Evaluating the Usability of Privacy Choice Mechanisms

Thesis Proposal

Hana Habib

April 2021

Abstract

Notice and choice has dominated the discourse on consumer privacy protection and is the foundation of existing privacy regulation in the United States. Under this paradigm, companies disclose their data handling practices to consumers, who in turn are expected to make decisions according to their privacy preferences. As such, many companies have incorporated consent notices and other privacy choices into their web interfaces. The notice and choice model presents several challenges for providing effective consumer privacy protection, one of which is related to the usability of privacy choice mechanisms. The design of consent and privacy choice interfaces can significantly affect consumer choices and their privacy outcomes. This thesis will highlight usability issues in interactions required to use privacy choices, as well as provide guidance for conducting usability evaluations of such interactions.

In this thesis, I will first describe a series of studies examining different usability aspects of existing privacy choices. The first two studies present an overview of how privacy choices related to email marketing, targeted advertising, and data deletion are commonly offered to consumers on the web and provide insight into the usability of these implementations. Among other shortcomings, these studies found discoverability issues with existing privacy choices. One potential means of making privacy choices more visible to consumers is through the use of icons. The next study described in this thesis explains the design and evaluation of new icons to effectively communicate the presence of privacy choices. In addition to discoverability issues, privacy choices may not always align well with user needs. The fourth study in this thesis explored this aspect of usability, and evaluated whether existing controls related to targeted advertising on a social networking platform actually address user goals related to their advertising experience on the platform.

My prior work, as well as previous studies from the literature, emphasize the importance of usability testing with regards to privacy choice and consent interfaces. Despite increased regulatory requirements and consumer pressure for privacy choice mechanisms, there is little direction for practitioners on how to systematically evaluate such interfaces. To address this need, I propose to compile comprehensive guidance for conducting such usability evaluations that will address different aspects of usability, such as discoverability and understandability. This guidance will include a breadth of HCI research methods, as well as example metrics for measuring specific usability problems. To demonstrate the application of this guidance and some of the trade-offs associated with each research method, I will conduct usability evaluations of two distinct privacy choice and consent interfaces.

Contents

1 Introduction

Notice and choice has served as the primary framework for consumer privacy protection in the United States. Under this model, companies are required to be transparent about their data collection and handling practices, and must provide controls to consumers to allow them to manage the privacy of their data according to their preferences. As such, web interfaces related to consent and privacy choices have become common. Legal and privacy experts have surfaced several limitations of the notice and choice model [16,93,108,115,117]. A major criticism is the lack of transparency and choice provided by traditional notice and choice mechanisms such as privacy policies [108]. Another critique is that the notice and choice model places the burden of privacy management on consumers, who often are required to make privacy decisions across multiple different services without full information regarding these choices [117]. Others argue that dark design patterns exploit inherent cognitive biases and limit the effectiveness of rational choice-making, which is necessary for a notice and choice model of privacy protection to work [127]. Despite these limitations, some still argue that individual decision-making and privacy choice should have a role within an effective consumer privacy protection framework [23, 105, 117].

Furthermore, the notice and choice framework has continued to serve as the foundation of legal and self-regulatory privacy efforts, many of which mandate certain types of privacy choices. Most recently, the General Data Protection Regulation in the European Union and California Consumer Privacy Act granted consumers the right to object to the processing of their information [35,99]. Other types of controls, such as opt-outs for email marketing have been mandated by United States law since 2003 [38]. These regulations place an emphasis on usability, requiring "plain" language and choices be available through "conspicuous" links [35,38,99]. Other efforts related to consumer privacy choices include guidelines developed by self-regulatory groups in the advertising industry that require member companies to provide controls over targeted advertising [28, 91] and technical standards like Do Not Track implemented in major web browsers [126].

Prior work has identified many deficiencies related to current consent and privacy choices available to consumers. First, there is evidence suggesting non-compliance with existing privacy laws and self-regulatory agreements [24, 26, 100]. Additionally, some privacy choice mechanisms offered to consumers are ineffective due to lack of enforcement and buy-in from companies handling consumer data [23]. Furthermore, prior studies have found usability issues with respect to privacy choice and consent interfaces. For example, some privacy choice mechanisms may require a high level of technical knowledge to configure [75]. Another usability obstacle is the use of dark patterns in privacy choice and consent interfaces that nudge users toward less privacy-protective options [20, 116]. Improving the effectiveness of the notice and choice model of privacy protection requires an emphasis on the usability of notice and choice mechanisms. This in turn requires developing novel transparency and privacy control mechanisms, as well as addressing usability issues in existing interfaces. The results of prior research in this domain emphasize the importance of testing consent and privacy choice interfaces for different aspects of usability, as these interfaces impact consumers' privacy outcomes.

This thesis, focused on the choice aspect of the notice and choice paradigm, contributes to a better understanding of how consent and privacy choice mechanisms can be improved. The first portion of this thesis will further explore different usability aspects of web-based privacy choices. First, it will provide an overview of how these privacy choices are provided in practice, particularly those related to email marketing, targeted advertising, and data deletion, and then describe different usability issues related to common interfaces for these privacy choices. Next, this thesis will summarize to what extent graphical icons can effectively communicate the presence of privacy choices. In the next chapter, this thesis will assess how well controls for targeted advertising on Facebook are aligned with user needs. The second portion of the thesis will propose comprehensive guidance for conducting systematic usability evaluations of consent and privacy choice interfaces. It will first describe the development of this guidance, which will include guidelines for practitioners on utilizing traditional HCI research methods to uncover different forms of usability issues. Finally, this thesis will apply the compiled guidance and present results from usability evaluations of two different consent and privacy choice interfaces.

Thesis Statement

This thesis will describe usability issues that limit the effectiveness of existing privacy choice mechanisms, provide guidelines for conducting systematic usability evaluations of privacy choice interfaces, and demonstrate the application of this guidance in two domains involving user consent or privacy choice.

2 Background & Related Work

This section provides an overview of the current regulatory framework that mandates certain types of privacy controls, including those explored in this thesis. It further describes prior work examining compliance with existing regulation. Next, this section provides an overview of studies exploring consumers' desire for privacy controls, the usability of current choice mechanisms, as well as alternative mechanisms for communicating privacy controls.[1] Last, is an introduction to existing frameworks and methods for exploring user interaction with systems, and how the relate to interfaces for consent and privacy control.

2.1 Privacy Choice Regulatory Framework

The European Union's General Data Protection Regulation (GDPR), a comprehensive privacy legislation having global impact, went into effect in May 2018. The GDPR emphasizes consumers' consent to the processing of their personal data for purposes that go beyond what is required to fulfill a contractual obligation or immediate business interests. In asking for consent, companies must present a clear, affirmative action, and ask visitors for agreement rather than incorporating the consent into default settings, such as pre-checked boxes (Art. 4). Consent should be in an easily accessible form, using simple, clear language and visualization, if needed; if the consumer is a child, the language must be understandable by a child (Art. 12). Moreover, visitors are allowed to withdraw their consent at any time (Art. 7). The GDPR also grants consumers whose data is collected in the European Union the "right to be forgotten." This stipulates that under certain circumstances, companies must comply with consumer requests to erase personal data (Art. 17). Additionally, consumers were granted "the right to object" when their personal data is processed for direct marketing purposes (Art. 21) [35]. In the wake of its enactment, the GDPR has inspired several other national privacy laws, including those in Canada, Japan, South Korea, Colombia, Argentina, and South Africa [114].

The GDPR also laid the groundwork for the California Consumer Privacy Act (CCPA), which went into effect in 2020. The California state law grants California residents the right to opt out of having their personal data sold to third parties, for example, for marketing purposes [99]. The initial proposed text of the regulations specified that this opt-out be provided through "an interactive form accessible via a clear and conspicuous link titled 'Do Not Sell My Personal Information,' or 'Do Not Sell My Info' on the business's website or mobile application," as well as an optional opt-out icon [97]. The CCPA also gives California residents the right to request their personal data be deleted, except in certain circumstances, such as when the information is needed to complete an unfinished transaction [99]. The California Privacy Rights and Enforcement Act (CPRA), which will go into effect in 2023, builds upon the CCPA. The law provides additional privacy rights to California consumers, including a right to opt out of a business using sensitive personal information and to opt out of the sharing of information with third parties (in addition to selling). Furthermore, the CPRA explicitly prohibits the use of dark design patterns in consent interfaces [98].

Other laws in the United States require privacy choice mechanisms in certain contexts. The Children's Online Privacy Protection Act of 1998 (COPPA), for example, requires online services that collect personal information of children under 13 years old to delete it upon parental request [39]. Additionally, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 established national standards for companies that send electronic commercial messages to consumers. It requires companies to provide consumers with a means to opt out of receiving communications, accompanied by a clear and noticeable explanation about how to use the opt-out. Once the commercial message is sent, opt-outs must be available to recipients for at least 30 days, and any opt-out request must be honored within 10 business days [38].

[1] This overview was adapted from the Background and Related Work sections of the studies described in this thesis [52–55].

In addition to legal requirements, there have been self-regulatory proposals related to privacy choices. Two protocols spearheaded by the World Wide Web Consortium (W3C) — the Platform for Privacy Preferences Project (P3P) and Do Not Track (DNT) — aimed to automatically apply consumer privacy preferences through browser-based settings [124,126]. However, unresolved ambiguities regarding the implementation of these protocols and lack of industry support led to poor adoption [23, 59]. Since the early 2000s, industry organizations in the United States and Europe — including the Network Advertising Initiative (NAI), Digital Advertising Alliance (DAA), and Interactive Advertising Bureau Europe (IAB Europe) — have adopted principles and self-regulatory requirements related to practices used in online behavioral advertising [28, 63, 91]. For example, member companies of the Digital Advertising Alliance (DAA) are required to provide opt-outs for tracking-based targeted advertising by placing an AdChoices icon and an approved text above an ad [28]. This requirement applies to data used by the company or transferred to other non-affiliated entities to deliver tailored ads, but not for other collection purposes [84]. These groups have also introduced guidelines to address new regulation. IAB Europe published the Transparency and Consent Framework for obtaining consumer consent under the GDPR [63]. The DAA also introduced the PrivacyRights icon, a green variant of the AdChoices icon, and an opt-out tool to address the CCPA's opt-out requirements for the sale of personal information [119].

2.2 Compliance with Privacy Choice Requirements

Prior studies have explored compliance related to privacy control requirements. An audit of top North American retailers in 2017 by the Online Trust Alliance found that 92% of websites surveyed offered unsubscribe links within messages. However, the study also revealed that compliance issues with CAN-SPAM still exist as some retailers offered broken unsubscribe links, or continued to send emails after the 10-business-days deadline [100]. This study highlights some of the additional potential issues with current privacy choice mechanisms that go beyond usability.

There is also evidence of mixed compliance with the GDPR. Degeling et al. found that, among the more than 6,000 European websites surveyed in 2018, 85% had privacy policies; many websites had updated their privacy policies or started to display cookie consent notices when the GDPR went into effect, likely in response to the GDPR's transparency requirements [27]. However, Soe at el. manually evaluated cookie consent notices on 300 online news outlets based on 13 heuristics and found that these notices may be violating the intent of the GDPR. Additionally, their results provide a reference for several types of common dark patterns specific to consent notices [116]. Furthermore, some major websites were found to still deliver targeted ads to European visitors who did not consent to the use of their personal data [26]. It is also unclear whether the changes websites are implementing actually serve to protect consumers. Facebook, for example, was criticized for their post-GDPR privacy changes, as users are still not able to opt out of Facebook's use of behavioral data to personalize their News Feeds or optimize its service [19]. Similarly, the Norwegian Consumer Council evaluated GDPR-related settings updates on Facebook, Google, and Windows 10, finding evidence that consumers are pushed to less privacy protective options through design techniques, such as obscured pre-selected defaults and privacy-protective settings being less salient than privacy-invasive ones [20].

Early research has also highlighted usability issues related to the CCPA's do-not-sell opt-out provision. Consumer reports found that some websites did not have the required do-not-sell link, and that consumers struggled to locate opt-out links on websites and complete opt-out processes offered by data brokers [81]. O'Connor et al. conducted a manual review and user study of websites' do-not-sell opt-out mechanisms and found that these processes are permeated with dark patterns which influence user behavior [96]. These studies underscore the need for usability testing guidance, such as that provided in this thesis, that can help detect the presence of dark patterns in privacy choice and consent interfaces.

Furthermore, studies have identified issues related to noncompliance with self-regulatory guidelines for targeted advertising. Hernandez et al. found in 2011 that among Alexa's US top 500 websites only about 10% of third-party ads used the AdChoices icon, and even fewer used the related text [57]. Less than half of DAA and NAI members examined by Komanduri et al. complied with the enhanced notice requirement of these organizations' guidelines [72]. In 2015, Cranor et al. reported that around 80% of the privacy policies of industry group members analyzed did not meet self-regulatory guidelines related to transparency and linking data with personally identifiable information [24]. This prior work demonstrates the limitations of

a purely self-regulatory approach to consumer privacy protection, and suggests that legislation must play a role under the notice and choice model of privacy protection.

2.3 Consumer Perceptions of Data Use

Prior studies have shown that consumers have long been uncomfortable with certain data handling practices commonly used by companies in the digital age. For example, in a survey conducted by Business Week and Harris Poll in 2000, 78% of respondents were concerned that companies would use their information to send junk emails [14]. Similarly, in another 1999 survey, 70% of respondents wanted to have the choice to be removed from a website's mailing list [25]. In Rader et al.'s interview study, awareness of data aggregation and cross-platform inferences increased the likelihood of privacy concern [103]. More recently, Murillo et al. examined users' expectations of online data deletion mechanisms and found that users' reasons for deleting data were varied and largely depended on the type of service [90]. Fiesler and Hallinan analyzed public reactions to two major data-sharing controversies and found strong outrage and concern relating to unexpected types of data use [42].

Most prior work on consumer attitudes toward the use of their personal data has focused on targeted advertising practices. Internet users consider targeted advertising a double-edged sword: targeted advertising stimulates purchases and is favored by consumers when it is perceived to be personally relevant; yet, it also raises significant privacy concerns due to the large amount of personal data being collected, shared, and used in a nontransparent way [10, 71]. Prior research has shown rich evidence of consumers' objection to data collection for targeted advertising purposes. In Turow et al.'s 2009 national survey, over 70% of respondents reported that they did not want marketers to collect their data and deliver ads, discounts, or news based on their interests [121]. Similarly, in McDonald and Cranor's 2010 survey, 55% of respondents preferred not to see interest-based ads, and many were unaware that opt-out mechanisms existed [86]. These findings are supported by qualitative work, such as Ur et al.'s 2012 interview study, in which participants generally objected to being tracked and sometimes found ads to be "creepy" [122].

Prior work has also found that consumers have an oversimplified, inaccurate, and/or incomplete ideas of how targeted advertising and data aggregation by large internet companies occur. For example, many consumers may not know that ads they see may be based on their email content [86]. Yao et al. showed that mental models about targeted advertising practices contain misconceptions, including conceptualizing trackers as viruses and speculating that trackers access local files and reside locally on one's computer. Others were completely unaware of targeted advertising practices [132]. In 2019, a Pew Research Center poll found that 74% of respondents did not know about the list of traits and interests that Facebook had gathered about them, about half were uncomfortable with how Facebook had categorized them, and 27% found the categorizations to be largely inaccurate [60]. In particular, consumers have been observed to have a low understanding of "third-party" data collection, advertising networks, and data aggregation across websites or apps [103, 122]. A 2020 study of Twitter users by Wei et al. found that, while almost all participants correctly understood targeting based on factors such as location, age, and keywords, the vast majority of participants did not correctly understand targeting using list-based audiences, behavioral inferences, or interactions with other mobile apps. Participants also tended to consider these approaches to be more privacy-invasive and unfair than targeting based on factors such as language or age [128].

Given consumers' privacy concerns and lack of complete understanding of companies' data handling practices surfaced by this prior work, it is imperative for companies to be respectful of user privacy in their treatment of consumer data. Furthermore, the research highlighted here suggests that consumers have varying privacy needs, thus usable privacy control mechanisms are necessary to enable consumers to adjust companies' handling of their data.

2.4 Usability of Privacy Choices

Despite significant privacy concerns, consumers struggle to protect their online privacy against targeted advertising for multiple reasons [22]. Two aspects that limit users' capabilities in dealing with targeted advertising include the asymmetric power held by entities in the targeted advertising ecosystem, and consumers' bounded rationality and limited technical knowledge to fully understand and utilize privacy-enhancing technologies [1, 2, 34]. Furthermore, the usability of websites' privacy communications has long been problem-

atic [85, 86]. Recent work has shown that privacy policies, where privacy choices are often disclosed, still exhibit low readability scores [36, 78]. Additionally, most websites fail to provide specific details regarding the entities with which they share data and the purposes for which data is shared [49].

Another barrier to the usability of privacy choices and consent mechanisms is the presence of dark patterns. Dark patterns in design can be used to surreptitiously achieve a business objective, often at the expense of the user [12]. Since the concept was introduced, different taxonomies have been developed to categorize dark patterns (e.g., [50,56,76]). Dark patterns have been found in different aspects of transparency and privacy, such as explanations of AI algorithms [18] and identity management controls [45], which overlap with the design of consent and privacy choice interfaces. Consent interfaces specifically have also been evaluated for dark patterns using different methodologies. Drawing from existing literature in design, law, and privacy, Gray et al. performed an interaction criticism of consent banners from four perspectives: the designer's intent, designed UI, end-user, and potential societal impact. By reviewing recordings from over 50 websites, they identified different stages of the consent task flow and common design choices that raised ethical dilemmas that warrant additional dialogue [51]. Nouwens et al. quantified the impact of different consent interface design choices through an online experiment, finding that the display of granular options within an initial cookie consent prompt decreased the probability of a user giving consent, while removing a "reject all" button increased the probability of consent [94].

Other studies have explored privacy choice and consent mechanisms for usability issues beyond dark patterns. A 2018 analysis by the Nielsen Norman group revealed usability issues related to unsubscribe options in marketing emails, such as inconspicuous links without visual cues indicating that they are clickable, long and complicated processes involving many check boxes and feedback-related questions prior to the final unsubscribe button, as well as messaging that might annoy or offend users [92]. The Global Privacy Enforcement Network (GPEN) reported that only half of the websites and mobile apps they evaluated provided instructions for removing personal data from the company's database in the privacy policy, and only 22% specified the retention time of inactive accounts [49]. An encouraging effort is the JustDelete.me database,[2] which rated the account deletion process of 511 web services as easy (i.e., "simple process"), medium ("some extra steps involved"), hard ("cannot be fully deleted without contacting customer services"), or impossible ("cannot be deleted"). More than half of the websites analyzed (54%) were rated as having an "easy" process for deleting an account from the website.

Others have evaluated opt-out tools for targeted advertising, which include third-party cookie blockers built into web browsers, browser extensions, and opt-out tools provided by industry self-regulatory groups. The effectiveness of these tools varies. Many opt-out options, for example, prevent tailored ads from being displayed but do not opt users out of web tracking [11]. A 2012 study found certain browser extensions and cookie-based tools to be helpful in limiting targeted text-based ads, but the 'Do Not Track option in browsers was largely ineffective [5]. Prior evaluations of targeted advertising opt-out tools have revealed numerous usability issues that can impose a heavy burden on users. For instance, using opt-out cookies is cumbersome, as these cookies can be easily modified by third-party companies and need to be manually installed and updated, and may be inadvertently deleted [84]. Browser extensions partially mitigate these issues but introduce other problems. Studies have found that users may have difficulty comprehending the information provided by tracker-blocking extensions, as well as with configuring these tools [75, 112]. Some of these tools have since been updated to address usability concerns. Opt-out tools offered by industry self-regulatory groups also exhibit low comprehension, as studies have found that the NAI's description of opt-out cookies led to the misinterpretation that the opt-out would stop all data collection by online advertisers, and DAA's AdChoices icon failed to communicate to web users that a displayed ad is targeted [86, 122]. Moreover, when the AdChoices icon is presented on a mobile device, it tends to be difficult for people to see [46].

The prior work described here reflects on some of the usability issues with current mechanisms for consent and privacy control. This thesis builds on this work by evaluating the usability of different types of privacy controls along various metrics. Moreover, this thesis will present guidance for conducting usability evaluations of privacy and consent interfaces so that usability issues may potentially be identified and addressed prior to the deployment of these interfaces.

[2] https://backgroundchecks.org/justdeleteme/

2.5 Mechanisms for Communicating the Presence of Privacy Choices

Privacy choices are often disclosed in privacy policies. However, research has shown that most users do not read privacy policies [88, 95] or struggle to comprehend them due to vague descriptions and jargon [9, 65, 87, 104]. Given the estimated time required to peruse privacy policies on visited websites, it would be unrealistic to expect users to read them routinely [85]. These findings suggest the need for alternative privacy notices that make privacy information more accessible and understandable [111]. Examples of such alternatives include privacy dashboards [47], privacy certifications and seals [8], privacy grades and scores [31, 48, 66, 102], privacy labels [33, 68, 70, 120], consent banners and pop-ups [80, 94, 123], and privacy icons [61, 64, 89, 107].

Privacy dashboards allow consumers to inspect the data companies have collected about them and adjust their privacy settings [106]. For example, the browser extension Ghostery provides an interface for users to learn which web trackers are present on visited websites and block or permit certain trackers [47]. Privacy seals and certifications, such as the Enterprise Privacy Certification by TrustArc (formerly TRUSTe) [8], are designed to signal that businesses comply with legal requirements or industry standards [106]. Privacy grades and scores indicate how well websites protect their users' privacy through numeric ratings, (e.g., ToS;DR [66], Privacy Finder [31, 48], and PrivacyGrade.org for mobile apps [102]). Privacy labels, similar to food nutrition labels, help users quickly learn about and compare privacy-related attributes of products or services, including websites [68, 69], Internet of Things devices [32, 33], search results [15, 120], and mobile apps [4, 70]. Privacy choices, mostly related to cookie management, are also presented in consent pop-ups and banners on websites [27].

Researchers have proposed various privacy icons as succinct indicators of complex privacy concepts. Some privacy icons represent specific data practices, such as Disconnect.me's icons for different types of tracking [29] and Mozilla's icons for retention periods and third-party data sharing and use [89]. Some only serve specific application domains, such as social media [64], web links [67], or webcams [30, 101], while others can apply across contexts [61]. Icons are also commonly used as security indicators (e.g., a lock in a browser's URL bar that indicates HTTPS [40]). However, prior work has found that users tend to ignore or misunderstand these indicators [44, 77, 113]. Fewer privacy icons are designed to convey privacy choice, consent, or opt-outs. The Stanford Legal Design Lab has proposed icons that could potentially indicate privacy choices, but they have not been empirically evaluated [118]. While the Data Protection Icon Set (DaPIS) has been user-tested, it is specific to GDPR consumer privacy rights [107] .

Icons have several advantages that can address the limitations of traditional privacy notices. Icons can visually communicate information concisely while circumventing language and cultural barriers [82]. Icons can be useful information markers since they are easy to recognize [13, 62]. When placed next to lengthy privacy statements, icons can enhance readability by helping users navigate the text [107]. In a review of iconography guidelines, Bühler et al. summarized principles for effective icons — they should be based on users' knowledge and needs, utilize well-known concepts, and closely mimic real-world objects [13]. However, designing comprehensible icons is challenging. Icons alone sometimes perform worse than text-only or icon-text interfaces in assisting learning [129]. Fischer-Hübner et al. therefore argue that icons should be used alongside text to illustrate data practices in privacy policies and aid user comprehension [43]. Beyond an icon's comprehensibility, discoverability is another challenge. For instance, the size, position, state, and color all impacted how visible the AdChoices icon was to users on a mobile device [46].

Privacy icons explored in prior work have primarily focused on communicating data practices, but few proposed privacy icons have received wide adoption. Even widely adopted icons, such as DAA's AdChoices icon, are problematic [46, 86, 122]. Not much work has focused on using icons to convey privacy choices effectively to consumers. This thesis fills this gap through a study that iteratively designed and evaluated privacy choice icons and associated link texts. Complementing prior research on icons for GDPR-specific user rights [107], this study focused on conveying the presence of general privacy choices, as well as the CCPA-mandated do-not-sell opt-out.

2.6 Evaluating the Usability of Privacy Choice Interactions

While there is no single definition of "usability" in the context of user interfaces, several frameworks have been developed to aid researchers and user experience professionals in systematically identifying and describing users' interaction with a system. The International Organization for Standardization (ISO) definition of usability includes aspects related to the effectiveness, efficiency, and satisfaction of a particular interface.

Quesenbery's definition also includes effectiveness and efficiency, and further defines usability as related to engagement, error tolerance, and ease of learning. Morville's UX honeycomb describes seven facets of describing an interface: useful, desirable, valuable, usable, findable, credible, and accessible [7]. The User Interaction Cycle, built upon Norman's theory of action, divides the cognitive and physical processes composing a user action into four stages: high-level planning (identifying goals and tasks), translation (formulating a plan given the interface), physical action (using the interface), and assessment (understanding the outcome of the action) [3]. More directly related to this thesis Feng et al. define the usability of "meaningful privacy choices" as related to five dimensions: effectiveness (whether privacy choices are aligned with user needs), efficiency (whether privacy choices can be exercised with minimal effort), user awareness (whether choices are effectively communicated to users), comprehensiveness (whether privacy choices communicate the full scope of the action), and neutrality (whether privacy choice interfaces exhibit any dark patterns) [41]. They further describe a design space for privacy choices, which is complementary to the usability testing guidelines that this thesis will contribute.

The field of Human-Computer Interaction (HCI) has adapted research methods from other disciplines to systematically explore user needs and identify usability issues throughout the development process of an interface. Hertzum describes five maxims related to usability evaluations that are often in tension with each other; the first three (robustness, validity, and completeness) apply to the methodology used for testing, while the last two (impact and cost) relate to integrating the results of the evaluation into the development process [58]. Some methods, including surveys, diary studies, interviews, focus groups, ethonographies, and usability tests, involve recruitment of individuals that ideally closely represent actual users of the deployed system [74]. Inspection-based methods, including heuristic evaluations and cognitive walkthroughs, rely on evaluators, often with user experience expertise, to identify potential usability issues with an interface [130]. Both user studies and inspection-based methods offer advantages and disadvantages. Though user studies provide better insights about user needs and more realistic perspectives related to how users may interact with a system compared to inspection-based evaluations, they may be costly to run. Inspection-based assessments can typically be conducted more quickly with fewer logistic barriers, but may only uncover certain types of usability issues [130]. Sandars argues that two or more evaluation techniques may be required to fully understand user needs [110]. However, as has become common adage,"testing one user is 100 percent better than testing none" [73].

Methods for usability testing are often applied for the purposes of accessibility testing. Accessibility is an important aspect of usability, with the key difference being that accessibility issues have a greater impact on people with disabilities or who use assistive technologies [109]. As such, multiple guidelines have been developed to help organizations ensure that their web interfaces are accessible. The most prominent of these is the W3C Accessibility Guidelines (WCAG) which has become the global standard for web accessibility [109, 125]. Since the release of the initial version of the guidelines multiple tools have been developed to facilitate organizations' use of the WCAG, including simple checklists and automated testing software [109]. This thesis can draw on existing guidelines for accessibility as they can provide direction as to what type of guidance would be most beneficial to practitioners in terms of testing the usability of privacy choice interfaces.

While usability testing of consent and privacy choice interfaces has many parallels with accessibility testing, one significant difference is understanding the influence of dark pattern designs on consumer choices. Though the academic literature on dark patterns has been rapidly expanding, there has been less of a focus on formalizing what defines a dark pattern and how to apply HCI research methods to systemically analyze interfaces for them. Recent work by Mathur et al. furthers the literature in this regard by categorizing prior dark pattern definitions and taxonomies and providing an overview of concepts similar to dark patterns discussed in other fields of study. Furthermore, they identified four normative perspectives that can aid in identifying dark patterns: individual welfare, collective welfare, regulatory objectives, and individual autonomy [83]. While Mathur et al. also demonstrate how HCI empirical methods can identify dark patterns, they discuss the application of methods broadly and across different contexts. Zagal et al. developed a more concrete evaluation framework, but it was exclusively for the context of game design [133]. This thesis builds on this prior work by providing detailed guidance that practitioners can use to systematically identify potential dark patterns in consent and privacy choice interfaces.

These guidelines for evaluating privacy choice interfaces would complement existing ones for evaluating the effectiveness of privacy disclosures [37, 111]. These evaluation guidelines could also utilize cognitive frameworks related to privacy and security decision-making, such as the Communication-Human Informa-

tion Processing (C-HIP) model from the field of warnings science [131] and the human-in-the-loop security framework which identifies different factors that may impact the behavior of a user interacting with a security or privacy interface, such as a privacy notice [21]. Previous studies have used HCI research methods to evaluate security and privacy disclosures against different components of the the human-in-the-loop model. Some have conducted evaluations of disclosures by measuring outcomes such as purchase behavior, taking into account factors related to the intentions of a "human receiver," or user of a privacy interface, such as privacy attitudes and motivations [33, 120]. One evaluation related to the capabilities attribute of a human receiver is an interview study by Emami-Naeini et al. which leveraged experts' knowledge to determine what privacy and security information would be helpful to consumers when purchasing Internet of Things (IoT) devices [32]. Some experiments have explored aspects of communication delivery by manipulating variables, such as the timing and placement of privacy disclosures, in realistic contexts of user decision-making where communication impediments may prevent users from noticing a disclosure in the first place [31, 70]. Other user studies relate to the communication processing aspect of the human receiver, including research by Balebako et al. which measured comprehension of standardized content for privacy disclosures [6] and Kelley et al. which measured knowledge retention from different formats of privacy disclosures [69]. While this prior work focused on evaluating privacy disclosures, similar approaches can be utilized for the evaluation of privacy choice and consent interactions and will be outlined in the guidelines presented in this thesis.

3 Previous Work

3.1 An Empirical Analysis of Data Deletion and Opt-Out Choices

Abstract

Many websites offer visitors privacy controls and opt-out choices, either to comply with legal requirements or to address consumer privacy concerns. The way these control mechanisms are implemented can significantly affect individuals' choices and their privacy outcomes. We present an extensive content analysis of a stratified sample of 150 English-language websites, assessing the usability and interaction paths of their data deletion options and opt-outs for email communications and targeted advertising. This heuristic evaluation identified substantial issues that likely make exercising these privacy choices on many websites difficult and confusing for US-based consumers. Even though the majority of analyzed websites offered privacy choices, they were located inconsistently across websites. Furthermore, some privacy choices were rendered unusable by missing or unhelpful information, or by links that did not lead to the stated choice. Based on our findings, we provide insights for addressing usability issues in the end-to-end interaction required to effectively exercise privacy choices and controls.

This study is complete and was published in the 2019 Proceedings of the Symposium on Usable Privacy and Security (SOUPS) [54].

Research Goal

Identify what choices related to email communications, targeted advertising, and data deletion websites offer, as well as how websites are presenting these privacy choices to their visitors.

Methods

We examined data deletion, email, and targeted advertising choices on 150 websites sampled from Alexa's ranking of global top 10,000 websites (as of March 22, 2018). To understand how privacy choices vary across a broad range of websites, we categorized these websites based on their reach (per million users), an indicator of how popular a website is, provided by the Alexa API. We developed an analysis template for the systematic analysis of the privacy choices offered by websites along multiple metrics. In completing the template, a member of the research team visited the home page, privacy policy, and account settings of each website examined, and answered the relevant template questions according to the privacy choices available. For each choice identified, we recorded where the privacy choice is located on the website, the user actions required in the shortest path to exercise the choice, and other information about the choice provided by the website. To ensure thorough and consistent analysis, two researchers independently analyzed the same

75 (50%) websites sampled evenly across categories. All disagreements in the analysis were reviewed and reconciled, and the remaining 75 websites were reviewed by only one researcher.

Results

- Privacy choices are commonly offered on websites across different traffic tiers, most often within the website's privacy policy, user account settings, or multiple locations.
- Text used to describe privacy choices within privacy policies has worse readability than the policy as a whole.
- There was no dominant wording for section headings in privacy policies where choices are described.
- There was ambiguity in what happens after exercising a choice, such as the scope of a targeted advertising opt-out and a time frame for when data would be deleted.
- Exercising privacy choices, on average, required between 3-5 user actions (clicks, hovers, checkboxes, etc.) in the end-to-end interaction.
- Potential usability issues included multiple links leading to different opt-out tools across multiple pages of the website and poor design of the interface required to use choices.

3.2 The Usability of Websites' Opt-Out and Data Deletion Choices

Abstract

We conducted an in-lab user study with 24 participants to explore the usefulness and usability of privacy choices offered by websites. Participants were asked to find and use choices related to email marketing, targeted advertising, or data deletion on a set of nine websites that differed in terms of where and how these choices were presented. They struggled with several aspects of the interaction, such as selecting the correct page from a website's navigation menu and understanding what information to include in written opt-out requests. Participants found mechanisms located in account settings pages easier to use than options contained in privacy policies, but many still consulted help pages or would send an email to request assistance. Our findings indicate that, despite their prevalence, privacy choices like those examined in this study are difficult for consumers to exercise in practice. We provide design and policy recommendations for making these website opt-out and deletion choices more useful and usable for consumers.

This study is complete and was published in the 2020 Proceedings of the Conference on Human Factors in Computing Systems (CHI) [52].

Research Goal

Conduct a holistic usability evaluation of the end-to-end interaction required to use common implementations of privacy choices related to email marketing, targeted advertising, and data deletion.

Methods

We conducted an in-lab study with 24 diverse participants, recruited locally in Pittsburgh, Pennsylvania. Each lab session began with an interview to learn about the participant's expectations of privacy choices. We then asked the participant to complete two privacy choice tasks on a lab computer, informed by our prior work which identified common patterns that websites used to offer controls for email marketing, targeted advertising, and data deletion [54]. The tasks differed by choice type (email marketing, targeted advertising, or data deletion) and task type (using a user account setting, a link from the privacy policy, or text instructions in the privacy policy). Each task was presented as a scenario, and participants were asked to use one of these privacy choices on a website while thinking aloud. We asked participants follow-up questions about their experiences using the assigned privacy choices, as well as any other privacy choices they may have used prior to the study. To analyze the study data, we conducted inductive coding on the interview transcripts. We also developed an analysis template to systematically count the interactions and errors made during

the tasks. We organized our findings according to the User Action Framework, which offers a systematic framework for assessing and reporting usability data [3].

Results

- Participants' expectations about privacy choice mechanisms and strategies for study tasks were dependent on choice type.
- Multiple paths to a privacy choice made it easier to find.
- Formatting of privacy polices and websites' choice of text labels caused confusion.
- Using some privacy choices required unnecessary effort for users, such as submitting written requests or completing complicated webforms.
- Participants were skeptical about the effectiveness of the privacy choices they used.

3.3 How to (In)Effectively Convey Privacy Choices with Icons and Link Texts

Abstract

Increasingly, icons are being proposed to concisely convey privacy-related information and choices to users. However, complex privacy concepts are difficult to convey through icons. We investigated which icons effectively signal the presence of privacy choices. In a series of user studies, we designed and evaluated icons and accompanying textual descriptions (link texts) conveying "choice," "opting-out," and "sale of personal information" — the latter an opt-out mandated by the California Consumer Privacy Act (CCPA). We identified icon-link text pairings that convey the presence of privacy choices without creating misconceptions, with a blue stylized toggle icon paired with "Privacy Options" performing best. The two CCPA-mandated link texts ("Do Not Sell My Personal Information" and "Do Not Sell My Info") accurately communicated the presence of do-not-sell opt-outs with most icons. Our results provide insights for the design of privacy choice indicators and highlight the necessity of incorporating user testing into the policy-making process.

This study is complete and will be published in the 2021 Proceedings of the Conference on Human Factors in Computing Systems (CHI) [55].

Research Goal

Investigate how to effectively convey to consumers the presence of privacy choices on websites through icons and accompanying text descriptions (link texts).

Methods

After a review of existing privacy iconography, we held ideation sessions and worked with graphic designers to develop icons intended to convey three concepts aligned with the goal of communicating the presence of privacy choices: "choice," "opting-out," 'and "sale of personal information." We conducted a pre-study to evaluate these icons through a survey deployed on Mechanical Turk. Participants were shown an icon condition at random and were asked their interpretation of the icon, expectation as to what clicking the icon would do, preferences for a privacy choices and do-not-sell icon, recognition of the AdChoices icon, and demographic questions. Our icon pre-study revealed the importance of an accompanying text description to help users understand icons, thus we developed a set of potential link texts intended to communicate the presence of privacy choices, including two link texts from CCPA regulations. We used a similar protocol to conduct another pre-study that evaluated the set of link texts, in which participants were shown a link text condition at random and were asked follow-up questions. To measure potential interaction effects between the icon and link text, and examine the impact of presenting an icon or text link on its own, we conducted a large-scale evaluation on Mechanical Turk using a nearly full-factorial experimental design with four icon conditions and six link text conditions, selected from our pre-studies. We implemented a between-subjects design in which each participant was shown an icon/link text pairing at random in the context of a fictitious online shoe retailer's website and then answered questions related to their interpretations and expectations

regarding the icon/text pair. After sharing results of this study with the Office of the California Attorney General (OAG), they proposed an opt-out icon that was similar (but not identical) to our stylized toggle icon. We conducted a follow-up evaluation of the OAG's icon, using the same approach. For both our main study and follow-up study, we conducted a thematic analysis of the qualitative data collected, which was used for descriptive and regression analyses to identify icons/link texts that would serve as effective privacy choices indicators.

Results

- A stylized toggle icon effectively communicated the concept of choice.
- Icon elements focusing on "do not" and "sell" were preferred to communicate an opt-out for the sale of personal information.
- Icons were often misunderstood when presented on their own without a text description.
- Link text including only the word "sell" without "info" would not be appropriate for conveying privacy choices or do-not-sell choices.
- The link text "Privacy Options" paired with a blue stylized toggle icon best conveyed the presence of privacy choices.
- The link texts included in the initial version of CCPA regulations ("Do Not Sell My Personal Information" and "Do Not Sell My Info") effectively led to the expectation of choices related to the sale of personal information in combination with most icons.
- Even minor design changes can severely reduce an icon's effectiveness and increase misconceptions, as in the case of the icon proposed by the OAG.

3.4 Identifying User Needs for Advertising Controls on Facebook

Abstract

We conducted a survey and lab study to explore user needs related to advertising controls on Facebook and determine where existing controls align with these needs. Our survey results highlight a range of user objectives related to controlling Facebook ads, including being able to select what ad topics are shown or what personal information is used in ad targeting. Some objectives are achievable with Facebook's existing controls, but participants seemed to be unaware of them, suggesting issues of discoverability. In our virtual lab study, participants noted areas in which the usability of Facebook's advertising controls could be improved, including the location, layout, and explanation of controls. Additionally, we found that users could be categorized into four groups based on their privacy concerns related to Facebook's data collection practices, objectives for controlling their ad experience, and willingness to engage with advertising controls. Our findings provide a set of user requirements for advertising controls, applicable to Facebook as well as other platforms, that would better align such controls with consumers' needs and expectations.

This study is complete and is in submission to the 2021 Proceedings of the Symposium on Usable Privacy & Security (SOUPS) [53].

Research Goal

Identify what Facebook users want to control about their advertising experience and evaluate how well current controls align with their expectations.

Methods

We conducted a preliminary survey on Mechanical Turk and Prolific. Participants answered up to 28 multiple-choice and open-ended survey questions on five topics: Facebook usage, attitudes toward Facebook ads, previous actions related to ads, Facebook's Ad Preferences page, and limitations of Facebook's advertising settings. After performing quality checks on the collected data, we used thematic analysis to categorize the

free responses and present descriptive statistics of survey results. We also performed an additional round of higher-level coding that incorporated responses to multiple questions to generate two lists: one of Facebook advertising controls that each user had mentioned using at any point in the survey and another of goals users had described related to controlling ads.

To anchor our discussion of Facebook's advertising controls, we developed study tasks related to Facebook advertising that involved user goals addressable by different existing controls. We used our survey results to evaluate which Facebook advertising controls would be the most interesting to include by mapping the available settings along two metrics: reported desirability and reported usage. This mapping uncovered four controls that corresponded to three areas that seemed interesting to explore: controls that had relatively higher reported usage and desirability, controls that had relatively lower reported usage but high desirability, and controls that had both relatively low reported usage and low reported desirability but that we speculated might be more desired if more users were aware of them. Lab sessions were held virtually over Zoom and consisted of a semi-structured interview portion followed by study tasks conducted on the participant's device. Each study task was presented as a scenario and participants were encouraged to think aloud while completing the tasks. We conducted an analysis of both the empirical data on how participants performed tasks and qualitative interview transcripts.

Results

- Facebook users have different goals related to the ads they see on the platform, including some that are already addressed by current controls.
- There seems to be a lack of awareness of these controls, suggesting issues of discoverability.
- While participants exhibited some understanding of Facebook's advertising practices, they did not fully understand the mechanisms enabling data collection from companies outside of Facebook.
- During session tasks, participants encountered difficulties finding, navigating, and understanding current ad controls, and expressed some skepticism regarding Facebook's efforts in providing these controls. They described various objectives related to the ads they see on Facebook, which were related to their overall opinions about Facebook ads and could be categorized into four groups.
- The Privacy Concerned had a higher level of concern related to Facebook tracking compared to other groups, and described privacy-related goals such as preventing cross-site tracking and receiving ads that were less personalized to their interests.
- The Advertising Curators did not mind the ads they saw on Facebook, and wanted to be able to adjust ad personalization so that ads are personalized even more to their interests.
- The Advertising Irritated complained that ads on the platform were annoying, and primarily wanted to be able to stop repetitive ads or have some way to limit the amount of advertising they see on Facebook.
- The Advertising Disengaged expressed a resigned acceptance that targeted ads and data collection practices that enable them are just the way the Internet functions, and described more of a variety of goals compared to other groups.

4 Ongoing & Future Work

4.1 Developing Guidance for Evaluating Privacy Choice Interfaces

Historically, companies may not have been motivated to exert more than minimal effort in testing the usability of consent interfaces and privacy choices. On the other hand, the poor usability of such interactions, including the use of dark patterns, may not always be intentional. Prior work suggests that designers consider user values including usability and privacy but are pulled to make contradictory design decisions to meet stakeholder goals [17]. Moreover, designers are not privacy experts and thus may not be familiar with methods to evaluate the effectiveness of consent and privacy choice experiences. Given the direction of

regulatory requirements, even companies that are less user-value centered in their design practices have motivation to change course and ensure the usability of their consent flows. As such, it is important to develop tools that simplify conducting such usability evaluations. A standard set of guidelines would both inform organizations about how to evaluate their privacy choice interfaces, but also could be used to justify why resources should be allocated to conduct such usability evaluations. These guidelines could serve as a set of best practices when testing privacy choice interactions.

I am proposing to develop comprehensive guidance that can be used by practitioners to evaluate privacy choice interface designs for different aspects of usability. These guidelines will be structured according to different possible goals of a usability evaluation. While these specific goals are yet to be identified, they may potentially be aligned with usability aspects of providing meaningful privacy choice (e.g., effectiveness, user awareness) [41] or correspond to stages of a user's interaction with a system [3]. The guidelines will then highlight HCI research methods that are best aligned with particular high-level study goals. So that these guidelines are beneficial to organizations with different levels of usability testing resources and can be applied in different stages of the interface development process, both inspection-based methods, such as heuristic evaluation and cognitive walkthrough, as well as user study methods, including surveys, interviews, and usability tests, will be described. For each method I will provide example questions and metrics that address the high-level study goals in the context of realistic user decisions. These will be drawn from normative perspectives related to dark patterns [83], classic approaches to usability testing, as well as my own prior work. Furthermore, I will highlight prior studies that align with particular high-level study objectives and different research methods.

The goal of these evaluation guidelines is to aid practitioners in increasing the usability of privacy choice and consent interfaces. While increasing the usability of such interfaces will help alleviate some of the burden of privacy decision-making from users, it is not a complete solution as users must still make multiple decisions across multiple different services. One possible solution involves AI agents to help automatically facilitate privacy choice consent decisions based on a user's preferences [79]. Until such systems are widely adopted, usability evaluation guidelines could help companies improve their privacy choice and consent interfaces. These guidelines could also be used by regulators as a means to hold companies accountable to rigorous usability testing of their privacy choice and consent processes.

4.2 Demonstrating the Privacy Choice Evaluation Guidelines

To demonstrate the utility of the compiled guidelines, I plan to apply them in evaluations of privacy choice and consent interfaces in two domains. Though the exact application domains have yet to be selected, ideally they will be as distinct from each other as possible when considering the possible design space of privacy choice interfaces [41], as well as aspects such as the novelty of the privacy choice interaction and how prevalent the type of privacy choice is in the wild. Possible domains or areas of exploration for these usability evaluations include:

- Cookie consent interfaces on a website
- Configuration of IoT device permissions through a mobile app
- Data-deletion related voice commands to a digital assistant
- User requirements for privacy choices in virtual reality contexts

I plan to conduct these evaluations using the questions and metrics directly from the compiled guidelines.

For both domains, I will first apply an inspection-based approach to usability evaluations. Inspection-based methods, including heuristic evaluation and cognitive walkthrough, are often logistically easier for companies to conduct and may be utilized throughout the development of an interface [130]. Such evaluations are typically an initial step for diagnosing severe usability issues in an interface but require domain or user experience expertise. I plan to utilize two different inspection-based approaches for each privacy choice domain to demonstrate the breadth of these research methods and highlight how they may describe different types of usability issues. I anticipate that the result of these evaluations will yield in a list of potential usability issues and corresponding justifications.

After conducting an inspection-based evaluation of both privacy choice domains, I plan to conduct a second evaluation of these interfaces with user study methods. As with my previous work exploring the

usability of website data deletion and opt-out choices which utilized both inspection-based and user study methods [52, 54], this will demonstrate the concept of "converging perspectives" [110] and highlight how user study approaches may differ from inspection-based approaches with respects to the types of usability issues uncovered. The two different user study methods will be selected after the evaluation guidelines have been developed. Both user studies will receive approval from the Carnegie Mellon Institutional Review Board (IRB) prior to recruitment of paid participants. These user studies could generate qualitative descriptions regarding the privacy choice interfaces, empirical results regarding some metric of performance (e.g., findability), as well as quantitative insights related to the prevalence of usability-related concepts (e.g., a particular user need). The analysis of these data points, in conjunction with the evaluations conducted with inspection-based approaches, will generate a comprehensive list of usability issues related to several facets of usability.

By demonstrating the breadth of possible research methods provided in the developed privacy choice evaluation guidelines, I hope to prove to practitioners that it is feasible to conduct evaluations of privacy choice interfaces. Furthermore, the resulting evaluations can serve as a concrete guide for conducting evaluations of other privacy choice interfaces. While usability testing is important for organizations to do with any interface, those related to privacy choice and consent must especially be usable to maintain trust with users and empower them to meaningfully express their privacy preferences. This is not only required by law, but is arguably a requisite for companies with a commitment to ethical data handling practices.

5 Thesis Outline

Below is an outline of the proposed thesis.

1. Introduction
2. Background & Related Work
   (a) Privacy Choice Regulatory Framework
   (b) Compliance with Privacy Choice Requirements
   (c) Consumer Perceptions of Data Use
   (d) Usability of Privacy Choices
   (e) Mechanisms for Communicating the Presence of Privacy Choices
   (f) Evaluating the Usability of Privacy Choice Interactions
3. An Empirical Analysis of Data Deletion and Opt-Out Choices
4. The Usability of Websites' Opt-out and Data Deletion Choices
5. How to (In)Effectively Convey Privacy Choices with Icons and Link Texts
6. Identifying User Needs for Advertising Controls on Facebook
7. Developing Guidelines for Evaluating Privacy Choice Interfaces
8. Demonstrating the Privacy Choice Evaluation Guidelines
9. Conclusion & Future Work

6 Task List & Timeline

1. An Empirical Analysis of Data Deletion and Opt-Out Choices. Complete (SOUPS 2019)
2. The Usability of Websites' Opt-out and Data Deletion Choices. Complete (CHI 2020)
3. How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. Complete (CHI 2021)

4. Identifying User Needs for Advertising Controls on Facebook. Complete (in submission to SOUPS 2021)

5. Developing Guidelines for Evaluating Privacy Choice Interfaces

   (a) Identify top-level organization of framework. Targeted completion date: April 9, 2021

   (b) Select research methods to be included in the framework. Targeted completion date: April 16, 2021

   (c) Identify questions and metrics for the different empirical methods. Targeted completion date: April 23, 2021

   (d) Relate prior work to the established framework. Targeted completion date: April 30, 2021

   (e) Formalize the framework as a publication (e.g., white paper, tech report, conference paper). Targeted completion date: May 28, 2021

6. Demonstrating the Privacy Choice Evaluation Framework (Targeted venue: CHI 2022)

   (a) Select two privacy choice/consent domains for usability evaluations. Targeted completion date: May 7, 2021

   (b) Plan and pilot user study evaluations of the selected privacy choice/consent interfaces. Targeted completion date: June 4, 2021

   (c) Conduct inspection-based evaluations of the selected privacy choice/consent interfaces. Targeted completion date: June 25, 2021

   (d) Conduct user study evaluations of the selected privacy choice/consent interfaces. Targeted completion date: July 30, 2021

   (e) Analyze and write usability evaluation results. Targeted completion date: August 20, 2021

7. Thesis writing. Targeted completion date: September 3, 2021

References

[1] Alessandro Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the Conference on Electronic Commerce (EC)*, pages 21–29, 2004.

[2] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[3] Terence S Andre, H Rex Hartson, Steven M Belz, and Faith A McCreary. The user action framework: A reliable foundation for usability engineering support tools. *International Journal of Human-Computer Studies*, 54(1):107–136, 2001.

[4] Apple Inc. App privacy details on the app store. `https://developer.apple.com/app-store/app-privacy-details/`, 2021.

[5] Rebecca Balebako, Pedro Leon, Richard Shay, Blase Ur, Yang Wang, and Lorrie Faith Cranor. Measuring the effectiveness of privacy tools for limiting behavioral advertising. In *Proceedings of the Web 2.0 Security and Privacy Workshop (W2SP)*. IEEE, 2012.

[6] Rebecca Balebako, Richard Shay, and Lorrie Faith Cranor. Is your inseam a biometric? Evaluating the understandability of mobile privacy notice categories. Technical Report CMU-CyLab-13-011, Carnegie Mellon University, 2013.

[7] Carol M Barnum. *Usability Testing Essentials: Ready, Set...Test.* Morgan Kaufmann, 2011.

[8] Paola Benassi. TRUSTe: An online privacy seal program. *Communications of the ACM*, 42(2):56–59, 1999.

[9] Jaspreet Bhatia, Travis D Breaux, Joel R Reidenberg, and Thomas B. Norton. A theory of vagueness and privacy risk perception. In *Proceedings of the International Requirements Engineering Conference (RE)*, pages 26–35, 2016.

[10] Alexander Bleier and Maik Eisenbeiss. The importance of trust for personalized online advertising. *Journal of Retailing*, 91(3):390–409, 2015.

[11] Sophie C Boerman, Sanne Kruikemeier, and Frederik J Zuiderveen Borgesius. Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, 46(3):363–376, 2017.

[12] Harry Brignull. Dark patterns: Deception vs. honesty in UI design. *Interaction Design, Usability*, 338, 2011.

[13] Daniel Bühler, Fabian Hemmert, and Jörn Hurtienne. Universal and intuitive? Scientific guidelines for icon design. In *Proceedings of the Conference on Mensch und Computer (MuC)*, pages 91–103. ACM, 2020.

[14] Bloomberg Businessweek. Business Week/Harris Poll: A Growing Threat. page 96, 2000.

[15] Simon Byers, Lorrie Faith Cranor, Dave Kormann, and Patrick McDaniel. Searching for privacy: Design and implementation of a P3P-enabled search engine. *Privacy Enhancing Technologies*, pages 314–328, 2004.

[16] Fred H. Cate. The limits of notice and choice. *IEEE Security & Privacy*, 8(2):59–62, 2010.

[17] Shruthi Sai Chivukula, Jason Brier, and Colin M. Gray. Dark intentions or persuasion? UX designers' activation of stakeholder and user values. In *Proceedings of the Conference Companion Publication on Designing Interactive Systems (DIS)*, page 87–91. ACM, 2018.

[18] Michael Chromik, Eiband Malin, Sarah Theres Völkel, and Daniel Buschek. Dark patterns of explainability, transparency, and user control for intelligent systems. In *Proceedings of the IUI Workshops*. ACM, 2019.

[19] Josh Constine. A flaw-by-flaw guide to Facebook's new GDPR privacy changes, May 2018. `https://techcrunch.com/2018/04/17/facebook-gdpr-changes/`.

[20] Norwegian Consumer Council. Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy. Technical report, 2018.

[21] Lorrie Faith Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the Workshop on Usability, Psychology, and Security (UPSEC)*. USENIX, 2008.

[22] Lorrie Faith Cranor. Can users control online behavioral advertising effectively? *IEEE Security & Privacy*, 10(2):93–96, 2012.

[23] Lorrie Faith Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications & High Technology Law*, 10:273, 2012.

[24] Lorrie Faith Cranor, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au. Are they worth reading? An in-depth analysis of online trackers' privacy policies. *Journal of Law and Policy for the Information Society*, 11:325, 2015.

[25] Lorrie Faith Cranor, Joseph Reagle, and Mark S Ackerman. Beyond concern: Understanding net users' attitudes about online privacy. Technical Report TR 99.4.1, AT&T Labs-Research, 1999.

[26] Paresh Dave. Websites and online advertisers test limits of European privacy law, 2018. `https://www.reuters.com/article/us-europe-privacy-advertising-gdpr/websites-and-online-advertisers-test-limits-of-european-privacy-law-idUSKBN1JS0GM`.

[27] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. We value your privacy...now take some cookies: Measuring the GDPR's impact on web privacy. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019.

[28] Digital Advertising Alliance. Self-regulatory principles for online behavioral advertising, July 2009. `http://digitaladvertisingalliance.org/principles`.

[29] Disconnect, Inc. Disconnect privacy icons, 2014. `https://github.com/disconnectme/privacy-icons`.

[30] Serge Egelman, Raghudeep Kannavara, and Richard Chow. Is this thing on? Crowdsourcing privacy indicators for ubiquitous sensing platforms. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 1669–1678. ACM, 2015.

[31] Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. Timing is everything? The effects of timing and placement of online privacy indicators. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 319–328. ACM, 2009.

[32] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an IoT privacy and security label? In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pages 771–788. IEEE, 2020.

[33] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2019.

[34] José Estrada-Jiménez, Javier Parra-Arnau, Ana Rodríguez-Hoyos, and Jordi Forné. Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, 100:32–51, 2017.

[35] European Parliament. Regulation (EU) 2016/679 of the European parliament and of the council, 2016. `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679`.

[36] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. Large-scale readability analysis of privacy policies. In *Proceedings of the International Conference on Web Intelligence (WI)*, pages 18–25. IEEE/WIC/ACM, 2017.

[37] Federal Trade Commission. Putting disclosures to the test, November 2016. `https://www.ftc.gov/system/files/documents/reports/putting-disclosures-test/disclosures-workshop-staff-summary-update.pdf`.

[38] Federal Trade Commission. CAN-SPAM Act: A compliance guide for business, March 2017. `https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business`.

[39] Federal Trade Commission. Children's online privacy protection rule: A six-step compliance plan for your business, June 2017. `https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance`.

[40] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking connection security indicators. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2016.

[41] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2021.

[42] Casey Fiesler and Blake Hallinan. "We are the product": Public reactions to online data sharing and privacy controversies in the media. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2018.

[43] Simone Fischer-Hübner, Erik Wästlund, and Harald Zwingelberg. UI prototypes: Policy administration and presentation–version 1. 2009. http://primelife.ercim.eu/images/stories/deliverables/d4.3.1-ui_prototypes-policy_administration_and_presentation_v1.pdf.

[44] Batya Friedman, David Hurley, Daniel C Howe, Edward Felten, and Helen Nissenbaum. Users' conceptions of web security: A comparative study. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, pages 746–747. ACM, 2002.

[45] Lothar Fritsch. Privacy dark patterns in identity management. In *Proceedings of the Open Identity Summit (OID)*, 2017.

[46] Stacia Garlach and Daniel Suthers. 'I'm supposed to see that?'AdChoices usability in the mobile environment. In *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*, 2018.

[47] Ghostery. Ghostery: Homepage, 2017. https://www.ghostery.com.

[48] Julia Gideon, Lorrie Faith Cranor, Serge Egelman, and Alessandro Acquisti. Power strips, prophylactics, and privacy, oh my! In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 133–144, 2006.

[49] Global Privacy Enforcement Network. GPEN Sweep 2017: User controls over personal information, October 2017. https://www.privacyenforcement.net/sites/default/files/2017%20GPEN%20Sweep%20-%20International%20Report.pdf.

[50] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. The dark (patterns) side of UX design. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2018.

[51] Colin M Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2021.

[52] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "It's a scavenger hunt": Usability of websites' opt-out and data deletion choices. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2020.

[53] Hana Habib, Sarah Pearman, Ellie Young, Jiamin Wang, Robert Zhang, Ishika Saxena, and Lorrie Faith Cranor. Identifying user needs for advertising controls on Facebook. In *Submission to the Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2021.

[54] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. An empirical analysis of data deletion and opt-out choices on 150 websites. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2019.

[55] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. Toggles, dollar signs, and triangles: How to (in)effectively convey privacy choices with icons and link texts. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2021.

[56] Munawar Hafiz. A collection of privacy design patterns. In *Proceedings of the Conference on Pattern Languages of Programs (PLoP)*. The Hillside Group, 2006.

[57] Jovanni Hernandez, Akshay Jagadeesh, and Jonathan Mayer. Tracking the trackers: The AdChoices icon, 2011. http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon.

[58] Morten Hertzum. Usability testing: A practitioner's guide to evaluating the user experience. *Synthesis Lectures on Human-Centered Informatics*, 13(1):i–105, 2020.

[59] Kashmir Hill. 'Do Not Track,' the privacy tool used by millions of people, doesn't do anything. *Gizmodo*, October 2018. https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.

[60] Paul Hitlin and Lee Rainie. Facebook algorithms and personal data. Technical report, Pew Research Center, 2019.

[61] Leif-Erik Holtz, Katharina Nocun, and Marit Hansen. Towards displaying privacy information with icons. In *Privacy and Identity Management for Life*, pages 338–348. Springer, 2010.

[62] William K Horton. *The Icon Book: Visual Symbols for Computer Systems and Documentation*. John Wiley & Sons, Inc., 1994.

[63] IAB Europe. EU framework for online behavioural advertising, April 2011. https://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf.

[64] Renato Iannella and Adam Finden. Privacy awareness: Icons and expression for social networks. In *International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods*, 2010. http://virtualgoods.org/2010/VirtualGoodsBook2010_13.pdf.

[65] Carlos Jensen and Colin Potts. Privacy policies as decision-making tools: An evaluation of online privacy notices. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 471–478. ACM, 2004.

[66] Michiel de Jong, Jan-Christoph Borchardt, Hugo Roy, Ian McGowan, Jimm Stout, Suzanne Azmayesh, Christopher Talib, Vincent Tunru, Madeline O'Leary, and Evan Mullen. Terms of service; didn't read, 2021. https://tosdr.org/en/frontpage.

[67] Saraschandra Karanam, Janhavi Viswanathan, Anand Theertha, Bipin Indurkhya, and Herre Van Oostendorp. Impact of placing icons next to hyperlinks on information-retrieval tasks on the web. In *Proceedings of the Annual Meeting of the Cognitive Science Society (CogSci)*, volume 32, pages 2834–2839. Cognitive Science Society, 2010.

[68] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. A "nutrition label" for privacy. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2009.

[69] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 1573–1582. ACM, 2010.

[70] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy as part of the app decision-making process. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 3393–3402. ACM, 2013.

[71] Hyejin Kim and Jisu Huh. Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising*, 38(1):92–105, 2017.

[72] Saranga Komanduri, Richard Shay, Greg Norcie, and Blase Ur. AdChoices? Compliance with online behavioral advertising notice and choice requirements. *A Journal of Law and Policy for the Information Society*, 7, 2011.

[73] Steve Krug. *Don't make me think!: A common sense approach to Web usability*. Pearson Education India, 2000.

[74] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, 2017.

[75] Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Faith Cranor. Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, 2012.

[76] Chris Lewis. *Irresistible Apps: Motivational design patterns for apps, games, and web-based communities*. Springer, 2014.

[77] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycock. Does domain highlighting help people identify phishing sites? In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 2075–2084. ACM, 2011.

[78] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(1):47–64, 2020.

[79] Bin Liu, Andersen Mads Schaarup, Florian Shaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2016.

[80] Dominique Machuletz and Rainer Böhme. Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(2):481–498, 2020.

[81] Maureen Mahoney. California Consumer Privacy Act: Are consumers' digital rights protected? Technical report, Consumer Reports, 2020. `https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf`.

[82] Manfredo Massironi. *The Psychology of Graphic Images: Seeing, Drawing, Communicating*. Psychology Press, 2001.

[83] Arunesh Mathur, Jonathan Mayer, and Mihir Kshirsagar. What makes a dark pattern...dark? Design attributes, normative considerations, and measurement methods. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2021.

[84] Jonathan R Mayer and John C Mitchell. Third-party web tracking: Policy and technology. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2012.

[85] Aleecia M McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *Journal of Law and Policy for the Information Society*, 4:543, 2008.

[86] Aleecia M McDonald and Lorrie Faith Cranor. Americans' attitudes about internet behavioral advertising practices. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*. ACM, 2010.

[87] Aleecia M Mcdonald, Robert W Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. A comparative study of online privacy policies and formats. In *Proceedings of the Symposium on Privacy Enhancing Technologies (PETs)*, pages 37–55. Springer, 2009.

[88] George R Milne and Mary J Culnan. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3):15–29, 2004.

[89] Mozilla. Privacy icons, February 2020. `https://wiki.mozilla.org/Privacy_Icons`.

[90] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. "If I press delete, it's gone" - User understanding of online data deletion and expiration. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 329–339. USENIX, 2018.

[91] Network Advertising Initiative. NAI code of conduct, 2018. `https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf`.

[92] Nielsen Norman Group. Top 10 design mistakes in the unsubscribe experience, April 2018. https://www.nngroup.com/articles/unsubscribe-mistakes/.

[93] Thomas B Norton. The non-contractual nature of privacy policies and a new critique of the notice and choice privacy protection model. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 27:181, 2016.

[94] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, page 1–13. ACM, 2020.

[95] Jonathan A Obar and Anne Oeldorf-Hirsch. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1):128–147, 2020.

[96] Sean O'Connor, Ryan Nurwono, and Eleanor Birrell. (Un)clear and (in)conspicuous: The right to opt-out of sale under CCPA. *arXiv preprint:2009.07884*, 2020.

[97] Office of the California Attorney General. California Consumer Privacy Act (CCPA): Proposed text of regulations, October 2019. https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

[98] Office of the California Attorney General. The California Privacy Rights and Enforcement Act of 2020, 2019. https://oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf.

[99] Office of the California Attorney General. California Consumer Privacy Act (CCPA): Final text of proposed regulations, August 2020. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.

[100] Online Trust Alliance. Email marketing & unsubscribe audit, December 2017. https://otalliance.org/system/files/files/initiative/documents/2017emailunsubscribeaudit.pdf.

[101] Rebecca S Portnoff, Linda N Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. Somebody's watching me? Assessing the effectiveness of webcam indicator lights. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 1649–1658. ACM, 2015.

[102] PrivacyGrade.org. Privacygrade.org, 2020. http://privacygrade.org/home.

[103] Emilee Rader. Awareness of behavioral tracking and information privacy concern in Facebook and Google. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, page 17, 2014.

[104] Joel R Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T Graves, Fei Liu, Aleecia McDonald, Thomas B Norton, and Rohan Ramanath. Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal*, 30:39, 2015.

[105] Joel R Reidenberg, N Cameron Russell, Alexander J Callen, Sophia Qasir, and Thomas B Norton. Privacy harms and the effectiveness of the notice and choice framework. *I/S: A Journal of Law & Policy for the Information Society*, 11:485, 2015.

[106] Joel R Reidenberg, N Cameron Russell, Vlad Herta, William Sierra-Rocafort, and Thomas B Norton. Trustworthy privacy indicators: Grades, labels, certifications, and dashboards. *Washington University Law Review*, 96, 2018.

[107] Arianna Rossi and Monica Palmirani. DaPIS: A data protection icon set to improve information transparency under the GDPR. *Knowledge of the Law in the Big Data Age*, 252:181–195, 2019.

[108] John A Rothchild. Against notice and choice: The manifest failure of the proceduralist paradigm to protect privacy online (or anywhere else). *Cleveland State Law Review*, 66:559, 2017.

[109] Richard Rutter, Patrick H Lauke, Cynthia Waddell, Jim Thatcher, Shawn Lawton Henry, Bruce Lawson, Andrew Kirkpatrick, Christian Heilmann, Michael R Burks, Bob Regan, et al. *Web Accessibility: Web Standards and Regulatory Compliance*. Apress, 2007.

[110] Elizabeth B-N Sanders. Converging perspectives: Product development research for the 1990s. *Design Management Journal*, 3(4):49–54, 1992.

[111] Florian Schaub and Lorrie Faith Cranor. Usable and useful privacy interfaces. In Travis Breaux, editor, *An Introduction to Privacy for Technology Professionals*, pages 176–299. IAPP, 2020.

[112] Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie Faith Cranor. Watching them watching me: Browser extensions' impact on user privacy awareness and concern. In *Workshop on Usable Security and Privacy (USEC)*. Internet Society, 2017.

[113] Stuart E Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The emperor's new security indicators. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pages 51–65. IEEE, 2007.

[114] Mark Scott and Laurens Cerulus. Europe's new data protection rules export privacy standards worldwide. *Politico*, January 2018.

[115] Robert H Sloan and Richard Warner. Beyond notice and choice: Privacy, norms, and consent. *Journal of High Technology Law*, 14:370, 2014.

[116] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. Circumvention by design - dark patterns in cookie consent for online news outlets. In *Proceedings of the Nordic Conference on Human-Computer Interaction (NordiCHI)*, 2020.

[117] Daniel J Solove. Privacy self-management and the consent dilemma. *Harvard Law Review*, 126:1880, 2012.

[118] Stanford Legal Design Lab. Icons for legal help, 2020. `https://betterinternet.law.stanford.edu/design-guide/icons-for-legal-help/`.

[119] The Digital Advertising Alliance. Digital advertising alliance announces CCPA tools for ad industry, November 2019. `https://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-announces-ccpa-tools-ad-industry`.

[120] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2):254–268, 2011.

[121] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. Americans reject tailored advertising and three activities that enable it, 2009. `https://ssrn.com/abstract=1478214.143`.

[122] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2012.

[123] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the Conference on Computer and Communications Security (CCS)*, pages 973–990. ACM, 2019.

[124] W3C Policy Languages Interest Group. Platform for privacy preferences (P3P) project, 2018. `https://www.w3.org/P3P//`.

[125] W3C Web Accessibility Initiative. Web content accessibility guidelines (WCAG) 2.1, 2018. `https://www.w3.org/TR/WCAG21/`.

[126] W3C Working Group. Tracking preference expression (DNT), 2019. `https://www.w3.org/TR/tracking-dnt/`.

[127] Ari Ezra Waldman. Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, 31, 2020.

[128] Miranda Wei, Madison Stamos, Sophie Veys, Nathan Reitinger, Justin Goodman, Margot Herman, Dorota Filipczuk, Ben Weinshel, Michelle L Mazurek, and Blase Ur. What Twitter knows: Characterizing ad targeting practices, user perceptions, and ad explanations through users' own Twitter data. In *Proceedings of the USENIX Security Symposium*, page 19. USENIX, 2020.

[129] Susan Wiedenbeck. The use of icons and labels in an end user application program: An empirical study of learning and retention. *Behaviour & Information Technology*, 18(2):68–82, 1999.

[130] Chauncey Wilson. *User Interface Inspection Methods: A User-Centered Design Method*. Newnes, 2013.

[131] Michael S Wogalter. Communication-human information processing (C-HIP) model. *Handbook of warnings*, pages 51–61, 2006.

[132] Yaxing Yao, Davide Lo Re, and Yang Wang. Folk models of online behavioral advertising. In *Proceedings of the Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)*, pages 1957–1969, 2017.

[133] José P Zagal, Staffan Björk, and Chris Lewis. Dark patterns in the design of games. In *Proceedings of the Foundations of Digital Games (FDG)*, 2013.