Human-Computer Studies*, 63(1-2):5–24, 2005.
16. L. Fuglsang. It and senior citizens: Using the internet for empowering active citizenship. *Science, Technology, & Human Values*, 30(4):468–495, 2005.
17. J. Füller, H. Mühlbacher, K. Matzler, and G. Jawecki. Consumer empowerment through internet-based co-creation. *Journal of Management Information Systems*, 26(3):71–102, 2009.
18. S. Garfinkel and H. R. Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.
19. D. Harborth and S. Pape. Examining technology use factors of privacy-enhancing technologies: The role of perceived anonymity and trust. 2018.
20. M. Maass, P. Wichmann, H. Pridöhl, and D. Herrmann. Privacyscore: improving privacy and security via crowd-sourced benchmarks of websites. In *Annual Privacy Forum*, pages 178–191. Springer, 2017.
21. N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.
22. M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao. Stealing pins via mobile sensors: actual risk versus user perception. *International Journal of Information Security*, 17(3):291–313, 2018.
23. V. Midha. Impact of consumer empowerment on online trust: An examination across genders. *Decision Support Systems*, 54(1):198–205, 2012.
24. U. Nwadike, T. Groß, and K. P. Coopamootoo. Evaluating users' affect states: towards a study on privacy concerns. In *IFIP International Summer School on Privacy and Identity Management*, pages 248–262. Springer, 2016.
25. K. O'Hara, M. M. Tuffield, and N. Shadbolt. Lifelogging: Privacy and empowerment with memories for life. *Identity in the Information Society*, 1(1):155–172, 2008.

26. N. Olivero and P. Lunt. Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, 25(2):243–262, 2004.
27. J. Pierson. Online privacy in social media: A conceptual exploration of empowerment and vulnerability. 2012.
28. G. D. Pires, J. Stanton, and P. Rita. The internet, consumer empowerment and marketing strategies. *European Journal of Marketing*, 40(9/10):936–949, 2006.
29. K. W. Thomas and B. A. Velthouse. Cognitive elements of empowerment: An interpretive model of intrinsic task motivation. *Academy of management review*, 15(4):666–681, 1990.
30. Y. Wang and A. Kobsa. Privacy-enhancing technologies. In *Handbook of research on social and organizational liabilities in information security*, pages 203–227. IGI Global, 2009.
31. L. Wathieu, L. Brenner, Z. Carmon, A. Chattopadhyay, K. Wertenbroch, A. Drolet, J. Gourville, A. Muthukrishnan, N. Novemsky, R. K. Ratner, et al. Consumer control and empowerment: A primer. *Marketing Letters*, 13(3):297–305, 2002.
32. A. Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX Security Symposium*, volume 348, 1999.
33. M. A. Zimmerman. Psychological empowerment: Issues and illustrations. *American journal of community psychology*, 23(5):581–599, 1995.