


EDITORIAL



## A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead

Christian Reuter <sup>a</sup>, Luigi Lo Iacono<sup>b</sup> and Alexander Benlian<sup>c</sup>

<sup>a</sup>Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt, Darmstadt, Hessen, Germany; <sup>b</sup>Cyber Security and Privacy, Hochschule Bonn-Rhein-Sieg University of Applied Sciences, Sankt Augustin Germany; <sup>c</sup>Information Systems & E-Services, Technical University of Darmstadt, Darmstadt, Germany

### ABSTRACT

In the last decades, research has shown that both technical solutions and user perceptions are important to improve security and privacy in the digital realm. The field of 'usable security' already started to emerge in the mid-90s, primarily focussed on password and email security. Later on, the research field of "usable security and privacy" evolved and broadened the aim to design concepts and tools to assist users in enhancing their behaviour with regard to both privacy and security. Nevertheless, many user interventions are not as effective as desired. Because of highly diverse usage contexts, leading to different privacy and security requirements and not always to one-size-fits-all approaches, *tailorability* is necessary to address this issue. Furthermore, *transparency* is a crucial requirement, as providing comprehensible information may counter reactance towards security interventions. This article first provides a brief history of the research field in its first quarter-century and then highlights research on the transparency and tailorability of user interventions. Based on this, this article then presents six contributions with regard to (1) privacy concerns in times of COVID-19, (2) authentication on mobile devices, (3) GDPR-compliant data management, (4) privacy notices on websites, (5) data disclosure scenarios in agriculture, as well as (6) rights under data protection law and the concrete process should data subjects want to claim those rights. This article concludes with several research directions on user-centred transparency and tailorability.

### KEYWORDS

Usable security; usable privacy; transparency-enhancing technologies; intervention mechanisms; security and privacy literacy



### CCS Concepts:

- Security and privacy → Social aspects of security and privacy; Usability in security and privacy;
- Human-centred computing → Empirical studies in visualisation.

### 1. Introduction

Addressing end users' needs and capabilities adequately is a decisive factor when aiming to enhance security and privacy. Hence, researchers stress the importance of finding effective ways to assist users to make informed and adequate security and privacy decisions, and act accordingly. While most transparency-enhancing technologies and user intervention mechanisms are one-size-fits-all approaches, they are often not as effective as they should be from a user perspective. Thus, context-aware, and user-centred

solutions constitute a current trend to increase transparency and intervention effectiveness. Considering variations in security and privacy behaviour is critical, both in terms of different contexts and different groups of end users. There are different types of transparency views and intervention mechanisms, ranging from default configurations to providing end users with risk information. When forcing people's decisions towards a desired outcome without being neither clear nor convenient, people tend to find workarounds. For example, if users are forced to adopt higher online security, it may reduce their willingness to follow the advice when the benefits are not clear and the desired behaviour appears to be a disproportionately big effort. In that case, users often choose convenience over security. To avoid this, it is necessary to provide both the required and desired information to users in a way that aligns with their internal representations

**CONTACT** Christian Reuter  reuter@peasec.tu-darmstadt.de  Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt, Pankratiusstraße 2, 64289 Darmstadt, Hessen, Germany

This article has been republished with minor changes. These changes do not impact the academic content of the article.

© 2022 Informa UK Limited, trading as Taylor & Francis Group

– so-called mental models. Once users understand the mechanisms they are confronted with, they could make better decisions.

This article aims to address the research on transparent and tailorable interventions for usable security and privacy. For this purpose, at first an overview about the history of the research field and current challenges is provided in Chapter 2. Subsequently, in Chapter 3 the topic of transparency and tailorability of user interventions is addressed with reference to several specific application fields. In Section 4, six articles on current research are presented, which partially address the challenges discussed in the previous sections with regards to different contexts and user groups. Building upon this, in Section 5, the road ahead in usable security and privacy research and corresponding areas for future research are outlined and a conclusion is given.

## 2. A brief history of usable security and privacy

The opinion that users are the weakest link in cyber security is widespread. This view is fuelled by security incidents in which human error is found to be the unintended cause of missing or malfunctioning means of protection. In doing so, users only act within the boundaries of the environment provided. Furthermore, it is important to recognise that users interacting with computerised systems aim to fulfil their primary task, which is never to take protective measures. Thus, if means of protection hinder users in completing their primary task, they will intentionally avoid, override, or circumvent them, thus rendering them *ad absurdum*. In contrast, a critical view of the lack of system-side support and usability that triggers unintentional and intentional misuse is often not common in cyber security. However, this perspective is urgently needed, as research has proven (Adams and Angela Sasse 1999). Security and user-friendliness are not mutually exclusive quality features of a system, as is commonly assumed (Sasse et al. 2016). Human factors are therefore very important for security and privacy (Sasse and Rashid 2021).

### 2.1. The beginnings and the launch of ‘usable security’ and ‘usable privacy’

The groundbreaking works ‘User-Centered Security’ (Zurko and Simon 1996), ‘Users Are Not the Enemy’ (Adams and Angela Sasse 1999), and ‘Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0’ (Whitten and Doug Tygar 1999), which manifest the beginning of the research field of usable security around 1996, already convey a different paradigm through their

titles. They address the problem of how systems can support users in the reliable use of security mechanisms. Researchers put user perceptions, expectations, and capabilities at the centre of development considerations to enable users to become a strong link in a security system or even ‘the strongest link’, which is a paradigm shift.

Interestingly, the first thoughts in the direction of explicitly considering users in the design and development of security mechanisms were expressed much earlier. When the Dutch-born linguist and cryptographer Auguste Kerckhoffs published two journal articles on ‘La Cryptographie Militaire’ in 1883, he listed six principles for the development of military ciphers in the first article (Kerckhoffs 1883). What is known as the ‘Kerckhoffs’ principle’ is an excerpt from the six principles according to which a cryptosystem should be secure even if everything about the system, except the key, is publicly known. A less known fact is that in his sixth principle, he states that ‘given the circumstances in which such a system is applied, it must be easy to use and must neither stress the mind nor require the knowledge of a long series of rules’. It took more than 100 years for this principle to be rediscovered in computer security research on usable password security. The same is true for the security principles proposed by Saltzer and Schroeder (1975). Amongst ‘Psychological Acceptability’, two aspects are important to achieve end users’ acceptance of protection measures: (i) user interfaces that promote usability, and (ii) congruence between internal system mechanisms and users’ mental models. The latter is indispensable and at the same time difficult to achieve, as there is often no self-evident mental representation for the complex concepts of technical protection mechanisms, as they do not exist in the physical world and therefore cannot be experienced, such as key pairs or public key certificates.

When the new research field of usable security was launched in the mid-90s (Zurko and Simon 1996), it focussed primarily on passwords and email security from the end user perspective, building on the pioneering work of Adams and Angela Sasse (1999), and Whitten and Doug Tygar (1999). The field gained further traction through special workshops, which over the years have become established venues that are now an integral part of the scientific discourse. In 2003, at the ACM Conference on Human Factors in Computing Systems (CHI), a first workshop was held that paired user studies with security analyses. Due to the success of the CHI workshop, a larger Workshop on Usable Privacy and Security Software (WUPSS) was organised in 2004. This led to the Symposium on Usable Privacy and Security (SOUPS) in 2005, which has been held annually since. Today, usable security is a recognised

field that is part of almost every human-computer-interaction (HCI) and security-related scientific venue.

A similar development path and timeline can be seen for the research area of usable privacy. Initial work focussing on the intersection of HCI and privacy research appeared around 1979 and focussed mainly on the employment context (Ganster et al. 1979). With the commercialisation of the World Wide Web and the subsequent development into Web 2.0, the focus shifted to the private and online privacy context as websites began to track and analyse their users' behaviour (Cranor and Garfinkel 2005). At that time, technical approaches such as the Platform for Privacy Preferences Project (P3P) (Hochheiser 2002) were proposed to increase user trust in the Web. P3P is a machine-readable language that can be used to manage data usage policies. When a user visits a website, P3P compares what personal information the user wants to share according to their policy and what information the website wants to receive according to its policy. If the two policies do not match, P3P informs the user and asks them if they are willing to visit the website and risk disclosing more personal information. P3P formed the basis for more than a decade of research to find out whether the standard could actually be used by consumers to express their privacy choices. Since the beginnings of usable privacy coincided with usable security, the workshops and conferences that emerged around 2005 also focussed on usable privacy. However, usable privacy-specific events have also emerged, most notably workshops at the annual Privacy Enhancing Technologies Symposium (PETS) since 2008.

## **2.2. The evolution of the 'usable security and privacy' field**

From this initial and still very narrowly focussed research, the field of usable security and privacy has evolved over the last decade to encompass broader topics, and also the variety of stakeholders has increased in recent years. For example, researchers have begun to address security and privacy issues of employees (Nicholson, Coventry, and Briggs 2018; Tolsdorf, Reinhardt, and Iacono 2022; Tolsdorf et al. 2021), sex workers (McDonald et al. 2021), people with disabilities (Hayes et al. 2019; Marne, Nasrullah, and Wright 2017; Napoli et al. 2021), refugees (Steinbrink et al. 2021), youth (Brodsky et al. 2021; Cranor et al. 2014; Lastdrager et al. 2017), and seniors (Frik et al. 2019). Topics that have recently been focussed on in academia still include passwords and passwordless authentication with all conceivable approaches, devices, and contexts of use

(Farke et al. 2020; Gerlitz, Häring, and Smith 2021; Golla et al. 2021; Kunke et al. 2021; Lassak et al. 2021; Lyastani et al. 2020; Owens et al. 2021; Tan et al. 2020; Ulqinaku et al. 2021; Wiefeling, Dürmuth, and Iacono 2020; Wiefeling et al. 2020). In the last years, usable security and privacy research also started to include developers and software engineers as a target user group (Gorski et al. 2021; Naiakshina et al. 2019; Plöger, Meier, and Smith 2021; Roth et al. 2021; Tahaei, Vaniea, and Saphra 2020). This was due to the fact that many security incidents in practice result from insecure code (Green and Smith 2016). Therefore, providing usable development support and tools is considered in research as a solution to achieve more secure code. This branch of research is also known as Developer-Centered Security (DCS). Furthermore, research has also focussed on email security. After numerous works on usable email encryption (Ruoti and Seamons 2019), phishing is back in the spotlight (Althobaiti, Meng, and Vaniea 2021; Hasegawa et al. 2021; Wash, Nthala, and Rader 2021), as it has become a serious threat in the era of working from home during the COVID-19 pandemic. For other technological developments that the COVID-19 pandemic has accelerated, such as remote communication or digital vaccination certificates, attitudes and preferences are also being explored (Emami-Naeini et al. 2021; Kowalewski et al. 2022). In addition, research continues to explore users' overall understanding, attitudes, and needs toward information technologies. Be it mental models about the IoT (Zheng et al. 2018; Zimmermann et al. 2018), encryption mechanisms (Krombholz et al. 2019; Wu and Zappala 2018), the internet (Brodsky et al. 2021; Kang et al. 2015), or conceptualisations of privacy in an information society (Oates et al. 2018; Tolsdorf et al. 2021).

Over the past two decades, the usable privacy research community, in particular, has made great efforts to explore people's attitudes, privacy concerns, and disclosure behaviours with the aim of understanding 'privacy'. This process has long been characterised by finding and studying a 'privacy paradox' (Brown 2001; Norberg, Horne, and Horne 2007), followed by numerous approaches with the aim to explain and resolve it (Gerber, Gerber, and Volkamer 2018) and Kokolakis (2017). The efforts culminated in numerous theories that have helped us to come closer to understanding privacy (Knijnenburg et al. 2022). However, the efforts made have also shown that the deeper one explores the question of what 'privacy' is, the more diverse and multifaceted it appears.

Furthermore, the implementation of new privacy legislation has had a major impact on the usable privacy domain. On the one hand, the problem arose that online

users were flooded with cookie banners that, contrary to the principle of privacy by design, exploited dark patterns to secure users' consent for the purpose of processing personal data (Machuletz and Böhme 2020). At the same time, numerous ideas were developed to address the transparency requirements of modern data protection laws – either by further developing existing transparency tools (Murmman and Fischer-Hübner 2017) or by developing new ideas. Approaches have been developed to make privacy statements easier to understand, for example with the help of privacy icons (Habib et al. 2021), comics (Knijnenburg and Cherry 2016; Tabassum et al. 2018), graph-based visualisations (Angulo et al. 2015; Schufrin et al. 2021), ordinary privacy nutrition labels (Emami-Naeini et al. 2022; Kelley et al. 2010; Railean and Reinhardt 2018), and hybrid labels that include privacy settings in the visualisation (Reinhardt, Borchard, and Hurtienne 2021). At the same time, research was carried out into how people's right to access their personal data can be designed and visualised in a meaningful way (Alizadeh et al. 2020; Veys et al. 2021), and made easily accessible via privacy dashboards (Bier, Kühne, and Beyerer 2016).

### 3. Transparency and tailorability of user interventions

While most user interventions – as external measures to encourage users' secure behaviour (e.g. by providing end users with risk information) – are one-size-fits-all approaches (giving the same intervention to all user groups), they are often not as effective as desired. Accordingly, already in Garfinkel and Lipford (2014) mentioned *personalisation* as one of the trends for the next decade.

The main reason for this is that users and use contexts are highly diverse and thus lead to individual intrinsic privacy and security requirements. Furthermore, a lack of transparent information may lead to reactance, which means that users tend to behave contrary to the proposed pattern. Providing comprehensible information may counter that reactance, also for security and privacy. Therefore, we would like to elaborate on the transparency and tailorability of user interventions.

#### 3.1. Transparency of user interventions

A major challenge is the *transparency* of user interventions in the areas of privacy and security. Often, cyber security and privacy measures are difficult for the average user to understand. Providing *transparency* in relevant aspects in cyber security and privacy is therefore critical to help users better understand interventions.

This has already been applied in various contexts, e.g. end user key verification services (Melara et al. 2015), and processing of personal data (Pulls, Peeters, and Wouters 2013). There are various measures to create transparency that take different levels into account. For example, transparency can be improved by visualising relevant information or by providing visual feedback on decisions in critical situations to respond to visual perception, as it provides 'the highest bandwidth channel from computer to the human' (Ware 2012, 2). Therefore, transparency should be considered an important part of the intervention design.

Transparency can be facilitated by presenting relevant information in a disaggregated way instead of showing an aggregated output. *Disaggregation* can be achieved, for instance, by applying suitable visualisation techniques such as radar charts (also known as star coordinate, spider chart, or polar chart) or parallel coordinates that allow multiple dimensions to be displayed at once without overwhelming end users. These visualisation techniques are considered an effective way for displaying information in a variety of contexts (Kwon and Lee 2016).

Concerning the visualisation of information, users' preferences regarding transparency are diverse. While for some users it is sufficient to only see an aggregated output of a calculation, others will not trust the output unless they can comprehend how it was generated. For the latter, algorithmic transparency is essential. There are mainly two different approaches to algorithms: *black-box* and *white-box* approaches (Cheng et al. 2019). In a black-box approach, the user can observe the input and the output but not what happens in between. As a result, this may lead to reactance for those who want to know how information is processed. *Reactance* can be seen as the result of the Backfire Effect (Nyhan and Reifler 2010), as an emotional reaction to paternalism or persuasion, leading users to tend to behave contrary to the proposed pattern. The advantage, however, of black-box approaches is that they are less likely to cause information overload. In contrast, white-box approaches enable the user to understand how the output was generated by making the underlying basis for output generation transparent to the user. This can be beneficial especially for individuals that are otherwise likely to feel reactance or mistrust (Hartwig and Reuter 2019). Such so-called explainable algorithms have become a highly relevant field of research, for instance, to understand how decisions in health and finance are made by machine learning techniques (Abdul et al. 2018; Cheng et al. 2019).

Currently, the majority of user intervention mechanisms are based on uni-dimensional visualisations of aggregated information. For instance, password metres



usually show aggregated results of metrics using colour code. However, these interventions only tell if a password is weak, but not why this is the case. This shows that they are black-box-based and, hence, do not let users know what to do to improve their passwords. In this way, the visualisation of a more comprehensive collection of information rather than just aggregated results can assist users in making informed security and privacy decisions (Ur et al. 2016). Here, white-box approaches can facilitate an understanding of why a certain output was generated by showing multiple dimensions in one visualisation. Thus, it is not only transparent to the users on which dimensions the calculation of password strength is based on, but also what is required to improve the password. Studies have emphasised that transparency and user control in the areas of security and privacy do not necessarily lead to users making consistent decisions (Acquisti, Adjerid, and Brandimarte 2013) and, thus, have to be implemented with caution. Therefore, it is crucial to further investigate the circumstances in which transparent interventions are more effective for specific user groups, than aggregated information (Hartwig and Reuter 2021). Providing transparent and comprehensible information to end users is highly relevant also with regard to other contexts such as fake news interventions, where findings regarding user interventions can benefit from each other when comparing the contexts of fake news and cyber security (Kaiser et al. 2021).

### 3.2. Tailorability of user interventions

A second major challenge is the *tailorability* of user interventions for privacy and security. A user-centred approach is generally recommended when trying to improve users' privacy and security (Franz et al. 2021; Stransky et al. 2021). However, many security and privacy systems are designed for the average user (Egelman and Peer 2015). Accordingly, compliance is limited to certain end users while others do not necessarily benefit. Furthermore, it has been shown that compliance is likely to improve when it is designed for an individual (Egelman and Peer 2015). To address this problem, a recent trend for user interventions is *personalisation*. Several researchers point out the advantages of using personalised interventions according to user traits instead of one-size-fits-all interventions (Knijnenburg 2017; Egelman and Peer 2015; Peer et al. 2019; Renaud et al. 2017; Jeske, Coventry, and Briggs 2014). For instance, some researchers argue that using tailored nudges can support users in making better privacy decisions (Knijnenburg 2017). A nudge is 'any aspect of the choice architecture that alters

people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives' (Thaler and Sunstein 2009, 6). To provide individuals with the subjectively most effective intervention, distinct *user groups* need to be identified. In this regard, there are various approaches to segment users. For example, different clusters of users have been identified: 'Fundamentalists, Lazy Experts, Technicians, Amateurs and the Marginally Concerned' (Dupree et al. 2016, 5228). Further, segmenting users according to their decision-making styles and risk-taking attitudes via short and established psychometric tests is suggested to predict privacy and security behaviour and accordingly show the best fitting user interventions (Egelman and Peer 2015). This idea was also followed up by conducting online experiments (Egelman, Harbach, and Peer 2016). The results suggest that the Security behaviour Intentions Scale (SeBIS) indeed predicts certain computer security behaviours. While several studies show promising advantages of personalised user interventions, only a few have implemented the concept within a cyber security context. The context of manual password creation remains relevant in usable security, as passwords continue to be the first choice for user authentication, despite various strong alternatives and end users' struggle to follow password requirements to create usable and strong passwords. Peer et al. (2019) tested people's decision-making styles to personalise interventions for stronger passwords in two online experiments. They argue that choosing a user intervention from a pool of multiple existing interventions could be more effective than showing the same to everyone (Peer et al. 2019). Applying five frequently used nudges (e.g. feedback on how long it takes to crack the password) according to the decision-making style of a person, the study found that decision-making styles can indeed indicate which user intervention is likely to be most effective. They achieved stronger passwords with personalisation than with one-size-fits-all interventions (Peer et al. 2019). Another study investigated the effectiveness of interventions depending on user characteristics, such as impulse control when selecting a public wireless network, by asking students in a role-playing game to select a network given a specific intervention (Jeske, Coventry, and Briggs 2014). Here, user differences were found to indeed play a role in security decision-making. Yet another study examined whether white-box-based multidimensional visualisations have a positive effect on password creation. Here, Hartwig and Reuter (2021) found that the intervention was particularly appreciated by players of role-playing games, giving reasons for further investigations.

In addition to personalisation based on specific user characteristics, customised needs can also be met by providing *control opportunities* for users themselves. These represent an alternative to the previously elaborated personalisation approaches. Here, it has been empirically shown that individuals who perceive more control over their privacy sometimes reveal more sensitive information than those who perceive less control over their privacy (Brandimarte, Acquisti, and Loewenstein 2013; Gerber, Gerber, and Volkamer 2018), also known as privacy paradox. Nevertheless, providing good and usable control opportunities to enable personalised user interventions might generally be a promising path to pursue, as long as possible caveats are taken into account.

### 3.3. Possible application fields: phishing and privacy protection

For illustration purposes, we highlight two contemporary and highly relevant application fields for user-centred interventions and transparency mechanisms in security and privacy, namely phishing and interdependent privacy protection.

*Phishing* is a frequently employed cyber attack to get hold of users' sensitive information, such as login details or bank account numbers. The consequences of a successful attack can reach from individual personal losses or compromised accounts, to complete organisations, or networks being infected with malware, often combined with ransom demands. It is crucial to keep in mind that phishing attacks do not primarily target hardware or software vulnerabilities, but rather the user – the human factor within the socio-technical system. While there are several tools and approaches that aim to identify malicious content automatically (see e.g. Tian et al. 2018; Verma and Dyer 2015), the increasingly sophisticated and personalised nature of phishing attacks makes it hard for algorithms to detect and block phishing emails, websites, or malicious software. This leaves a large amount of responsibility to the user, so that user-centred interventions and transparency mechanisms play a key role in helping users to protect themselves.

Key questions to answer in this area are amongst others: (1) Which phishing attack vector (e.g. email, URL, website, malware) does the intervention address? (2) When (pre-decision, during decision, post-decision) does the intervention take place? (3) Does the intervention require user interaction? Research and practice have developed a number of user-oriented interventions against phishing attacks to address these questions. Among those are education and training approaches

(e.g. Canova et al. 2015; Kumaraguru et al. 2009), where users develop knowledge and skills that they can apply to real-world phishing attempts. Moreover, awareness-raising measures or design considerations (e.g. Marforio et al. 2016; Nicholson, Coventry, and Briggs 2017; Petelka, Zou, and Schaub 2019) aim to guide users towards secure online behaviour in situ. More recent research has developed a taxonomy of user-oriented phishing interventions (Franz et al. 2021) including educational interventions (e.g. Text-based, video-based, or in-class education), training (e.g. serious games, embedded training, mindfulness-based training), awareness-raising warnings (e.g. interactive warnings, passive warnings), and anti-phishing designs (e.g. colour coding, highlighting, customising), which users need to navigate through when being pushed towards secure online behaviour.

*Interdependent privacy protection* is a second important and salient application field for user-centred interventions and transparency mechanisms. In online contexts such as social media or e-commerce, privacy losses or violations are 'not always trivial to perceive and decide upon, neither for users nor for regulators' (Garcia 2017, 1). Privacy is a highly complex affair, with one crucial factor being the various types of inherent connections among individuals and their personal data (Biczók et al. 2021; Spiekermann et al. 2022). Take the example of LinkedIn, a professional social network, that relies on users' opinions on their contacts' skills (e.g. 'Help us identify Anna Smith's top skill') in order to offer and sell personalised job opportunities. Another example: When a user installs a third-party application on Facebook, the application might collect not only the user's personal data, but also that of their friends. While sharing data might be advantageous for (some) consumers or users, too much transparency could at the same time pose risks to other actors, e.g. in terms of privacy or a business's market position (Linsner et al. 2021). Depending on how great the risk is perceived, the respective digital behaviour changes. This is particularly relevant with regard to vulnerable social groups, such as refugees (Steinbrink et al. 2021). These examples demonstrate that a person's privacy is not only affected by their own decisions, but also by those of other individuals or organisations, which we refer to as interdependent privacy, where 'personal information is shared without the knowledge and/or direct consent of the data subject' (Biczók et al. 2021). Presently, the issue of interdependent privacy displays a regulatory loophole even for the European Union (EU) General Data Protection Regulation (GDPR) (Kamleitner and Sotoudeh 2019), which confines itself to a dyadic understanding of privacy (e.g. between a company

and a consumer), while leaving room for grey areas with regard to interdependent privacy infringements.

Key questions to answer in this research field are for example: (1) What are the underlying mechanisms of users' decision-making when protecting or disclosing others' personal information online? (2) To what extent can interdependent privacy infringements be reduced via design choices, such as transparency mechanisms? Although previous research on how to safeguard against interdependent privacy is still scarce, the literature on digital nudging (Weinmann, Schneider, and vom Brocke 2016) might help to provide a solid foundation for adequate protection mechanisms: Popular mechanisms are, for example, default options, positioning, colour coding, reminding of the consequences, or enabling social comparison (e.g. Caraban et al. 2019; Schneider et al. 2020; Roethke et al. 2020). Regarding users' preferences towards the design of a privacy nudge, Schöbel et al. (2020) have found default mechanisms, presentation or framing (e.g. red colour for risk), as well as privacy-related information to be among users' most preferred privacy nudges. Kamleitner and Mitchell (2019) have suggested several interventions to improve interdependent privacy protection across stakeholders, e.g. requiring additional steps of decision control in the transfer process or a preview of the actual data which is about to be shared. These suggestions provide a valuable foundation for the design of nudges in an interdependent privacy context.

#### 4. Contributions to transparency and tailorability

In order to contribute to the state of the art in transparency and tailorability for usable security and privacy, we searched for authors that are willing to address current challenges with their research efforts. We received 13 submissions for this special issue. After two rounds of rigorous reviewing, six articles were accepted for publication. These are presented in the following.

The article '*Exploring people's perceptions and support for data-driven technology in times of COVID-19: the role of trust, risk, and privacy concerns*' by Brahim Zarouali, Joanna Strycharz, Natali Helberger, Claes de Vreese (Universiteit van Amsterdam) addresses societal responses to, as well as the democratic legitimacy of data-driven technological applications during the COVID-19 pandemic. In the struggle against the spread of the virus, containment and tracking strategies of many European governments included the collection and use of online data. In a national representative survey in the Netherlands, the authors investigated whether the general public supports state technologies that make

use of these data. The result in form of a typology revealed three different social groups, namely sceptical, carefree, and neutral respondents, which differed with regard to trust perceptions, risk beliefs, and privacy concerns. Besides clear correlations of the groups with demographic characteristics, different support levels regarding specific governmental digital solutions were also found.

The article '*User-centred Multimodal Authentication: Securing Handheld Mobile Devices using Gaze and Touch Input*' by Mohamed Khamis, Karola Marky, Andreas Bulling and Florian Alt (University of Glasgow & University of Stuttgart & Universität der Bundeswehr München) addresses multimodal authentication schemes for the secure use of mobile devices. Since mobile devices store a large amount of sensitive personal data and metadata, such as emails or photographs, the protection of this data by secure authentication is essential. The authors, however, note that such mobile devices are often only secured by so-called single-modal authentication schemes, which can easily be bypassed. Consequently, a multimodal authentication is proposed, where several potential attacks, namely shoulder surfing, smudge attacks, and thermal attacks, are considered at the same time. Moreover, guidelines for enhanced usability and security of user authentication on mobile devices are presented.

The article '*Data Cart – Designing a tool for the GDPR-compliant handling of personal data by employees*' by Jan Tolsdorf, Florian Dehling, and Luigi Lo Iacono (University of Applied Sciences Bonn-Rhein-Sieg) addresses the usability of data protection compliant personal data management tools. Here, the authors concentrate on the needs of employees who process sensitive personal data in their everyday job and therefore have to comply with strict data protection guidelines and laws. For this purpose, a tool was developed following a human-centred design approach to assist employees with data management and data protection compliance. By using the developed tool, employees felt more confident in dealing with sensitive personal data and had the impression that the tool would help them to improve their overall data protection awareness, reduce errors, and increase work efficiency. This builds a strong case for increased integrated implementation of Privacy by Design in digitalisation processes.

The article '*Transparency of privacy notices: The effect of the sequential context on comprehension*' by Mariavittoria Masotina and Anna Spagnolli (Università di Padova) addresses the connection between the understandability of privacy notices on websites and their sequential context. Privacy notices – for which website operators are required to obtain users' consent – are often not clearly understood, which is related to the

sequential context in which those notices are displayed. Three studies were conducted to test whether the comprehensibility of privacy notices was improved when users could link it to a certain action preceding the appearance of the notice, measuring participants' comprehension, perceived comprehension, and response. In the first two studies, the sequential connection with the action triggering the notice was either maintained or broken, and respective references to the triggering action were altered. In the third study, different sequential environments were investigated. The results indicate that the understandability of a privacy notice is significantly more enhanced by linking it to a previous action or service than by changing the content of the notice.

The article '*Supporting Users in Data Disclosure Scenarios in Agriculture through Transparency*' by Sebastian Linsner, Franz Kuntke, Enno Steinbrink, Jonas Franken and Christian Reuter (Technical University of Darmstadt) addresses the transparent collaboration and exchange of operational data between enterprises in the field of agriculture. While agricultural enterprises need to share operational data, the disclosure of sensitive data could be disadvantageous. At the same time, increased control and transparency could also lead to information overload and increased workload. This is especially challenging for small enterprises which have to keep pace with current developments of digitalisation. During a pre-study with German farmers, the authors explored current data sharing scenarios and inquired requirements for data sharing solutions. The evaluation of a respective prototype tested by practitioners showed that transparent data sharing tools need to be flexible, secure, adapted to their workflows, and store and process data locally. While the application is accompanied by higher time expenditure, it is easy to use and raises users' awareness.

The article '*Finding, Getting, Understanding: The user journey for the GDPR's right to access*' by Dominik Pins, Timo Jakobi, Gunnar Stevens, Fatemeh Alizadeh and Jana Krüger (University of Siegen & University of Applied Sciences Bonn-Rhein-Sieg) addresses the discrepancy between rights under data protection law and the concrete process if data subjects want to claim those rights. Awareness and control over the collection and use of personal data are seen as key elements of digital sovereignty. This sovereignty is also protected under law, in that data subjects have the right to access information about the data collected about them. However, it is unclear how this right can be asserted in concrete terms. This question was addressed by the creation of a five-phase user experience journey regarding the right to access (finding, authentication, request, access,

and data use), which was subsequently conducted and evaluated by 59 participants. Based on 422 data sets spanning 139 organisations, the authors identified several interdependencies between process design and user satisfaction.

## 5. Conclusion and the road ahead

This article has highlighted the interdependencies between the enhancement of security and privacy and users' needs and technical savvy. Research in the field of usable security and privacy has shown that it is essential to consider the user as a central factor for cyber security, in that measures for enhanced security have to be simple, practical, time-saving, and plausible. This is reached through the consideration of transparency in such a way that the measures applied are comprehensible for the user. In addition, the aspect of tailorability is also taken into account, meaning that user interventions are personalised according to users' knowledge, behaviour, and wishes.

Table 1 presents several research directions and questions on user-centred transparency and tailorability interventions for usable privacy and security that are based on the literature and the articles published in this special issue. We specifically highlight four research frontiers related to (1) user outcomes, heuristics and groups, (2) core paradoxes and trade-offs, (3) new technologies and affordances, and (4) research methods, which researchers may want to consider in their future research endeavours.

In sum, this article provides an introduction and the background for our special issue, which provides an overview of current contributions on usable security and privacy research with a focus on user-centred interventions and transparency mechanisms. With regard to such user interventions, the presented concepts and tools consider the issues of transparency and tailorability, in particular. Here, difficulties and challenges due to different requirements regarding different application contexts and end user groups are addressed through various technical and conceptual approaches. In addressing user needs, while at the same time providing user-friendly ways for privacy and security enhanced behaviour, the authors of the presented articles have covered various thematic fields. These include societal responses to data-driven technical applications and their democratic legitimacy; the secure use of mobile devices through the application of multi-modal authentication; easier and more secure processing of sensitive data via data protection compliant personal data management tools; transparency and understandability of privacy



**Table 1.** Transparency, Tailorability, and the Road Ahead in Usable Security and Privacy Research

User-Centred Interventions	Exemplary Intervention Mechanisms	Major Application Areas in USP Research	Research Directions and Questions
Transparency	Mental models based Visualisations or Audibilisations of e.g. policies, feedback, warning messages, information (flows) using dashboards; dedicated application features; disaggregation, white-box approaches	<ul style="list-style-type: none"> <li>User Authentication (e.g. password managers, biometrics, CAPTCHAs)</li> <li>Secure Messaging and Encryption (e.g. private/interorganisational data exchange)</li> <li>Anti-Phishing Efforts</li> <li>Storage (e.g. assured deletion, durability)</li> <li>Device Pairing (e.g. in IoT contexts)</li> <li>Web Privacy and Fair Information Practice (e.g. cookie banner, consent management, privacy dashboards)</li> <li>Policy Specification and Interaction</li> <li>Mobile/Smart Device Security and Privacy (e.g. voice assistants)</li> <li>Social Media Privacy (e.g. interdependent privacy)</li> <li>Security Administration</li> <li>Developer-Centred Security</li> </ul>	<p><i>User Outcomes, Heuristics and Groups</i></p> <ul style="list-style-type: none"> <li>What kind of user reactions depending on perceptions, attitudes, willingness and behaviours can we identify in response to intervention mechanisms across application contexts (e.g. user acceptance/reactance)?</li> <li>What do user sense-making-processes (i.e. mental models) and heuristics look like in detail?</li> <li>Which differences in interventions do various user groups and stakeholders (e.g. employees, people with disabilities, children, seniors, developers, administrators) need across all phases of product design, use, and support?</li> <li>How can usable security and privacy research outcomes be channelled (e.g. principles, guidelines, patterns) to enable developers to easily incorporate and apply them in their designs?</li> </ul> <p><i>Core Paradoxes and Trade-offs</i></p> <ul style="list-style-type: none"> <li>Disentangling the transparency paradox: Does higher transparency always lead to higher data disclosure?</li> <li>Is the discrepancy observed in many studies between users' privacy intentions and their actual behaviour a privacy paradox or the result of inadequate research methods?</li> <li>If there is such a thing as a privacy paradox, how can it be overcome?</li> <li>Finding a sweet spot in the trade-off between user effort and control: How to strike an optimal balance between usability and security/privacy?</li> </ul> <p><i>New Technologies and Affordances</i></p> <ul style="list-style-type: none"> <li>How should challenges posed by new technologies that are increasingly equipped with sensors and AI-based capabilities (e.g. wearables, smart home devices) be addressed?</li> <li>How can user-centred interventions based on transparency and tailorability be applied across different modalities (e.g. speech/voice control)?</li> </ul> <p><i>Research Methods</i></p> <ul style="list-style-type: none"> <li>How can longitudinal research methods (e.g. field experiments, ethnographic studies) be used to complement prevailing cross-sectional research methods (i.e. surveys, lab/online experiments)?</li> <li>How do one-off user-centred interventions differ from interventions along an entire user journey?</li> </ul>
Tailorability	Personalisation, nudging, customisation, user self-control, individual trainings		

notices in connection with the sequential context of these notices; transparent collaboration and exchange of operational data between agricultural enterprises in the trade-off between data disclosure, time-saving, and user-friendliness; and the concrete assertion of privacy rights under data protection law as a key element of digital sovereignty.

In conclusion, we hope that this article at hand can contribute to advancing the current discourse on the topic of usable security and privacy and help stimulate and inspire future research in our discipline.

## Acknowledgments

We would like to thank the editor-in-chief of Behaviour and Information Technology, Prof. Panos Markopoulos, for giving us the opportunity to edit this special issue and all authors and reviewers for their contributions to make this special issue possible.

## Disclosure statement

No potential conflict of interest was reported by the authors.

## Funding

This research work has been funded by the German Federal Ministry of Education and Research (BMBF, 16KIS1508) and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE, by the Centre Responsible Digitality and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB1119: CROSSING (236615297), and Accountable AI (471168026).

## ORCID

Christian Reuter  <http://orcid.org/0000-0003-1920-038X>

## References

- Abdul, Ashraf, Jo Vermeulen, Danding Wang, Brian Y. Lim, and Mohan Kankanhalli. 2018, April. "Trends and Trajectories for Explainable, Accountable and Intelligible Systems: An HCI Research Agenda." In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Vol. 2018, 1–18. ACM. doi:10.1145/3173574.3174156.

- Acquisti, Alessandro, Idris Adjerid, and Laura Brandimarte. 2013. "Gone in 15 Seconds: The Limits of Privacy Transparency and Control." *IEEE Security & Privacy* 11 (4): 72–74.
- Adams, Anne, and Martina Angela Sasse. 1999. "Users Are Not the Enemy." *Communications of the ACM* 42 (12): 40–46. doi:10.1145/322796.322806.
- Alizadeh, Fatemeh, Timo Jakobi, Alexander Boden, Gunnar Stevens, and Jens Boldt. 2020. "GDPR Reality Check – Claiming and Investigating Personally Identifiable Data from Companies." In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*. IEEE, 120–129. doi:10.1109/EuroSPW51379.2020.00025.
- Althobaiti, Kholoud, Nicole Meng, and Kami Vaniea. 2021. "I Don't Need an Expert! Making URL Phishing Features Human Comprehensible." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*, Article 695, 17. New York, NY, USA: Association for Computing Machinery. doi:10.1145/3411764.3445574.
- Angulo, Julio, Simone Fischer-Hübner, Tobias Pulls, and Erik Wästlund. 2015. "Usable Transparency With the Data Track: A Tool for Visualizing Data Disclosures." In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA)*, 1803–1808. Seoul, Republic of Korea: ACM Press. doi:10.1145/2702613.2732701.
- Biczók, Gergely, Kévin Huguenin, Mathias Humbert, and Jens Grossklags. 2021. "Call for Papers: Special Issue on Managing Multi-Party, Interdependent Privacy Risks." *Computers and Security*. <https://www.journals.elsevier.com/computers-and-security/call-for-papers/managing-multi-party>
- Bier, Christoph, Kay Kühne, and Jürgen Beyerer. 2016. "PrivacyInsight: The Next Generation Privacy Dashboard." In *Privacy Technologies and Policy* (Lecture Notes in Computer Science), edited by Stefan Schiffner, Jetzabel Serna, Demosthenes Ikonomou, and Kai Rannenberg, 135–152. Cham: Springer International Publishing. doi:10.1007/978-3-319-44760-5\_9
- Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. 2013. "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science* 4 (3): 340–347.
- Brodsky, Jessica E., Arshia K. Lodhi, Kasey L. Powers, Fran C. Blumberg, and Patricia J. Brooks. 2021. "It's Just Everywhere Now: Middle-school and College Students' Mental Models of the Internet." *Human Behavior and Emerging Technologies* 3 (4): 495–511. doi:10.1002/hbe2.281.
- Brown, Barry. 2001, Marh 26. "Studying the Internet Experience." Research Report HPL-2001-49. HP Laboratories Bristol. 24 pages.
- Canova, Gamze, Melanie Volkamer, Clemens Bergmann, and Benjamin Reinheimer. 2015. "NoPhish App Evaluation: Lab and Retention Study." In *NDSS Workshop on Usable Security*.
- Caraban, Ana, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 2019. "23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*, 1–15. New York, NY, USA: Association for Computing Machinery doi:10.1145/3290605.3300733.
- Cheng, Hao-Fei, Ruotong Wang, Zheng Zhang, Fiona O'Connell, Terrance Gray, F. Maxwell Harper, and Haiyi Zhu. 2019. "Explaining Decision-Making Algorithms through UI: Strategies to Help Non-Expert Stakeholders." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–12. ACM. doi:10.1145/3290605.3300789.
- Cranor, Lorrie Faith, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. "Parents' and Teens' Perspectives on Privacy In a Technology-Filled World." In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS)*, 19–35.
- Cranor, Lorrie Faith, and Simson Garfinkel, eds. 2005. *Security and Usability: Designing Secure Systems That People Can Use*. Beijing; Sebastapol, CA: O'Reilly.
- Dupree, Janna Lynn, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. "Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5228–5239. ACM. doi:10.1145/2858036.2858214.
- Egelman, Serge, Marian Harbach, and Eyal Peer. 2016. "Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS)." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 5257–5261. doi:10.1145/2858036.2858265.
- Egelman, Serge, and Eyal Peer. 2015. "The Myth of the Average User: Improving Privacy and Security Systems Through Individualization." In *Proceedings of the 2015 New Security Paradigms Workshop*, 16–28. doi:10.1145/2841113.2841115.
- Emami-Naeini, Pardis, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2022. "An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices." *IEEE Security & Privacy* 20 (2): 31–39. doi:10.1109/MSEC.2021.3132398.
- Emami-Naeini, Pardis, Tiona Francisco, Tadayoshi Kohno, and Franziska Roesner. 2021. "Understanding Privacy Attitudes and Concerns Towards Remote Communications During the {COVID-19}." In *Proceedings of the 17th Symposium on Usable Privacy and Security (SOUPS)*, 695–714.
- Farke, Florian M., Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. 2020. "You Still Use the Password After All – Exploring FIDO2 Security Keys in a Small Company." In *Sixteenth Symposium on Usable Privacy and Security (SOUPS '20)*, 19–35. USENIX Association. <https://www.usenix.org/conference/soups2020/presentation/farke>.
- Franz, Anjuli, Gregor Albrecht, Verena Zimmermann, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. 2021. "Still Plenty of Phish in the Sea – A Taxonomy of User-Oriented Phishing Interventions and Avenues for Future Research." In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 339–358.
- Frik, Alisa, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. "Privacy and Security Threat Models and Mitigation Strategies of Older Adults." In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 21–40. USENIX Association. <https://www.usenix.org/conference/soups2019/presentation/frik>.

- Garster, Daniel C., Richard W. Woodman, Jerome Adams, Michael McCuddy, Howard Fromkin, and Paul D. Tolchinsky. 1979. "Information Privacy in Organizations: An Examination of Employee Perceptions and Attitudes." In *Proceedings of the 39th Annual Conference of the National Academy of Management*, 262–266.
- Garcia, David. 2017. "Leaking Privacy and Shadow Profiles in Online Social Networks." *Science Advances* 3: 1–6. doi:10.1126/sciadv.1701172.
- Garfinkel, Simson L., and Heather Richter Lipford. 2014. *Usable Security. History, Themes, and Challenges*. Synthesis Lectures on Information Security, Privacy, and Trust 5, 1–124. San Rafael, California (USA): Morgan & Claypool. doi:10.2200/S00594ED1V01Y201408SPT011.
- Gerber, Nina, Paul Gerber, and Melanie Volkamer. 2018. "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior." *Computers & Security* 77: 226–261. doi:10.1016/j.cose.2018.04.002.
- Gerlitz, Eva, Maximilian Häring, and Matthew Smith. 2021. "Please Do Not Use !?\_ or Your License Plate Number: Analyzing Password Policies in German Companies." In *Seventeenth Symposium on Usable Privacy and Security (SOUPS '21)*, 17–36. USENIX Association. <https://www.usenix.org/conference/soups2021/presentation/gerlitz>.
- Golla, Maximilian, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M. Redmiles. 2021. "Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns." In *30th USENIX Security Symposium (USENIX Security '21)*. USENIX Association. <https://www.usenix.org/conference/usenixsecurity21/presentation/golla>.
- Gorski, Peter Leo, Sebastian Moller, Stephan Wiefeling, and Luigi Lo Iacono. 2021. "I Just Looked for the Solution!" - On Integrating Security-Relevant Information in Non-Security API Documentation to Support Secure Coding Practices." *IEEE Transactions on Software Engineering*, 1–1. doi:10.1109/TSE.2021.3094171.
- Green, Matthew, and Matthew Smith. 2016. "Developers are Not the Enemy!: The Need for Usable Security APIs." *IEEE Security & Privacy* 14 (5): 40–46. doi:10.1109/MSP.2016.111.
- Habib, Hana, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. "Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*, 1–25. New York, NY, USA: Association for Computing Machinery. doi:10.1145/3411764.3445387.
- Hartwig, Katrin, and Christian Reuter. 2019. "TrustyTweet: An Indicator-Based Browser-Plugin to Assist Users in Dealing with Fake News on Twitter." In *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*, 1858–1869.
- Hartwig, Katrin, and Christian Reuter. 2021. "Nudging Users Towards Better Security Decisions in Password Creation Using Whitebox-based Multidimensional Visualizations." In *Behaviour & Information Technology (BIT)*, 1–24. doi:10.1080/0144929X.2021.1876167.
- Hasegawa, Ayako A., Naomi Yamashita, Mitsuaki Akiyama, and Tatsuya Mori. 2021. "Why They Ignore English Emails: The Challenges of Non-Native Speakers in Identifying Phishing Emails." In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 319–338. USENIX Association. <https://www.usenix.org/conference/soups2021/presentation/hasegawa>.
- Hayes, Jordan, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. 2019. "Cooperative Privacy and Security: Learning from People with Visual Impairments and Their Allies." In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS)*, 1–20.
- Hochheiser, Harry. 2002, November. "The Platform for Privacy Preference as a Social Protocol: An Examination Within the U.S. Policy Context." *ACM Trans. Internet Technol.* 2 (4): 276–306. doi:10.1145/604596.604598.
- Jeske, Debora, Lynne Coventry, and Pam Briggs. 2014, April. "Nudging Whom How: IT Proficiency, Impulse Control and Secure Behaviour." In *Proceedings of the CHI Workshop on Personalizing Behavior Change Technologies*, 1–4.
- Kaiser, Ben, Jerry Wei, Elena Lucherini, Kevin Lee, Nathan Matias, and Jonathan Mayer. 2021. "Adapting Security Warnings to Counter Online Disinformation." In *30th USENIX Security Symposium (USENIX Security 21)*.
- Kamleitner, Bernadette, and Vince Mitchell. 2019. "Your Data is My Data: A Framework for Addressing Interdependent Privacy Infringements." *Journal of Public Policy & Marketing* 38 (4): 433–450. doi:10.1177/0743915619858924.
- Kamleitner, Bernadette, and Mahshid Sotoudeh. 2019. "Information Sharing and Privacy as a Socio-Technical Phenomenon." *TATuP Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis* 29: 68–71. doi:10.14512/tatup.28.3.68.
- Kang, Ruogu, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security." In *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*, 39–52. Ottawa: USENIX Association.
- Kelley, Patrick Gage, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 1573. Atlanta, Georgia, USA: ACM Press. doi:10.1145/1753326.1753561.
- Kerckhoffs, Auguste. 1883, January. "La Cryptographie Militaire." *Journal des sciences militaires* IX: 5–38.
- Knijnenburg, Bart. 2017. "Privacy? I Can't Even! Making a Case for User-Tailored Privacy." *IEEE Security and Privacy* 15 (4): 62–67. doi:10.1109/MSP.2017.3151331.
- Knijnenburg, Bart, and David Cherry. 2016. "Comics as a Medium for Privacy Notices." In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.
- Knijnenburg, Bart P., Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano, eds. 2022. *Modern Socio-Technical Perspectives on Privacy*. Cham: Springer International Publishing. doi:10.1007/978-3-030-82786-1.
- Kokolakis, Spyros. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 64: 122–134. doi:10.1016/j.cose.2015.07.002.



- Kowalewski, Marvin, Franziska Herbert, Theodor Schnitzler, and Markus Dürmuth. 2022. "Proof-of-Vax: Studying User Preferences and Perception of Covid Vaccination Certificates." *Proceedings on Privacy Enhancing Technologies (PoPETs)* 22 (1): 317–338.
- Krombholz, Katharina, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. 2019. "If HTTPS Were Secure, I Wouldn't Need 2FA' -- End User and Administrator Mental Models of HTTPS." In *2019 IEEE Symposium on Security and Privacy (SP)*, 246–263. doi:10.1109/SP.2019.00060.
- Kumaraguru, Ponnurangam, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. "School of Phish: A Real-World Evaluation of Anti-Phishing Training." In *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1–12.
- Kunke, Johannes, Stephan Wiefeling, Markus Ullmann, and Luigi Lo Iacono. 2021. "Evaluation of Account Recovery Strategies with FIDO2-Based Passwordless Authentication." In *Open Identity Summit 2021 (OID '21)*. Gesellschaft für Informatik e.V.
- Kwon, Bum Chul, and Bongshin Lee. 2016. "A Comparative Evaluation on Online Learning Approaches using Parallel Coordinate Visualization." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 993–997. ACM. doi:10.1145/2858036.2858101.
- Lassak, Leona, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server': Mitigating Users' Misconceptions about FIDO2 Biometric Webauthn." In *30th USENIX Security Symposium (USENIX Security '21)*, 91–108. USENIX Association. <https://www.usenix.org/conference/usenixsecurity21/presentation/lassak>.
- Lastdrager, Elmer, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. "How Effective is Anti-Phishing Training for Children?." In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS)*, 229–239.
- Linsner, Sebastian, Franz Kuntke, Enno Steinbrink, Jonas Franken, and Christian Reuter. 2021. "The Role of Privacy in Digitalization—Analyzing Perspectives of German Farmers." *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2021 (3): 334–350. doi:10.2478/popets-2021-0050.
- Lyastani, Sanam Ghorbani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. 2020. "Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication." In *2020 IEEE Symposium on Security and Privacy (SP '20)*, 268–285. IEEE. doi:10.1109/SP40000.2020.00047.
- Machuletz, Dominique, and Rainer Böhme. 2020. "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs After GDPR." *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2020: 481–498. doi:10.2478/popets-2020-0037.
- Marforio, Claudio, Ramya Jayaram Masti, Claudio Soriente, Kari Kostiaainen, and Srdjan Capkun. 2016. "Evaluation of Personalized Security Indicators as an Antiphishing Mechanism for Smartphone Applications." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 540–551.
- Marne, Sonali Tukaram, Mahdi Nasrullah, and Matthew Wright. 2017. "Learning System-assigned Passwords: A Preliminary Study on the People with Learning Disabilities." In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS)*.
- McDonald, Allison, Catherine Barwulor, Michelle L. Mazurek, Florian Schaub, and Elissa M. Redmiles. 2021. "It's Stressful Having All These Phones': Investigating Sex Workers' Safety Goals, Risks, and Practices Online." In *30th USENIX Security Symposium (USENIX Security 21)*, 375–392. USENIX Association. <https://www.usenix.org/conference/usenixsecurity21/presentation/mcdonald>.
- Melara, Marcela S., Aaron Blankstein, Joseph Bonneau, Edward W. Felten, and Michael J. Freedman. 2015. "CONIKS: Bringing Key Transparency to End Users." In *24th USENIX Security Symposium (USENIX Security 15)*, 383–398.
- Murmann, Patrick, and Simone Fischer-Hübner. 2017. "Tools for Achieving Usable Ex Post Transparency: A Survey." *IEEE Access* 5: 22965–22991. doi:10.1109/ACCESS.2017.2765539.
- Naiakshina, Alena, Anastasia Danilova, Eva Gerlitz, Emanuel von Zezschwitz, and Matthew Smith. 2019. "If You Want, I Can Store the Encrypted Password': A Password-Storage Field Study with Freelance Developers." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Glasgow, Scotland Uk: ACM. doi:10.1145/3290605.3300370.
- Napoli, Daniela, Khadija Baig, Sana Maqsood, and Sonia Chiasson. 2021. "I'm Literally Just Hoping This Will Work': Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities." In *Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS)*, 263–280.
- Nicholson, James, Lynne Coventry, and Pam Briggs. 2017. "Can we Fight Social Engineering Attacks by Social Means? Assessing Social Salience as a Means to Improve Phish Detection." In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, SOUPS '17*, 285–298.
- Nicholson, James, Lynne Coventry, and Pam Briggs. 2018. "Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection." In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 443–457.
- Norberg, Patricia A., Daniel R. Horne, and David A. Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors." *Journal of Consumer Affairs* 41 (1): 100–126. doi:10.1111/j.1745-6606.2006.00070.x.
- Nyhan, Brendan, and Jason Reifler. 2010. "When Corrections Fail: The Persistence of Political Misperceptions." *Political Behavior* 32 (2): 303–330. doi:10.1007/s11109-010-9112-2.
- Oates, Maggie, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. "Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration." *Proceedings on Privacy Enhancing Technologies* 2018 (4): 5–32. doi:10.1515/popets-2018-0029.
- Owens, Kentrell, Olabode Anise, Amanda Krauss, and Blase Ur. 2021. "User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators." In *Seventeenth Symposium on Usable Privacy and Security*



- (SOUPS '21), 57–76. USENIX Association. <https://www.usenix.org/conference/soups2021/presentation/owens>.
- Peer, Eyal, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. 2019. “Nudge Me Right: Personalizing Online Nudges to People’s Decision-Making Styles.” *SSRN Electronic Journal* 1–27.
- Petelka, Justin, Yixin Zou, and Florian Schaub. 2019. “Put Your Warning Where Your Link is: Improving and Evaluating Email Phishing Warnings.” In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–15.
- Plöger, Stephan, Mischa Meier, and Matthew Smith. 2021. “A Qualitative Usability Evaluation of the Clang Static Analyzer and libFuzzer with CS Students and CTF Players.” In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 553–572. USENIX Association. <https://www.usenix.org/conference/soups2021/presentation/ploger>.
- Pulls, Tobias, Roel Peeters, and Karel Wouters. 2013. “Distributed Privacy-Preserving Transparency Logging.” In *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, 83–94.
- Railean, Alexandr, and Delphine Reinhardt. 2018. “Let There Be LITE: Design and Evaluation of a Label for IoT Transparency Enhancement.” In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, 103–110. Barcelona, Spain: ACM. doi:10.1145/3236112.3236126.
- Reinhardt, Daniel, Johannes Borchard, and Jörn Hurtienne. 2021. “Visual Interactive Privacy Policy: The Better Choice?” In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*, 1–12. New York, NY, USA: Association for Computing Machinery. doi:10.1145/3411764.3445465.
- Renaud, Karen, Verena Zimmerman, Joseph Maguire, and Steve Draper. 2017. “Lessons Learned from Evaluating Eight Password Nudges in the Wild.” In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER)*, 25–37. USENIX Association. <https://www.usenix.org/conference/laser2017/presentation/renaud>.
- Roethke, Konstantin, Johannes Klumpe, Martin Adam, and Alexander Benlian. 2020. “Social Influence Tactics in E-commerce Onboarding: The Role of Social Proof and Reciprocity in Affecting User Registrations.” *Decision Support Systems* 131: Article ID 113268. doi:10.1016/j.dss.2020.113268.
- Roth, Sebastian, Lea Gröber, Michael Backes, Katharina Krombholz, and Ben Stock. 2021. “12 Angry Developers – a Qualitative Study on Developers’ Struggles with CSP.” In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21)*, 3085–3103. ACM. doi:10.1145/3460120.3484780.
- Ruoti, Scott, and Kent Seamons. 2019. “Johnny’s Journey Toward Usable Secure Email.” *IEEE Security Privacy* 17 (6): 72–76. doi:10.1109/MSEC.2019.2933683.
- Saltzer, Jerome H., and Michael D. Schroeder. 1975. “The Protection of Information in Computer Systems.” *Proceedings of the IEEE* 63 (9): 1278–1308.
- Sasse, M. Angela, and Awais Rashid. 2021. *The Cyber Security Body of Knowledge v1.1.0*, 2021. University of Bristol, Chapter Human Factors. KA Version 1.0.1. <https://www.cybok.org/>.
- Sasse, M. Angela, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea. 2016. “Debunking Security-Usability Tradeoff Myths.” *IEEE Security & Privacy* 14 (5): 33–39. doi:10.1109/MSP.2016.110.
- Schneider, David, Johannes Klumpe, Martin Adam, and Alexander Benlian. 2020. “Nudging Users Into Digital Service Solutions.” *Electronic Markets* 30: 863–881. doi:10.1007/s12525-019-00373-8.
- Schöbel, Sofia, Torben Jan Barev, Andreas Janson, Felix Hupfeld, and Jan Marco Leimeister. 2020. “Understanding User Preferences of Digital Privacy Nudges? A Best-Worst Scaling Approach.” In *Hawaii International Conference on System Sciences (HICSS)*. <https://www.alexandria.unisg.ch/257810/>.
- Schufirin, M., S. L. Reynolds, A. Kuijper, and J. Kohlhammer. 2021. “A Visualization Interface to Improve the Transparency of Collected Personal Data on the Internet.” *IEEE Transactions on Visualization and Computer Graphics* 27 (2): 1840–1849. doi:10.1109/TVCG.2020.3028946.
- Spiekermann, Sarah, Hanna Krasnova, Oliver Hinz, Annika Baumann, Alexander Benlian, Henner Gimpel, Irina Heimbach, et al. 2022. “Values and Ethics in Information Systems.” *Business & Information Systems Engineering* 64 (2): 247–264. doi:10.1007/s12599-021-00734-8.
- Steinbrink, Enno, Lilian Reichert, Michelle Mende, and Christian Reuter. 2021. “Digital Privacy Perception of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight.” In *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing*.
- Stransky, Christian, Dominik Wermke, Johanna Schrader, Nicolas Huaman, Yasemin Acar, Anna Lena Fehlhaber, Miranda Wei, Blase Ur, and Sascha Fahl. 2021. “On the Limited Impact of Visualizing Encryption: Perceptions of E2E Messaging Security.” In *Seventeenth Symposium on Usable Privacy and Security (SOUPS)*, 437–454.
- Tabassum, Madiha, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. “Increasing User Attention with a Comic-Based Policy.” In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*, 1–6. New York, NY, USA: Association for Computing Machinery. doi:10.1145/3173574.3173774.
- Tahaei, Mohammad, Kami Vaniea, and Naomi Saphra. 2020. “Understanding Privacy-Related Questions on Stack Overflow.” In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery. doi:10.1145/3313831.3376768.
- Tan, Joshua, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2020. *Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-Strength, Minimum-Length, and Blocklist Requirements*, 1407–1426. New York, NY: Association for Computing Machinery. doi:10.1145/3372297.3417882.
- Thaler, Richard, and Cass Sunstein. 2009. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New York (USA): Penguin.
- Tian, Ke, Steve T. K. Jan, Hang Hu, Danfeng Yao, and Gang Wang. 2018. “Needle in a Haystack: Tracking Down Elite

- Phishing Domains in the Wild.” In *Proceedings of the Internet Measurement Conference 2018, IMC '18*, 429–442.
- Tolsdorf, Jan, Florian Dehling, Delphine Reinhardt, and Luigi Lo Iacono. 2021. “Exploring Mental Models of the Right to Informational Self-Determination of Office Workers in Germany.” *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2021 (3): 5–27. doi:10.2478/popets-2021-0035
- Tolsdorf, Jan, Delphine Reinhardt, and Luigi Lo Iacono. 2022. “Employees’ Privacy Perceptions: Exploring the Dimensionality and Antecedents of Personal Data Sensitivity and Willingness to Disclose.” *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2022 (2): 68–94. doi:10.2478/popets-2022-003.
- Ulqinaku, Enis, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Čapkun. 2021. “Is Real-Time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks Against FIDO Protocols.” In *30th USENIX Security Symposium (USENIX Security '21)*, 3811–3828. USENIX Association. <https://www.usenix.org/conference/usenixsecurity21/presentation/ulqinaku>.
- Ur, Blase, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. “Do Users’ Perceptions of Password Security Match Reality?” In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 3748–3760. ACM. doi:10.1145/2858036.2858546.
- Verma, Rakesh, and Keith Dyer. 2015. “On the Character of Phishing URLs: Accurate and Robust Statistical Learning Classifiers.” In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, CODASPY '15*, 111–122.
- Veys, Sophie, Daniel Serrano, Madison Stamos, Margot Herman, Nathan Reiting, Michelle L. Mazurek, and Blase Ur. 2021. “Pursuing Usable and Useful Data Downloads Under GDPR/CCPA Access Rights via Co-Design.” In *Proceedings of the 17th Symposium on Usable Privacy and Security (SOUPS)*, 217–242.
- Ware, Colin. 2012. *Information Visualization: Perception for Design*. 3rd ed. Boston: Morgan Kaufmann.
- Wash, Rick, Norbert Nthala, and Emilee Rader. 2021. “Knowledge and Capabilities that Non-Expert Users Bring to Phishing Detection.” In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 377–396.
- USENIX Association. <https://www.usenix.org/conference/soups2021/presentation/wash>.
- Weinmann, Markus, Christoph Schneider, and Jan vom Brocke. 2016. “Digital Nudging.” *Business & Information Systems Engineering* 58 (6): 433–436. doi:10.1007/s12599-016-0453-1
- Whitten, Alma, and J. Doug Tygar. 1999. “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.” In *Proceedings of the 8th USENIX Security Symposium (USENIX Security '99)*, Vol. 348. <https://www.usenix.org/legacy/events/sec99/whitten.html>.
- Wiefeling, Stephan, Markus Dürmuth, and Luigi Lo Iacono. 2020. “More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication.” In *36th Annual Computer Security Applications Conference (ACSAC '20)*, 203–218. ACM. doi:10.1145/3427228.3427243.
- Wiefeling, Stephan, Tanvi Patil, Markus Dürmuth, and Luigi Lo Iacono. 2020. “Evaluation of Risk-Based Re-Authentication Methods.” In *35th IFIP TC-11 International Conference on Information Security and Privacy Protection (IFIP SEC '20)*, 280–294. Springer International Publishing. doi:10.1007/978-3-030-58201-2\_19
- Wu, Justin., and Daniel Zappala. 2018. “When Is a Tree Really a Truck? Exploring Mental Models of Encryption.” In *Proceedings of the 14th Symposium on Usable Privacy and Security (SOUPS)*. 395–409.
- Zheng, Serena, Noah Aphorpe, Marshini Chetty, and Nick Feamster. 2018. “User Perceptions of Smart Home IoT Privacy.” *Proceedings of the ACM on Human-Computer Interaction* 2 (CSCW): 200:1–200:20. doi:10.1145/3274469.
- Zimmermann, Verena, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. 2018. “‘Home, Smart Home’ – Exploring End Users’ Mental Models of Smart Homes.” In *Mensch und Computer 2018 - Workshopband*, 407–417. Bonn, Germany: Gesellschaft für Informatik e.V. doi:10.18420/muc2018-ws08-0539
- Zurko, Mary Ellen, and Richard T. Simon. 1996. “User-Centered Security.” In *Proceedings of the 1996 Workshop on New Security Paradigms (NSPW)*, 27–33. Lake Arrowhead, California, USA: ACM Press. doi:10.1145/304851.304859