

Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments

Citation for published version (APA):

Nelissen, L. G. M., & Funk, M. (2022). Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments. *International Journal of Design*, 16(1), 75-92.
<https://doi.org/10.57698/v16i1.05>

Document license:
CC BY-NC

DOI:
[10.57698/v16i1.05](https://doi.org/10.57698/v16i1.05)

Document status and date:
Published: 01/04/2022

Document Version:
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.



Rationalizing Dark Patterns: *Examining the Process of Designing Privacy UX Through Speculative Enactments*

Lei Nelissen*, Mathias Funk

Department of Industrial Design, Eindhoven University of Technology, Eindhoven, the Netherlands

Connected products and applications increasingly leverage users' personal data in their core functions. Designing privacy-sensitive interfaces for such data-related applications is a delicate craft. There is often tension between designers and changing user perceptions of privacy, data monetization, legal requirements, and organizational power structures, often resulting in designer complicity in privacy violations. This work examines the process of designing privacy-oriented interfaces in terms of compliance, ethics, and creativity, and specifically how designers weigh competing interests in resolving an ethical conflict. We study this through a speculative enactment, ChoiceBox, in which 33 design students and professional designers explore UX design through a privacy lens with a series of fictional clients. The resulting interviews and wireframes are analyzed for Privacy UX insights. The results show a limited awareness of how legal principles affect design practice, and how some designers easily violated boundaries in terms of ethics—even their own. We show how designers are not immune to enacting and rationalizing dark patterns of Privacy UX, and how speculative enactments can be a tool to foreground crucial issues of friction and ambiguity regarding end-user privacy and data protection in design education and practice.

Keywords – Privacy UX, User Interfaces, Privacy by Design, Privacy Paradox, Speculative Enactments, UX Ethics and Law.

Relevance to Design Practice – The intersection of service design and end-user data is fraught with dark patterns and data protection issues. We showcase ChoiceBox, a speculative enactment to help designers assess and incorporate Privacy UX more critically into their practices, which involves new strategies and an awareness of how to deal with the tension between end-user data protection rights and business interests.

Citation: Nelissen L., & Funk, M. (2022). Rationalizing dark patterns: Examining the process of designing privacy UX through speculative enactments. *International Journal of Design*, 16(1), 75-92. <https://doi.org/10.57698/v16i1.05>

Introduction

Companies deal with increasing personal data, and they are handling it poorly (Davies, 2015; Electronic Privacy Information Center, 2018; Newman, 2018). Every new data scandal erodes some of the trust in technology (Populus & Ipsos MORI, 2017), and designers shaping interfaces to privacy-sensitive data or functionality are at risk of, amongst other things, desensitizing their users (Utz et al., 2019; Villebro et al., 2018), or worse, conditioning them to accept a “new normal” (Brunton & Nissenbaum, 2019; Hoffmann et al., 2016) in terms of online privacy. While new legislation (such as the EU GDPR or US CCPA) offers promise in ameliorating online privacy, design practice frequently fails to account for recent developments in public policy. At the same time, there is a need to recognize that addressing privacy is not only synonymous with solving surveillance problems (Zuboff, 2015), compliance problems (Mohan et al., 2019; Nouwens et al., 2020) or security problems (Boniface et al., 2019), but it is also a means of establishing privacy as a fundamental human right (Council Of Europe, 1950; Kirkham, 2020; UN General Assembly, 1948).

GDPR

The European General Data Protection Regulation, passed in 2016 and effective from May, 2018 (European Parliament, Council of the European Union, 2016), is a European law that

updates an earlier set of regulations on personal data processing to match the border-agnostic nature of data in the modern age (Peterson et al., 2011), shifting the focus from where the data processing occurs to where the subject is located. The GDPR frames data protection from a legal perspective, formally mandating the practice of Privacy by Design, a concept that was popularized by Langheinrich in 2001, in the context of ubiquitous computing (Langheinrich, 2001), though its history may be traced to an earlier workshop in 2000 (see <http://www.cfp2000.org/>). Langheinrich developed six principles guiding systems design, based on legal principles: notice, choice and consent, proximity and locality, anonymity and pseudonymity, security and access, and recourse. These are primary principles in the GDPR as well. Moreover, the legal requirements for these principles have been operationalized in the form of *GDPR consent notices*, in which users are presented with explicit choices regarding their privacy when accessing a website (Degeling et al., 2019). Research has found that these screens paradoxically limit user choice by virtue

Received October 19, 2020; Accepted March 19, 2022; Published April 30, 2022.

Copyright: © 2022 Nelissen & Funk. Copyright for this article is retained by the authors, with first publication rights granted to the *International Journal of Design*. All journal content is open-access and allowed to be shared and adapted in accordance with the *Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License*.

*Corresponding Author: lei@codified.nl

of their particular design, and through the employment of nudging tactics that steer users towards a choice that is beneficial to the website operator (Utz et al., 2019).

The inclusion of Privacy by Design could be seen as an attempt by law-making bodies to cement the law in practice (i.e. for designers), however, this inclusion can be described as contentious (Koops & Leenes, 2014; I. Rubinstein & Good, 2013; I. S. Rubinstein, 2011; Spiekermann, 2012). Among oft-heard criticism of the GDPR by engineering, design, and law scholars alike is a lack of definition of practical requirements (Koops & Leenes, 2014; I. Rubinstein & Good, 2013) and a lack of inclusion of end-user goals (Ayalon & Toch, 2019; Information Commissioner's Office, 2014). Moreover, Terpstra et al. (2019) argue that the focus on notice and consent prohibits user reflection and the informed decision making on which these principles are based.

Privacy Paradox

An important phenomenon in the context of online privacy is the privacy paradox (Norberg et al., 2007), which entails how stated user preferences towards privacy contrast with users' actual behavior, and has been studied since the popular emergence of the internet (B. Brown, 2001). With internet usage growing exponentially in terms of intensity (International Telecommunication Union, 2019), complexity (e.g. personalization (Moon, 2000; Postma & Brokke, 2002), and its impact on daily life (McMillan & Morrison, 2006)), the definition has been broadened to include the disconnect between user privacy preferences and behavior (Norberg et al., 2007).

Despite extensive research, there is no clear evidence as to why the privacy paradox (still) exists (Barth & de Jong, 2017). Barth & de Jong reveal that despite extensive prior research, the existing theories are too simplistic to cover the complex cognitive processes of decision-making in regard to privacy, preventing a unifying theory from being established. Moreover, as most studies have been based on self-reported behavior, there is a need for further investigations where actual user behavior is studied.

Regardless of the potential cognitive reasons for the privacy paradox, it is apparently easier—at a basic level—to stretch one's personal boundaries in terms of privacy than forego the

benefits offered by modern web services. Given this shift, it is not unreasonable to suggest that the systems themselves are involved in the problem, potentially implicating interfaces and their designers.

Dark Patterns

A second related phenomenon is the growing use of dark patterns, i.e., user experience (UX) design patterns that trick users into doing things they did not intend to do (Brignull, 2011). While dark patterns can be seen in design traditions of persuasive design (Fogg, 2009) and behavior change theories such as nudging (Thaler & Sunstein, 2008), their outcomes negatively impact citizens. Dark patterns are seen as related to the privacy paradox. Given that there is an abundance of literature (Graßl et al., 2021; Terpstra et al., 2019; Wong & Mulligan, 2019) on the topic of responsibly designing interfaces, why is the current state of online privacy standards so underwhelming (Utz et al., 2019)?

And yet, attributing the problems to corporate decision making and poor end-user awareness alone does not do justice to the role that design plays—in both its potential for negative and positive effects. In the EU, the poor state of data protection has led to a regulatory counter-movement in the form of the General Data Protection Regulation. Since its introduction, its focus on transparency, control, and consent has been steadily changing the Privacy UX landscape through major court decisions, for instance, ruling that “Silence, pre-ticked boxes, or inactivity should not therefore constitute consent” (*VZBV v. Planet49*, 2019). More court rulings and resulting fines that further define the landscape are still expected (Hill, 2019).

Privacy UX

It is arguable that HCI forms a perfect backdrop for solving exactly these issues, because of its rich user-centered history (Cooley, 2000), its nature in questioning human values in the practice (Bannon, 1995; Borning & Muller, 2012; Kirkham, 2020; Shilton, 2013), as well as its tradition of tackling wicked problems (Buchanan, 1992). Additionally, HCI has a storied tradition of design ethics (Albrecht, 2007; Cummings, 2006; Salvo, 2001; van den Hoven, 2007; Verbeek, 2006), with some mentions of privacy and ethics as intricately connected (Munteanu et al., 2015; Reynolds & Picard, 2004). However, addressing the ethics in the practice of UX is a recent phenomenon, for instance, as seen in dark patterns. Gray et al. build upon this work by also describing properties of the ‘asshole designer’ responsible for creating dark patterns (Gray et al., 2020). More specifically, Gray and Chivukula address the need for ethical mediation in UX practice through group interviews with practitioners. They propose a framework for categorizing and addressing Ethical Design Complexity through the lens of the individual designer's practices, organizational practices, and applied ethics (Gray & Chivukula, 2019).

In this research, we respond to a particular cue by Wong and Mulligan, which calls for the inclusion of design criteria and designers in the practice of Privacy by Design (2019). They argue that current HCI work is much too partial to address and

Lei Nelissen is a design technologist with a MSc in Industrial Design from the Department of Industrial Design at the Eindhoven University of Technology. His research interests and professional work concern the operationalization of privacy legislation in both systems and user experiences, focusing on integrative qualities and meaningful choices. He has a broad range of professional experience in the cross-section of user experience design and web technologies, working for De Jongens van de TU (Eindhoven), Studio Tast (Eindhoven), Southern Cross Austereo (Sydney) and Philips Experience Design. He currently works at BMD Studio, a design studio based in Eindhoven, where he is further developing user experiences involving the management of personal information.

Mathias Funk is Associate Professor in the Future Everyday group in the Department of Industrial Design at the Eindhoven University of Technology (TU/e). He has a background in Computer Science and a PhD in Electrical Engineering (from TU/e). His research interests include methods and tools for designing with data, designing systems of smart things, and interfaces for musical expression. In the past he has researched at Philips Consumer Lifestyle and Philips Experience Design, Intel Labs (Santa Clara), National Taiwan University of Science and Technology, and National Taiwan University. He is also the co-founder of UXsuite, a high-tech spin-off from TU/e.

solve privacy problems, and offers inadequate support. Rather, they would prefer to see more critical approaches to privacy, by “*encouraging more holistic reflections and discussions by explicitly drawing connections among privacy’s social, legal, and technical aspects*” (Wong & Mulligan, 2019, p. 13).

Since (interaction) design programs educate new generations of UX designers on how to implement privacy protections in their future design practice, the field has a vital influence on the future implementation of interfaces for any data-processing system. However, practices at the intersection of User Experience Design and privacy are under-explored and an issue of ongoing design research (Gray et al., 2018; Nouwens et al., 2020; Yao et al., 2019). We particularly see such issues emerge in the case of consent banners (Gray, Santos, et al., 2021), and a growing tendency to identify such forms of manipulative UX *dark* or *evil* (Graßl et al., 2021; Gray, Chivukula, et al., 2021). Given the state of UX in connection with dark patterns and nudging, one might argue that UX is often geared against privacy protection in practice, despite UX definitions and pretensions. A clear definition of Privacy UX has not yet emerged, as most available resources refer to addressing the legal issues raised by privacy law. To contrast this, and to provide a working definition in this article, we refer to the attitudes and design patterns required for designing privacy-friendly interfaces and artefacts such as Privacy UX. Legislation is an explicit and enforceable aspect of Privacy UX, with legislation providing ground rules for the practice, while raising the bar from voluntary, unilateral attempts at compliance.

This research aims to explore, evaluate, and reflect upon the process of designing user interfaces in the context of *GDPR consent notices*, a common frustration for end-users (Obar & Oeldorf-Hirsch, 2018). In the remainder of this paper, we study this through speculative enactments involving 33 design (under)graduate students, PhD students, and practitioners. After presenting the study and its findings, we interpret the results, discuss limitations, and conclude with an outlook on future work and design recommendations for Privacy UX.

Speculative Enactments with ChoiceBox

In order to further investigate the noted issues on Privacy UX, we require a canvas we can use to explore the responsibilities and issues associated with it. We have chosen to create a speculative enactment (Elsden et al., 2017) to allow for reflection upon these issues in an open-ended, collaborative manner, and perhaps to even come to an understanding of the solution space. As noted by Kozubaev et al:

As HCI takes on pressing societal challenges, design futuring has an important role to play in troubling dominant techno-logics and imagining critical alternatives; a role that must necessarily be reflective” (2020, p. 10).

Speculative enactments are described by Elsden et al. as a research approach in which participants are placed in a speculative environment or scenario, and are then urged to think about a

possible future (Elsden et al., 2017; Kozubaev et al., 2020), not dissimilar to *provotypes* (Boer & Donovan, 2012). They spring from a design fiction (Sterling, 2009) background, and have been argued to help participants critically address possible futures through playful speculation. It is precisely this detachment from current reality that is necessary to shift participants’ designs from the viable to the possible—and beyond. Meanwhile, this outside perspective on the problem allows for an easier transition into institutional reflection, a necessity when treating privacy in HCI as per Wong et al. In a related vein, Gaver et al. (2003) argue expressly for the inclusion of ambiguity in specific designs that raise topics and ask questions without dictating answers.

The guidelines and prerequisites set by Elsden et al. were employed to generate the materials and circumstances of a speculative enactment. Firstly, the context of privacy necessitated a design activity in which value conflicts would be present: a user interface design. By scoping this design to *GDPR Consent Notices*, conflicts are explicitly brought to the forefront. While designing these notices is not necessarily an everyday task, it is plausibly a part of a UX Designer’s daily work. Moreover, by focusing on a creative activity, the enactment allows participants to follow existing routines, as well as allowing them to explore real-world consequences.

Ethical mediators were also included in the design of the exercise; these are described by Gray and Chivukula as the “*relationship of the designer to knowledge and work practices*” (2019, p. 9). Given the role of ethics in Privacy UX, Gray and Chivukula elaborate on the necessity of studying organizational practices, individual practices, and applied ethics as key factors in understanding the ethical mediation that forms the basis of a design. Thus, we recognize not only individual ethics, but also influences from the environment, in the form of colleagues and organizations, whether they be negative or positive. These factors had to be explicitly represented in the scenario.

Finally, the speculative approach comes to life through three elements: (1) a roleplay in which participants assume a Junior UX Designer position in the fictional *WOWH Design Agency*; (2) a set of clients for this agency, each requiring a *GDPR Consent Notice* to be designed by the participant; (3) the ChoiceBox device, a data management device that acts as a canvas for *GDPR Consent Notices*.

In this section, these three elements, their relation to each other, and their intentions are discussed in detail. Together, they form the *ChoiceBox speculative enactment*, or in short: *ChoiceBox*. With ChoiceBox, we explore how the notion of user ownership of data affects the user experience of privacy, while also considering the complex power dynamics that are a part of the Privacy UX process. The *ChoiceBox speculative enactment* is fully fictional and exists only as digital sketches.

Employment by WOWH

As part of the scenario, participants find themselves employed by the *WOWH Design Agency*, a fictional UX design consultancy. They are employed as Junior UX Designers on a team with two Senior UX Designers, all reporting to the Product Owner: *Oscar Meyernie*.

The purpose of the fictional employment is to situate the participant in a working environment with professional responsibilities. The participant's chief responsibility is performing the work that is asked of them. The choices a participant makes are framed in a deliberately messy context of applied ethics, politics, and conflicting business and personal values, in order to elucidate the daily problems a designer might run into when dealing with consent and GDPR in UX Design. The context of the design agency is similar to *Bear & Co*, in which conflicting values were likewise simulated (Berner et al., 2019).

Clients

A design activity necessitates some form of assignment that requires design. In the case of *WOWH*, this comes in the form of a set of fictional clients: *Planarr*, *Budget.me*, and *Jobby*. All clients are start-ups, heavily invested in data, complete with business models, logos, and backstories. As part of their respective launches, these clients require screens in which consumers consent to share the data that is used by the applications. The client scenarios, including their collected data types, have been summarized in Table 1.

ChoiceBox Device

Note: ChoiceBox is used interchangeably to refer to the fictional device (as is described in this subsection) as well as the entirety of the speculative enactment (as is described in the overarching section).

In order to create a canvas which the participants could design against, the ChoiceBox *device* was conceptualized. This helped set design constraints and prevent discussions on implementation




details. Furthermore, the ChoiceBox device helped participants to make sense of the assignment from a design perspective. It was designed with the intent to provide a means for reaching deeper questions more easily.

The *ChoiceBox* device is a fictional hardware appliance that stores personal data in the comfort of a consumer's own home. It functions as the *diegetic prototype* (Elsden et al., 2017, p. 5293) in the speculative enactment. As detailed in Figure 1, the ChoiceBox device is a square box that features four buttons as well as an indicator in the form of an LED-strip running along the top edge around the sides. In the same vein as the Solid POD (Mansour et al., 2016; Solid Project, 2020), it provides localized data storage to establish metaphorical data ownership and it fully mediates personal data exchange to establish trust. The indicator and buttons were added to establish a semblance of an actual product, but their functions were not elaborated on during the study. During the research, the ChoiceBox device was presented as the digital sketch seen in Figure 1.

User consent and choices are handled through a mobile companion application that is bundled with the ChoiceBox device. Third party applications can request access to a user's data through this application (see Figure 2). The mobile application presents these requests to the user on a screen, and designing this screen is the assignment given to the participants. Although some information about the mobile application is provided (such as the logo, the user objective, and displayed data), the application itself is a deliberate blank slate for participants.

The conceptual ChoiceBox product, device, and mobile app were framed and introduced as a neutral platform that exclusively facilitates data access requests through its UI, without judging or

Table 1. Overview of client scenarios, split by business description, background and data types processed.

Client	 planarr	 budget.me	 jobby
Description	Social meeting planner	Automatic personal budgeting, notifications and insights	AI-powered job placement
Background	Sensitivity of planned events; General visitor and click tracking issues ^a	Anonymity and privacy of financial data; Implications of standardized access to finances ^b	Algorithmic bias ^c ; Legality of personal information in context of job searches ^d
Data processed	<ul style="list-style-type: none"> Name Email-address Contact list (i.e. names and e-mail addresses of others) IP address 	<ul style="list-style-type: none"> Name E-mail address IP address Bank account numbers Past transactions Future transactions 	<ul style="list-style-type: none"> Name E-mail address IP address Employment history Previous job applications Income history Birth date Sex ^e Marital status Diplomas and grades for education and/or vocational training Union membership status ^e Religious affinity ^e

Notes: a. Manjoo, 2019

b. European Commission, 2019; Hauptert & Gabert, 2019; Noctor, 2018; Privacy First, 2019

c. Chen et al., 2019; Hajian et al., 2016; Obermeyer & Mullainathan, 2019

d. Vickers, 2007

e. Generally unlawful to process under the GDPR or other European laws

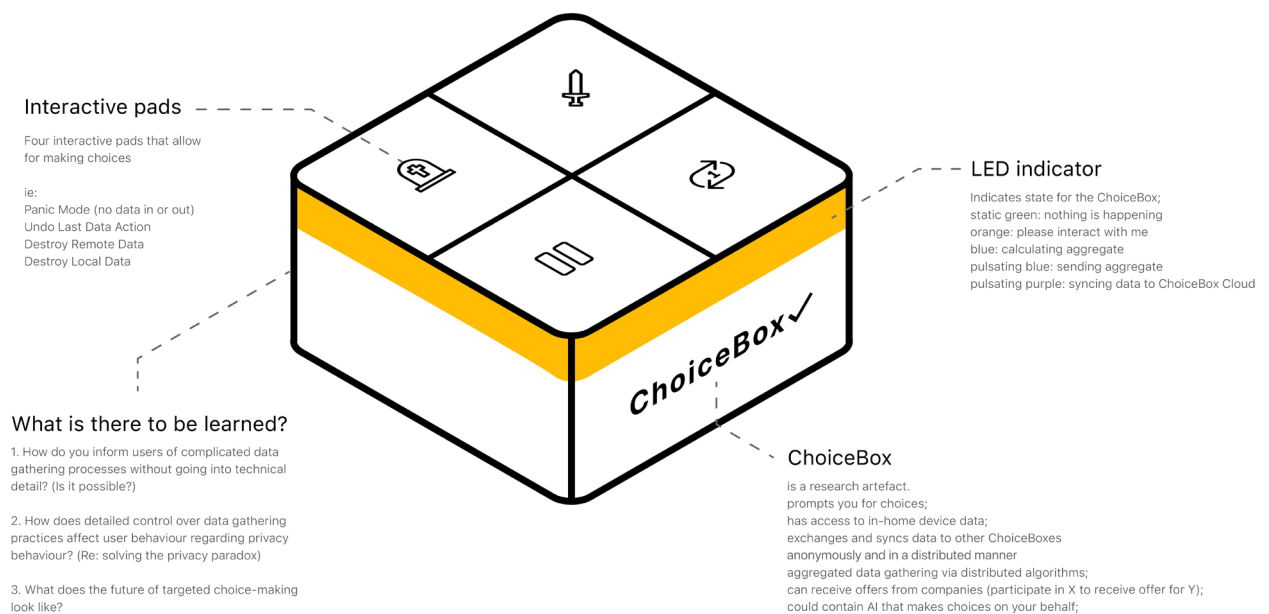


Figure 1. Design impression of the fictional ChoiceBox.

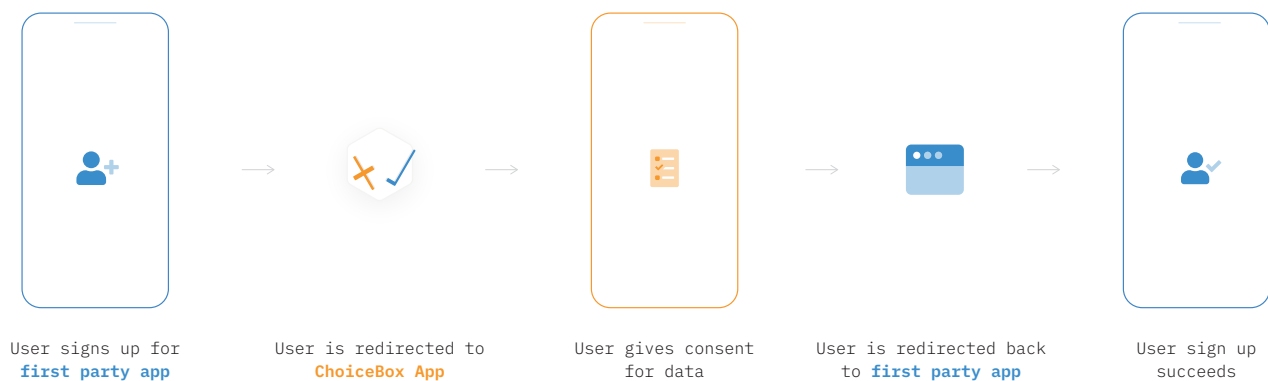


Figure 2. The presented flow between ChoiceBox and a WOWH client application.

manipulating the data that is requested by third-party applications. Because of this, the organization behind the ChoiceBox was described as a neutral non-profit, funded by grants and donations. The ChoiceBox concept finds inspiration in HCI work investigating the implications of decentralization (Guy, 2017; Oppl & Stary, 2019; Troncoso et al., 2017), e.g. *Safebook* (L. Cutillo et al., 2009; L. A. Cutillo et al., 2010) and *Databox* (Mortier et al., 2016). In the context of applying speculative artefacts in design research, ChoiceBox finds inspiration in *design fiction probes*, specifically *Hawkeye* (Noortman et al., 2019), although no physical artefact was created in this study.

Method

In the study, groups of participants took part in a design session according to the *ChoiceBox* speculative enactment (see previous section). In these sessions, participants sketched three wireframes for three respective clients of the fictional WOWH design agency. After each design iteration, participants discussed their choices in the context of privacy and the GDPR. The session concluded with

a final discussion on more general topics involving privacy, the GDPR, ethics, tools, and designers' responsibilities. The process is summarized as Figure 3.

Participants

The study was conducted in nine design sessions, each with 3-5 designers (see Table 2). The general inclusion criterion was to have a creative disposition in a design-related field. While consideration was given to including end-users as participants for the study, the commonality of consent notices (which was confirmed by all participants) made all design participants equally knowledgeable as end-users. The participants consisted of 12 BSc students, 13 MSc students, 5 PhD students, and 3 professional practitioners, all affiliated with Eindhoven University of Technology in the Netherlands. Participants were recruited via word-of-mouth and were not compensated for their participation. The participants were segmented into groups of (under)graduate students, PhD students, and professional practitioners, in order to study whether participant expertise and skill was a contributing factor in designing

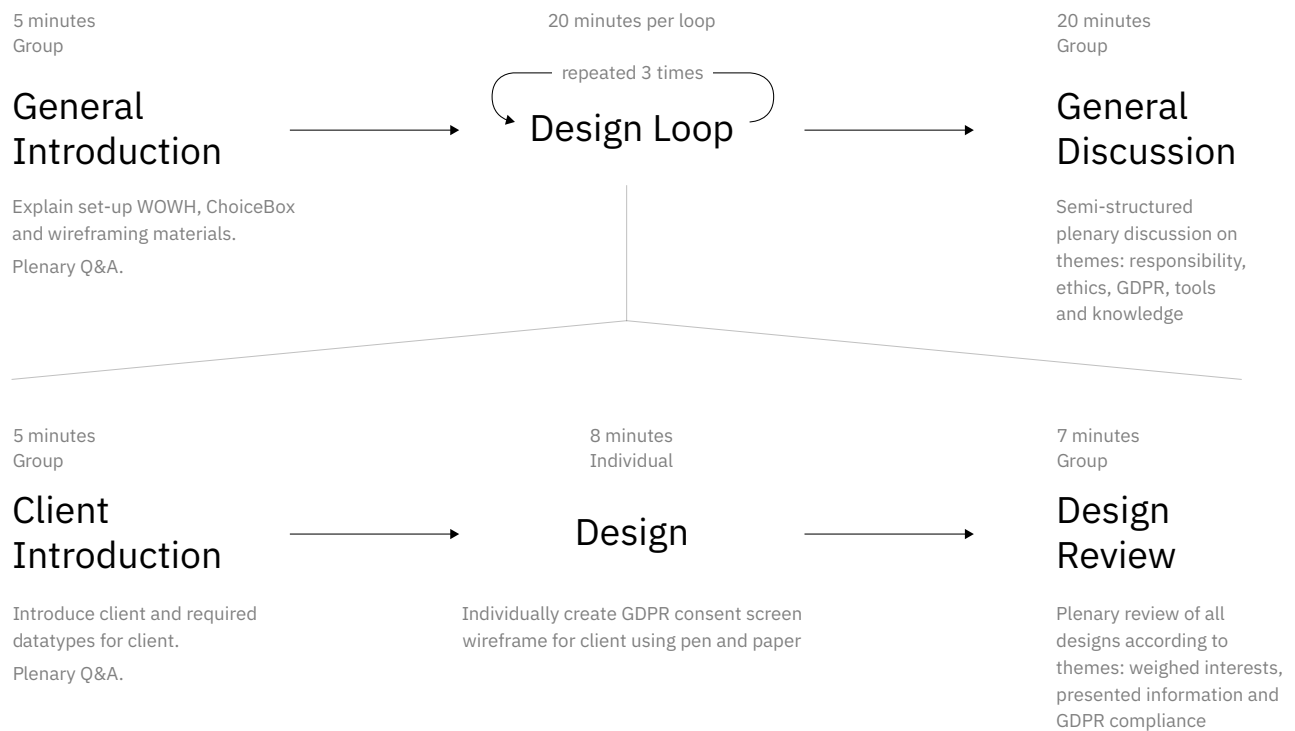


Figure 3. Schematic overview of how design sessions were conducted.

Table 2. Overview of design sessions that were conducted with participants, including participant backgrounds and pseudonymous participant codes (drawn from Greek mythology).

Session #	Background	Participants	Participants' Codes
1	BSc Students	3	Athena, Ananke, Dionysus
2	MSc Students	5	Thalassa, Uranus, Achlys, Thanatos, Phanes
3	BSc Students	3	Themis, Phoebe, Gaia
4	BSc Students	3	Thethys, Aion, Chronos
5	MSc Students	3	Tartarus, Aphrodite, Pontus
6	MSc Students	5	Poseidon, Hera, Chaos, Hyperion, Nemesis
7	PhD Students	5	Zeus, Erebus, Hephaestus, Demeter, Ares
8	BSc Students	3	Artemis, Hestia, Apollo
9	Professionals	3	Theia, Aether, Coeus

for privacy. Before starting a session, all participants signed an informed consent form that detailed the requirements and contents of the study. An ethical approval request for the study was submitted to and approved by the institutional ethical review board.

The sessions were audio and video recorded. After the sessions, the resulting designs were gathered and documented, and the recorded audio and video were transcribed verbatim. The sessions were conducted in English or Dutch, according to the participant composition of a particular session.

According to the scenario, participants were employed on a team of UX designers as part of WOWH, but there was no assumption of different roles between participants. All participants acted as “Junior UX Designers” according to their assignment brief and executed the same brief simultaneously.

The discussions were not explicitly situated in the speculative enactment, but rather took place outside it, as general inquiries related to the study.

Creative Materials

In order to facilitate rapid iteration in the sessions, and so as to be able to spend time equally on design and discussion activities, additional materials were created for this study. Firstly, an A3 paper template was created which featured the outline of a smart phone screen and a background marker paper pattern. This template was created with paper prototyping in mind, due to its capability to generate quick and dirty, divergent designs and accessibility (Sefelin et al., 2003). Participants used these

templates to sketch the elements that are present in a user interface (i.e. wireframing), rather than the exact aesthetics (D. M. Brown, 2010). Additionally, a UI stencil was provided with commonly used UX design elements, inspired by the Apple Human Interface Design guidelines (Apple, 2019) and others (such as <https://fontawesome.com/>; UI Stencils, 2020), as seen in Figure 4.

Experiment Session

Each session lasted for approximately 90 minutes, and was divided into three phases: introduction, design, and discussion. In order to ensure consistency and minimize researcher influence on the study, a protocol was drawn up with specific instructions for the researcher. Besides addressing practical issues such as required materials, spaces, and activities, it also included a minute-by-minute timeline of events as they were to occur during the session. Lastly, it included unambiguous instructions for conducting discussions, detailing which prompts and questions were to be put forward.

Introduction Phase

During the introduction phase, participants were presented with ChoiceBox and their employment with WOWH (see Figure 5). The researcher answered any remaining questions, for which most answers could be found in the existing briefs.

Design Phase

Afterwards, the first client and their specific data requirements were introduced through a client scenario brief. The requirements were to be implemented using fictional web applications which required access to specific data points that would be available from an end-user's ChoiceBox. The client scenarios were communicated through a data specification A4 sheet (e.g. see Figure 6). Any questions about the client scenarios were answered, after which participants spent 7-8 minutes designing a screen for a given client scenario, using a provided sheet, color pens, the stencil for common UX elements (see Figure 4), and a booklet containing GDPR guidelines, made by the UK's Data and Marketing Association (Data & Marketing Association, 2017). The stencil and GDPR booklet were added after a pilot study, in which time spent on getting designs right and speculating on the GDPR prevented in-depth discussions on the designs and their implications.



Figure 4. The UX stencil and design sheet shown in use.

Employment Details

You are employed by WOWH Studio, a design consultancy that is focused on building applications and platforms for its plethora of clients. It is headquartered in Eindhoven's Strijp-T, a former industrial area, repurposed as a business district. Your role within the company is that of **Junior UX Designer**, a position that you have held since joining the company, three years ago. You are situated in a team, with three other Senior UX Designers, and you report to the Product Owner, Oscar Meyernie.

Wireframing

In this position, you are responsible for making the designs of web and mobile applications. You do this by first making paper wireframes, and then visually designing and mocking up the interactions, in e.g. Adobe XD.

For your current assignment, you are designing the privacy interfaces for a number of clients. The first step in this is to do the paper wireframes. The most important thing for paper wireframes is to design the content, instead of the graphics. Think of a wireframe as a blueprint for an UI Design. For instance, it is important to know where the buttons of your application are located, and what text is on the buttons, but the color and shape of the buttons are unspecified.



Example of a Paper Wireframe
Design by Samuel Adaramola

WOWH

ChoiceBox

Figure 5. Sheet detailing participants' employment with WOWH.

Jobby Specification

Jobby is a job placement site, which is designed to make finding your new job easy as pie. We do this by creating a detailed profile of you. Our algorithm extracts skills, knowledge and other parameters set by employer to match you with your dream job. Instead of writing cover letters and applications, Jobby will match you to your perfect job and starts a personal trajectory with this company. There, you'll get an interview in the same week. We focus explicitly on making sure you find a workplace that suits you in combination with your dream job. With our extensive database of jobs, we have the job that matches your personal situation perfectly!

The process is free for applicants, and is paid for by the companies who are filling a position. We need to have access to as much data as is available, to make sure that our algorithm can find a perfect match.

Data Needed

- | | |
|-----------------------------|---------------------------|
| • Name | • Marital status |
| • E-mail address | • Diplomas and grades for |
| • IP Address | • High school |
| • Employment history | • Higher education |
| • Previous job applications | • Vocational Education |
| • Income history | • Training |
| • Birth date | • Union membership status |
| • Sex | • Religious affinity |



ChoiceBox

Figure 6. Sheet detailing Jobby background and data processed.

Afterwards, the participants presented their designs to the group, and annotated the user interactions. Lastly, the participants were encouraged by the researcher to discuss the user-centeredness, information presence, and GDPR-compliance of their designs. Additionally, perceived invasiveness and legality were discussed in the latter two client scenarios (*Budget.me* and *Jobby*).

This loop of introduction, design, and review was repeated three times, for each of the three scenarios. The scenarios gradually increased in data complexity and amounts, as the applications were scripted to operate closer to the limits of what is permitted by national and European law.

Discussion Phase

At the end of the session, the larger implications of the work the participants had done was discussed. Again, this discussion was often initiated by participants according to their and others' work. The discussions were conducted as semi-structured group interviews. Additionally, the researcher posited the following set of questions to the group (if these points had not already been brought up by the participants):

- Should designers be the ones that make decisions like these [ethical judgements on businesses]?
- Should designers be implicated in [the practice of] *Privacy by Design*?
- What do designers need, in order to make better decisions in this space [dealing with GDPR and making ethical judgements]?
- Do you consider yourself to be (professionally) privacy-literate in the legal sense?
- How do you balance commercial and ethical interests [as a designer]?

Analysis

Through the collected designs and discussions, we explore further how the designers in these sessions came to their designs and conclusions. In analyzing the results from the sessions, the designs and the discussions are treated separately. Firstly, the designs are judged and analyzed on their qualities in relation to privacy, the GDPR, and dark patterns, in order to establish what

the output of their design process was. After this, the discussions are analyzed for themes by means of reflexive thematic analysis (Braun & Clarke, 2006, 2019) in order to establish the underlying cognitive processes and choices.

Design Analysis

All 99 designs were analyzed and coded by the researchers in three phases. Firstly, all chosen UI elements and interactions were documented and coded according to various categories: UI elements, interaction, inclusion of ChoiceBox technology, and a meta/miscellaneous category for codes that fit multiple categories (or no categories at all). The first set of codes was developed following a familiarization pass of the generated designs, after which a set of themes was established. Additional codes were then added to the themes during the coding process as necessary. The coding proceeded in further iterations until all artefacts were judged against the same set of codes. The final set was visualized and reviewed by another researcher.

Secondly, all designs were subjected to a qualitative content analysis (Neuendorf, 2017) for compliance issues, using guidelines described by Nouwens et al. (2020). Lastly, both aforementioned phases informed a similar analysis for dark patterns in the designs, using the guidelines put forth by Gray et al. (2018). While most patterns were clearly worded and identifiable thanks to both excellent guidelines (e.g. preselection, not all data processors listed), others were much more ambiguous (e.g. *toying with emotion*, or "*sharing more information about yourself than you really intended to*" (Gray et al., 2018, p. 4)). To combat this, we established particular tells (such as not mentioning third parties for *listing all data processors*, or opt-out interfaces for *privacy zuckering*). These tells were based on examples provided in both guidelines, as well as our earlier codes. However, this analysis remains imperfect, as not all scenarios include the possibility for infraction (e.g. *listing all data processors* in *Jobby*), and thus we could not account for progressive insights in the duration of the session during the analysis. Furthermore, the consulted frameworks contained a limited sample of examples and are thus by no means an exhaustive means to identify compliance issues and dark patterns, especially if the participants contrived novel patterns of their own accord.

Table 3. Prevalence of compliance issues and dark patterns in the 99 designs made by participants.

Instance of compliance issue / dark pattern		Planarr	Budget.me	Jobby	Total
Compliance Issues	Not all data processors listed	27 (82%)	23 (70%)	0 (0%)	50 (51%)
	Inclusion of contentious data	0 (0%)	0 (0%)	15 (46%)	15 (15%)
	Involuntarily given or ambiguous consent	4 (12%)	4 (12%)	0 (0%)	8 (8%)
	No purpose limitation	0 (0%)	0 (0%)	1 (3%)	1 (1%)
Dark Patterns	Privacy Zuckering	27 (82%)	23 (70%)	1 (3%)	51 (52%)
	Preselection	4 (12%)	4 (12%)	0 (0%)	8 (8%)
	Hidden Information	0 (0%)	0 (0%)	4 (12%)	4 (4%)
	Toying with emotion	1 (3%)	1 (3%)	0 (0%)	2 (2%)

Compliance Issues

All designs were scrutinized according to GDPR compliance and other compliance issues. Nouwens et al. define categories of guidelines, particularly in the context of consent: (1) that consent is freely given and unambiguous—implicit or opt-out consent offers no legal basis for consent; (2) that consent is specific and informed—“users must consent in relation to a particular and specific purpose for processing data,” and also that consent is invalid unless all processors are explicitly named—“having to navigate further to third party websites to reject tracking is non-compliant”; and (3) that data protection is efficient and timely (2020, p. 2). More specific guidelines were included (on e.g. visual equivalence, cookie walls, withdrawing consent) and reviewed in the analysis, but not found to apply for any of the participants’ designs.

Additionally, the third client scenario (Jobby) included a request for a user’s religion and union membership. The GDPR considers these two types of data of a special category of sensitive data, and imposes strict additional requirements (e.g. lawful condition, no other reasonable way of achieving purpose, limited use in automated decision making) for the processing of this data (European Parliament, Council of the European Union, 2016). Whether these requirements can be satisfied by the application is deeply contentious, and as such, the inclusion of said data types in interfaces can be described as contentious as well.

Validating the designs against these guidelines (see top half of Table 3), we conclude that a majority of designs violated the requirement for listing all data processors. *Planart* and *Budget*. *Me* included third parties who served targeted advertisements and purchased bulk user data, respectively. Few designs listed these uses of data explicitly in their designs. While *Jobby* did not include a third-party processor, nearly half of participants did include requests for the previously described contentious data in their designs. Lastly, eight designs featured opt-out consent, violating the requirement for freely given and unambiguous consent. A single design clustered multiple data types in such a way that no consent could be given for them individually, which violated purpose limitation.

Dark Patterns

Gray et al. establish a series of guidelines to recognize and categorize dark patterns, based on earlier work by Brignull (2011), broadly distinguishing five categories of dark patterns: (1) nagging: redirection of expected functionality; (2) obstruction: making a procedure more difficult than necessary; (3) sneaking: hiding or disguising relevant information; (4) interface interference: manipulation that privileges certain actions over others; and (5) forced action: the requiring of an action to access some functionality (Gray et al., 2018). All individual patterns were evaluated against the submitted designs.

Firstly, Privacy Zuckering—tricking a user into sharing more data than they intended to (i.e. forced action)—was established in a majority of designs, especially in the first two scenarios. This relates to the compliance issue of unmentioned

data processors, where the absence of notice of third-party processing can be interpreted as a dark pattern of the *forced action* category, which was present in 51 designs. The automation of a user choice, for instance through pre-selection of a consent checkbox, is established as a dark pattern of the *interface interference* category, which was present in eight designs. Thirdly, hidden information—options or actions relevant to the user but not made immediately accessible—was found to be present in four designs, but only in *Jobby*. This was linked to grouped data types where particularly sensitive data types were not immediately visible for the user. This is considered to be a dark pattern of the *interface interference* category. Lastly, two designs were found to be toying with emotion—evoking emotion to persuade a user into a certain action. In this case, participants used language such as “Hell Yeah” to indicate one preferred option over another. This is considered to be a dark pattern of the *interface interference* category, within the *aesthetic manipulation* subcategory.

UI Elements and Interactions

Additionally, all designs were analyzed for common and uncommon UI design patterns. Particularly interesting (but uncommon) positive patterns were identified, such as explicitly showing (an example of) the data to be shared, independent user ratings for privacy practices, indicators for the amount of risk associated with sharing certain data types, drag-and-drop sorting data types, and giving consent for individual data points. Various other interaction styles such as chatbots, assistants, and Tinder-style swiping cards signaling consent were also present in designs. Negative novel approaches featured large checkmarks indicating GDPR-compliance (most designs were in fact non-compliant) or opaque grouping of data types. These might be classified as dark patterns in their own right—Gray’s Aesthetic Manipulation and Hidden Information, respectively. This hints at a wider gamut of Privacy UX issues than compliance alone.

Analysis of the Discussions

The resulting transcripts of the discussions were analyzed by one researcher for recurring comments, friction, struggles, opinions, and process thoughts. All non-discussion parts were excluded from analysis. The researcher became familiar with the data through manually transcribing and reviewing the discussions. Individual excerpts were then coded, after which themes were established that contained loosely grouped codes.

The themes were conceptually centered around the idea of designing privacy-conscious consent. Hence, we established that most themes loosely following the setup of the design review, with the questions described at the end in *Discussion Phase* being a major influence. The initial themes thus followed the ethical mediation (Gray & Chivukula, 2019) that was at the center of the speculative enactment. The preliminary themes were then reviewed by a second researcher, after which a final set of themes was established. These themes were then substantiated with participant quotes.

GDPR

Legislation, particularly the GDPR, affects new designs that are being made, but who bears responsibility for implementing legal boundaries in design? Who interprets what the GDPR means for design practice, and are those people designers? There is room for some interpretation in the GDPR, yet there is also an abundance of clear requirements, particularly when it comes to consent. If participants are not aware of these requirements, how can we expect them to be followed? This was recognized by participants when they found practical information to be lacking, or found the provided information (the GDPR checklist) overwhelming. Participants remarked that they were familiar with the law, but not with how the practice related to design. In contrast, a minority of participants (<5) were familiar with how the GDPR affected UX Design.

On multiple occasions during the discussions phase, participants were asked whether they felt their designs conformed to the GDPR, based on their understanding and available information. Most discussions centered on the use of on-by-default or off-by-default toggles and switches, with few participants initially realizing that their designs were not compliant. Inconsistencies with design practice or even systems practice were also pointed out by participants.

Gaia: I think in my case I actually do fulfill most of them except “we told individuals they could refuse consent without detriment”. [...] In some cases, you do need that function, or that feature needs that data.

Thanatos: [...] for instance, [the checklist] says “we use clear, plain, easy to understand language”. Well that can be the case, but if there are three pages of clear, plain, easy to understand language, it can be that easy, but still, no one will read it.

Another set of remarks was made regarding the disconnect between the law and current practice, particularly in cookie consent screens:

Hephaestus: Frankly, I’ve seen looser consent pages after the GDPR, so I think it’s fine. [...] I’ve seen ones [that] are worse.

Demeter: I agree.

Hephaestus: Right? If they’re working, then mine should work too, right?

Researcher: So, is it then OK?

Hephaestus: By speculation, yes. Yeah.

This particular stance on the GDPR, namely, looking at what is happening in the field instead of referring to the legal framework, was shared by other participants (about one fifth). Despite differing opinions on the GDPR, its enforcement, and whether it was necessary to apply it to the work, nearly all participants were eventually able to distinguish compliance when following the provided checklist.

Thanatos: I feel like the law should give me some kind of backup as a designer. Since I try to do the right thing for the user.

Data Sensitivity

Some data, e.g. financial data, can be considered to be more or less private than other types of data. Some types of data, such as race and gender, are explicitly protected from processing by the GDPR. How does this heterogeneous sensitivity of data affect designs? And who decides what is considered to be sensitive data?

As the analysis of the designs shows, opt-in and temporary sharing increased in usage after the first scenario. The most common explanation related to the sensitivity of data in the second and third scenario, most notably for financial data, sex, grades, and marital status. Participants also created measures that addressed the sensitivity of these types of data, for instance by adding explicit risk indicators or warnings.

Ares: [on financial data] I think it’s very private information. For example, if you have a t-shirt on saying how much money you have on your bank account. [...] it would give some funny situations.

[...]

Hephaestus: There’s things I own [that] I don’t necessarily need my parents to know.

Some participants took on user perspectives while reviewing their designs and practices, and some took issue with the algorithmic handling of some of the data.

Themis: [...] if they search for one with certain skills, then it shouldn’t matter what sex I am. It’s [...] because I’m female. We are often [disadvantaged because] of that.

Almost all participants were able to judge how their designs affected end-user choice, with some even explicitly suggesting that dark patterns be incorporated as a thought experiment. Moreover, some participants were also aware of the complex nature of how algorithms use data to make decisions, a key modern frustration (Upchurch, 2018).

Responsibility

If designers have an influence on the side effects of their designs, then what are the major drivers for making choices directly related to these side effects? Moreover, where lies the allegiance of a designer, and who is ultimately responsible for the design and its implications?

On one end of the spectrum were designers who stressed the individual designer’s responsibility for providing the end user with an honest presentation at all times. They considered the awareness of existing requirements and the implications of their designs as an inherent aspect of designing, and acted accordingly. There was an acknowledgement of privilege in raising these issues with employers, and yet some emphasized that raising these issues was the least that one could do.

Chronos: As a UX Designer building for these systems, I take no sympathy in it if you didn’t know. Because that is part of the homework you do. [...] people rely on it blindly. With that much power comes responsibility.

On the other end of the spectrum were participants who stressed that the responsibility lies with the organization, and that designers should stick to doing their jobs. They shared the belief that one should change jobs if the values of an organization are misaligned with one's own values regarding individual responsibility.

Uranus: I don't know if you need to put the responsibility with the designer. [...] speaking for myself, I would probably not do a deep dive in the ethical implications of my design. [...] Of course, as a designer, there is some ethics, but it is up to the company what they can and cannot use in their operations.

Demeter: But I think you explicitly put us in it in a junior role [...] so I would say "do your job", which is to get [...] as much consent as possible. So within that boundary, as a designer you should make it as interesting as possible to get, as long as the people outside that box agree with the boundaries that they set [...], otherwise I would say you would reject [the job].

Naturally, most participants took a more balanced and nuanced stance towards responsibility, emphasizing both an awareness of the implications of their designs, as well as the limits of a Junior UX Designer's agency.

Gaia: So I think honestly if I were just designing to pay the bills. There is like, Okay. Yeah, this is a skill I have. So let's use it and the company wants this, so okay.

A particularly interesting discussion occurred regarding whether it was okay to include warnings in a design as a means of indicating a lack of comfort with a design, rather than just walking away:

Aphrodite: You could say "it's not GDPR-compliant and thus we won't do the job", but then the job goes to a company with looser morals. I find that I am taking more responsibility by pointing out the issues to an end-user. [...] because otherwise the problem does not become smaller in this world.

In the end, most participants agreed that while it is hard for a designer to 'change the world', one can at least recognize and point out issues with a design to employers and clients.

Knowledge

If there are strict requirements, for instance via the GDPR, that are part of the design process, who bears responsibility for making sure these guidelines are followed? Is knowledge of these guidelines required to be a UX designer?

Since the GDPR checklist was quite heavily used as a reference during the design sessions, it is implied that at least some sort of tool is required to help designers determine compliance. Participants provided varying responses to questions about whether they possessed the right knowledge to be able to create UX designs.

Chronos: From a GDPR perspective I don't know what's legal [...]. I don't know if employers are allowed to ask that. [...] there are some things that just, could straight up be discriminatory...

One common topic was education, which makes sense given the demographics of the participants. Some participants said they would appreciate a course focused on the legal and ethical aspects of design, and indicated that in the event that they had already taken such a course, it was too generic to be applied in practice.

Another common theme was that there should be an organization which provides the knowledge and tools (such as a checklist) to help designers with Privacy UX issues. This organization was imagined to be either an 'authority', i.e., a governmental body at the national or European level, or a non-profit, as envisioned in the ChoiceBox enactment. The latter was mentioned often as a good source for this knowledge given the tight coupling of policy to technology, creating actionable design guidance.

A final theme was whether designers should be the ones making legal judgements. While most participants found that, at a surface level, this should be the responsibility of a legal department within an organization, it was also clear that this would be unattainable for smaller businesses or individual designers. Some participants deferred responsibility for this legal judgement to the client.

The Economic Value of Transparency

Participants remarked that when asked how they would defend their designs, being considered privacy-friendly has value for a business, and might attract a larger userbase than a privacy-hostile business. Participants argued that this is one way to rationalize privacy-friendly designs in a commercial context.

Researcher: You have added three toggles before you can give permissions to use financial data. Why is that?

Coeus: Because I know that the user cares. The user will not appreciate it being hidden away. I am convinced it is better to be transparent about it, because you will gain trust with the user and then they are more inclined to give access to their data.

Coupling between features and data in particular was mentioned quite often in discussions as a mechanism for showing the user that they have control over what happens with their data. However, this approach does pose some questions as to whether this practice would be compatible with the current reading of the GDPR.

Participants also used the argument of 'sunk costs' to rationalize investing in Privacy UX: since companies must comply anyway, they might as well do it right, and reap privacy consciousness as a marketing benefit. Prior work in design, marketing, and psychology supports this view: perceived online privacy influences user behavior positively towards privacy-aware businesses (Foxman & Kilcoyne, 1993; Tang et al., 2008; Tsai et al., 2011; Udo, 2001).

Aether: I wonder if it's allowed to positively stimulate to tick boxes. Because I think that it could be very easy to sell this [as a designer] to Jobby, because they get the chance to incorporate a process that they likely see as a tedious requirement fully into their service.

When summarizing these findings, we find participants naturally addressing not only the designed product, but even more so the process of design and its implications. We find examples of practical problems as well as institutional issues that are an inherent part of Privacy UX design. Consequently, we wonder how we can foreground and resolve the presented dilemmas from macro and micro perspectives.

Discussion

We discuss the role of ethics in design and subsequently its relation to experience and the knowledge required to make ethics work in practice. Similarly, we discuss the knowledge and interpretation that designers might require of the GDPR. Lastly, we propose ways of disseminating this knowledge through tools and experiences, such as the ones used in (or created for) this research, and more broadly speaking, in design research.

(Un)Ethical Design

All participants have previously signed and are bound by the Netherlands Code of Conduct for Research Integrity (Algra et al., 2018), which is a code of ethics for students and researchers that explicitly lists data processing and GDPR conformance as a mandatory aspect of professional conduct. Thus, the participants are required to create designs that take into account end-users' best interests, and must be aware of the legal requirements applicable to their designs (Algra et al., 2018, p. 28). It bears noting, however, that such requirements often exist as formalities, rather than being explicitly enforced.

This research shows that once participants are familiar with previously identified issues, most can eventually assume a position of critical judgement towards the legislation. This is evidenced by the increasing adoption of opt-in throughout the scenarios. Apart from this, some participants raised concerns about the impact of algorithms and risks of data sharing. Participants were retroactively able to describe whether their designs took user interests to heart, while others chose not to do so in spite of this knowledge (e.g., Demeter and Gaia in *GDPR*). The number of compliance issues confirms this. Some participants offered excuses as to why they were unable to act ethically, citing clients who are unwilling to budge on requirements or a responsibility to their employer to "do as they're told". However, justifications such as "everyone's doing it" or "we have to run a business" are insufficient for unethical, incompliant, or illegal work. While designers cannot be held universally responsible for unethical designs, designing ethically (or at the very least remaining compliant within the applicable legal frameworks) should be the norm that each designer aspires to as a professional.

The inclusion of cues from a fictional design company also demonstrates the ethical mediation acted out by the individual designers. Despite the clearly fictional design context of ChoiceBox, the participants engaged in unethical designs. Considering that no pressure was applied to participants to design incompliant designs, this effect could potentially be much larger

in (commercial) practice. This characterizes Privacy UX as an ethically complex issue as regards design. Fortunately, this offers opportunities to challenge and change the Privacy UX status quo, for instance through design leadership and evangelizing UX practices to stakeholders and practitioners alike (Gray et al., 2015).

Ethical Knowledge and Experience in UX Design

For most participants in this research, choices were more attributable to a lack of training and experience than ill intent. This means that the design community will have to seek better ways of educating modern designers about ethical issues, their responsibility, and viable approaches in order to prepare them for the challenges of daily design practice. Some participants mentioned having taken ethics courses during their education, but found the content misaligned with their practice, and ultimately ineffective.

We should create better tools for ethical education, for which the ChoiceBox scenario could be used as a starter. Engaging students through speculative enactments and scenarios, and running them through lively experiences involving grey areas in design, could help students explore their own ethical boundaries, rather than being lectured on a black and white perception of reality. It is key that individuals be confronted with ethical challenges and realize that their intuitive judgements may be insufficient to guide the ethical implications of their designs. Under further pressure from the design status quo and ill-intentioned stakeholders, they are finally given an opportunity to reflect with more experienced sparring partners. This process prepares students to recognize where their own ethical lines should be drawn, and should reduce the likelihood that such lines are crossed—in contrast to the existing process, which students may find overwhelming. Gray, Chivukula et al. have previously highlighted that "awareness [does] not consistently result in ethically-sound decisions, underscoring the need for more pragmatically-focused ethical training in computing education" (2021, p. 237). We see ChoiceBox as a helpful starting point in giving shape to such goals.

Lastly, extending the scope of design practice, designers should also be aware of how data processing and algorithms affect user experiences, particularly when the algorithm suggests the possibility of enhancing current biases (Chen et al., 2019; Hajian et al., 2016; Obermeyer & Mullainathan, 2019).

Disseminating GDPR Knowledge among Designers

Governmental agencies, such as the Dutch Data Protection Authority, offer more materials to help understand the GDPR (Autoriteit Persoonsgegevens, n.d.), but they focus on system perspectives, not necessarily on UX. While practical advice is certainly helpful in designing these interfaces, these tools tend to overlook the macro perspectives on designing for privacy, e.g. the transparency and consent that are the backbone of privacy by design.

Therefore, we conclude that there is a broad established need to have accessible tools and resources for UX designers—and perhaps even designers in general—that will allow them

to navigate the legal and ethical implications of designs that process data, from both macro and micro perspectives. This will require careful consideration of these laws, given some practical inconsistencies (e.g. applications that cannot run without some data), while leaving room for promoting the values in the GDPR. Given that the GDPR offers handles for designers when justifying user-centered design decisions, there could be a greater focus on it (or related laws) in design curricula and practice. Using jurisprudence as a basis for incorporating values in design is an active topic of research in HCI, and we see this as a welcome addition to its practice (Kirkham, 2020).

Role of Speculative Enactments

Another positive aspect of the use of speculative enactments was its ability to prompt reflection on the part of the participants. Multiple engagements with participants show a reversal of their initial positions or a distancing from previous designs (such as *Ares* and *Themis*) after confronting certain issues. Some even used the canvas provided by ChoiceBox to comment on privacy on a more institutional level, seeing ChoiceBox as a potential institutional entity focused on resolving the practical legal and ethical issues that the designers encountered.

Enacting a speculative portrayal of designing for consent helps designers explore the grey areas in which designers work, rather than resorting to a black and white picture of ethics. This quality has been noted before by Wong et al. in a similar approach using design workbooks (Wong et al., 2017), but also in the use of speculative enactments with professionals and designers, thus prompting institutional reflection in the field of HCI.

In this respect, we see ChoiceBox as a tool through which designers engage with their preconceptions about what privacy means for them and how they deal with it. The speculative nature of ChoiceBox mediates and moderates this challenge precisely because of the ambiguity inherent in determining how privacy should be handled in design. Moreover, as an *ethical mediation*, ChoiceBox facilitates personal and institutional reflection that precedes change.

As far as success factors for a Privacy UX speculative enactment are concerned, we see particular value in specific requirements described by Elsdén et al (Elsden et al., 2017). We view *diegetic work* (i.e. materials and circumstances) as crucial for participants to meaningfully engage with the premise of the enactment, and we see potential for improving on *ChoiceBox* in many ways (e.g. situation in an office, involvement with stakeholders, actual prototypes, etc.). In this respect, we also value (un)intentionally incorporating conflict in the constructed future (e.g. *how did ChoiceBox end up extensively processing commercial consent requests and what are the consequences?*), given that such conflicting situations and values characterize the present as well. Finally, we highlight the value of group discussions in the *afterglow* (Lindley et al., 2014) of the enactment. Having participants discuss implications of designing for consent is much more valuable in the context of choices *they made*, rather than choices *they could possibly make*, in a time and space far away from now.

Privacy is a UX Problem

The wording of the GDPR as well as the court hearings on UI implementations (*VZBV v. Planet49*, 2019) put privacy firmly in UX territory. Similar research has consistently made such connections (Gray, Santos, et al., 2021; Utz et al., 2019). While these obligations are less practical for most design practitioners because of their formulation, translations from legalese to design guidelines have been and continue to be made (Autoriteit Persoonsgegevens, n.d.; Data & Marketing Association, 2017; Schaub et al., 2018), mostly in the form of checklists. These works are indispensable as all designers are confronted with privacy issues in their work, most notably in the form of GDPR consent notices. We also stress the relevance of recent research on *bright patterns* (contrasting *dark patterns*), which highlights broader alternatives to the Privacy UX status quo (Graßl et al., 2021).

At the same time, we must acknowledge that setting the bar for privacy as low as what is required by law ignores the role designers can play in addressing privacy issues, thus doing them a grave injustice. Contrarily, the GDPR is full of values and aspirations (e.g. privacy by design) for which design practice is exceptionally positioned to support through means such as value-sensitive design (Cummings, 2006; Friedman, 1996) and co-design (Steen, 2013; Steen et al., 2011), amongst other methods. While the concept of human-centered design may have fallen out of favor in recent years (Forlizzi, 2018), our inability to get simple consent interactions right shows that designers need to better engage with its principles. When it comes to tools that make Privacy UX work more feasible, we strongly suggest going beyond the letter of the law and targeting the values behind legislation such as the EU GDPR, Brazil's LGPD, Australia's Privacy Amendment, Japan's Act on Protection of Personal Information, California's CCPA, and many others.

Similarly, we stress a recognition of responsibility on the part of designers to care for the moral and legal obligations of privacy. The design research tradition of speculation is especially valuable. We contribute and recommend speculative enactments, like ChoiceBox, as a way of confronting the legal and ethical issues inherent in privacy in a lighthearted, open-ended fashion, thus providing designers with experience in dealing with these issues. Given the intensive involvement with the ChoiceBox sessions, we specifically advocate for the inclusion of such tools in design education as a means of preparing prospective designers for privacy work in practice.

Lastly, handling privacy poorly is bad for business, with incompliant data becoming a toxic asset in the near future. Designers are in the best position to investigate what makes a privacy-aware business work, e.g., through experimenting with feasible business models through service design (Forlizzi & Zimmerman, 2013). This particular suggestion has been made in the context of HCI research and practice before, and we aim to build upon it by providing further implementation details related to Privacy UX. We call upon the HCI community to further investigate which tools are necessary for improving the state of Privacy UX, not only in the form of methods and guidelines, but also in concrete use cases embedded in practice.

Limitations

While the participant group was quite diverse in terms of experience and UX design expertise, the group was more homogenous in terms of age (18–32), and the surveyed population was native to the Netherlands. The stencil and template used in the study might have limited and influenced participant behavior and designs. As the use of the stencil was optional, and the included elements are deemed standard, we consider this influence to be small, especially given that some participants created UI elements which deviated from the stencil. More generally, the practice of speculative enactments usually calls for appropriate settings, materials, and cultural probes (Elsden et al., 2017). However, in view of the goals of the design sessions—namely the ethical and legal aspects of Privacy UX—we decided to focus our efforts on the scenario, rather than props and environments, even though they may have contributed to a more immersive experience. Furthermore, the design tasks were quite short (7–8 minutes per task). While other researchers often take longer for such tasks (e.g. 45 minutes (Gray, Chivukula, et al., 2021)), we saw value in keeping tasks short in order to allow participants time for discussion and reflections between design tasks, and we consequently designed tools that made such short design iterations possible. Additionally, not all participants may have treated the exercise seriously given its speculative nature. This may have resulted in designs that deliberately tested limits. Although this might seem to counteract the purpose, as a matter of fact, it does not: deliberately testing boundaries can be a powerful way to better understand the boundaries themselves and creatively explore them in the process. Lastly, the group-focused discussion might have favored more vocal members. This risk was taken deliberately to encourage the joint reflection that is, perhaps, the hallmark of ethical mediation.

Conclusion

In this paper, we have studied the concept of Privacy UX, i.e., the attitudes and design patterns that are needed for the design of privacy-sensitive interfaces, through a speculative enactment exercise in which 33 students and professionals participated. *ChoiceBox* is a scripted design exercise based around designing privacy-sensitive UX in the context of three data sharing scenarios using GDPR consent notices. The results show that designers are complicit in enacting dark patterns in Privacy UX. Additionally, designers are often unaware of the effects that new legal privacy-protecting frameworks such as the GDPR have on their practice. *ChoiceBox* as a speculative enactment can raise designers' awareness about the conflicts of interest that are inherent in the day-to-day of UX practice. We see this as a promising application in practice and education. We invite the design community to take these issues to heart and acknowledge the role designers play in privacy issues—there is power in being complicit.

Acknowledgements

A heartfelt gratitude is extended to all participants in the study, for their thorough and engaging discussions. These insights would not have been possible without your cooperation. Moreover, we

would like to thank both Arnout Terpstra (SURF) and Renee Noortman (TU/e) for their involvement in shaping the ideas that are expressed here; we have greatly enjoyed your expertise in designing for privacy and design fiction, respectively. Further thanks for reviewing this piece go out to Joep Frens, Yaël van Engelen, and Seiji Bernabela. Finally, we thank the reviewers at IJDesign for their valuable feedback and thoughtful remarks.

References

1. Albrechtslund, A. (2007). Ethics and technology design. *Ethics and Information Technology*, 9(1), 63–72. <https://doi.org/10.1007/s10676-006-9129-8>
2. Algra, K., Bouter, L., Hol, A., van Kreveld, J., Andriessen, D., Bijleveld, C., D'Alessandro, R., Dankelman, J., & Werkhoven, P. (2018). *Netherlands code of conduct for research integrity 2018*. Koninklijke Nederlandse Akademie voor Wetenschappen. <https://www.vsnul.nl/files/documents/Netherlands%20Code%20of%20Conduct%20for%20Research%20Integrity%202018.pdf>
3. Apple. (2019, October 4). *Human interface guidelines*. <https://developer.apple.com/design/human-interface-guidelines/>
4. Ayalon, O., & Toch, E. (2019). Evaluating users' perceptions about a system's privacy: Differentiating social and institutional aspects. In *Proceedings of the fifteenth symposium on usable privacy and security* (pp. 41–59). USENIX Association.
5. Bannon, L. J. (1995). From human factors to human actors: The role of psychology and human-computer interaction studies in system design. In R. Baecker (Ed.), *Readings in human-computer interaction* (pp. 205–214). Elsevier.
6. Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
7. Berner, A., Seyfried, M., Nordenskjöld, C., Kuhberg, P., & Shklovski, I. (2019). Bear & Co: Simulating Value Conflicts in IoT Development. In *Extended abstracts of the SIGCHI conference on human factors in computing systems*. ACM. <https://doi.org/10.1145/3290607.3313271>
8. Boer, L., & Donovan, J. (2012). Prototypes for participatory innovation. In *Proceedings of the designing interactive systems conference* (pp. 388–397). ACM. <https://doi.org/10.1145/2317956.2318014>
9. Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., & Santos, C. (2019). Security analysis of subject access request procedures: How to authenticate data subjects safely when they request for their data. In M. Naldi, G. Italiano, K. Rannenberg, M. Medina, & A. Bourka (Eds.), *Lecture Notes in Computer Science: Vol. 11498. Privacy technologies and policy* (pp. 182–209). Springer. https://doi.org/10.1007/978-3-030-21752-5_12
10. Borning, A., & Muller, M. (2012). Next steps for value sensitive design. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 1125–1134). ACM. <https://doi.org/10.1145/2207676.2208560>

11. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
12. Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, 11(4), 589–597. <https://doi.org/10.1080/2159676X.2019.1628806>
13. Brignull, H. (2011, November 1). Dark patterns: Deception vs. honesty in UI design. *A list apart*. <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/>
14. Brown, B. (2001). Studying the Internet experience. *HP Laboratories Technical Report*, 49(HPL-2001-49), 1–23.
15. Brown, D. M. (2010). Communicating design: Developing web site documentation for design and planning. New Riders.
16. Brunton, F., & Nissenbaum, H. (2019, September 25). The fantasy of opting out. *The MIT Press Reader*. <https://thereader.mitpress.mit.edu/the-fantasy-of-opting-out/>
17. Buchanan, R. (1992). Wicked problems in design thinking. *Design Issues*, 8(2), 5–21. <https://doi.org/10.2307/1511637>
18. Autoriteit Persoonsgegevens. (n.d.). *Checklist: Houd grip op persoonsgegevens* [Checklist: Keep a grip on personal data]. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/checklist_houd_grip_op_persoonsgegevens_def.pdf
19. Chen, R.-C., Ai, Q., Jayasinghe, G., & Croft, W. B. (2019). Correcting for recency bias in job recommendation. *Proceedings of the 28th ACM international conference on information and knowledge management* (pp. 2185–2188). ACM. <https://doi.org/10.1145/3357384.3358131>
20. Cooley, M. (2000). Human-centered design. In R. Jacobson (Ed.), *Information design* (pp. 59–81). MIT Press.
21. Council Of Europe. (1950). The European convention on human rights.
22. Cummings, M. L. (2006). Integrating ethics in design through the value-sensitive design approach. *Science and Engineering Ethics*, 12(4), 701–715. <https://doi.org/10.1007/s11948-006-0065-0>
23. Cutillo, L. A., Molva, R., & Strufe, T. (2010). On the security and feasibility of Safebook: A distributed privacy-preserving online social network. In M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, & G. Zhang (Eds.), *IFIP advances in information and communication technology: Vol. 320. Privacy and identity management for life* (pp. 86–101). Springer. https://doi.org/10.1007/978-3-642-14282-6_7
24. Cutillo, L., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine*, 47(12), 94–101. <https://doi.org/10.1109/MCOM.2009.5350374>
25. Data & Marketing Association. (2017). *GDPR checklist*. <https://dma.org.uk/article/dma-advice-gdpr-checklist>
26. Davies, H. (2015, December 11). Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users. *The Guardian*. <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>
27. Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy ... now take some cookies: Measuring the GDPR's impact on web privacy. *Informatik Spektrum* 42, 345–346. <https://doi.org/10.1007/s00287-019-01201-1>
28. Electronic Privacy Information Center. (2018). *EPIC - Equifax data breach*. <https://epic.org/privacy/data-breach/equifax/>
29. Elsdén, C., Chatting, D., Durrant, A. C., Garbett, A., Nissen, B., Vines, J., & Kirk, D. S. (2017). On speculative enactments. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 5386–5399). ACM. <https://doi.org/10.1145/3025453.3025503>
30. European Commission. (2019, September 13). Frequently asked questions: Making electronic payments and online banking safer and easier for consumers. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555
31. European Parliament, Council of the European Union. (2016, April 27). Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. <http://data.europa.eu/eli/reg/2016/679/oj>
32. Fogg, B. (2009). A behavior model for persuasive design. In *Proceedings of the 4th international conference on persuasive technology* (Article no., 40). ACM. <https://doi.org/10.1145/1541948.1541999>
33. Forlizzi, J. (2018). Moving beyond user-centered design. *Interactions*, 25(5), 22–23. <https://doi.org/10.1145/3239558>
34. Forlizzi, J., & Zimmerman, J. (2013). Promoting service design as a core practice in interaction design. In *Proceedings of the 5th international congress of International Association of Societies of Design Research* (pp. 1–12). <http://design-cu.jp/iasdr2013/papers/1202-1b.pdf>
35. Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing*, 12(1), 106–119. <https://doi.org/10.1177/074391569501200111>
36. Friedman, B. (1996). Value-sensitive design. *Interactions*, 3(6), 16–23.
37. Gaver, W. W., Beaver, J., & Benford, S. (2003). Ambiguity as a resource for design. *New Horizons*, 1(5), 233–240. <http://doi.org/10.1145/642611.642653>
38. Graßl, P., Schraffenberger, H., Borgesius, F. Z., & Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, 3(1), 1–38. <https://doi.org/10.33621/jdsr.v3i1.54>
39. Gray, C. M., & Chivukula, S. S. (2019). Ethical mediation in UX practice. In *Proceedings of the SIGCHI conference on human factors in computing systems* (Paper 178). ACM. <https://doi.org/10.1145/3290605.3300408>
40. Gray, C. M., Chivukula, S. S., & Lee, A. (2020). What kind of work do “asshole designers” create? Describing properties of ethical concern on reddit. In *Proceedings of the ACM Designing Interactive Systems Conference* (pp. 61–73). ACM. <https://doi.org/10.1145/3357236.3395486>

41. Gray, C. M., Chivukula, S. S., Melkey, K., & Manocha, R. (2021). Understanding “dark” design roles in computing education. In *Proceedings of the 17th ACM conference on international computing education research* (pp. 225–238). ACM. <https://doi.org/10.1145/3446871.3469754>
42. Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In *Proceedings of the SIGCHI conference on human factors in computing systems* (Paper 534). <https://doi.org/10.1145/3173574.3174108>
43. Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Article 172). ACM. <https://doi.org/10.1145/3411764.3445779>
44. Gray, C. M., Toombs, A. L., & Gross, S. (2015). Flow of competence in UX design practice. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 3285–3294). ACM. <https://doi.org/10.1145/2702123.2702579>
45. Guy, A. (2017). *Presentation of self on a decentralised web* [Doctoral dissertation, The University of Edinburgh]. Edinburgh Research Archive. <http://hdl.handle.net/1842/29537>
46. Hajian, S., Bonchi, F., & Castillo, C. (2016). Algorithmic bias: From discrimination discovery to fairness-aware data mining. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining* (pp. 2125–2126). ACM. <https://doi.org/10.1145/2939672.2945386>
47. Hauptert, V., & Gabert, S. (2019). Short paper: How to attack PSD2 internet banking. In I. Goldberg & T. Moore (Eds.), *Lecture notes in computer science: Vol. 11598. Financial cryptography and data security* (pp. 234–242). Springer. https://doi.org/10.1007/978-3-030-32101-7_15
48. Hill, R. (2019, March 14). Year 1 of GDPR: Over 200,000 cases reported, firms fined €56 meeelli... oh, that’s mostly Google. *The Register*. https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/
49. Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), 1–18. <https://doi.org/10.5817/CP2016-4-7>
50. Information Commissioner’s Office. (2014). *Conducting privacy impact assessments code of practice*. <https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf>
51. International Telecommunication Union. (2019). *Measuring digital development: Facts and figures 2019*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019_r1.pdf
52. Kirkham, R. (2020). Using European human rights jurisprudence for incorporating values into design. In *Proceedings of the ACM designing interactive systems conference* (pp. 115–128). ACM. <https://doi.org/10.1145/3357236.3395539>
53. Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the ‘privacy by design’ provision in data-protection law. *International Review of Law, Computers & Technology*, 28(2), 159–171. <https://doi.org/10.1080/13600869.2013.801589>
54. Kozubaev, S., Elsdén, C., Howell, N., Søndergaard, M. L. J., Merrill, N., Schulte, B., & Wong, R. Y. (2020). Expanding modes of reflection in design futuring. In *Proceedings of the SIGCHI Conference on human factors in computing systems* (pp. 1–15). ACM. <https://doi.org/10.1145/3313831.3376526>
55. Langheinrich, M. (2001). Privacy by design—Principles of privacy-aware ubiquitous systems. In G. D. Abowd, B. Brumitt, & S. Shafer (Eds.), *Lecture notes in computer science, Vol: 2201. Ubicomp 2001: Ubiquitous computing* (pp. 273–291). Springer. https://doi.org/10.1007/3-540-45427-6_23
56. Lindley, J., Sharma, D., & Potts, R. (2014). Anticipatory ethnography: Design fiction as an input to design ethnography. In *Ethnographic praxis in industry conference proceedings* (pp. 237–253). Wiley. <https://doi.org/10.1111/1559-8918.01030>
57. Manjoo, F. (2019, September 23). I visited 47 sites. Hundreds of trackers followed me. *The New York Times*. <https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html>
58. Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulmaga, A., & Berners-Lee, T. (2016). *Solid: A platform for decentralized social applications based on linked data* (pp. 1–16). http://emansour.com/research/lusail/solid_protocols.pdf
59. McMillan, S. J., & Morrison, M. (2006). Coming of age with the internet: A qualitative exploration of how the internet has become an integral part of young people’s lives. *New Media & Society*, 8(1), 73–95. <https://doi.org/10.1177/1461444806059871>
60. Mohan, J., Wasserman, M., & Chidambaram, V. (2019). Analyzing GDPR compliance through the lens of privacy policy. In V. Gadepally, T. Mattson, M. Stonebraker, F. Wang, G. Luo, Y. Laing, & A. Dubovitskaya (Eds.), *Lecture notes in computer science: Vol. 11721. Heterogeneous data management, polystores, and analytics for healthcare* (pp. 82–95). Springer. https://doi.org/10.1007/978-3-030-33752-0_6
61. Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, 26(4), 323–339. <https://doi.org/10.1086/209566>
62. Mortier, R., Lodge, T., Brown, T., McAuley, D., Greenhalgh, C., Zhao, J., Crowcroft, J., Wang, L., Li, Q., Haddadi, H., Amar, Y., Crabtree, A., & Colley, J. (2016). Personal data management with the databox: What’s inside the box? In *Proceedings of the ACM workshop on cloud-assisted networking* (pp. 49–54). ACM. <https://doi.org/10.1145/3010079.3010082>
63. Munteanu, C., Molyneaux, H., Moncur, W., Romero, M., O’Donnell, S., & Vines, J. (2015). Situational ethics: Rethinking approaches to formal ethics requirements for human-computer interaction. In *Proceedings of the 33rd SIGCHI conference on human factors in computing systems* (pp. 105–114). ACM. <https://doi.org/10.1145/2702123.2702481>
64. Neuendorf, K. A. (2017). *The content analysis guidebook*. SAGE Publications. <https://doi.org/10.4135/9781071802878>
65. Newman, L. H. (2018, October 12). *Google+ exposed data of 52.5 million users and will shut down in April*. *Wired*. <https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/>

66. Noctor, M. (2018). PSD2: Is the banking industry prepared? *Computer Fraud & Security*, 2018(6), 9–11. [https://doi.org/10.1016/S1361-3723\(18\)30053-8](https://doi.org/10.1016/S1361-3723(18)30053-8)
67. Noortman, R., Schulte, B. F., Marshall, P., Bakker, S., & Cox, A. L. (2019). Hawkeye—Deploying a design fiction probe. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paper No. 422). ACM. <https://doi.org/10.1145/3290605.3300652>
68. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100–126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
69. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. <https://doi.org/10.1145/3313831.3376321>
70. Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1), 1–20. <https://doi.org/10.1080/1369118X.2018.1486870>
71. Obermeyer, Z., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm that guides health decisions for 70 million people. In *Proceedings of the conference on fairness, accountability, and transparency* (p. 89). ACM. <https://doi.org/10.1145/3287560.3287593>
72. Oppl, S., & Stry, C. (2019). *Designing digital work: Concepts and methods for human-centered digitization*. Springer. <https://doi.org/10.1007/978-3-030-12259-1>
73. Peterson, Z. N. J., Gondree, M., & Beverly, R. (2011). A position paper on data sovereignty: The importance of geolocating data in the cloud. In *Proceedings of the 3rd USENIX conference on hot topics in cloud computing* (pp. 1–5). USENIX Association. <https://www.usenix.org/conference/hotcloud11/position-paper-data-sovereignty-importance-geolocating-data-cloud>
74. Populus., & Ipsos MORI. (2017). *HSBC trust in technology*. HSBC. <https://www.hsbc.com/-/files/hsbc/media/media-release/2017/170609-updated-trust-in-technology-final-report.pdf>
75. Postma, O. J., & Brokke, M. (2002). Personalisation in practice: The proven effects of personalisation. *Journal of Database Marketing & Customer Strategy Management*, 9(2), 137–142. <https://doi.org/10.1057/palgrave.jdm.3240069>
76. Privacy First. (2019, January 7). *European PSD2 legislation puts privacy under pressure. Privacy First demands PSD2 opt-out register*. <https://www.privacyfirst.eu/focus-areas/financial-privacy/672-privacy-first-demands-psd2-opt-out-register.html>
77. Reynolds, C., & Picard, R. (2004). Affective sensors, privacy, and ethical contracts. In *Extended abstracts of the SIGCHI conference on human factors and computing systems* (pp. 1103–1106). ACM. <https://doi.org/10.1145/985921.985999>
78. Rubinstein, I., & Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkely Technology Law Journal*, 28(2), 1335–1413. <https://doi.org/10.2139/ssrn.2128146>
79. Rubinstein, I. S. (2011). Regulating privacy by design. *Berkely Technology Law Journal*, 26(3), 1405–1456. <https://doi.org/10.15779/Z38368N>
80. Salvo, M. J. (2001). Ethics of engagement: User-centered design and rhetorical methodology. *Technical Communication Quarterly*, 10(3), 273–290. https://doi.org/10.1207/s15427625tcq1003_3
81. Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2018). A design space for effective privacy notices. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge handbook of consumer privacy* (1st ed., pp. 365–393). Cambridge University Press. <https://doi.org/10.1017/9781316831960.021>
82. Sefelin, R., Tscheligi, M., & Giller, V. (2003). Paper prototyping—What is it good for? A comparison of paper- and computer-based low-fidelity prototyping. In *Extended abstracts of the SIGCHI conference on human factors in computing systems* (pp. 778–779). ACM. <https://doi.org/10.1145/765891.765986>
83. Shilton, K. (2013). Values levers: Building ethics into design. *Science, Technology, & Human Values*, 38(3), 374–397. <https://doi.org/10.1177/0162243912436985>
84. Solid Project. (2020). *Use Solid apps*. <https://solidproject.org/use-solid/>
85. Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM*, 55(7), 34–37. <https://doi.org/10.1145/2209249.2209263>
86. Steen, M. (2013). Co-design as a process of joint inquiry and imagination. *Design Issues*, 29(2), 16–28. https://doi.org/10.1162/DESI_a_00207
87. Steen, M., Manschot, M., & Koning, N. D. (2011). Benefits of co-design in service design projects. *International Journal of Design*, 5(2), 53–60.
88. Sterling, B. (2009). Design fiction. *Interactions*, 16(3), 20–24.
89. Tang, Z., Hu, Y., & Smith, M. D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems*, 24(4), 153–173. <https://doi.org/10.2753/MIS0742-1222240406>
90. Terpstra, A., Schouten, A. P., de Rooij, A., & Leenes, R. E. (2019). Improving privacy choice through design: How designing for reflection could support privacy self-management. *First Monday*, 24(7). <https://doi.org/10.5210/fin.v24i7.9358>
91. Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.
92. Troncoso, C., Isaakidis, M., Danezis, G., & Halpin, H. (2017). Systematizing decentralization and privacy: Lessons from 15 years of research and deployments. *Proceedings on Privacy Enhancing Technologies*, 2017(4), 404–426. <https://doi.org/10.1515/popets-2017-0056>
93. Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 254–268. <https://doi.org/10.1287/isre.1090.0260>

94. Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information Management & Computer Security*, 9(4), 165–174. <https://doi.org/10.1108/EUM0000000005808>
95. UI Stencils. (2020). *iPhone stencil kit*. <https://www.uistencils.com/products/iphone-stencil-kit>
96. UN General Assembly. (1948). *Universal declaration of human rights*. <http://www.un.org/en/universal-declaration-human-rights/>
97. Upchurch, T. (2018, April 8). *To work for society, data scientists need a hippocratic oath with teeth*. Wired UK. <https://www.wired.co.uk/article/data-ai-ethics-hippocratic-oath-cathy-o-neil-weapons-of-math-destruction>
98. Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the SIGSAC conference on computer and communications security* (pp. 973–990). ACM. <https://doi.org/10.1145/3319535.3354212>
99. van den Hoven, J. (2007). ICT and value sensitive design. In P. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.), *The information society: Innovation, legitimacy, ethics and democracy. In honor of Professor Jacques Berleur s.j.* (Vol. 233, pp. 67–72). Springer. https://doi.org/10.1007/978-0-387-72381-5_8
100. Verbeek, P.-P. (2006). Materializing morality: Design ethics and technological mediation. *Science, Technology, & Human Values*, 31(3), 361–380. <https://doi.org/10.1177/0162243905285847>
101. Vickers, L. (2007). *Religion and belief discrimination in employment: The EU law*. European Commission, Directorate-General for Employment, Social Affairs and Equal Opportunities.
102. Villebro, M., Shklovski, I., Rossi, L., & Bjørstorp, A. (2018). Comfortably numb: Danish teens’ attitudes, towards social media platforms. In *Proceedings of the 9th international conference on social media and society* (pp. 187–196). ACM. <https://doi.org/10.1145/3217804.3217911>
103. VZBV v. Planet49, C673/17 EU (2019). <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0673>
104. Wong, R. Y., & Mulligan, D. K. (2019). Bringing design to the privacy table: Broadening “design” in “privacy by design” through the lens of HCI. In *Proceedings of the SIGCHI conference on human factors in computing systems* (Paper No. 262). ACM. <https://doi.org/10.1145/3290605.3300492>
105. Wong, R. Y., Mulligan, D. K., Van Wyk, E., Pierce, J., & Chuang, J. (2017). Eliciting values reflections by engaging privacy futures using design workbooks. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW), Article 111. <https://doi.org/10.1145/3134746>
106. Yao, Y., Basdeo, J. R., Kaushik, S., & Wang, Y. (2019). Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the SIGCHI conference on human factors in computing systems* (Paper No. 198). ACM. <https://doi.org/10.1145/3290605.3300428>
107. Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>