Evaluating the Usability of Privacy Choice Mechanisms

Hana Habib

CMU-ISR-21-109
September 2021

Institute for Software Research
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Thesis Committee:
Lorrie Faith Cranor (Chair)
Alessandro Acquisti
Norman Sadeh
Rebecca Balebako (Google)

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Societal Computing.

Keywords: Privacy, usability, choice interfaces, opt-out choices, advertising controls, usability evaluations, privacy icons, privacy regulation

To those in need of usable privacy controls.

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 related to existing privacy choice mechanisms, 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 choice mechanisms. 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 controls. One potential means of making privacy choice mechanisms more visible to consumers is through the use of icons. The third study described in this thesis explains the design and evaluation of new icons and accompanying text descriptions to effectively communicate the presence of privacy choices. In addition to discoverability issues, privacy choice mechanisms 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 interfaces through which privacy choice mechanisms are provided. Despite increased regulatory requirements and consumer pressure for privacy choice mechanisms, there is little direction for design and privacy practitioners on how to systematically evaluate such interfaces. To address this need, I developed comprehensive guidance for conducting such evaluations that pertain to different aspects of usability, such as user awareness and comprehension of privacy choice interfaces. This guidance provides an overview of HCI research methods, as well as example heuristics, prompts, and metrics, for measuring specific usability problems in privacy choice interfaces. To demonstrate the application of this guidance, the final study described in this thesis evaluated the impact of different design aspects of cookie consent notices, providing actionable recommendations that would improve the usability of these interfaces.

Acknowledgments

The work presented in this thesis would not be possible without the guidance of several mentors. I especially would like to thank my advisor Dr. Lorrie Cranor for always providing me the support I needed throughout my PhD. I also appreciate the invaluable feedback provided by other members of my committee: Dr. Alessandro Acquisti, Dr. Rebecca Balebako, and Dr. Norman Sadeh. Other faculty research mentors I would like to acknowledge include Dr. Lujo Bauer, Dr. Nicolas Christin, and Dr. Florian Schaub.

I am extremely grateful for my co-authors' contributions to this work, including those by Aditi Jannu, Megan Li, Sarah Pearman, Neha Sridhar, Chelse Swoopes, Jiamin Wang, Ellie Young, Yixin Zou, Dr. Joel Reidenberg, and Dr. Yaxing Yao. I also would like to recognize Dr. Yuanyuan Feng, Dr. Justin Hepler, Dr. Liz Keneski, Dr. Hanna Schraffenberger, and members of the Usable Privacy Project for their insights on this research.

I am thankful to members of the CUPS lab and other CyLab colleagues whose camaraderie and knowledge-sharing greatly shaped this thesis; particularly Aurelia Augusta, Jessica Colnago, Kyle Crichton, Pardis Emami-Naeini, Abbby Marsh, Maggie Oates, and Josh Tan. I am also deeply appreciative of the dedicated members of the ISR Staff, especially Tiffany Todd and Connie Herold for their support throughout my PhD.

Last, I would like to thank my family and friends for their endless love and encouragement. I am particularly grateful for my husband and son who make life better in so many ways.

Contents

List of Figures

List of Tables

Chapter 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, mechanisms related to consent and privacy choice have become common. However, the notice and choice model is an imperfect solution to privacy protection in today's digital age [20, 109, 124, 131, 133]. A major criticism is the lack of transparency and choice provided by traditional notice and choice mechanisms such as privacy policies [124]. 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 [133]. 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 [144]. Despite these limitations, legal and privacy experts still argue that individual decision-making and privacy choice should have a role within an effective consumer privacy protection framework [28, 121, 133].

Furthermore, the notice and choice framework has continued to serve as the foundation of legal and self-regulatory privacy efforts, which mandate certain types of privacy choices. 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 [42, 115]. Other types of controls, such as opt-outs for email marketing have been mandated by United States law since 2003 [46]. These regulations place an emphasis on usability, requiring "plain" language and choices be available through "conspicuous" links [42, 46, 115]. 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 [34, 107] and technical standards like Do Not Track implemented in major web browsers [143].

Prior work has identified many deficiencies related to current consent and privacy choice mechanisms available to consumers. First, there is evidence suggesting non-compliance with existing privacy laws and self-regulatory agreements [30, 32, 116]. Additionally, some privacy choice mechanisms offered to consumers are ineffective due to lack of enforcement and buy-in from companies handling consumer data [28]. 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 [89]. Another usability obstacle is the use of dark patterns in privacy choice and consent interfaces that nudge users toward less privacy-protective options [3, 25, 132]. 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 contributes to a better understanding of how current consent and privacy choice mechanisms can be improved. Specifically, the work described focuses on "opt-out" choice mechanisms, which allow consumers to deny some aspect of data collection or processing, as they are the most common implementation of choice under the current notice and choice paradigm. The first portion of this thesis furthers explore different usability aspects of web-based privacy choice mechanisms. First, it provides an overview of how these privacy choices are provided in practice, particularly mechanisms related to email marketing, targeted advertising, and data deletion (Chapter 3), and then describes different usability issues related to common implementations of these privacy choice mechanisms (Chapter 4). Next, this thesis summarizes to what extent graphical icons can effectively communicate the presence of privacy choices (Chapter 5). In the next chapter, this thesis assesses how well controls for targeted advertising on Facebook are aligned with user needs (Chapter 6). The second portion of this thesis proposes and demonstrates a comprehensive set of guidelines for conducting systematic usability evaluations of consent and privacy choice interfaces. It first describes the development of this guidance, which defines seven high-level usability objectives for privacy choice interfaces and includes guidelines for practitioners on utilizing traditional HCI research methods to uncover usability issues (Chapter 7). Finally, this thesis demonstrates the application of this guidance in an extensive usability evaluation of cookie consent interfaces, which demonstrated the impact of different design choices on overall usability (Chapter 8).

Thesis Statement

This thesis describes usability issues that limit the effectiveness of existing privacy choice mechanisms, provides guidelines for conducting systematic usability evaluations of privacy choice interfaces, and demonstrates the application of this guidance in a comprehensive evaluation of cookie consent interfaces.

Chapter 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 they 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) [42]. 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 [130].

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 [115].

[1]This overview was adapted from the Background and Related Work sections of the studies described in this thesis [61, 62, 63, 64].

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 [113]. 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 [115]. 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 [114].

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 [47]. 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 [46].

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 [141, 143]. However, unresolved ambiguities regarding the implementation of these protocols and lack of industry support led to poor adoption [28, 68]. 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 [34, 74, 107]. 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 [34]. 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 [100]. 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 [74]. 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 [135].

Though privacy legislation including the GDPR and CCPA have provided some amount of baseline privacy protection, these legislative and self-regulatory efforts have primarily resulted in additional privacy choices being available for consumers. The availability of these choices provides consumers greater control over how their digital data is used and handled by companies, empowering individual decision-making.

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 [116]. 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 [33]. 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 [132]. 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 [32]. 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 [24]. 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 [25].

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 [97]. 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 [112]. 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 [66]. Less than half of DAA and NAI members examined by Komanduri et al. complied with the enhanced notice requirement of these organizations' guidelines [85]. 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 [30]. 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 [18]. Similarly, in another 1999 survey, 70% of respondents wanted to have the choice to be removed from a website's mailing list [29]. In Rader et al.'s interview study, awareness of data aggregation and cross-platform inferences increased the likelihood of privacy concern [119]. 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 [106]. 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 [50].

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 [12, 84]. 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 [137]. 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 [102]. 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" [139].

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 [102]. 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 [149]. 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 [70]. 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 [119, 139]. 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 [145].

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 Choice Mechanisms

Despite significant privacy concerns, consumers struggle to protect their online privacy against targeted advertising for multiple reasons [27]. 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, 41]. Furthermore, the usability of websites' privacy communications has long been problematic [101, 102]. Recent work has shown that privacy policies, where privacy choices are often disclosed, still exhibit low readability scores [44, 94]. Additionally, most websites fail to provide specific details regarding the entities with which they share data and the purposes for which data is shared [58].

Another barrier to the usability of privacy choice 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 [16]. Since the concept was introduced, different taxonomies have been developed to categorize dark patterns (e.g., [59, 65, 91]). Dark patterns have been found in different aspects of transparency and privacy, such as explanations of AI algorithms [23] and identity management controls [54], which overlap with the design of consent and privacy choice interfaces. Consent interfaces specifically have also been evaluated for dark patterns using different methodologies. Utz et al. conducted a field study exploring the impact of four design variables, finding that position of the interface, choices offered, nudging patterns, and language used in the interface text impact users' interactions with the interface [140]. 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 [60]. 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 [110]. In contrast, studies have also shown how design patterns could be used to nudge users toward more privacy-protective options in different contexts [3].

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 [108]. 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% spec-

ified the retention time of inactive accounts [58]. 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 [13]. 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 [6]. 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 [100]. 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 [89, 128]. 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 [102, 139]. Moreover, when the AdChoices icon is presented on a mobile device, it tends to be difficult for people to see [55].

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 (Chapters 3, 4, 5, 6, 8). Moreover, Chapter 7 of this thesis presents 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.

2.5 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 [104, 111] or struggle to comprehend them due to vague descriptions and jargon [11, 76, 103, 120]. Given the estimated time required to peruse privacy policies on visited websites, it would be unrealistic to expect users to read them routinely [101]. These findings suggest the need for alternative privacy notices or additional tools that make privacy information more accessible and understandable [127]. Examples of such alternatives include privacy dashboards [8, 56], privacy certifications and seals [10], privacy grades and scores [37, 57, 77, 118], privacy labels [39, 80, 82, 136], consent banners and pop-ups [96, 110, 140], and privacy icons [71, 75, 105, 123].

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

Privacy dashboards allow consumers to inspect the data companies have collected about them and adjust their privacy settings [122]. 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 [56], while the Opt-Out Easy browser extension surfaces opt-out choice mechanisms from a website's privacy policy [8]. Privacy seals and certifications, such as the Enterprise Privacy Certification by TrustArc (formerly TRUSTe) [10], are designed to signal that businesses comply with legal requirements or industry standards [122]. Privacy grades and scores indicate how well websites protect their users' privacy through numeric ratings, (e.g., ToS;DR [77], Privacy Finder [37, 57], and PrivacyGrade.org for mobile apps [118]). Privacy labels, similar to food nutrition labels, help users quickly learn about and compare privacy-related attributes of products or services, including websites [80, 81], Internet of Things devices [39, 40], search results [19, 136], and mobile apps [5, 82]. Privacy choices, mostly related to cookie management, are also presented in consent pop-ups and banners on websites [33].

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 [35] and Mozilla's icons for retention periods and third-party data sharing and use [105]. Some only serve specific application domains, such as social media [75], web links [78], or webcams [38, 117], while others can apply across contexts [71]. Icons are also commonly used as security indicators (e.g., a lock in a browser's URL bar that indicates HTTPS [48]). However, prior work has found that users tend to ignore or misunderstand these indicators [53, 93, 129]. 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 [134]. While the Data Protection Icon Set (DaPIS) has been user-tested, it is specific to GDPR consumer privacy rights [123] .

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 [98]. Icons can be useful information markers since they are easy to recognize [17, 73]. When placed next to lengthy privacy statements, icons can enhance readability by helping users navigate the text [123]. 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 [17]. However, designing comprehensible icons is challenging. Icons alone sometimes perform worse than text-only or icon-text interfaces in assisting learning [146]. Fischer-Hübner et al. therefore argue that icons should be used alongside text to illustrate data practices in privacy policies and aid user comprehension [51]. 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 [55].

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 [55, 102, 139]. 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 (Chapter 5). Complementing prior research on icons for GDPR-specific user rights [123], 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 [9]. 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) [4]. 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) [49]. They further describe a design space for privacy choices, which is complementary to the usability testing guidelines that this thesis contributes in Chapter 7.

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 [67]. 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 [87]. 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 [147]. 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 [147]. Sandars argues that two or more evaluation techniques may be required to fully understand user needs [126]. However, as has become common adage,"testing one user is 100 percent better than testing none" [86].

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 is-

sues have a greater impact on people with disabilities or who use assistive technologies [125]. 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 [125, 142]. 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 [125]. This thesis draws on existing guidelines for accessibility as they provide direction as to what type of guidance is 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 [99]. 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 [150]. 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 described in Chapter 7 complement existing ones for evaluating the effectiveness of privacy disclosures [45, 127]. These evaluation guidelines could also utilize cognitive frameworks related to privacy and security decision-making, such as the Communication-Human Information Processing (C-HIP) model from the field of warnings science [148] 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 [26]. 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 [39, 136]. 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 [40]. 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 [37, 82]. 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 [7] and Kelley et al. which measured knowledge retention from

different formats of privacy disclosures [81]. While this prior work focused on evaluating privacy disclosures, similar approaches can be utilized for the evaluation of privacy choice and consent interactions and are outlined in the guidelines presented in Chapter 7 of this thesis.

Chapter 3

An Empirical Analysis of Data Deletion and Opt-Out Choices

As described in Chapter 1, the dominant approach for dealing with privacy concerns online, especially in the United States, has largely centered around the concepts of notice and consent [121]. Along with transparency, consumer advocates and regulators have asserted the need for consumers to have control over their personal data [**? ? ?**]. This has led some websites to offer different types of privacy controls, such as opt-outs for email communications or targeted ads, and mechanisms for consumers to request removal of their personal data from companies' databases.

Despite the availability of privacy controls, including mechanisms created by industry self-regulatory groups (e.g., the Digital Advertising Alliance [34]) as well as those mandated by legislation, consent mechanisms appear to have failed to provide meaningful privacy protection [28, 124]. For example, many consumers are unaware that privacy choice mechanisms exist [55, 102, 139]. Additionally, past research has identified usability and noncompliance issues with particular types of opt-outs, such as those for email communications and targeted advertising [41, 66, 85, 89, 116]. This thesis builds on this prior work by contributing a large-scale and systematic review of website privacy choices, providing deeper insight into how websites offer such privacy choices and why current mechanisms might be difficult for consumers to use.

This chapter details findings from an in-depth heuristic analysis of opt-outs for email communications and targeted advertising, as well as data deletion choices, available to US consumers. Through a manual review of 150 English-language websites sampled across different levels of popularity, we analyzed the current practices websites use to offer privacy choices, as well as issues that may render some choices unusable. Our empirical analysis focused on two research questions: 1) What choices related to email communications, targeted advertising, and data deletion do websites offer? and 2) How are websites presenting those privacy choices to their visitors?

We found that most websites in our sample offered choices related to email marketing, targeted advertising, and data deletion where applicable: nearly 90% of websites that mentioned

This chapter is a lightly edited version of a paper previously published as: Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Floriah 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). 2019 [61].

using email communications or targeted advertising in their privacy policy provided an opt-out for that practice, and nearly 75% offered a data deletion mechanism. These choices were provided primarily through website privacy policies, but were often also presented in other locations. Furthermore, our heuristic evaluation revealed several reasons why people may find these choices difficult to use and understand. In over 80% of privacy policies analyzed, the policy text omitted important details about a privacy choice, such as whether a targeted advertising opt-out would stop all tracking on a website, or the time frame in which a request for account deletion would be completed. Though a less frequent occurrence, some policies contained opt-out links that direct the user to a page without an opt-out, or referred to non-existent privacy choices. We further observed a lack of uniformity in the section headings used in privacy policies to describe these choices. Compounded, these issues might make privacy choices hard to find and comprehend.

This chapter makes the following contributions:

- A better understanding of the mechanisms websites currently use to provide choices related to these practices.
- Analysis of how current mechanisms may fall short in helping consumers take advantage of available choices.
- Discussion of a foundation for future research into the development of best practices for the implementation of privacy choice mechanisms.

3.1 Methodology

We developed an analysis template for the systematic analysis of data deletion, email, and targeted advertising choices offered by websites along multiple metrics. Our analysis included websites sampled across different ranges of web traffic that were registered primarily in the United States.

3.1.1 Template for Analysis

We implemented a comprehensive template in Qualtrics to facilitate standardized recording of data for researchers' manual content analysis of websites. For the purpose of our analysis, we defined opt-outs for email communications as mechanisms that allow users to request that a website stop sending them any type of email message (e.g., marketing, surveys, newsletters). Any mention of an advertising industry website or opt-out tool, as well as descriptions of advertising-related settings implemented by the website, browser, or operating system (e.g., "Limit Ad Tracking" in iOS) was considered as an opt-out for targeted advertising. We identified data deletion mechanisms as a means through which users can delete their account or information related to their account, including via an email to the company.

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 complete the template, researchers were asked to:

1. Visit the homepage of the website.
2. Note if there was a notice to consumers regarding the use of cookies on the website.
3. Create a user account for the website using an alias and email address provisioned for this analysis.
4. Review any targeted advertising opt-outs on a page linked from the homepage that describes advertising practices (i.e., an "AdChoices" page).
5. Visit the website's privacy policy.
6. Review any email communications in the privacy policy.
7. Review any targeted advertising opt-outs in the policy.
8. Review any data deletion mechanisms in the policy.
9. Note whether the privacy policy mentions Do Not Track.
10. Note any other privacy choices in the privacy policy and linked pages providing privacy information.
11. Review any email communications opt-outs in the user account settings.
12. Review any targeted advertising opt-outs in the user account settings.
13. Review any data deletion mechanisms in the user account settings.
14. Note any other privacy choices in the account settings.

At every stage, researchers also made note of practices for offering privacy controls that seemed particularly detrimental or beneficial to usability throughout the Interaction Cycle, a framework for describing the end-to-end interaction between a human and a system [4].

To refine the template, our research team conducted six rounds of pilot testing with 25 unique websites from Amazon Alexa's[1] ranking of top 50 US websites. For every round of piloting, two researchers independently analyzed a small set of websites. We then reconciled disagreements in our analysis, and collaboratively revised the questions in the template to ensure that there was a mutual understanding of the metrics being collected.

3.1.2 Website Sample

We examined 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 selected two thresholds to divide websites and categorized them as: *top websites* (ranks 1 - 200), *middle websites* (ranks 201 - 5,000), and *bottom websites* (ranks ¿ 5,000). These thresholds were identified by plotting websites' reach against their rank, and observing the first two ranks at which reach leveled off. Our analysis included 50 *top*, 50 *middle*, and 50 *bottom* websites randomly selected from each range. We stratified our sample as such, since consumers may spend significant time on websites in the long tail of popularity. The stratified sample enables us to understand the privacy choices provided on low-traffic websites, and how they differ from choices on popular websites.

The ICANN "WHOIS" record of 93 websites in our sample indicated registration in the United States, while other websites were registered in Europe (26), Asia (11), Africa (4), Central

[1] Amazon Alexa Top Sites: https://www.alexa.com/topsites

America/the Caribbean (2), or contained no country related information (14). In constructing our sample, we excluded porn websites to prevent researchers' exposure to adult content. To simplify our data collection, we also excluded a handful of websites drawn during our sampling that required a non-email based verification step, or sensitive information like a social security number (SSN) or credit card, to create a user account. Due to the language competencies of the research team, we only included websites written in English, or those with English versions available. All websites included in our study were analyzed between April and October 2018. Data collected from our pilot rounds are not included in our analysis. The types of websites included in our sample ranged from popular news and e-commerce websites to university and gaming websites.

Due to the GDPR, many websites were releasing new versions of their privacy policies during the period of our data analysis. In October 2018 we reviewed all websites in our dataset that had been analyzed prior to May 25, 2018, the GDPR effective date, and conducted our analysis again on the 37 websites that had updated their privacy policy. Our reported findings are primarily based on the later versions of these policies, but we also compared the pre- and post-GDPR versions for these websites, and highlight differences.

3.1.3 Data Collection

The researchers involved in data collection went through a training process during which they completed the template for several websites prior to contributing to the actual dataset. To ensure thorough and consistent analysis, two researchers independently analyzed the same 75 (50%) websites sampled evenly across categories. Cohen's Kappa ($\kappa = 0.82$) was averaged over the questions in which researchers indicated whether or not privacy choice mechanisms were present on the page being analyzed. All disagreements in the analysis were reviewed and reconciled, and the remaining 75 websites were coded by only one researcher. Analyzing one website took 5 to 58 minutes, with an average of 21 minutes spent per website. This variance in analysis time was related to websites' practices. For example, websites that did not use email marketing or targeted advertising could be reviewed more quickly. To prevent browser cookies, cookie settings, or browser extensions from affecting website content, researchers collected data in Google Chrome's private browsing mode, opening a new browser window for each website.

3.1.4 Limitations

The privacy choices we reviewed may not be representative of all websites. Our sample only included English-language websites, which may not be reflective of websites in other languages. We also only included websites from Alexa's top 10,000 list. Websites with lower rankings may exhibit a different distribution of choices than that observed in our sample. Moreover, in the process of random sampling, we excluded a small number of websites, primarily for financial institutions, that required sensitive personal information (e.g., SSN or credit card) for account registration. Considering the sensitive nature of this type of personal information, these websites may offer privacy choices through different means or offer other choices. However, our sample still includes many websites that collect credit card information and other sensitive personal information, but do not require it for account creation. Despite these exclusions, we are confident

the websites we analyzed provide broad coverage of websites' most prominent practices for offering opt-outs and deletion mechanisms.

Additionally, since our analysis was conducted using US IP addresses, we may not have observed privacy choices available to residents of other jurisdictions (such as the EU) with other legal privacy requirements. Our analysis thus only reflects privacy choices available to US-based consumers.

Lastly, our study cannot provide definite conclusions about how consumers will comprehend and utilize the privacy choices we analyzed. We chose a content analysis approach in order to be able to gain a systematic overview of current practices in provisioning opt-out choices, which was not provided by prior work at this scale. Nonetheless, based on prior opt-out evaluations and design best practices, we hypothesize that certain design choices (e.g., multiple steps to an opt-out choice) will appear difficult or confusing to users. Our findings also surface many other issues that pose challenges to consistent privacy choice design. The effects of these issues on consumers could be studied in future work.

3.2 Results

Our manual content analysis of 150 websites revealed that privacy choices are commonly available, but might be difficult to find and to comprehend. We identified several factors that likely negatively impact the usability of privacy choices, such as inconsistent placement, vague descriptions in privacy policies, and technical errors.

3.2.1 Overview of Privacy Policies

Nearly all of the websites in our sample included a link to a privacy policy from the home page. The only websites that did not include a privacy policy were three bottom websites. Of the 147 policies analyzed, 15% (22) were a corporate policy from a parent company. In line with prior findings, comprehension of the text that describes privacy choices requires advanced reading skills [44]. However, about a third of policies in our analysis adopted tables of contents to present the information in a structured way, or linked to separate pages to highlight particular sections of the policy.

Privacy choices text has poor readability. For websites in our sample that had a privacy policy, we recorded the policy text and marked out the portions that described privacy choices. We then conducted a readability analysis using the text analysis service readable.io.

As reported in Table 3.1, the Flesch Reading Ease Scores (FRES) for text related to email opt-outs, targeted advertising opt-outs, and data deletion choices received means and medians of about 40 on a 0 to 100 point scale (with higher scores indicating easier-to-read text) [**?**]. The analyzed text for all three types of privacy choices on the Flesch-Kincaid Grade Level (FGL), a grade-based metric, had means and medians around 13, which implies the text requires the audience to have university-level reading abilities. On Flesch's 7-level ranking system, over 90% of the analyzed privacy choices were described in text that was "very difficult," "difficult," or "fairly difficult" to read.

	Flesch Reading Ease		Flesch-Kincaid	
	Mean	SD	Mean	SD
Email Comm.	39.54	13.55	13.89	3.40
Targeted Adv.	39.38	15.41	13.72	4.48
Data Deletion	38.98	17.89	14.28	5.40
Privacy Policies	45.80	10.72	10.20	2.44

Table 3.1: Readability scores for privacy policy text describing email opt-outs, advertising opt-outs, and deletion choices.

Privacy policies as a whole had better, but not ideal, readability, compared to privacy choice text: our analyzed privacy policies had a mean FRES of 45.80 and a mean FGL of 10.20, which align with prior readability evaluations of privacy policies, both across domains [44] and for particular categories (e.g., social networking, e-commerce, and healthcare websites [**?** **?**]). Nevertheless, literacy research suggests materials approachable by the general public should aim for a junior high reading level (i.e., 7 to 9) [**?**]. These statistics of our analyzed privacy policies and text related to privacy choices, which were all post-GDPR versions, suggest that most of them still fail to comply with the GDPR's "clear and plain language" requirement, a key principle of transparency.

Some websites use table of contents and support pages. We also observed that a significant portion of the policies in our sample were organized using a table of contents. Of the 147 privacy policies, 48 (33%) included a table of contents, which provides a road map for users to navigate a policy's sections. Additionally, 53 (36%) policies linked to secondary pages related to the company's privacy practices. For example, Amazon and Dropbox have individual pages to explain how targeted advertising works and how to opt-out.

3.2.2 Presence of Privacy Choices

In this section, we first focus on whether and where choices were present on the websites analyzed. More details about how these choices are described in policies are presented in Section 3.2.3. We found that privacy choices are commonly offered across all three website tiers. Beyond privacy policies, websites often provide opt-outs and data deletion choices through other mechanisms, such as account settings or email.

Privacy choices are prevalent. All three types of privacy choices were prevalent in our sample. As seen in Table 3.2, 89% of websites with email marketing or targeted advertising offered opt-outs for those practices, and 74% of all websites had at least one data deletion mechanism. The location of privacy choices across top, middle, and bottom websites is displayed in Figure 3.1. Top websites were found to provide more privacy choices than middle and bottom websites.

	Email Comm.	Targeted Adv.	Data Deletion
# of sites applicable	112	95	150
# of sites choice present	100	85	111
% of applicable sites	89%	89%	74%

Table 3.2: Summary of the availability of each type of privacy choice and websites on which they are applicable.

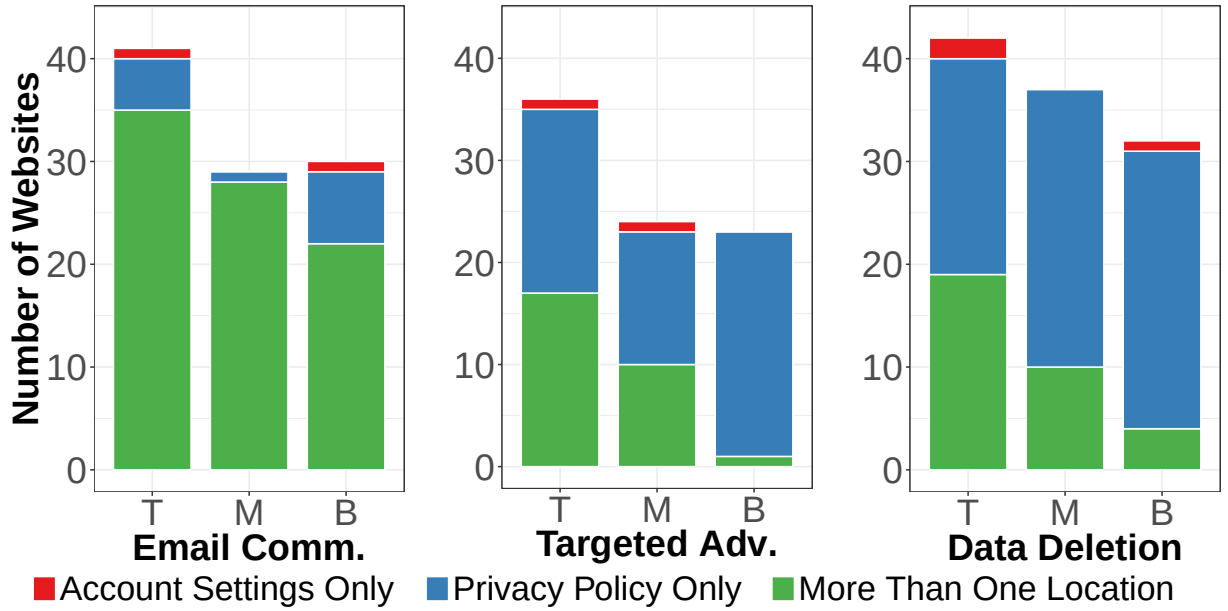


Figure 3.1: Location of privacy choices for top, middle, and bottom websites. Top websites offered the most privacy choices.

Email opt-outs were links in policies and emails. Most often, opt-outs for email communications were offered in multiple ways. Nearly all (98 of 100) websites offering email communication opt-outs presented the opt-out for emails in the privacy policy; however, only 31 policies included a direct link to the opt-out page, while 70 stated that users could unsubscribe within emails. Additionally, 51 websites had an opt-out in the account settings, the majority of which (33) lead to the same opt-out described in the privacy policy, and 15 websites provided a choice for email communication during account creation.

Advertising opt-outs were links in privacy policies. Websites primarily used their privacy policy to provide opt-outs for targeted advertising. Of 85 websites that offer at least one targeted advertising opt-out, 80 provided them in the privacy policy. Among them, 74 also provided at least one link, while the remaining just described an opt-out mechanism with text, such as "...you can opt out by visiting the Network Advertising initiative opt out page." However, 58 websites had multiple links leading to different opt-out tools, which may cause confusion about

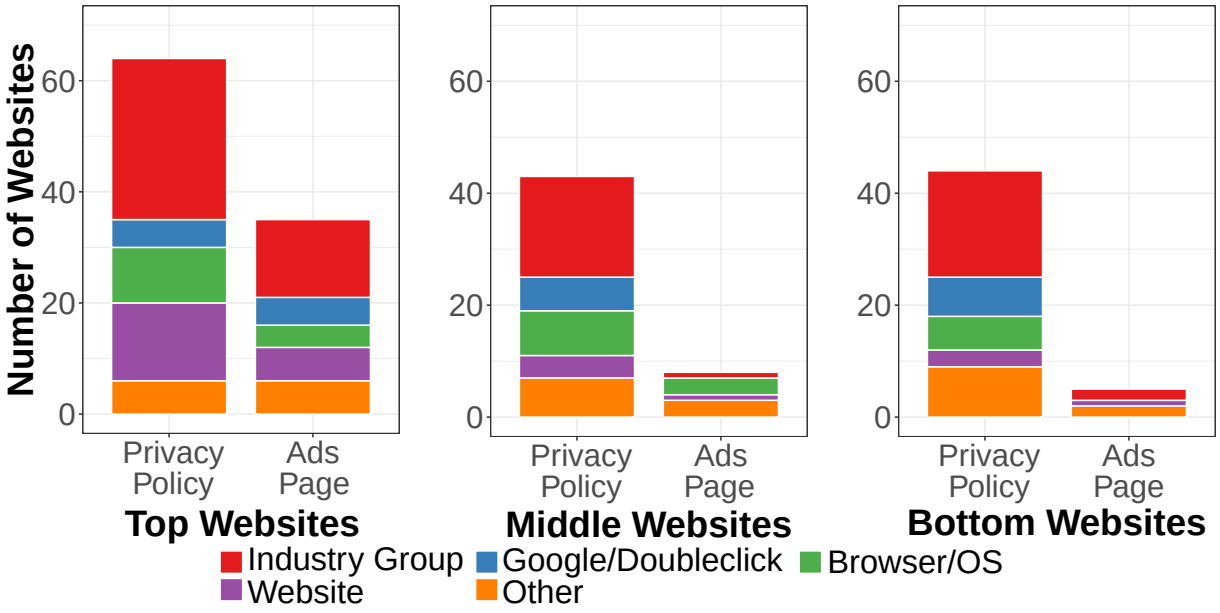


Figure 3.2: Distribution of different types of targeted advertising opt-outs in privacy policies and "About Ads" pages across top, middle, and bottom websites.

which tool visitors should prioritize and what the differences are.

On 26 websites, an "AdChoices" page linked from the homepage described the website's advertising practices and presented opt-out choices. Among them, 15 used text containing the words "ad choices" to refer to the page; others labeled the page as "interest-based ads," "cookie information" or "cookie policy." Additionally, 12 websites included opt-outs in the user account settings, 11 of which led to the same opt-out page presented in the policy.

As seen in Figure 3.2, many websites referred to opt-out tools provided by advertising industry associations. However, 27% of opt-out links pointing to the DAA or NAI directed visitors to their homepages, instead of their opt-out tools. This creates a substantial barrier for people to opt-out because visitors still need to find the appropriate opt-out tool on the DAA and NAI websites. Conversely, 21 of 22 links to the European Interactive Digital Advertising Alliance (EDAA) in the website policies led directly to the EDAA's opt-out tool. Less common, some websites provided advertising opt-outs implemented by Google or the website itself. Others provided instructions for adjusting cookie or ad related settings in the browser or operating system, such as the "Limit Ad Tracking" setting in iOS. The use of other services like TrustArc (formerly TRUSTe) or Evidon was also relatively rare.

Data deletion controls were provided in privacy policies and account settings. We observed that 111 websites in our sample (74%) provided data deletion mechanisms to their users, which is higher than the 51% in the sample analyzed by GPEN in 2017 [58]. Among websites offering deletion mechanisms, 75 only provided the choices through the privacy policy, three only displayed them in the user account settings, and 33 provided them through multiple locations. However, even when data deletion choices are described in the privacy policy, only 27 policies

included a direct link to a data deletion tool or request form. The more common practice was to offer instructions about how to email a data deletion request, as was done in 81 policies.

The GDPR contributed to more deletion controls. In our sample, 37 websites updated their privacy policy around the GDPR effective date. Four websites added their privacy policies post-GDPR. Most of the 37 websites had already included descriptions of privacy choices before the GDPR effective date, especially for marketing opt-outs (29 out of 37). In our sample, the GDPR had the greatest impact on data deletion controls, with 13 websites adding instructions for deleting account data to their post-GDPR privacy policy. However, such dramatic change was not observed for marketing and targeted advertising opt-outs.

Websites include other data collection controls. Though less common, some websites described additional privacy-related opt-outs in their privacy policy and account settings. Opt-outs for web analytic services (e.g., Google Analytics) were offered by 21% (31) of websites. Interestingly, 17 websites offered opt-outs for the sharing of personal information with third parties. For example. CNN's privacy policy[2] stated that "We may share the Information with unaffiliated Partners and third parties…" and provided a link to an opt-out from such sharing. Additionally, nine websites described controls offered by the website, browser, or operating system related to the use of location history or location data.

Only 28 of the 150 websites analyzed (19%) displayed a cookie consent notice on their home page, alerting users that cookies are being used on the website and getting consent to place cookies in the user's browser. Among them, only five offered a means to opt out or change cookie related settings. However, as these websites were accessed from US IP addresses, we may have observed different practices than those offered to EU-based visitors. Prior work has found a substantial increase in cookie consent notices on European websites post-GDPR [33].

Do Not Track has low adoption. Of the 150 websites analyzed, only eight (5%) specified that they would honor Do Not Track (DNT), a mechanism that allows users to express that they wish not to be tracked by websites, while 48 (32%) explicitly stated that the website will not honor it [143]. Another 91 (61%) did not specify whether or not they would respect the DNT header, which is in violation of the California Online Privacy Protection Act (CalOPPA) [**?**].

3.2.3 Descriptions of Choices in Privacy Policies

In addition to analyzing whether privacy choices are present in privacy policies, we analyzed *how* those choices are presented or described. We found a lack of consensus in the wordings used to present privacy choices. Additionally, many websites provided little information regarding what actually happened when a targeted advertising opt-out or data deletion choice was exercised, thus potentially confusing or misleading users.

[2]https://www.cnn.com/privacy

N-Gram	Email Comm.	Targeted Adv.	Data Deletion
how we use	9	5	2
opt out	13	7	2
person* data	8	1	10
person* inform*	7	2	13
third part*	0	14	2
we collect	15	7	5
we use	11	5	2
your choic*	11	9	10
your inform*	7	3	10
your right*	9	2	20

Table 3.3: Bigrams and trigrams occurring in at least 5% of privacy policy section headings. Counts are the number of policies (out of 147) in which a n-gram occurred in the headings of sections containing a privacy choice. Some policies described the same privacy choice under multiple headings, or used multiple n-grams in a heading.

There is no dominant wording for section headings. Table 3.3 summarizes common bigrams and trigrams in policy section headings related to privacy choices. Across policies, similar headings were used to present all three types of privacy choices, e.g., referring to collection and use of personal data or information, or describing a visitor's rights or choices. In contrast, the bigram "opt out" more commonly referred to choices related to email communications or targeted advertising. Similarly, advertising opt-outs were sometimes presented under sections describing third parties, which is not as applicable to the other two types of privacy choices. However, no single n-gram occurred in more than 20 of the policies we analyzed. This lack of consistency across websites could make locating privacy choices across websites difficult for visitors. Furthermore, some policies included multiple headings related to privacy choices, which could also potentially add significant burden to visitors.

Most marketing opt-outs are first-party. Among the 98 websites that provided at least one marketing communication opt-out in their privacy policy, 80 websites offered opt-outs from the website's own marketing or promotions. Additionally, 20 policies stated it is possible to opt out of marketing or promotions from third-party companies, and 19 policies specified that visitors could opt out of receiving website announcements and updates. Other less common forms of emails sent by websites that could be opted out from included newsletters, notifications about user activity, and surveys. Some websites offered opt-outs for different types of communications, such as SMS communications (10) and phone calls (8).

Targeted advertising opt-outs are ambiguous. We observed that privacy policies typically did not describe whether visitors were opting out of tracking entirely or just the display of targeted ads. Only 39 of the 80 websites that offered opt-outs for targeted advertising within their privacy policy made this distinction within the policy text. Among them, 32 websites explicitly

stated that the opt-out only applied to the *display* of targeted ads. This lack of distinction could be confusing to visitors who desire to opt-out of *tracking* on the websites for targeted advertising purposes.

The same ambiguity exists with respect to whether an opt-out applies across multiple browsers and devices. Seventy-three websites' policies did not specify whether the opt-out would be effective across different devices, and 72 did not clarify whether the opt-out applied across all the browsers a visitor uses.

Data deletion mechanisms vary by website. The data deletion mechanisms presented in the privacy policies of 108 websites varied. Visitors had the option to select certain types of information to be removed from their account on 80 websites. Furthermore, 41 websites offered the option to have the account permanently deleted, and 13 allowed visitors to temporarily suspend or deactivate their account.

How soon the data would actually be deleted was often ambiguous. Ninety of 108 websites offering deletion did not describe a time frame in which a user's account would be permanently deleted and only four policies stated that information related to the account would be deleted "immediately." Another three claimed the time frame to be 30 days, and two websites said the deletion process could take up to one year.

3.2.4 Usability of Privacy Choices

Our analysis included how many steps visitors had to take to exercise a privacy choice. We found that email communications opt-outs, on average, required the most effort. We also recorded specific usability issues on 71 websites (30 top, 23 middle, and 18 bottom) that could make privacy choices difficult or impossible to use, such as missing information and broken links.

Privacy choices require several user actions. We counted user actions as the number of clicks, hovers, form fields, radio buttons, or check boxes encountered from a website's home page up until the point of applying the privacy choice. Table 3.4 displays summary statistics related to the shortest path available to exercise choices of each type. Opt-outs for email communications and data deletion choices, on average, contained more user actions, particularly check boxes and form elements, compared to opt-outs for targeted advertising. This is likely due to the reliance on the DAA and NAI opt-out tools, which typically required two or three clicks to launch the tool. Data deletion and email communications choices, on the other hand, often required form fields or additional confirmations. At the extreme end, 38 user actions were required to complete the New York Times' data deletion request form, which included navigating to the privacy policy, following the link to the request form, selecting a request type, selecting up to 22 check boxes corresponding to different New York Times services, filling in eight form fields, selecting four additional confirmation boxes, and completing a reCAPTCHA.[3]

Policies contain missing, misleading, or unhelpful information. Many choice mechanisms were confusing or impossible to use because of statements in the website's privacy policy. In six

[3]reCAPTCHA: https://www.google.com/recaptcha/intro/v3.html

	Clicks	Boxes	Hovers	Form	Other	Total
Email Comm.	2.90	1.68	0.38	0.33	0.17	**5.32**
Targeted Adv.	2.80	0.10	0.25	0.00	0.01	**3.16**
Data Deletion	2.93	1.05	0.23	1.07	0.05	**5.32**

Table 3.4: Average number of actions required in the shortest path to exercise privacy choices, counted from the home page up until, but not including, the action recording the choice (i.e., "save/apply" button).

instances, text in the policy referred to an opt-out, but that opt-out did not exist or the website did not provide vital information, such as an email address to which visitors can send privacy requests. Six websites included misleading information in the policy text, such as presenting the Google Analytics opt-out browser extension as an opt-out for targeted advertising,[4] and omitting mentions of targeted advertising in the privacy policy while providing opt-outs elsewhere on the website. Additionally, seven websites mentioned user accounts in the privacy policy but no mechanisms to create a user account were observed on the website. Two of these cases were TrustedReviews and Space.com, whose policies covered multiple domains, including some with user accounts. These issues appeared in fairly equal frequency across top, middle, and bottom websites.

Some websites had broken choice mechanisms and links. We also recorded 15 instances in which provided links to relevant privacy choice information or mechanisms were broken or directed to an inappropriate location, such as the website's homepage, or the account settings for a parent website. We further observed that four websites offered choice mechanisms that did not appear to properly function. For example, on Rolling Stone's email preferences page, selections made by visitors seemed to be cleared on every visit. GamePress's data deletion request form was implemented by Termly and did not seem to refer to GamePress, making it unclear where and how the form would be processed.

Some websites made poor design choices. We noted several website design choices that may impact the usability of privacy choices. On ten websites, we observed a privacy policy displayed in an unconventional format, such as in a PDF or in a modal pop-up dialogue, instead of a normal HTML page. This may impact how well visitors can search for privacy choices in a policy. Another design choice that impacted searchability was collapsing the policy text under section headings; keyword search is not effective unless all sections are opened. Five policies also had stylistic issues with their policies, such as including opt-out links that were not clickable or advertisements in the middle of the policy. Some websites offered burdensome pages for managing email communication settings, requiring visitors to individually deselect each type of communication sent by the website. Others placed the option for opting out of all communications *after* a long list of different types of content, rather than before it, making it less visible. For example,

[4]Google merged its advertising and analytics platforms in July 2018, but the Google Analytics opt-out extension only pertains to analytics tracking.

Amazon offered this option after listing 79 different communications, which rendered it invisible until scrolling much further down the page.

Aids for privacy choice expression

Conversely, a few websites made additional efforts to make their privacy choices more accessible to visitors. Many opt-outs (such as the Google Ad Settings page) went into effect once a visitor expressed a privacy choice, and did not require the additional step of pressing a confirmation (i.e., "save/apply"). Some, like Metacrawler, centralized the privacy choices related to email communications, targeted advertising, and data deletion into a single section of the policy. Others, including Fronter, were diligent about providing links to related privacy information, such as regulation or the privacy policies of third parties used by the website. To further aid visitors, three websites (BBC, Garena, and LDOCE Online) presented important privacy information in a "Frequently Asked Questions" format. Moreover, Google and Booking.com, provided users with a short video introducing their privacy practices.

3.3 Improving Privacy Choices

Our findings indicate that certain design decisions may make exercising privacy choices difficult or confusing, and potentially render these choices ineffective. We provide several *design* and *policy* recommendations for improving the usability of web privacy choices. Our recommendations not only serve as concrete guidelines for website designers and engineers, but also have the potential to help policy makers understand current opt-out practices, their deficiencies, and areas for improvement. These suggestions could then be integrated into future guidelines, laws, and regulations.

Our discussion is based on the Interaction Cycle, which divides human interaction with systems into four discrete stages [4]. It serves as a framework to highlight the cognitive and physical processes required to use choice mechanisms, and in turn synthesizes our findings to address specific usability barriers. We mapped the expression of online privacy choices to the Interaction Cycle as: 1) finding, 2) learning, 3) using, and 4) understanding a privacy choice mechanism.

3.3.1 Finding Privacy Choices

Use standardized terminology in privacy policies. As noted in Section 3.2.3, no single n-gram was present in an overwhelming majority of privacy policy section headings in which choices were described, and there was much variation in how websites offered privacy choices. For example, data deletion mechanisms were placed under headings like "What do you do if you want to correct or delete your personal information?" in some policies, but under more general headings like "Your Rights" in others. Even more confusing, some policies contained multiple titles similar to both of these.

Inconsistencies across different privacy policies may make finding specific privacy choices difficult. We recommend that future privacy regulations include requirements for standardized privacy policy section headings. Such guidance exists for privacy notices of financial institutions

in the United States, as well as data breach notifications to California residents [**? ?**]. Our results highlight the most common terms that websites already use in providing privacy choices, which could serve as a foundation for formulating such guidance.

Unify choices in a centralized location. Websites sometimes offer different opt-out choices on different pages of the website for the same opt-out type. This problem is most salient for targeted advertising opt-outs, which could appear either in privacy policies, account settings, or an individual "AdChoices" page linked to from the home page. Furthermore, some privacy policies did not link to the "AdChoices" page or the account settings where the advertising opt-outs were located. Therefore, by looking at just the privacy policy, which may be where many users would expect to find privacy choices, visitors would miss these opt-outs available to them.

One potential solution is having all types of privacy choices in a centralized location. This can be achieved as a dedicated section in the privacy policy, or even as an individual page with a conspicuous link provided on the home page. However, it will likely require regulatory action for many companies to prioritize reorganizing their current opt-outs in this way.

3.3.2 Learning How To Use Privacy Choices

Simplify or remove decisions from the process. Another practice that adds to the complexity of exercising opt-outs is the presence of links to multiple tools. For instance, more than one third (58) of our analyzed websites provided links to multiple advertising opt-outs. To simplify the privacy choice process, websites should unify multiple choice mechanisms into a single interface, or provide one single mechanism for a particular type of privacy choice. If not technically feasible, websites should help visitors distinguish the choices offered by each mechanism.

Ensure all choices in the policy are relevant. The use of one policy for a family of websites might be the reason for some of the points of confusion highlighted in Section 3.2.4. These corporate "umbrella policies" might explain cases where we observed links from the privacy policy directing to unrelated pages on a parent company's website, or references to account settings even when the website does not offer mechanisms to create user accounts. While maintaining one policy may be easier for parent companies, this places a substantial burden on visitors to identify the practices that apply to a particular website.

To mitigate such issues, companies should carefully check if the information provided in the privacy policy matches the websites' actual practices. If an umbrella policy is used across multiple websites, practices should be clearly labelled with the websites to which they are applicable. Regulatory authorities should further exert pressure by emphasizing the necessity of having accurate privacy policies and conducting investigations into compliance.

3.3.3 Using Privacy Choices

Simplify multi-step processes. We noted that privacy choices typically require multiple steps, which may frustrate and confuse users. As described in Section 3.2.4, our analyzed privacy choices required an average of three to five user actions prior to pressing a button to apply the

choice, assuming the visitor knew which pages to navigate to in advance. On the extreme end, completing one deletion request form required 38 user actions, as the interface included several boxes related to different services offered by the website. Though this type of interface allows users to have greater control, websites should also have a prominent "one-click" opt-out box available to visitors.

It is also conceivable that many companies may deliberately make using privacy choices difficult for their visitors. In this case, it is up to regulators to combat such "dark patterns." [3**?**] Though it may be unrealistic to set a threshold for the maximum number of user actions required to exercise a privacy choice, regulators should identify websites where these processes are clearly purposefully burdensome and take action against these companies. This would both serve as a deterrent to other companies and provide negative examples. Precedents of such regulatory action have emerged, such as a ruling by the French Data Protection Authority (the "CNIL") which found that Google fails to comply with the GDPR's transparency requirement as its mobile phone users need "up to five or six actions to obtain the relevant information about the data processing" when creating a Google account [**?**].

Some of our analyzed websites have already provided exemplary practices to simplify privacy choices, e.g., automatically applying privacy choices once the user selects or deselects an option, rather than requiring the user to click an additional "save" or "apply" button. Clicking an additional button may not be intuitive to users, especially if it is not visible without scrolling down the page. Removing this extra step would avoid post-completion errors, in which a user thinks they have completed privacy choice, but their choice is not registered by the website. A requirement that all changes in privacy settings must be automatically saved could be integrated into regulations and related guidelines. However, any changes should be made clear to the user to avoid accidental changes.

Provide actionable links. Our findings show that the use of links pointing to privacy choices was not ubiquitous, and varied substantially across different types of privacy choices; 93% of websites that offered the choice to opt out of targeted advertising provided at least one link, whereas the percentage for email communication opt-out and data deletion choice was 32% and 24% respectively. Websites that do not provide links usually provide text explanations for the opt-out mechanisms instead. However, visitors may not follow the text instructions if significant effort is required, such as checking promotional emails in their personal inbox for the "unsubscribe" link, or sending an email to request their account to be deleted. We also found that some websites may not provide sufficient guidance to support exercising a privacy choice.

Our findings point to the necessity to enhance the actionability of privacy choices by providing links. However, there should be a careful decision about how many links to include and where to place them. Ideally, only one link for one particular type of opt-out should be provided. When multiple links are presented on the same page, there needs to be sufficient contextual information to help users distinguish these links. Of equal importance is the functionality of provided links. In our analysis, we observed a few instances in which the provided links were broken, directed to an inappropriate location, or had styling that easily blended in with text. These practices reduce the actionability of the corresponding privacy choice and negatively impact the user experience.

3.3.4 Understanding Privacy Choices

Describe what choices do. We found that privacy policies did not provide many details that informed visitors about what a privacy choice did, particularly in the cases of targeted advertising opt-outs and data deletion choices. Among all websites that provided targeted advertising opt-outs, fewer than 15% distinguished opting out of tracking from opting out of the display of targeted ads, or indicated whether the opt-out was effective on just that device or browser or across all their devices and browsers. Similarly, among all websites that provided data deletion choices, only 19% stated a time frame for when the account would be permanently deleted.

Future regulations could stipulate aspects that must be specified when certain opt-outs are provided (e.g., the device that the opt-out applies to). This may reduce instances where visitors form expectations that are misaligned with a companies' actual practices.

3.4 Conclusion

We conducted an in-depth empirical analysis of data deletion mechanisms and opt-outs for email communications and targeted advertising available to US consumers on 150 websites sampled across three ranges of web traffic. It is encouraging that opt-outs for email communications and targeted advertising were present on the majority of websites that used these practices, and that almost three-quarters of websites offered data deletion mechanisms. However, our analysis revealed that presence of choices is not the same as enabling visitors to execute the choice. Through our holistic content analysis, we identified several issues that may make it difficult for visitors to find or exercise their choices, including broken links and inconsistent placement of choices within policies. Moreover, some policy text describing choices is potentially misleading or likely does not provide visitors with enough information to act. Design decisions may also impact the ability of visitors to find and exercise available opt-outs and deletion mechanisms. We offer several design and policy suggestions that could improve the ability of consumers to use consent and privacy control mechanisms.

Chapter 4

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

As outlined in Chapter 2, an expanding body of privacy regulations requires websites and online services to present users with notices and choices regarding the usage of their data. These regulations aim to provide transparency about data processing policies and give users access and control over their own data. Some regulations — such as the General Data Protection Regulation (GDPR) and a few US laws — include specific usability requirements [**? ? ?**]. In part due to these regulations, privacy controls now seem to be ubiquitous on websites. Particularly common are opt-outs for email communications or targeted ads, options for data deletion, and controls and consent for use of cookies, as highlighted by the results detailed in Chapter 3.

However, availability does not imply usability, leaving open the question of whether these controls are actually useful to consumers. The results described in Chapter 3 indicate potential usability issues with the types of controls studied. However without an exploration of how users may interact with such controls, it is difficult to definitively determine whether the issues identified lead to usability barriers in practice. Past user studies have found various usability problems with available privacy controls, particularly in tools for limiting targeted advertising (e.g., [55, 90]). This research described in this chapter expands on that work by exploring the usability of websites' own opt-outs for targeted ads. Furthermore, it examines choices beyond those related to advertising, providing insight into the usability of email marketing and data deletion choices required by the CAN-SPAM Act and GDPR, respectively.

This chapter details an in-lab usability study with 24 participants. Participants were first asked about their expectations regarding websites' data practices and privacy controls. They completed two tasks that were representative of common practices for offering privacy choices, as identified in Chapter 3. Tasks differed by the choice type (opting out of email communication, opting out of targeted ads, or requesting data deletion), choice location (account settings, privacy policy), and mechanism type (described in policy text, link from policy text).

We find that despite general awareness of deletion mechanisms and opt-outs for advertising

This chapter is a lightly edited version of a paper previously published as: 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). 2020 [62].

and email, participants were skeptical of the effectiveness of controls provided by websites. and resorted to consulting help pages or contacting the website. Participants also expressed desire for additional controls over data sharing and deletion.

This chapter makes the following contributions:

- A holistic usability evaluation of the end-to-end interaction required to use common implementations of privacy controls for email marketing, targeted advertising, and data deletion.
- Design implications applicable for making these online opt-out and deletion choices more usable and useful to consumers.

4.1 Study Design

We conducted a lab study with 24 participants. In this section we describe our study design and data analysis approach.

4.1.1 Study Session Components

Each lab session consisted of an interview portion followed by a set of tasks conducted on a lab computer. Participants were also asked follow-up questions after completing each task.

Interview

The first portion of the study session, a semi-structured interview, had a median length of 11 minutes (min: 5 minutes, max: 22 minutes). First, we asked participants what types of data they thought websites collected about them and how they thought it was used. Next we asked participants what types of controls they expected to have over how websites could use their data, as well as where they expected to be able to find these controls. To learn more about expectations related to email marketing, targeted advertising, and data deletion specifically, we asked participants to recall a recent time when they received a marketing email, saw a targeted ad, and provided a website with personal information. For each, we followed up with questions about what types of control they thought were available, and how they would attempt to exercise that control.

Task Selection

In the second portion of the study session, we asked each participant to complete two opt-out tasks on a lab computer. In each task, participants were asked to use a privacy choice on a website while thinking aloud. Each privacy choice task was one of the following: opting out of email newsletters from a website, opting out of targeted advertising on a website, or requesting deletion of personal information from a website. Although other privacy choices exist, we wanted to examine the usability of a set of choices over different types of data handling practices. Additionally, the choices selected are prevalent in the current online ecosystem and fall under legal or other regulatory requirements.

In prior work, we reviewed controls for email marketing, targeted advertising, and data deletion on 150 websites and found that these choices are most commonly presented using one of

Website Name	Task Type	PP — AS	# Actions	Mechanism
majorgeeks.com	email	AS	9	checkbox
foodandwine.com	email	PP	5	link to email options
internshala.com	email	PP	9	text, refer to emails
wordpress.com	ads	AS	9	toggle option
colorado.edu	ads	PP	16	links to opt-out tools
coinmarketcap.com	ads	PP	10	text, delete cookies
phys.org	deletion	AS	9	delete account
nytimes.com	deletion	PP	46	link to request form
runescape.com	deletion	PP	9	text, email request

Table 4.1: The websites used for email opt-out, targeted advertising opt-out, and date deletion tasks and their associated mechanisms in the privacy policy (PP) and account settings (AS), as well as the minimum number of user actions required to exercise each control.

three patterns: a user account setting, a link from the privacy policy, or text instructions in the privacy policy [**?**]. To identify specific tasks for this user study, we examined the collected empirical data and looked for websites that used just one of the three patterns (some websites used more than one pattern, e.g., both a user account setting and privacy policy link). For each of the *task types*, we selected three websites that followed these patterns, resulting in a set of nine websites. The websites selected and their choice mechanisms in the privacy policy or user account settings are presented in Table 4.1.

To minimize learning effects and prevent fatigue, we counter-balanced and stratified tasks such that each participant completed two different task types. One task was selected to be on a website with an account settings mechanism and the other task on a website with a privacy policy mechanism, allowing us to examine the usability of the most common practices used by websites. This resulted in 12 possible groupings of the websites selected for the study. We recruited 24 participants and assigned a pair of participants to each grouping, with each member of the pair performing the tasks in the inverse order.

Task Introduction

Prior to each study session, researchers opened a new window in Google Chrome's Incognito mode and logged into a Gmail account created for the study. Before being given their first task, participants were told that they could use this Gmail account and could search online for any information that they needed to complete the task. Participants were also notified that, if applicable, they could assume they had user accounts on the websites they would visit for the study tasks. Participants were not required to use their own credentials or personal information for any of the tasks, and instead were provided with credentials created for the study through printed index cards when reaching the log-in step on the website.

We described the email opt-out, targeted advertising opt-out, and deletion tasks to participants as the following scenarios:

> You just got the tenth update email from [website] today, and now you want to stop receiving them.
>
> You've been seeing advertisements on [website] for a pair of shoes that you searched for last month, and now you want to stop seeing them.
>
> You're uncomfortable with [website] keeping a record of your location, and want to remove all of your data from the company's databases.

After being read the appropriate scenario, participants were instructed to open a new browser tab or proceed as they would at home while thinking aloud.

Task Follow-Up

After each task, we asked a set of follow-up questions regarding the participant's experience with the task and their understanding of what effects their actions would have. We also asked about their past experiences with similar tasks and their familiarity with the website used in the task.

After participants completed both tasks and the task follow-up questions, we asked them which task they found easier, and why. We also asked about their past choices to use opt-out mechanisms or privacy controls on websites. Lastly, we inquired as to whether they wished websites offered any additional controls related to privacy or personal data and what they thought they should look like.

4.1.2 Data Collection

One researcher moderated all participant sessions. A second researcher attended each session to take notes. At the beginning of their session, participants completed a consent form that described the nature of the interview and tasks and notified participants that audio and screen recordings would be captured. We audio-recorded participants' responses to interview questions, comments and questions during the computer tasks, and responses to follow-up questions after the computer tasks. Participants' actions during the computer tasks were screen-recorded. This study was approved by the Institutional Review Boards (IRB) at Carnegie Mellon University and the University of Michigan.

The 24 participants were recruited locally in Pittsburgh, Pennsylvania using Craigslist, Reddit, and a university subject pool. In recruitment posts, potential participants were invited to complete a screening survey with questions about demographics, as well as engagement in four common privacy practices selected from a Pew Research Center survey [**?**]. A sample of participants — diverse in gender, age, and educational attainment — was selected from among the respondents. Those who completed the in-lab study session were compensated with a $20 Amazon gift credit. The study sessions lasted a median of 50 minutes (min: 30 minutes, max: 78 minutes). The large variance in session duration was related to how fast participants were able to complete their tasks. While all participants attempted their tasks, those who stated they did not know what to do next or still had not completed the task after eight minutes were given a hint to log in or look for a "privacy-related page" (depending on the task). This threshold of eight minutes was determined through pilot sessions. Any assistance provided was noted and incorporated into our analysis.

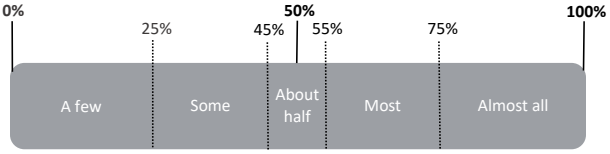


Figure 4.1: Terminology used to present relative frequency of themes.

4.1.3 Data Analysis

Interview recordings were transcribed using an automated transcription service (`temi.com`), and a researcher then corrected errors in the transcripts. The use of a third-party transcription service was IRB-approved, and participants consented to the sharing of recordings with a third-party service. We took extra measures to preserve participants' privacy prior to uploading the recordings by removing any personally identifying details, such as name and address, that a small number of our participants revealed during their interview. We conducted inductive coding on the interview transcripts. To develop an initial codebook, one researcher performed open coding to identify themes and merged common codes as needed. Two researchers then collaboratively revised the codebook after individually coding a random sample of six interviews using the initial iteration of the codebook and reviewing all disagreements in their coding. After coming to an agreement on the codebook, the remainder of the interviews were double-coded. Any disagreements were again reviewed and reconciled.

We created an analysis template to systematically count the interactions and errors made during the tasks. One researcher reviewed all screen recordings of the session tasks along with any researcher notes from the session to create initial counts of interactions and errors. Another researcher then reviewed and confirmed the interactions recorded.

We organized our findings according to the User Action Framework, which offers a systematic framework for assessing and reporting usability data. Within this framework, Andre et al. [4] adapted Norman's theory of human-computer interaction [**?**] and discuss user interaction in terms of four cyclic phases: high-level planning ("users determine what to do"), translation ("users determine how to do it"), physical action ("users do the physical actions they planned"), and assessment ("users assess the outcome of their actions"). We previously applied this framework to online privacy choices in our empirical analysis of opt-out and data deletion actions across websites, and mapped these phases of the interaction to *finding*, *learning*, *using*, and *understanding* privacy choice mechanisms [**?**]. Here we apply the same framework to the actions we observed in the lab.

As our study was primarily qualitative, we do not report exact numbers when presenting most of our study findings. However, following recent qualitative work at CHI [39], we adopted the terminology presented in Figure 4.1 to provide a relative sense of frequency of major themes.

4.1.4 Limitations

The exploratory nature of this study provides insights into possible usability issues with common practices used to provide privacy choices, but cannot provide quantitative claims about how

frequently these issues may occur in the real world. Similarly, our limited sample size of 24 participants, though diverse, was not representative of all internet users, and likely over-represented technically savvy users.Thus the frequency of issues reported by our participants may not reflect the frequency with which these issues would be encountered by a general population. However, it is unlikely that less technically savvy users would face fewer issues when opting out or deleting their data. As such, the issues and opinions highlighted only represent a subset of all possible ones.

While our sample of nine websites was representative of the common practices websites use to provide privacy choices, it is not representative of all types or categories of websites that exist. Our results may not generalize to other types of websites, particularly those that are more complex than those included in our sample and offer multiple products or services. Additionally, design variations and specific peculiarities of each website may have impacted the difficulty of exercising the privacy choices present and thus participants' opinions. However, this was a deliberate trade-off as using live websites allowed us to gain insight into the usability of real-world privacy choices. We note specific features that seemed particularly detrimental or helpful when exercising privacy controls.

While our study was designed to mitigate learning effects, it is still possible that participants used knowledge acquired in their first task to complete their second task. Similarly, while we avoided directly mentioning "privacy" or "security" during the pre-task interview (unless a participant brought up the topic), the questions may have biased participants to think more about privacy and security than they otherwise would have.

4.2 Participants

Table 4.2 provides a summary of participant demographics, as well as which tasks participants were assigned. In our sample, 13 participants identified as female and 11 as male. Our sample had a wide distribution of ages, but skewed towards higher levels of educational attainment. Six participants reported having an education in or working in computer science, computer engineering, or IT. In their responses to the screening survey, all 24 participants reported to have cleared cookies or browsing history, 22 had refused to provide information about themselves that was not relevant to a transaction, 13 had used a search engine that does not keep track of search history, and 10 added a privacy-enhancing browser plugin like DoNotTrackMe or Privacy Badger. This distribution is somewhat higher than that found by Pew [**?**], suggesting our sample may be more privacy-aware than the general public. Almost all participants reported having prior experience with controls for email marketing, and most had prior experiences with advertising and deletion controls.

4.3 Results

We next present our findings structured around the four stages of the interaction cycle: finding, learning, using, and understanding privacy choice mechanisms. We highlight participants' expectations, actual performance in session tasks, as well as website practices that make exercising

ID	Gender	Age	Education	Technical	Task 1	Task 2
P1	F	35-44	Professional		majorgeeks	runescape
P2	F	18-24	Bachelors		wordpress	internshala
P3	F	25-34	Some college		wordpress	foodandwine
P4	M	55-64	Bachelors		wordpress	nytimes
P5	F	45-54	Bachelors		wordpress	runescape
P6	F	25-34	Masters		phys	internshala
P7	F	45-54	Associates		phys	foodandwine
P8	F	25-34	Bachelors		phys	coinmarketcap
P9	F	25-34	Bachelors		phys	colorado
P10	M	25-34	Masters	X	colorado	majorgeeks
P11	M	55-64	Masters		nytimes	majorgeeks
P12	F	18-24	Associates		internshala	wordpress
P13	M	35-44	Some college	X	foodandwine	wordpress
P14	F	18-24	Bachelors		nytimes	wordpress
P15	M	18-24	Bachelors		runescape	wordpress
P16	F	55-64	Bachelors	X	foodandwine	phys
P17	M	45-54	Associates	X	coinmarketcap	phys
P18	M	55-64	High school		colorado	phys
P19	F	55-64	Masters		majorgeeks	coinmarketcap
P20	M	35-44	Associates	X	majorgeeks	colorado
P21	F	35-44	Masters		majorgeeks	nytimes
P22	M	25-34	Bachelors		coinmarketcap	majorgeeks
P23	M	18-24	Masters		internshala	phys
P24	M	25-34	Bachelors	X	runescape	majorgeeks

Table 4.2: Participant demographics (gender, age, education, technical background) and task assignments.

privacy choices more difficult for users and those that make it easier.

4.3.1 Planning: Finding Privacy Choices

Participants expected to find privacy choices within the context of how a website uses their data (for example, unsubscribe links within emails) or on a user account settings page. The presence of multiple paths to a privacy control made the control easier to find.

Expectations are dependent on choice type

In response to pre-task questions, some participants mentioned expecting to find data-use controls in the account settings or on a privacy settings page. A few participants mentioned consent dialogues, either through the browser or the website. Additionally, a few participants described browser settings or functions, such as private browsing and plugins.

Participants had similar responses when describing where they would like privacy controls to be placed. Half of the participants suggested that controls should be placed within a website's account settings. Some preferred to see privacy controls in context on the website (e.g., where data is collected). Other suggestions provided by participants included being able to email a company with requests and receiving monthly digest emails summarizing the data the website has about them.

When asked about email marketing controls, almost all participants mentioned unsubscribe links within emails. Some also described more granular controls, such as the ability to select which marketing messages to receive or to change the frequency of emails through website account settings. Some described other control mechanisms, such as contacting the website and using unsubscribe features built into email clients.

To control the display of targeted advertising, about half the participants mentioned privacy enhancing strategies, such as using ad-blocking extensions, clearing the browser history, using private browsing mode, changing browser settings, or using a privacy-protective search engine. A few participants mentioned being able to find controls by interacting with the corner of an advertisement (likely referring to the DAA's AdChoices icon or ad controls provided by social media sites). Only a few participants mentioned controls for advertising being available in the account settings. A few also mentioned avoiding clicking on ads as a type of control.

Most participants expected deletion controls to be available in the account settings, and some believed that deletion could be achieved by contacting the website. Only a few participants mentioned finding deletion controls elsewhere on the website, such as in a frequently-asked-questions page.

Participants' initial strategies varied by choice type

Most of the 16 participants assigned to an email opt-out task first looked for or used an unsubscribe link in an email sent by the website, which could be found in the provided Gmail account. Almost all participants reported using such links prior to the study. A few had other initial strategies for finding unsubscribe mechanisms, such as using the search feature of the browser to find the term "unsubscribe" on the home page or the search feature of the website to find the privacy policy.

Participants used a variety of strategies for completing their targeted advertising opt-out task, some of which were more effective than others. Some first went to the account settings, while only a few first looked in the privacy policy. A few explained that they would try to find an ad on the website and look for an icon leading to opt-out options. A few went into the browser settings to look for advertising-related options, while a few others immediately resorted to emailing the website for help. As P18 reasoned, *"Well, if they're not able to help then they would respond back and say here is the correct way to opt out of what you're looking for."* A few participants looked for opt-out choices on other pages, such as the website's cookie policy, terms of service, and frequently-asked-questions page.

Participants had a more uniform set of strategies for deletion mechanisms. Most immediately logged into the website. A few resorted to frequently-asked-questions pages or contacting the website. Finally, a few participants looked for account-related information in registration emails from the website.

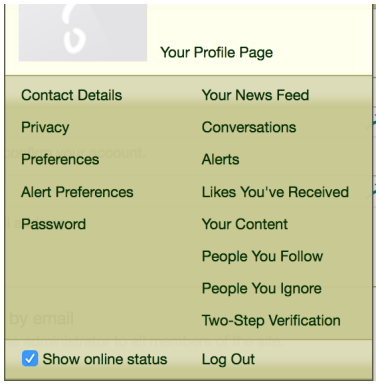


Figure 4.2: Screenshot of settings menu on `majorgeeks.com` where participants had difficulty finding the correct path to e-mail opt-outs.

Policy and settings mechanisms required assistance

Almost all participants required assistance finding the account setting or privacy policy mechanism related to their study task. On the three websites that had privacy choices in account settings, some were able to use the mechanism on their own after being prompted to log into the website, but a few needed further guidance to look within the account settings to complete the task. P6, who was unable to find the advertising opt-out on `wordpress.com` described the process: *"It's what I call a scavenger hunt. I've gone all throughout this website, apparently a legitimate website, but I still can't do what I really like to do."* On the six websites where the privacy choices were in the privacy policy, some were able to find the privacy choice text or link without guidance (however P10 admitted they were prompted to think about privacy because of the pre-task interview). A few were able to use the choice mechanism after they were given the hint to look for a privacy-related page, while a few others did not initially see the control in the policy and required prompting to look further.

Poor labels cause confusion

On two of the websites, there were multiple pages that had labels with words that were related to what the task was. For example, some participants assigned to opt out of email marketing from `majorgeeks.com` went to a different settings page called "alert preferences" that included settings related to notifications received while on the website. The correct setting could be found under the "privacy" or "contact details" settings pages. However, as seen in Figure 4.2, these options were presented in a list with no descriptions. Similar confusion occurred on `coinmarketcap.com` where a few participants assigned to find controls related to targeted advertising went to a page linked from the homepage called "advertisers" with information for companies that wished to place ads on the site. This suggests that more descriptive labels on these websites would help users find choice mechanisms more easily.

Multiple paths made choices easier to find

On some websites, there were multiple paths to the same choice mechanism, which made them easier to find. All participants assigned to request data deletion from `nytimes.com` first visited the account settings, where they found a link to the privacy policy, which in turn contained a link to the request form. Similarly, most participants assigned to request data deletion from `runescape.com` used the site's search feature or looked through its support pages and found a page titled "Your Personal Data Rights," which provided a summary of the same information provided in the privacy policy. However, one additional location where participants expected an opt-out choice for email marketing was on the page to subscribe to emails. All four participants assigned to find the opt-out link in `foodandwine.com`'s privacy policy clicked on the prominent "subscribe" button on the homepage and expected to find a means to unsubscribe.

4.3.2 Translation: Learning Privacy Choices

Participants had clear expectations about what choices available to them should do. We also observed several design decisions made by websites that impacted participants' comprehension of these choices.

Participants desired controls over data sharing and deletion

Participants demonstrated incomplete mental models of the choices that were provided to them, especially when describing controls related to how websites can use collected data in the abstract. The only website-offered controls that were mentioned by multiple participants were cookie consent notices and security controls, such as encryption or multi-factor authentication. A few participants mentioned withholding information about themselves when using a website or avoiding using a website entirely. However, a few participants discussed deletion controls prior to being prompted.

Participants' understanding of website-provided controls appeared more concrete when asked about specific practices, such as email marketing, targeted advertising, and data deletion. As mentioned earlier, nearly all reported that they had used unsubscribe links within emails. Related to advertising, some participants expected to be able to report a particular advertisement as irrelevant. Half of the participants who mentioned this type of control also mentioned seeing such a control on a social media website, such as Facebook or Twitter. Only a few expected to be able to opt-out of targeted advertising entirely. When asked about choices related to data deletion, some were unaware of deletion controls offered by websites, but about half expected to be able to delete data from their profile and some mentioned being able to delete their entire account. Nearly all participants who mentioned a deletion mechanism stated that they had used such controls in the past.

When asked about privacy controls they wished websites offered, most participants mentioned controls for data sharing and deletion. As P11 stated, *"Well in the ideal world, you should be able to tell the website, look, I'm giving you this information, but don't share it."* A few mentioned wanting to tell websites to not save their information, while a few others desired greater controls over content that is displayed to them, such as recommended articles. More broadly, a

few participants expressed a desire for greater transparency about data sharing or existing controls. However, a few others stated that they were satisfied with their current privacy options or could not articulate additional desired control mechanisms.

Formatting and text cause confusion

Another usability issue that made it difficult for participants to interpret choices was poor formatting and explanatory text. Most participants trying to find information about opt-outs for advertising in `coinmarketcap.com`'s privacy policy clicked on the link to install the Google Analytics opt-out browser extension, likely due to the placement of a link in policy text referring to advertisers and the use of cookies. However, the opt-out extension only opts users out of Google's tracking for analytics purposes, and not advertising. Similarly, most participants assigned to `runescape.com` found a page related to data rights, but had difficulty figuring out how to actually request deletion because of the page's format. As seen in Figure 4.3, removing your personal data appears to be a clickable option. However this is not the case and most were confused about why nothing appeared to happen. The text description provided after a list of data rights directs users to complete a subject access request form, labelled as "Make a Subject Access Request," which is linked after a button labelled "Fix it Fast: Account Settings." Most participants who saw this page incorrectly clicked on the account settings link instead of requesting deletion through emailing the contact provided on the page or the request form, as instructed. The placement of these two links made it unclear which privacy rights listed on the page could be accomplished through each mechanism.[1]

Conversely, `colorado.edu`'s privacy policy contained links to the three advertising opt-out tools in a single paragraph, which led participants to at least see all three tools (even if none actually selected all three, as discussed in the next subsection).

On `phys.org` a clear "Manage account" button visible on the landing page of the account settings conveyed the correct interaction path to almost all participants assigned to the website. However, some of the participants who clicked this button and saw the setting to delete the account were unsure whether that mechanism would also delete their data, and navigated away from the page to look for other options. A statement indicating that profile data will be erased permanently was not presented until after clicking the initial delete button. However, once participants saw this confirmation they were assured that the mechanism would accomplish their task.

4.3.3 Physical Action: Using Privacy Choices

Exercising privacy choices required a high level of effort from participants, as measured by the number of actions such as clicks, scrolls, and checkboxes in the interaction path of using a choice mechanism. Certain practices used by the websites in our sample made exercising choices more difficult.

[1]This page on `runescape.com` was updated after our study. The new version partially addresses these issues by reducing the page's text. However, it is still unclear which privacy rights listed can be accomplished by the two mechanisms shown.

Figure 4.3: List of data rights available on `runescape.com` which misleadingly seem clickable.

High level of effort exerted in exercising policy choices

Figure 4.4 displays the number of user actions in participants' interaction path when using privacy choices located in the account settings and privacy policy. Using a choice mechanism in account settings resulted in an average of 26.1 user actions (min: 8, max: 43, sd: 11.5). Interactions using links in the privacy policy had 37.5 actions (min: 11, max: 59, sd: 15.2), on average, and those with text instructions in the policy had 57.6 (min: 18, max: 87, sd: 27.5). While policy links took participants exactly where they needed to go, text instructions were vague and required extra effort to figure out what to do. Furthermore, participants took many more steps than the shortest, ideal path for completing a task. The shortest interaction path for account settings mechanisms would have taken 9 total actions averaged over the three websites, while policy link choices needed 22.3, and policy text required 9.3.

Most participants who used the account settings mechanisms on `wordpress.com` or `phys.org` said that they were easy to use because of the simplicity of the setting. For example, P6 described the account deletion process on `phys.org`: *"It said delete my account which was pretty clear. And then there was this other page that like made it very clear that that's what was going to happen."* Some noted that these mechanisms were easy to find. A few appreciated that, unlike another mechanism they used, the account settings option would be applied right away and did not require a response from the website. Nearly all participants assigned to opt out of emails from `majorgeeks.com` also found the mechanism straightforward or easy to use, but most found the setting hard to find.

Participants who were assigned to tasks with privacy choice links or text instructions in the website's privacy policy explicitly mentioned that they found these mechanisms hard to find or that finding them required too much reading. Reactions to the data deletion request form on `nytimes.com` were mixed. Most participants disliked being presented with many similar-seeming options related to data processing, only being able to submit one request type at a time,

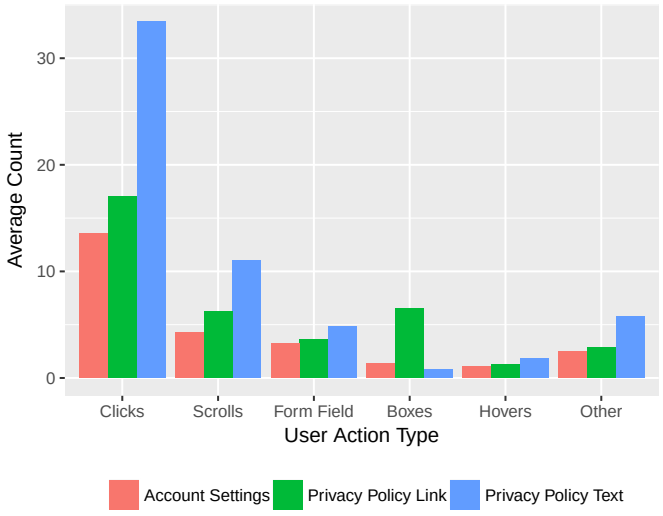


Figure 4.4: Number of clicks, scrolls, form fields, check boxes, hovers, and other user actions, averaged over all websites, in the participants' interaction with account settings and policy choices.

or having to manually select 22 services from a list. However, others reported that the policy was easy to find through the account settings and the form was straightforward to use.

Unsubscribe links within emails were also considered straightforward to find and use. Participants highlighted user-friendly features these pages that they encountered previously or during the study. These included opt-outs that were automatically applied without extra confirmation or entry of their email address, as well as interfaces that allowed users to select emails from the website they would like to continue to receive (as long as a button to opt-out of all emails was visibly present).

Choices require unnecessary user effort

Some practices used by websites for offering privacy choices place undue burden on users. An example is requiring users to submit written requests, a common practice websites use to offer data deletion [**?**]. Participants had difficulties articulating such requests. P4, who was trying to opt-out of targeted advertising on `wordpress.com`, drafted a message to customer service that asked *"How can I delete a specific webpage that is contacting me?"* Additionally, a few participants who wrote account deletion or unsubscribe requests did not include all the information the website would need to act on their request, such as the username or email address.

Another practice that complicates opt-out choices for users is offering multiple links to different opt-out tools. The privacy policy for `colorado.edu` contained links to advertising opt-out tools offered by the DAA, NAI, and Google. All participants assigned to this website visited only one or two of the three links. Participants had varying justifications for which links they clicked on. Half selected the DAA and NAI links because they (correctly) believed they would apply to multiple third-parties and not just Google. However, many entities participate in both industry opt-out programs, and participants may not have realized the overlap. Another explained that they chose to click on the Google advertising opt-out because they were already within Google's

ecosystem (i.e., using Google Chrome and Gmail) so they thought the opt-out would be more broadly applied, especially if they stayed logged into the Google account. Though Google owns the largest online advertising exchange, using an industry provided opt-out tool may have greater impact on limiting targeted ads.

Simple design flaws also place extra burden on users. For example, on `majorgeeks.com` when a user changes a setting it is not automatically saved; users have to press a "save" button at the bottom of the page. The website also does not provide a warning that there are unsaved changes. A few participants assigned to this website found the correct opt-out setting but did not press "save," resulting in lost changes and the opt-out not being applied. This is an example of a post-completion error [**?**]. In contrast, a warning reminded a few participants assigned to `wordpress.com` to save their changed settings.

4.3.4 Assessment: Understanding Privacy Choices

Participants expressed skepticism that the privacy choices they use will actually be honored by websites. Websites were also unclear about what happens when such controls are used.

Skepticism of privacy choice effectiveness

During the pre-task interview, participants expressed doubts that data-related controls companies offered actually were effective. A few thought that there was nothing they could do to control ads, or were skeptical that available control mechanisms changed which ads were displayed. As P16 explained, *"It's like the door open/close on the elevator. It's just there to make you feel like you have some power. But I really don't think it does anything."* Others assumed data-sharing agreements between companies precluded opt-outs. P12 explained, *"I think it would be really difficult to like kind of untether them from each other cause I know they have a lot of agreements with each other and stuff like that."* Some expressed skepticism that their data would actually be permanently deleted by a company when requested. As P6 stated, *"I think that I could like go through the motions of deleting the information, but I feel like it might still be there even if I tried to delete it."*

We also noted that skepticism of deletion choices persisted even after participants used deletion mechanisms in the study. A few participants assigned to `phys.org` believed they were simply deactivating their account and that their account data would not actually be deleted by the company. A few others assigned to `nytimes.com` or `runescape.com` were unsure whether or not their data would be fully deleted.

We observed that participants had more confidence in the mechanisms they used to opt-out of email marketing, due in part to prior experience. Almost all participants who used an email opt-out believed that they would eventually stop receiving emails from which they opted out, even if it takes a few days. A few mentioned they might receive a final email to confirm their unsubscribe request.

Confusion about scope of targeted advertising opt-outs

Most participants assigned to use an advertising opt-out had misconceptions about whether the mechanism they used would be effective across different browsers or devices. Some who used cookie based opt-outs on `coinmarketcap.com` or `colorado.edu` were unsure or had misconceptions about whether they would continue seeing targeted ads. Most misconceptions were related to inaccurate mental models of how cookies were stored, with some believing that they were synced to a user's Google profile. Thus they believed that any changes to cookies made using Chrome on a computer would prevent them from seeing targeted ads when they used Chrome on their phone.

4.4 Discussion

We conducted an in-lab study with 24 participants to explore the usability and usefulness of privacy controls. Our results highlight several design and policy implications for how websites, particularly those that offer a small number of privacy choices such as those in our sample, should present controls for email marketing, advertising, and deletion. However, further study is needed before these initial findings can be translated to broader policy or design recommendations.

4.4.1 Design Implications

We noted several design decisions that made completing the privacy choice tasks particularly difficult, as well as some that seemed to aid participants. Our findings are especially relevant to controls in user account settings or privacy policies.

Provide unified settings in a standard location

Unifying privacy choices into a single, standard location (perhaps in the form of a dashboard) would likely make these controls easier for users to find. Some participants recognized that many websites have controls in account settings pages and looked for controls there. If the practice of putting privacy choices in account settings was more widely adopted and promoted, it is likely that most users would learn to look there. However, privacy controls for which a login is not essential should also be available without requiring users to log in or even to have an account.

Privacy controls could also be implemented as an interface within web browsers, which in turn could convey users' choice information to websites in a computer-readable format. This could allow for opting out once for all websites (the idea behind the Do Not Track mechanism), or for all websites that meet certain criteria. It could also save users the effort of finding choice mechanisms on websites and instead allow them to go to the choice menu in their web browser, where they would be provided with available choices that could be exercised through the standard interface.

Supplement with additional paths and in-place controls

Even after unifying choices in one place, websites should still offer multiple paths to those controls so that they are easy to find. Links to privacy controls should be placed anywhere users might look, such as the account settings, privacy policy, and website help pages. For example, all participants assigned to the `nytimes.com` reached the deletion request form in the privacy policy through the account settings, not the link in the website footer mandated by the California Online Privacy Protection Act (CalOPPA). Websites should ensure that if they have multiple links or mechanisms they are consistent with each other and lead to the same results.

Control mechanisms that are offered within the context of how data is used by the website can also supplement unified privacy dashboards. With email marketing, participants in our study were generally aware of unsubscribe links in emails and thought they were easy to find. Similarly, a few participants recalled the ability to control targeted ads on a website by interacting with the corner of an ad.

Reduce effort required to understand and use choice

Websites in our study imposed much of the effort required to exercise privacy choices onto users. It was up to users to distinguish between multiple targeted advertising opt-out tools and figure out how to articulate written deletion requests. For these choices to actually be useful, websites need to place more effort into packaging them into simple settings offered through the website. The mechanisms participants favored the most in our study were toggles or clearly-labelled buttons offered in the account settings. Such settings could automatically place opt-out requests through commonly used industry tools such as those offered by the DAA and NAI, or trigger database queries to remove a user's personal information.

How privacy controls are labelled and organized in a unified privacy dashboard will impact their usability. Our study highlighted that imprecise navigation labels may confuse users. Within a page, controls should be clearly organized and labelled. Websites should conduct user testing with the design of their particular privacy dashboard pages to ensure that people can find the information they need.

Bolster confidence that choices will be honored

Participants in our study were skeptical that privacy choices would actually be honored by websites. Better communication about what exactly a setting does also could help relieve skepticism. For example, `phys.org` stated the time period after which account data would be deleted in the final step of the account deletion process. Websites should also provide confirmation that a choice has been applied after users complete the process. A confirmation message can be displayed within the website itself if the choice is immediately applied. For choices, such as email unsubscribes, that require time to process and complete, at minimum there should be a confirmation message that acknowledges the request and provides a clear estimate of how long it will take to honor the request. For requests, such as those for data deletion, that may take more time before the choice is fully applied, the website should also send a confirmation email.

4.4.2 Public Policy Implications

The recent enactment of comprehensive privacy legislation, such as the GDPR and CCPA, require companies to not only offer privacy choices, but also make them usable. Prior laws, such as the CAN-SPAM Act, included requirements for privacy mechanisms to be clear and conspicuous. Our results indicate that website privacy choices similar to those in our study remain difficult for users to find and use, but that some of these usability requirements are having an impact.

We observed that unsubscribe links within emails had better usability relative to the user account and privacy policy mechanisms we studied. This is likely an effect of CAN-SPAM Act requirements. From our study, it is apparent that unsubscribe links are widely used and that, over time, people have learned to expect these links in the marketing emails they receive. For other regulation to have similar impact, design guidelines for how websites should present privacy choices may be helpful. Guidance on where and how privacy controls should be presented will likely lead to less variation among websites and could allow users to develop consistent expectations. Moreover, future regulation should incorporate the results of usability studies to inform these design guidelines or could require websites to conduct user testing to ensure that choices are useful and usable for consumers.

4.5 Conclusion

We conducted a 24-participant in-lab usability evaluation of privacy controls related to email marketing, targeted advertising, and data deletion. Our findings highlight the need to better align the location and functionality of choices to user expectations of where to find these choices and how to operate them. Additionally, simple interface changes, including better labeling and use of confirmation messaging, would make choices more useful and increase users' confidence in their effectiveness. Furthermore, the relative success of unsubscribe links mandated by the CAN-SPAM Act suggests that the standardization of choices through regulation could improve the usability of choices.

Chapter 5

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

It is clear that the mechanisms that websites commonly use to provide privacy notice and choice are fraught with issues. Privacy policies, commonly used to provide notice, are lengthy [33, 101] and full of jargon [44]. Among other issues, the research detailed in Chapters 3 and 4 demonstrated that privacy choice mechanisms are difficult to find, as their location varies across websites. Privacy advocates, legal experts, and academic researchers have argued for standardized mechanisms to provide privacy notices and choices [28, 122**?**]. Requirements that privacy notices and choices be clear and accessible have also emerged in recent regulation, such as the California Consumer Privacy Act (CCPA) [113] and Europe's General Data Protection Regulation (GDPR) [42]. Researchers have explored ways to help consumers find and understand privacy-related information and choices. Examples include privacy dashboards [8, 56], certifications [10], scores [57, 118], labels [40, 80, 81], pop-ups [140**?**], as well as icons [35, 38, 71, 75, 105, 123**?**].

In principle, icons can communicate concepts quickly and concisely across linguistic and cultural differences [**?**]. Icons can be recognized and memorized more easily than other UI elements with richer information [123]. However, privacy concepts can be difficult to convey through icons [38, 122**?** **?**]. Prior attempts at developing icons have primarily focused on conveying information about data flows or specific data practices (e.g., [35, 105, 123**?**]). The concept of choice has been less explored in previous privacy iconography research — even though privacy choices are a key component of consumer privacy regulation [28, 42, 113].

The study detailed in this chapter investigates how to effectively convey to consumers the presence of privacy choices on websites through icons and accompanying descriptions (which we refer to as link texts). In particular, this study considers the presence of generic privacy choices and an opt-out for the sale of personal information, as mandated by the CCPA. We first developed 11 icons that center on three choice-related concepts: the broad idea of *choice*, the action of *opting-out*, and choices regarding *the sale of personal information*, before selecting

This chapter is a lightly edited version of a paper previously published as: 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). 2021 [64].

five icons for further refinement and evaluation. Because icons — especially new ones — are rarely fully self-explanatory [71], we further evaluated 16 link texts to accompany the icon, including two link texts mandated by the CCPA. We then conducted a nearly full-factorial online experiment (n=1,468) to assess how well different combinations of the most promising icons and link texts from the pre-studies communicated the presence of privacy or do-not-sell choices. Finally, we conducted an experiment to test an icon that the California Attorney General's Office (OAG) proposed for the CCPA opt-out [**?**] after we shared our initial results with them.

The results of this study suggest that a blue stylized toggle icon best conveyed the idea of choices, whereas icons focused on the sale of personal information created misconceptions about what would happen after clicking the icon. The Digital Advertising Alliance's Privacy Rights icon [**?**] and the older AdChoices icon [**?**], as comparison points for our newly designed icons, suggested "more information" but not "choice." For icon-text combinations, "Privacy Options" paired with the blue stylized toggle icon best conveyed the presence of privacy choices. The link texts mandated by the CCPA ("Do Not Sell My Personal Information" and "Do Not Sell My Info") effectively conveyed the expectation of choices related to the sale of personal information in combination with most icons. Our follow-up study of the OAG's icon revealed that even minor design changes could severely reduce an icon's comprehension and increase misconceptions.

This chapter makes the following contributions:

- Demonstration of an iterative evaluation approach that explores the comprehension of new icons and link texts.
- Identification of promising icon and link text pairings that effectively indicate privacy choices to consumers.
- Valuable insights for future work in the design of privacy choice indicators.

5.1 Study Overview

Between November 2019 and February 2020, we conducted a series of studies to iteratively design and evaluate two types of icons and associated link texts: one indicating the presence of generic privacy controls on websites, and the other indicating choices related to the sale of personal information, as required by the CCPA. Our research involved two pre-studies (one focusing on icons and the other on link texts), a large-scale online experiment to evaluate icon-link text combinations, and a follow-up evaluation of an icon that the Office of the California Attorney General (OAG) had proposed based on our initial findings.

Icon Pre-Study (Section 5.2, n=520) We developed 11 privacy icons that center on three choice-related concepts: the broad idea of *choice*, the action of *opting out*, and choices regarding *the sale of personal information*. We iteratively refined and tested these icons to identify which to include in our main experiment. Our icon pre-study suggests that a stylized toggle switch was promising for conveying the presence of choice; three icons that included dollar signs, slashes, stop signs, and ID cards were good candidates for conveying the CCPA do-not-sell opt-out.

Link Text Pre-Study (Section 5.3, n=540) We tested 16 textual descriptions, or link texts, to accompany the icons we developed. We analyzed how each link text, when displayed alone, was interpreted by participants; and identified three link texts ("Privacy Options," "Privacy Choices," and "Personal Info Choices") with mostly correct interpretations. The two CCPA link texts ("Do

Not Sell My Personal Information" and "Do Not Sell My Info") effectively indicated choices related to the sale of personal information, but did not generalize to broader privacy-related choices.

Icon-Text Combinations Evaluation (Section 5.4, n=1,468**)** We conducted a large-scale, nearly full-factorial online experiment to evaluate how well 23 combinations of icons and link texts, selected from our pre-studies, communicated the presence of privacy choices and do-not-sell choices. We showed participants one icon-text combination on a screenshot of a fictitious online shoe retailer webpage, mimicking how users may see such privacy choice indicators in the real world. A blue stylized toggle icon paired with the link text "Privacy Options" best conveyed the presence of privacy choices. The two CCPA link texts effectively conveyed the presence of do-not-sell opt-outs when paired with most icons.

OAG Icon Evaluation (Section 5.5, n=421**)** After we shared our results with the OAG, they proposed an icon for the CCPA's do-not-sell opt-out, which was similar to our stylized toggle icon but with notable deviations. We conducted a follow-up experiment to explore the impact of the icon's toggle style and color on expectations for do-not-sell choices. Compared to our stylized toggle icon, participants were much more likely to perceive the OAG's proposed icon as a toggle switch rather than a static icon.[1]

5.2 Icon Pre-Study

We developed 11 icons related to privacy choices and evaluated how users interpreted the icons with and without a text description. We found that a stylized toggle icon effectively communicated the concept of choice, but communicating the concept of "privacy choice" was difficult without text. While icons with arrows to depict removal were mostly unsuccessful, icon elements focusing on "do not" and "sell" could communicate an opt-out for the sale of personal information. However, participants often misunderstood an icon without a text description.

5.2.1 Icon Development

Icon ideation

To explore potential icon candidates, we leveraged existing privacy iconography to generate three key concepts in line with our objectives: the broad concept of *choice*, the action of *opting out*, and a specific opt-out related to the *sale of personal information* for the CCPA. We did not attempt to design an icon that visualizes privacy since privacy is a broad concept with many interpretations [**?**]. Additionally, we did not test existing privacy and security icons since they are already known for representing other concepts unrelated to privacy choices (e.g., lock or shield for HTTPS indicator [48]), or focus on specific data practices [123].

To capture a wide range of icon ideas embodying the three choice-related concepts we identified, we conducted design ideation activities at our institutions with colleagues interested in

[1]In December 2020, the OAG published the fourth set of modifications to the CCPA regulations [**?**], recommending that businesses use our blue stylized toggle icon next to the CCPA link text when notifying consumers of their right to opt out of the sale of personal information. The OAG maintains a website that includes documents relevant to CCPA rulemaking [**?**].

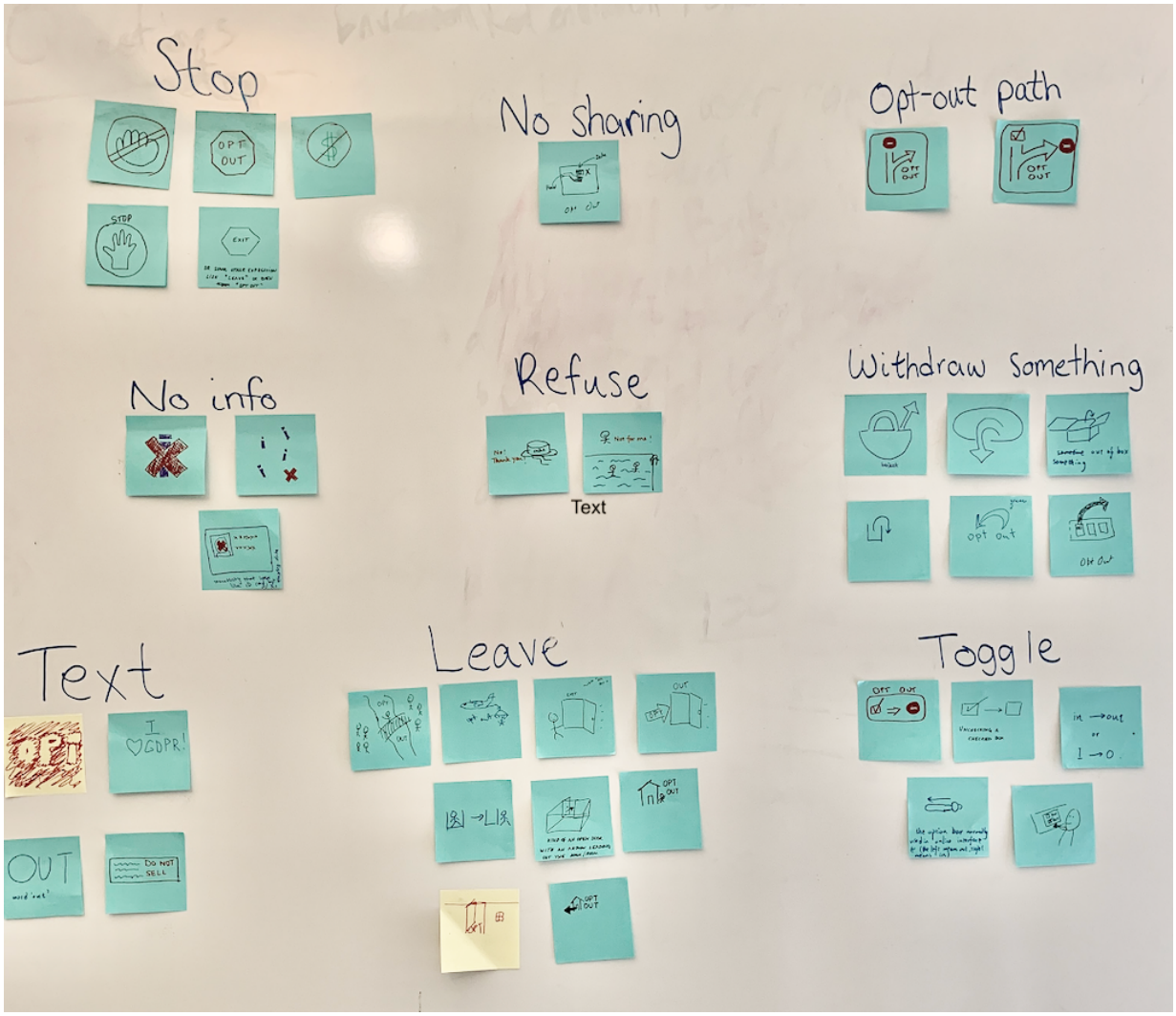


Figure 5.1: Common themes that emerged in one of the brainstorming sessions for an icon that conveyed *opting-out*.

privacy and security research. During the activities, participants drew ideas on sticky notes and discussed themes with the group. We then conducted affinity diagramming [87] of the sketches by grouping similar ideas and identifying themes in the visual elements participants used to represent the three concepts (see Figure 5.1). In selecting themes to iterate upon further, we eliminated those focusing on privacy more than choice due to our goal of conveying choice. We also eliminated themes that seemed too abstract from privacy choice (e.g., leaving or refusing something) or difficult to graphically depict (e.g., third parties). Considering that web icons are generally small, we further eliminated themes that would produce unrecognizable icons when shrunk down in size due to complexity (e.g., exchange/trade-off of data for money). In the end, we identified five themes (see Table 5.1) that had the potential to represent our three choice-related concepts effectively.

Choice Concept	Icon Themes	Preliminary Icons
Privacy choice/consent	• toggle switch • change toggle or checkbox choice	*Stylized-Toggle* *Changed-Choice* *DoNot-Checked*
Opting Out	• withdrawing something from a basket or box	*Box-Arrow* *Circle-Arrow* *Folder-Arrow*
Do-Not-Sell Choices	• no money/selling • stop selling personal info	*DoNot-Dollar* *Slash-Dollar* *Stop-Dollar* *ID-Card* *Profile*
Existing icons		*DAA Privacy Rights* *DAA AdChoices*

Table 5.1: Icon themes that emerged in ideation sessions for each choice-related concept, and the corresponding icons included in our preliminary testing.

Refinement with graphic designers

Next, we worked with three graphic designers to develop icons for the five themes. The graphic designers worked individually with sketches from our brainstorming sessions as a starting reference, and were encouraged to produce variants and alternative designs, such as varying the shape or size of icon elements. The research team jointly reviewed the graphic designers' work and selected 11 icon designs as candidates for user testing in the icon pre-study.

Table 5.1 shows all 11 candidate icons. Three icons were intended to convey the broad idea of *choice*: one featured a toggle — a standard UI element for turning on or off settings [**?**]; and two featured checkboxes (transitioning from a checked to an unchecked box, or negating a checkbox), since checkboxes are common in online forms and consent interfaces [**?**]. Three icons were intended to convey the action of *opting out*, which is analogous to withdrawing consent: two had an arrow coming out of simple shapes (a circle and a box); and the third used a file folder to represent personal data. Five icons were intended to convey *do-not-sell* choices: three used different negations of a dollar sign to represent stopping a sale, and two further included a "person" element to represent personal data. To minimize potentially biasing effects of color in our pre-study, we created the initial versions of our icons in black and white. Additionally, we included the DAA's AdChoices [**?**] and Privacy Rights [**?**] icons in our icon pre-study as a benchmark for industry practices.

5.2.2 Preliminary Icon Testing

We conducted an initial round of user testing on all 11 candidate icons to decide which to test in subsequent studies. We developed an online survey to capture qualitative and quantitative responses that would help us identify feasible icons for indicating the presence of generic privacy choices and do-not-sell choices.

Study protocol

Our initial testing sought to identify difficult-to-interpret icons and specific icon elements that help indicate privacy or do-not-sell choices. We implemented a between-subjects design, in which we showed each participant one of the icon candidates at random without context. To examine the impact of placing a link text next to the icon (as required by the CCPA), half of the participants saw the icon displayed with the text "Do Not Sell My Personal Information." We hypothesized this text would aid the comprehension of icons intended to convey do-not-sell choices.

After presenting the icon, we asked participants to provide open-ended responses regarding their interpretation of the icon and their expectations of what would happen if they clicked on it — this was to capture their unprimed impressions of the icon. As a complementary quantitative data point, we next showed participants all icons, asked them to select which one would best convey the presence of privacy choices and do-not-sell choices respectively, and explain the rationale behind their selection.[2] We then asked participants about their familiarity and expectations regarding the DAA's AdChoices icon [34] to evaluate the recognizability and comprehension of an already widely deployed privacy choice icon. Lastly, we collected participants' demographic information and asked about awareness of a US law that required companies to provide a "do not sell" option. Appendix **??** includes the full set of survey questions.

For this and all subsequent studies, we did not collect personal data from participants, and we instructed participants to avoid revealing personal information in their open-ended responses. The Institutional Review Boards at Carnegie Mellon University and the University of Michigan approved all study protocols.

Recruitment and sample demographics

We recruited 240 participants from Amazon's Mechanical Turk (MTurk) to ensure roughly 20 responses per condition — a sufficient number for capturing a variety of opinions for descriptive analysis. We set the recruitment filter as US residents over 18 years old, with a 95% or higher approval rate. Before answering survey questions, participants reviewed a consent form and confirmed their age and residency eligibility. The average study completion time was 5.25 minutes, and participants were compensated $1.00 (average $11.43/hour).

In line with demographic characteristics of MTurk workers [**?**], our samples for this and the subsequent studies were diverse but not representative of the US general population: they skewed younger, more male, and more educated. We summarize participant demographics here once as

[2]The Privacy Rights icon was green when presented alone but black-and-white when presented with other icons to eliminate the impact of color on participants' selection.

they were fairly uniform across all studies, and provide detailed demographics for each study in Appendix **??**. Participants were residing in most US states (with 10-20% living in California) and somewhat tech-savvy (with 23-48% reporting education or job experience in computer science, computer engineering, or IT). 3-10% of participants reported awareness of a US law that required companies to provide a "do not sell" option, with relatively higher percentages in the icon-text combinations and OAG toggle evaluations, indicating a potential increase of awareness after the CCPA went into effect. Once a participant completed one of our studies, we did not permit them to participate in any subsequent studies evaluating icons and link texts.

Data analysis

We conducted a thematic analysis [**?**] of participants' qualitative responses. One author examined a subset of the qualitative data to identify common themes and developed an initial codebook. The team then discussed the initial codebook, adding and modifying codes as necessary. To ensure high consistency in coding, two authors coded 20% of all responses and additional responses if needed until reaching a Cohen's κ of at least 0.7, which is considered sufficient agreement [**?**] (average κ=.81 across all questions).[3] Most responses mapped clearly to a code, and ambiguous responses were discussed by multiple researchers before being coded. After we achieved high inter-coder reliability, one researcher coded the remaining responses. We calculated descriptive statistics of coded qualitative data but did not conduct any hypothesis testing, as our primary objective for this pre-study was to eliminate from further consideration icons that appeared confusing or did not effectively convey intended concepts. Eleven responses were excluded from analysis, as they only included text that did not respond at all to the open-ended questions. We note the number of responses excluded from the analysis for this and subsequent studies in Appendix **??**.

Findings

As shown in Table 5.2, most icons did not lead to their intended interpretations when shown alone. Participants did not exhibit a clear preference for which icon best represented generic privacy choices, but most chose *Slash-Dollar* as the icon for representing do-not-sell choices.

A stylized toggle icon best conveyed "choice." Among the three icons that were intended to convey choice, participants commonly associated *Stylized-Toggle* with the notion of choosing or selecting something. Participants thought of "completion" (i.e., marking something as completed or completed downloads), rather than choice, upon seeing *DoNot-Checked*. *Changed-Choice* received a variety of interpretations, suggesting that it would not work well for indicating privacy choices either.

Icons for conveying "opting out" were confusing. Though two participants interpreted *Box-Arrow* as "removing something" (as intended), other participants interpreted it differently. Participants mostly interpreted *Circle-Arrow* as something related to motion, and focused on the

[3]Responses to the AdChoices interpretation lacked variations, meaning that a single disagreement between coders would cause a significant drop in Cohen's κ. For this question, we used inter-coder percentage agreement instead to measure inter-coder reliability and ensured the percentage agreement was at least 75%.

folder element rather than the arrow in *Folder-Arrow*; neither prompted participants to think of opting out.

Dollar signs suggested payment rather than selling. All icons intended for do-not-sell choices conveyed a sense of payment or money, but not selling. Interpretations included "cash or American dollars are not accepted," "something is free," "something requires payment," and "something related to an account balance." Promisingly, three participants connected *ID-Card* with a person and money, which aligns with its intended purpose of signaling do-not-sell choices.

No clear preference for the privacy choices icon. Participants were divergent in their opinions of which icon best represented choices about the use of personal information (see Figure 5.2). *Stylized-Toggle* was selected most frequently, though *ID-Card*, *DAA*, and *Folder-Arrow* were not far behind. In open-ended responses, participants identified certain icon elements that conveyed privacy choices to them, including "select/choose" (32.3%), "money/selling" (21.0%), "personal information" (19.2%), and "stop/do not" (16.6%). The mentioning of "money/selling" and "stop/do not" suggests potential priming effects from the question that asked about the best icon for do-not-sell choices or the "Do Not Sell My Personal Information" link text when presented.

Slash-Dollar preferred as "do-not-sell" icon. Participants exhibited a clear preference for which icon best represented do-not-sell choices as 38.9% selected *Slash-Dollar* (see Figure 5.2). In open-ended responses, participants mentioned "money/selling" (48.9%), "stop/do not" (46.7%) and "personal information" (21.0%) as important icon elements for conveying do-not-sell choices. Participants preferred "stop/do not" to be represented by a circle with a slash, rather than an octagonal stop sign or a do-not-enter sign, as indicated by the stark difference between *Slash-Dollar* and *DoNot-Dollar*/*Stop-Dollar*. This suggests that the octagon shape in *Stop-Dollar* may be difficult to recognize as a stop sign without color, and the "do not enter" sign in *DoNot-Dollar* was not widely recognized, or was misidentified as a minus sign.

5.2.3 Refined Icon Testing

Our preliminary testing suggested comprehension issues with most icons but surfaced some promising candidates. In selecting icons for further testing, we included *Stylized-Toggle* and *ID-Card* as candidates for privacy choices: the former appeared to communicate "choice" well, and the latter was ranked highly by participants in preliminary testing. For do-not-sell icon candidates, we included *Slash-Dollar* due to participants' preferences and *Stop-Dollar* to explore whether color would increase recognition of the stop sign.

We evaluated refined versions of the four icons mentioned above and the DAA's Privacy Rights icon (see Figure 5.3) to further narrow down icon selections for the larger-scale icon-text evaluation. Specifically, we colored the stop sign and slash red in *ID-Card*, *Stop-Dollar*, and *Slash-Dollar*, and made the dollar sign in *Slash-Dollar* more readable. We colored *Stylized-Toggle* blue — a neutral color that does not convey a particular state, unlike green or red.

Study protocol

We followed the same protocol as before to evaluate the five icons. To mitigate a potential priming effect, we randomized the order of the "best icon" questions for privacy/do-not-sell

choices. We recruited 280 participants (roughly 28 per condition) to detect a medium effect size (.3) [**?**] with at least 80% power for our planned statistical analysis. We aimed for a medium effect size due to the study's exploratory nature and to save the budget for oversampling in the icon-text evaluation. The average study completion time was 4.50 minutes, and each participant received $1.00 (average $13.30/hour).

Data analysis

We followed the same qualitative data analysis approach as before (κ=.79). Additionally, we collaboratively categorized the codes used to analyze open-ended responses to "What does this symbol communicate to you?" as *correct* or *incorrect* interpretations regarding the icon's intended purpose. We then used these binary labels as the dependent variable of Chi-squared tests (or Fisher's exact tests when applicable) to determine whether the overall difference in study conditions were statistically significant. Follow-up pairwise comparisons were adjusted with Holm-Bonferroni corrections.

Findings

Participants interpreted *Stylized-Toggle* as an indicator of some form of choice, and preferred it over other candidates for conveying generic privacy choices. Consistent with the preliminary testing, participants preferred *Slash-Dollar* for communicating do-not-sell choices. The CCPA link text's presence made participants more likely to expect an icon to lead to do-not-sell choices.

Stylized-Toggle was interpreted as intended. Table 5.3 provides common interpretations of each icon when displayed without the CCPA link text. A Fisher's exact test showed significant differences between icons, when presented alone, in generating correct interpretations that align with the icon's intended meaning ($p<.001$, $V=.58$). Pairwise comparisons found that *Stylized-Toggle* was more likely to be interpreted correctly compared to other icons (all $p<.001$). Open-ended responses suggested that *Stylized-Toggle* was primarily interpreted as an option to "accept/decline" or "activate/deactivate" something. In contrast, the interpretations of other icons often misaligned with their intended meanings. The DAA's Privacy Rights icon conveyed an option to "get more information" but did not suggest a choice or opt-out. Common interpretations of *Slash-Dollar*, were "something is free or does not require money" or "cash or American dollars were not accepted." *ID-Card* was mostly interpreted as "something costs money." *Stop-Dollar* was similarly associated with money, but not selling.

Clear icon preference for privacy choices and do-not-sell choices. As shown in Figure 5.4, when the icons were colorized, participants exhibited a clear preference for *Stylized-Toggle* to represent choices about the use of personal information. 16.8% of participants explicitly stated that a toggle "with a checkmark and an X in it" nicely conveyed choice. Similar to the preliminary testing, *Slash-Dollar* was selected most frequently as the icon for conveying do-not-sell choices; *ID-Card* ranked second (see Figure 5.4).

CCPA link text led to expectations of do-not-sell choices. A Chi-squared test showed that participants who saw the CCPA link text were significantly more likely to interpret the icon as its intended meaning ($p<.001$, $\phi=.38$). Of the 139 participants who saw an icon with the CCPA link text, 43.2% (60) expected some form of choice to stop websites from selling their personal

information. 13.7% (19) expected the ability to configure the types of personal information they could prevent from being sold or entities to which information is sold. 31.7% (44) expected being immediately opted out of the sale of personal information after clicking. There was no significant difference between icons in creating any of these expectations, suggesting that the link text impacted participants' expectations rather than the icon. Notably, the CCPA link text's presence did not eliminate misconceptions, such as expecting a different type of privacy choice (e.g., opting out of data collection on the website) or interpreting the link text as a warning not to give out their personal information to websites.

DAA's AdChoices icon still mostly unknown. Even though the DAA launched its AdChoices icon in 2010, only 40 (14.3%) participants recalled seeing this icon before. The most common expectation of the AdChoices icon was that it provided more information about something, as indicated by 152 (54.3%) participants. Only six participants expected it would lead them to choices related to targeted advertising. Our results confirm Leon et al.'s 2011 findings that there is little recognition of the AdChoices icon [90] — time and widespread adoption does not seem to have increased consumer awareness of this icon.

5.3 Link Text Pre-Study

We developed and iteratively evaluated potential link texts to accompany our icons and aid comprehension. "Privacy Choices" emerged as the best candidate for conveying generic privacy controls with few misconceptions, closely followed by "Privacy Options." The CCPA link text variants performed well in conveying do-not-sell opt-outs but did not generalize to other types of privacy controls.

5.3.1 Link Text Development

We generated link text candidates by identifying words or phrases corresponding to the three icon concepts we focused on (*choice*, *opting-out*, and *do-not-sell*). During our ideation, we observed that link texts could follow a pattern of two components: a privacy-focused prefix and, optionally, a choice-focused suffix. We wanted to explore whether the general prefix "privacy" or the more specific prefix "personal info" would more clearly convey the type of choices. For the suffix, we hypothesized that the broad terms "choices" and "options" would create different expectations compared to "opt-out," a more specific type of choice. We also included the two CCPA do-not-sell opt-out texts [113] and their variants — including an abbreviated version ("Don't Sell My Info"), and versions emphasizing *choice* rather than information (e.g., "Do-Not-Sell Choices") — to control for confounds and explore potential alternatives to the CCPA link texts.

Our initial set included 14 link texts revolving around six words or phrases: personal info/privacy/do-not-sell for the prefix, and choices/options/opt-outs for the suffix. After preliminary testing, we eliminated four with poor comprehension and added two for further testing. Table 5.4 shows the full set of link texts we evaluated.

5.3.2 Preliminary Link Text Testing

We tested the initial link text set using a similar protocol as the icon pre-study. Based on the findings, we eliminated four candidates from subsequent testing and added two more variants of the CCPA link texts.

Study protocol

We showed each participant one of the 14 candidate link texts at random, styled as a hypertext link but non-clickable, without an icon or other context. We asked participants to describe their expectations of what would happen if they clicked on the link and interpretations of specific text components. Then, we presented eight scenarios constructed from open-ended responses from the icon pre-study and asked participants to rate the likelihood that clicking on the link would lead to each scenario. Two scenarios were accurate expectations related to privacy notices and choices, three were accurate expectations related to do-not-sell, and three were misconceptions (see Q3 in Appendix **??**). Lastly, participants were asked demographic questions and about their familiarity with the CCPA. We recruited 140 participants on MTurk (roughly ten responses per condition) to have a diverse set of qualitative responses for descriptive analysis. The average study completion time was 4.20 minutes, and each participant received $1.00 (average $14.29/hour).

Data analysis

We coded participants' open-ended responses using the same thematic analysis approach as in the icon pre-study (κ=.89). The coded data was used for descriptive analysis only, as our primary goal was to identify link texts with high rates of misconceptions and eliminate them from further consideration.

Findings

Our preliminary testing of link texts suggested a greater influence of the prefix, rather than the suffix, on expectations of what happens after clicking the link. "Personal information" was understood as personally-identifiable information, and its absence led to misconceptions about the word "sell."

"Personal information" was primarily interpreted as PII (personally identifiable information). When asked to interpret the phrase "personal information," "personal info," or "info," 33 of the 57 participants (57.9%) who saw a corresponding link text listed examples of PII, such as name and birthday. 11 participants interpreted the phrase as demographic information, such as age or gender. Nine participants thought it referred to their IP address or location, and another nine believed it referred to cookies or past activities on the website or elsewhere.

"Sell" on its own was often misunderstood. Without an explicit reference to personal information, participants struggled to identify the subject to which "sell" referred. Among the 45 participants who saw one of the "do not sell" variants without "personal information" or "my info," 18 (40.0%) thought the sale referred to a physical product. Four thought the sale was

related to stocks or money, and five did not know what the sale is about. Given that participants saw the link text with no further context, it is not surprising that such misconceptions occurred.

5.3.3 Refined Link Text Testing

Our preliminary testing showed that link texts containing the word "sell" without "info" did not convey privacy choices or do-not-sell choices well. Therefore, we eliminated four corresponding link texts from further testing but retained "Do-Not-Sell Options," which conveyed a control/choice related to personal information about as frequently as "Privacy Opt-Outs" and "Personal Info Options." We added two new link texts ("Do Not Sell My Info Choices" and "Do Not Sell My Info Options") to assess how adding choice-related suffixes would affect the interpretation of the CCPA-mandated link texts. We did not test "Do Not Sell My Info Opt-Outs," as our preliminary testing suggested "opt-outs" might be less intuitive than "choices" or "options."

Study Protocol

We recruited 400 additional participants, roughly 33 per condition, to detect a medium effect size (.3) with at least 80% power for our planned statistical analysis comparing expectations generated by the candidate link texts. The average study completion time was 4.1 minutes, and participants were compensated $1.00 (average $14.63/hour). Since we used the same protocol and survey instrument, we aggregated participant responses with those collected from the preliminary testing for the analysis.

Data Analysis

We followed the same qualitative data analysis approach as in previous studies; two authors coded 20% of the data (κ=.81) and one author coded the remainder. For this and the following studies, we structured the codebook hierarchically by grouping codes into four categories (high-level codes) for category-level analysis. Specifically, we labeled "yes" or "no" for whether a code conveyed (1) the concept of choice; (2) the ability to opt out of the sale of personal information; (3) the concept of privacy broadly; and (4) misconceptions.[4] Three authors completed the mapping for all codes together and resolved any disagreements. We then used the values of these categorizations as the dependent variables in Pearson chi-square or Fisher's exact tests, with link text conditions as the independent variable. Pairwise comparisons were Holm-Bonferroni corrected.

Findings

As seen in Figure 5.5, participants' expectations significantly varied across link texts. "Privacy Choices" created the least misconceptions. The CCPA link texts and their variants successfully led to expectations of do-not-sell choices.

[4]For example, the response "It would give you the option to not have your personal information given, shared, or sold to someone else" was coded as "choices: do not sell." For high-level categories, the code was labeled as "yes" for conveying choice and do-not-sell, and "no" for conveying privacy or a misconception.

Link text suffix did not impact expectations of choices. 47.9% of participants expected to see some form of choices, including those related to privacy and do-not-sell. As seen in Figure 5.5, there was a significant overall difference between conditions ($p<.001$, $V=.27$). Pairwise comparisons revealed that the only significant difference was between "Privacy Options" and "Do-Not-Sell Options" ($p=.04$); 67.6% and 25.0% of participants in those conditions expressed expectations of choices, respectively. The choice-related suffixes (i.e., "choices," "options," or "opt-outs") did not appear to impact participant expectations of choices, given the small differences between link texts with the same privacy-related prefix.

CCPA link text variants led to expectations of do-not-sell choices but did not generalize. As seen in Figure 5.5, there was a significant difference between conditions in generating expectations of do-not-sell choices ($p<.001$, $V=.34$), or something more broadly related to privacy ($p<.001$, $V=.42$). Link texts beginning with "Do Not Sell" most often led to expectations of do-not-sell choices, with "Do Not Sell My Info Choices" performing significantly better than "Personal Info Options" ($p=.005$), "Privacy Options" ($p=.008$), and "Privacy Choices" ($p=.04$) in this regard. 35.0% of participants who saw "Do Not Sell My Info Choices" expected do-not-sell choices, whereas no participants who saw "Personal Info Options" or "Privacy Options" expressed the same expectation. However, link texts beginning with "Do Not Sell" did not effectively convey broader privacy-related information or options. "Privacy Options," "Privacy Choices," and "Privacy Opt-Outs" were all significantly better than "Do-Not-Sell Options" (all $p<.001$), "Do Not Sell My Info Choices" ($.0003 < p < .012$), "Don't Sell My Info" ($.001 < p < .04$), and "Do Not Sell My Info" ($.002 < p < .05$) for this purpose. 67.1% of participants who saw a "Privacy" prefixed link text described a privacy-related expectation, compared to 21.4% who saw a "Do Not Sell" prefixed link text.

"Privacy Choices" generated the least misconceptions. As seen in Figure 5.5, the distribution of misconceptions were not even across conditions ($p<.001$, $V=.39$). Pairwise comparisons revealed that "Privacy Choices" created significantly fewer misconceptions than "'Do Not Sell My Info" ($p=.04$). Among the 63 participants who saw one of the link texts beginning with "Do Not Sell," some thought the link would lead to phishing/malware risks (16), investment advice (8), the site's policy on selling items (8), and ads for privacy products or other services (6).

Some link texts might apply to both privacy choices and do-not-sell choices. In examining participants' Likert responses to the predefined scenarios, five link texts were rated as "definitely" or "probably" likely to lead to choices about how personal information is used and shared by over three quarters of participants. Among them, "Personal info Choices," "Privacy Opt-Outs," "Do Not Sell My info Options," and "Privacy Options" were also among the top five link texts rated as "definitely" or "probably" likely to lead to the scenario describing choices about the sale of personal information. This suggests that these four link texts had the potential to convey both generic privacy choices and do-not-sell choices relatively well.

5.4 Icon-Text Combinations Evaluation

Our pre-studies suggested a need for combining icons with link texts, consistent with prior research and recommendations [51, 146]. Icons alone do not necessarily translate to correct expectations even with a certain degree of familiarity [123**?**], as reflected by our findings on the

DAA's AdChoices icon. Similarly, link text alone might not stand out. Pairing the two together can attract user attention and aid comprehension [73]. We conducted a large-scale evaluation to find icon-text combinations that accurately convey privacy choices and do-not-sell choices.

5.4.1 Method

For icons, we selected *Stylized-Toggle* and *Slash-Dollar*, since they were the most preferred for indicating privacy choices and do-not-sell choices respectively. We also included DAA's Privacy Rights icon because of its potential for widespread adoption by DAA member companies. For link texts, we selected "Privacy Options" and "Privacy Choices" since they best generated expectations of choices/controls and expectations related to privacy (see Figure 5.5). We also included the two CCPA-mandated link texts since they conveyed do-not-sell choices well. We did not include any variants of the CCPA link texts since the choice-related suffix did not influence participant expectations. Additionally, we included "Personal Info Choices" since Likert responses to predefined scenarios suggested it worked well to communicate both do-not-sell choices and broader privacy controls.

Study protocol

To measure to what extent icons and link texts interact with each other in shaping participant expectations, we used a nearly full-factorial experimental design including four icon conditions and six link text conditions (a total of 23 conditions). The four icon conditions were the DAA's Privacy Rights icon, *Slash-Dollar*, *Stylized-Toggle*, and no icon. The six link text conditions were "Do Not Sell My Personal Information," "Do Not Sell My Info," "Privacy Choices," "Privacy Options," "Personal Info Choices," and no link text. We excluded the combination of no icon and no link text since participants would not see any information. Our examination of icon-text combinations was exploratory — even though the pre-studies indicated that some icons and link texts perform better than others for certain purposes, interaction effects might exist between the icon and text, making it difficult to generate specific hypotheses.

We followed a between-subjects design, showing each participant an icon-text combination at random. While we presented icons and link texts with no context in the pre-studies, here we showed the icon and link text together on a fictitious online shoe retailer website (see Figure 5.6) to emulate how consumers might encounter them in the wild. We modified the eight scenarios for Likert questions based on common expectations uncovered in the link text pre-study; two were correct expectations, two were semi-correct expectations, and the rest were misconceptions about unwanted outcomes (see Q3 in Appendix **??**). We recruited 1,468 MTurk participants (roughly 64 per condition) based on heuristics that would allow us to run planned regressions [**?**]. The average study completion time was 4.55 minutes, and participants were compensated $1.00 (average $13.19/hour).

Data analysis

We followed the same qualitative analysis approach as in the link text pre-study (κ=.83) before using the data for quantification.[5] We coded participants' responses about expectations to identify common themes, then categorized individual codes based on whether they convey the idea of choice, do-not-sell choices, privacy broadly, or misconceptions. We then ran logistic regressions using these high-level code categories as the dependent variable, the icon-text combination condition as the main independent variable, and participant demographics as control independent variables. We ran additional logistic regressions with the same independent variables on a binary variable that represented participants' expected likelihood of each predefined scenario.[6] We applied Holm-Bonferroni corrections to p-values in all regressions since we conducted multiple tests without preplanned hypotheses [**?**]. Detailed regression results are provided in Tables **??** and **??** as part of Appendix **??**.

5.4.2 Findings

We found significant differences between icon-text conditions in creating expectations of privacy choices or do-not-sell choices; link texts impacted participant expectations more than icons in this regard. Furthermore, *Slash-Dollar* and "Personal Info Choices" generated more misconceptions than the other icons or link texts.

Conveying privacy choices. Regressions of participants' categorized open-ended expectations (Table **??** in Appendix **??**) compared how well different icon-text combinations conveyed the concepts of choice (e.g., "My choices would pop up on the screen") and privacy (e.g., "It will enable a more private experience"). Compared to *Toggle-Privacy Options* as the baseline, combinations including the "Privacy Options" or "Privacy Choices" link text, as well as *Stylized-Toggle* by itself, performed similarly in generating privacy-related expectations; participants in all other combinations were significantly less likely to expect something related to privacy ($.005<OR<.13$, all $p<.001$). Furthermore, participants were significantly less likely to expect some form of choice when seeing the link text "Personal Info Choices" without *Stylized-Toggle*, or *DAA/Dollar* without an accompanying link text ($.03<OR<.27$, $.001<p<.03$).

Figure 5.7a shows participants' Likert responses to the generic privacy choice scenario. Overall, *Toggle-Privacy Options* was the best candidate for conveying "choices about how personal information is used or shared": 93.4% of participants who saw this combination thought they would definitely or probably be led to privacy choices. Regressions of Likert responses (Table **??** in Appendix **??**) further showed that participants were significantly more likely to expect privacy choices when seeing *Toggle-Privacy Options*, compared to *Toggle-Do Not Sell My Personal Information*, *Slash-Dollar* icon alone, and *DAA* icon alone ($.03<OR<.17$, $.001<p<.009$). However, the differences between *Toggle-Privacy Options* and other conditions with "Privacy Options" as the link text were minimal and not significant in regressions. Most combinations

[5]There was little diversity in responses to the question regarding the meaning of "sell" in the link text. Thus, we used percentage agreement rather than Cohen's κ to measure inter-coder reliability and ensured the percentage agreement was at least 75%.

[6]"Definitely" and "probably" were coded as "expected" (expecting the scenario would happen) and the other answer options were coded as "unexpected."

involving the "Privacy Options" and "Privacy Choices" link texts effectively conveyed privacy choices.

Conveying do-not-sell choices. Regressions of participants' categorized open-ended expectations indicated that the two CCPA-mandated link texts significantly outperformed other link texts in creating the expectation of do-not-sell choices (e.g.,"It would let you opt out of them selling your information"). Relative to "Do Not Sell My Personal Information" with no icon, all conditions with the link texts "Privacy Options," "Personal Info Choices," and "Privacy Choices" performed significantly worse in generating expectations of do-not-sell choices ($.01<OR<.13$, all $p<=.001$). There were no significant differences between "Do Not Sell My Personal Information" or "Do Not Sell My Info" in this regard.

Figure 5.7b shows participants' Likert responses to the do-not-sell choices scenario. The three conditions with the highest percentage of definitely/probably responses all included one of the CCPA link texts: *No Icon-Do Not Sell My Info* (82.1%), *DAA-Do Not Sell My Info* (70.5%), and *No Icon-Do Not Sell My Personal Information* (67.8%). Regressions on Likert responses further showed that *No Icon-Do Not Sell My Personal Information* performed significantly better than the *DAA* ($OR=.06$, $p<.001$) and *Slash-Dollar* icons alone ($OR=.28$, $p=.04$) in conveying do-not-sell choices, suggesting effectiveness of the CCPA link texts in this regard.

Stylized-Toggle was occasionally perceived as an actual control button. While *Toggle-Privacy Options* conveyed privacy choices well and the two CCPA mandated link texts conveyed do-not-sell choices well, putting *Stylized-Toggle* next to the CCPA link texts led to an unintended consequence. 40.0% of participants who saw *Toggle-Do Not Sell My Personal Information* expected that clicking on them would definitely or probably "give the website permission to sell my personal information." *Stylized-Toggle* significantly increased the likelihood of this misconception compared to no icon ($OR=5.25$, $p=.02$) when combined with the "Do Not Sell My Personal Information" link text. This suggests that participants might perceive *Stylized-Toggle* as an actual control switch for the sale of one's personal information on the website when the icon was next to the CCPA link texts. However, we did not observe a similar pattern in participants' open-ended expectations — this expectation only emerged when we explicitly asked participants whether clicking the icon would give the website permission to sell their personal information, indicating a potential priming effect.

Misconceptions with Slash-Dollar icon and "Personal Info Choices." Regressions of participants' categorized open-ended expectations revealed that *Slash-Dollar* without a link text significantly increased the likelihood of misconceptions relative to *Toggle-Privacy Options* ($OR=67.2$, $p<.001$). Among the 371 participants who saw *Slash-Dollar*, 33 (8.9%) expressed expectations of payment options, particularly related to secure or encrypted payment (e.g., "It would present your rights to pay through secure links"). These findings indicate that the *Slash-Dollar* icon, even when paired with a link text, might be too suggestive of payment, transaction, or other financial concepts that do not concern personal information.

Also relative to *Toggle-Privacy Options*, all conditions with "Personal Info Choices" increased the likelihood of misconceptions ($11.9<OR<18.1$, $.005<p<.04$). Only 42.0% of participants who saw "Personal Info Choices" accurately interpreted choices as controls related to the collection, processing, and sharing of their personal data or broader privacy choices, compared to 66.5% of those who saw "Privacy Choices." Misinterpretations of choices most frequently included profile settings related to purchasing shoes (16.7%; e.g., "Probably it would let you input

your shoe size, height, favorite styles, etc. for a more customized look"). Other misconceptions included that the link would lead to choices about shoe styles or sizes available on the website (13.1%) and choices related to payment methods (1.6%). The remaining participants were either not sure about or did not specify the types of choices they expected.

5.5 OAG Icon Evaluation

In February 2020, the California Attorney General's office (OAG) released the first set of modifications to the CCPA regulations [**?**] after we had shared our results with them. The proposed modifications included an opt-out icon (*CalAG-Toggle*) that was similar, but not identical to our *Stylized-Toggle* icon (see Figure 5.8).

Our icon-text combinations evaluation suggested that *Stylized-Toggle* might occasionally be perceived as an actual control switch rather than an icon when paired with the CCPA-mandated link texts. We were concerned that *CalAG-Toggle* would make this misconception even more likely for two reasons. First, *CalAG-Toggle* closely resembled the toggle switch in iOS (see Figure 5.8). By contrast, *Stylized-Toggle* used a checkmark and "X" to visually convey the availability of options and a dividing line to differentiate it from a real toggle control. Second, *CalAG-Toggle* being in red created a potentially confusing double negative when paired with "Do No Sell My Personal Information." One could interpret it as either "my data is currently being sold" (because red indicates the setting "Do Not Sell My Personal Information" being off), or "my data is currently not being sold" (because red indicates the sale of personal information is prohibited). In contrast, *Stylized-Toggle* used blue, a neutral color that does not convey a particular state. We conducted a follow-up study to examine whether the style and color of *CalAG-Toggle* might diminish icon comprehension compared to *Stylized-Toggle*.

5.5.1 Method

We used the method already employed in our icon-text combinations evaluation to test the OAG's proposed icon.

Study protocol

To understand to what extent icon style and color jointly shape participant interpretations, we implemented a full factorial design that included two color conditions (red, blue) and three style conditions (six conditions total). In addition to *Stylized-Toggle* and *CalAG-Toggle*, we created a third style condition, *CalAGX-Toggle* (see Figure 5.8), which seeks to improve the visual aesthetics of *CalAG-Toggle* by enlarging the "X" to make it visually equivalent to the circle.

As before, we used a between-subjects design, showing participants one of the six icons at random next to "Do Not Sell My Personal Information" on a fictitious online shoe retailer website. In addition to their open-ended expectations, we asked participants about the likelihood of eight scenarios occurring on a Likert scale. In order to understand whether participants viewed the toggle as an actual control switch, we included two misconception scenarios of immediate settings changes (see Q3 in Appendix **??**). We recruited 421 MTurk participants (roughly 70 per

condition) for this study based on heuristics for running our planned regressions [**?**]. The average study completion time was 4.6 minutes, and participants were compensated $1.00 (average $13.04/hour).

Data analysis

We used the same approach employed in our previous studies to analyze qualitative data (κ=.90). Additionally, we grouped codes into high-level categories as to whether the code conveyed (1) any misconceptions or (2) the icon was perceived as an actual control switch. We then ran logistic regressions on these coded expectations and Likert responses (converted into a binary variable) to scenarios. We treated the interaction term [**?**] between icon color and style as the key independent variable, and participant demographics as the control independent variables.[7] Detailed regression results are provided in Tables **??** and **??** of Appendix **??**. We did not apply corrections to p-values since we ran a small number (2) of regressions with preplanned hypotheses (i.e., *Stylized-Toggle* would perform better than *CalAG/CalAGX-Toggles*) [**?**].

5.5.2 Findings

We found that *Stylized-Toggle* better conveyed do-not-sell choices than the OAG's proposed opt-out icon and its variant with fewer toggle-related misconceptions. The icon's color (red or blue) did not significantly alter participant expectations in most cases.

***Stylized-Toggle* better created expectations of do-not-sell choices.** Figure 5.9 shows expectations of what would happen after clicking an icon. The most frequent expectation regarding *Stylized-Toggle* (29, 21.2%) was to be directed to a page with choices about the sale of personal information, a correct and desired interpretation according to the CCPA [113]. This expectation, however, was mentioned much less often in conditions involving *CalAG-Toggle* (16, 11.9%) and *CalAGX-Toggle* (10, 7.6%). The significant differences were confirmed by regressions on Likert responses to the do-not-sell choices scenario, in which participants who saw *Stylized-Toggle* were significantly more likely to expect "it will lead me to a page where I can choose whether or not the website can sell my personal information" compared to *CalAG-Toggle* (OR=.40, p<.001) and *CalAGX-Toggle* (OR=.41, p=.001).

***Stylized-Toggle* led to fewer toggle-related misconceptions.** Regressions on participants' categorized open-ended expectations revealed that *CalAG-Toggle* and *CalAGX-Toggle* were significantly more likely to generate misconceptions compared to *Stylized-Toggle* (OR=2.3, OR=2.4; both p=.003). Examples of these misconceptions include perceiving the toggle icon as an actual switch, expecting a negative outcome (e.g., more tracking), or believing that nothing would happen. Specifically, participants who saw *CalAG-Toggle* and *CalAGX-Toggle* were significantly more likely to perceive the toggle as an actual control switch compared to *Stylized-Toggle*

[7]Following statistical analysis guidelines [**?**], for any model in which the interaction effect between style and color was not significant, we compared its performance with another model without the interaction term (i.e., style and color was examined in isolation as main effects). If the "interaction model" provided a much better fit to the data than the "main effect only model," we report results from the first model; otherwise, we report results from the latter model.

(OR=2.4, p=.003; OR=2.4, p=.004). A participant quote that conveyed this misconception is "It would change between red and green depending on if I wanted to allow it."

As shown in Figure 5.9, the most frequent expectation in conditions involving *CalAG-Toggle* (38, 28.4%) and *CalAGX-Toggle* (30, 22.7%) was that the icon was an actual toggle switch currently set to "Do Not Sell My Personal Information" — clicking would give the website permission to sell the user's personal information, which is the opposite of the intended meaning. Users who have this notion might avoid clicking the icon or link text for fear of losing their privacy and thus lose the opportunity to exercise the do-not-sell opt-out. In contrast, only 10 (7.3%) participants who saw *Stylized-Toggle* mentioned this misconception.

Another misconception that occurred for all three icon styles (9, 6.6% for *Stylized-Toggle*; 8, 6.0% for *CalAG-Toggle* and 12, 9.1% for *CalAGX-Toggle*) was that the website is currently selling the user's personal information, and that clicking the toggle would stop it. Participants who held this misconception understood the icon's purpose but misinterpreted the icon's functionality — according to the CCPA [113], the icon should take users to respective settings but is unlikely to result in immediate changes. Regressions on the Likert responses for the respective scenario revealed interaction effects between toggle style and color; *Stylized-Toggle* in blue significantly decreased the likelihood of this misconception compared to *Stylized-Toggle* in red (OR=2.78, p=.006) and *CalAGX-Toggle* in blue (OR=2.75, p=.009). This misconception is not particularly problematic as it is less likely to discourage users from clicking. However, a privacy choice icon ideally should communicate both its intention and its function accurately.

5.6 Discussion

Our findings provide insights into the design and effectiveness of icons and link text in conveying privacy choices. Below we discuss our study's limitations and outline implications for design practice and privacy regulations.

5.6.1 Limitations

Our research has several limitations. First, we recruited all participants from Mechanical Turk, and they were more educated and tech-savvy than the U.S. general population. Nonetheless, prior work has shown that MTurkers are more demographically diverse than student samples [**?**] and that they offer similar responses to security and privacy surveys as traditional participant pools [**?**]. Second, our experiments focused on one application scenario (a fictitious online shoe retailer), which might have primed participants (e.g., to associate the dollar sign with payment and "sell" with shoe discounts). That noted, participants' responses for our best performing icons/link texts did not indicate that the website context affected their interpretations. Third, we measured the perception and comprehension of the icon/text by presenting them in a static screenshot; we did not measure whether participants would notice the icon/text on their own or how participants would interact with the provided choices as that was not the focus of this study.[8] Fourth, we did not investigate accessibility issues or evaluate the use of icons with screen

[8]We measured participants' attention to the icon/link text in another study for the OAG [**?**]. Specifically, we showed participants a website screenshot and asked them a question about a nearby link, then removed the

readers. Lastly, we did not directly compare our privacy choice icons with icons focusing on different privacy-related aspects (e.g., those that seek to visualize the concept of privacy itself or specific data practices [123]), which could be a contribution of future work.

5.6.2 Design Implications

Icons for privacy choices should be rooted in simple and familiar concepts. *Stylized-Toggle* was participants' favorite privacy choice icon in the pre-study, and performed best in conveying privacy choices when paired with "Privacy Options" in the icon-text combinations evaluation. *Stylized-Toggle* adopts a minimalistic design and conveys the notion of choice using a toggle — a familiar and common UI element representing the ability to make selections [**?**]. Nonetheless, the OAG icon evaluation shows the importance of an icon *taking inspirations from* rather than *copying* other familiar UI elements to convey the intended concept without creating confusion. Conversely, the icons that were comprehended poorly and thus excluded after the icon pre-study either attempted to convey a more abstract concept (e.g., the three icons that intended to convey ''opt out") or appeared too complicated as they combined multiple concepts (e.g., *ID-Card* and *Profile* combined elements representing "do not," "personal information," and "money/selling").

Our findings suggest that an icon for privacy choices should focus on a simple and familiar concept, like choice, instead of abstract or complex concepts. For the same reason, we hypothesize that a choice-focused icon would work better than an icon attempting to convey "privacy" in indicating privacy choices — future work is needed to validate this hypothesis, as we did not test privacy-focused icons. While prior work has proposed graphical representations of privacy — such as sunglasses, keyholes, locks, and cameras — users' mental models of privacy are diverse and nuanced [**?**]. Instead, we opted to highlight the notion of choice through the icon and use the word "privacy" in the accompanying text. As our findings show, this effectively clarified the type of choice the icon represents.

Icons should be accompanied by link texts. In line with prior work suggesting that icons and text information should appear in conjunction [**? ? ?**], our findings show that link text has a significant impact on the icon's comprehension. Participants who saw an icon without a link text exhibited more misconceptions. Even when participants correctly recognized the concept of choice, payment, or stopping, they often failed to connect those concepts to personal information without a text description. In our icon-text combinations evaluation, conditions without link text performed comparatively worse. These findings suggest the importance of placing a descriptive link text next to an icon to aid comprehension and reduce misconceptions. This does not undermine the merits of icons — they still complement and reinforce a text description with a visual depiction, which aids recognition [73], enables textual descriptions to be more concise [51], and conveys concepts across language barriers [123]. Any icon should come with a text description when first introduced, and once it has been broadly adopted, further testing is needed to evaluate whether the text description can be removed.

Usability issues of the AdChoices icon persist despite wide adoption. Even though thousands of companies have adopted the DAA's AdChoices icon [**?**], our participants struggled to

screenshot and asked them to describe any icon/link text they had noticed that would help them opt out of the sale of personal information. Less than half of the participants could accurately recall seeing the icon/link text for do-not-sell opt-outs.

recognize it or accurately interpret it. In the icon pre-study, only 14% of participants recalled seeing the icon before, and even fewer correctly associated it with advertising choices. This finding echoes prior work conducted nearly a decade ago [90, 139], and shows that comprehension of this icon has not improved much since then. Coloring the AdChoices icon in green — as done by DAA's Privacy Rights icon — did not improve comprehension either. Most participants thought of "more information" upon seeing the lowercase "i" and perceived the triangle shape as an audio/video play button. Icons have the potential to acquire a universal communicative power after being used over time even when their constitutive elements may not be intuitive, as demonstrated by the gear icon for settings [**?**] or the three arrow triangle for recycling [**?**]. However, our findings suggest that this is not the case for the two DAA icons, as our participants rarely associated them with privacy, do-not-sell, or other types of choices. Rather than adopting a problematic icon and expecting users will understand it over time, our findings demonstrate the importance of evaluating initial icon designs with user testing to ensure the icon is comprehensible.

Privacy choice indicators are only one component of usable privacy choices. Prior work has shown that users struggle to find privacy choices on websites [4, 61**?**]. Our research seeks to help users with this discovery problem. Our proposed icon-text combinations could serve as gateways leading users to website privacy choices, especially if a standard mechanism were to be adopted and used consistently. Nevertheless, privacy choice indicators alone are insufficient. Designing indicators to help users locate privacy choices is only the first step in improving end-to-end interactions with those choices. The indicators have to compete with many other UI elements for users' attention, and they still place the burden of accessing, learning, and exercising privacy choices on users [28**?** **?**]. Therefore, the interfaces users encounter after clicking on an icon/link text should be designed to minimize user effort. For instance, a web form for the CCPA do-not-sell opt-out could provide a conspicuous global "opt out" option on top, with more granular options presented below [108]. For a more substantial reduction in user burden, privacy choice indicators should be part of automated mechanisms [**?** **?** **?**], such as APIs that allow users to control privacy settings across websites in their web browsers, or personalized privacy assistants that learn users' privacy preferences and semi-automatically configure settings for them [**?** **?** **?** **?**].

5.6.3 Public Policy Implications

Incorporate user testing into the policy-making process. Researchers have argued that privacy interfaces should be developed through a user-centric and iterative design process involving user testing at early stages [127**?** **?**]. Unfortunately, most existing privacy laws either do not emphasize usability or include vague requirements for presenting privacy choices in UI design. For instance, the Federal Trade Commission (FTC) advocates that any privacy notice or choice must be "clear and prominently displayed" [**?**] but does not provide specific guidance on how to achieve this [**?** **?**]. In contrast, the widely adopted model privacy notice for US financial institutions was the product of an iterative design and testing process [**?**]. Another positive example is the guidance for GDPR compliance from the UK Information Commissioner's Office [**?**], which included visual examples to illustrate what constitutes valid consent [**?**]. The OAG's consideration of our research in the CCPA rule-making process further demonstrates that incorporating user-tested privacy interfaces into privacy laws is not only necessary but also fea-

sible. The OAG removed their proposed opt-out icon from the CCPA regulations [**?**] after we shared our findings with them about how their icon could generate critical misconceptions. Subsequently, the fourth set of modifications to the CCPA regulations recommended businesses use our blue stylized toggle icon to convey the presence of do-not-sell opt-outs [**?**].

Mandate unified privacy choices indicators. Even though the CCPA has an optional icon for conveying do-not-sell opt-outs [**?**], we consider it unrealistic and inefficient for privacy laws to require a specific icon or UI element for each privacy choice that businesses might offer, voluntarily or to comply with regulations. A web page with many different indicators is likely to confuse or overwhelm consumers [**?**]. Instead, mandating a standardized privacy choices indicator that direct users to all privacy choices in one place (e.g., a centralized privacy dashboard, account settings, or dedicated privacy choices page) would provide numerous benefits. For lawmakers, this approach is more economical compared to the significant time and resources required to develop, test, and oversee the enforcement of individual privacy choice indicators. Consumers would also appreciate a consistent and thus learnable path to navigate and exercise privacy choices [**?**]. Our research shows that *Stylized-Toggle* paired with the link text "Privacy Options" could be a good candidate for such a unified privacy choices indicator.

User-tested icons should be paired with public outreach and education. User testing can identify poor privacy choice indicators with comprehension issues, such as the DAA icons or the OAG proposed icon [**?**], that would require significantly more effort in consumer education. However, even for icons that have gone through rigorous testing, consumer education is still needed to raise awareness, communicate the icon's purpose, and dispel misconceptions. In our research, even the best-performing *Stylized-Toggle* icon generated misconceptions occasionally. We find little documentation on associated education or public outreach efforts for most existing privacy icons. While there have been education campaigns for the AdChoices icon in the US and Europe [**?** **?**], consumer awareness remains low, as we and others have found [139**?**]. Whether this is due to ineffective messaging or insufficient reach is unclear. We suggest that effective education campaigns for new privacy choice icons need to address the misconceptions uncovered in initial user testing, create an active and engaging learning experience [**?**], and possibly use personalized education content tailoring toward individual users' characteristics [**?** **?**].

5.7 Conclusion

We conducted a series of studies to design and evaluate icons and link texts for conveying the presence of general privacy choices and the CCPA-mandated opt-out for the sale of personal information. While most icons we tested were poorly interpreted without a link text, a stylized toggle icon effectively conveyed the notion of choice and performed the best in conveying privacy choices when paired with "Privacy Options." The two CCPA-mandated link texts ("Do Not Sell My Personal Information" and "Do Not Sell My Info") accurately communicated do-not-sell opt-outs combined with most icons. Our results provide implications for designers and policymakers by highlighting the importance of accompanying icons with text descriptions, using standardized visual indicators to help users locate privacy choice mechanisms, and incorporating user testing into policy-making processes.

Acknowledgements

We thank our study participants and graphic designers for their insights in generating and refining the icons, as well as the anonymous reviewers for their thoughtful feedback. This research was supported in part by a NortonLifeLock Graduate Fellowship, the Carnegie Corporation of New York, Innovators Network Foundation, grants from DARPA and AFRL under the Brandeis program (FA8750-15-2-0277), and grants from the National Science Foundation (NSF) Secure and Trustworthy Computing program (CNS-1330596, CNS-1801316, CNS-1914486). The US Government is authorized to reproduce and distribute reprints for governmental purposes not withstanding any copyright notice thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as representing the official policies or endorsements, either expressed or implied, of DARPA, AFRL, NSF, or the US Government. We wish to dedicate this paper to our co-author, Prof. Joel Reidenberg, who sadly passed away in 2020.

Name	Icon	Common Interpretations (# of Participants)
Stylized-Toggle		**accept/decline** (4); **activate/deactivate** (2); true/false (2); mark as completed (1)
Changed-Choice		okay/exit options (1); **accept/decline** (1); true/false (1); opposite is true (1); no guesses (2)
DoNot-Checked		**activate/deactivate** (2); mark as completed (2); completed downloads (2); **accept/decline** (1)
Box-Arrow		**removing something** (2); okay/exit options (2); email or message (1); no guesses (1)
Circle-Arrow		move forward/go (3); email or message (1); no guesses (2)
Folder-Arrow		folder/file (4); email or message (3)
DoNot-Dollar		cancel payment (2); losing money (2); low balance (2); money/paying (2); cash/dollars not accepted (1); something is free or requires no money (1)
Slash-Dollar		cash/dollars not accepted (4); something is free or requires no money (3); money/paying (1)
Stop-Dollar		money/paying (4); account balance (2); something costs money (2); something is free or requires no money (1); cash/dollars not accepted (1)
ID-Card		payment method (4); **something related to a person and money** (3); something costs money (2); account balance (1); no guesses (1)
Profile		money/paying (2); stop spending money (2); something costs money (2);
DAA		more information (3); move forward/go (2); play button (2)

Table 5.2: Participants' coded open-ended responses to "What does this symbol communicate to you?" from conditions in which the icon was shown without a link text in the icon preliminary testing, along with a code's number of occurrences. Interpretations that align with the icon's intended meaning are bolded.

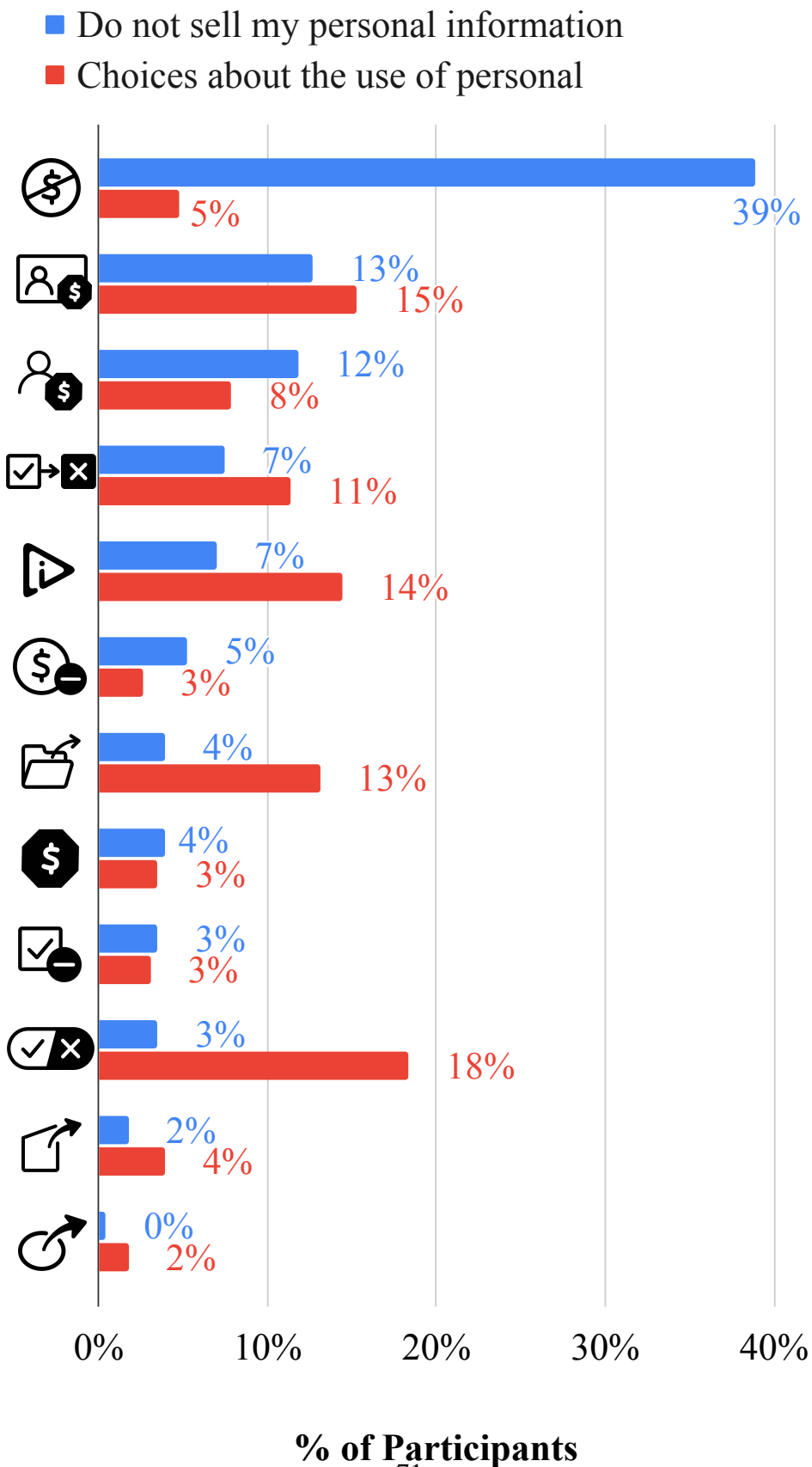


Figure 5.2: Preliminary testing participants' selections for an icon that best conveys there's an option to (1) "tell websites 'do not sell my personal information"' (blue); and (2) "make choices about the use of my personal information" (red).

Figure 5.3: Promising icons from preliminary testing in their refined versions.

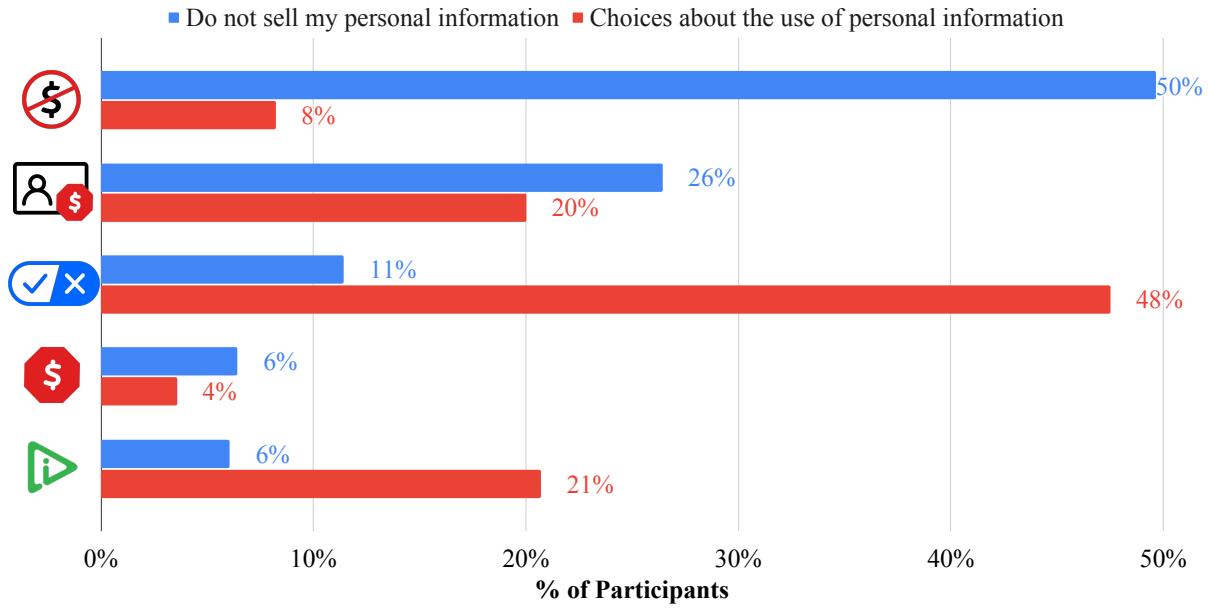


Figure 5.4: Refined testing participants' selections for an icon that best conveys that there's an option to "tell websites 'do not sell my personal information"' (blue); and "make choices about the use of my personal information" (red).

Name	Icon	Common Interpretations (# of Participants)
ID-Card		something costs money (9); sending money to someone (5); money/paying (5); **something related to a person and money** (3); account balance (3) ; price related (2) ; payment methods accepted by website (2)
Slash-Dollar		something is free or requires no money (12); cash/dollars not accepted (6); money/paying (4); **selling is not allowed** (1)
Stop-Dollar		money/paying (10); stop spending money (5); something costs money (4); price related (3); sale/discount (3); no guesses (3)
Stylized-Toggle		**accept/decline something** (11); **activate/deactivate something** (4); true/false (4); okay/exit options (3)
DAA		more information (11); play button (7); move forward/go (3); ad related (2)

Table 5.3: Participants' coded open-ended responses to "What does this symbol communicate to you?" from conditions in which we showed the icon without a link text in the refined icons study, along with a code's number of occurrences. Interpretations that align with the icon's intended meaning are bolded.

- Do Not Sell My Personal Information
- Do Not Sell My Info
- Don't Sell My Info
- Do Not Sell[b]
- Don't Sell[†]
- Do-Not-Sell Choices[†]
- Do-Not-Sell Options
- Do-Not-Sell Opt-Outs[†]
- Privacy Options
- Privacy Opt-Outs
- Privacy Choices
- Personal Info Choices
- Personal Info Options
- Personal Info Opt-Outs
- Do Not Sell My Info Choices[h]
- Do Not Sell My Info Options[††]

[b]Preliminary link text testing only
[h]Refined link text testing only

Table 5.4: Link texts tested in the link text pre-study.

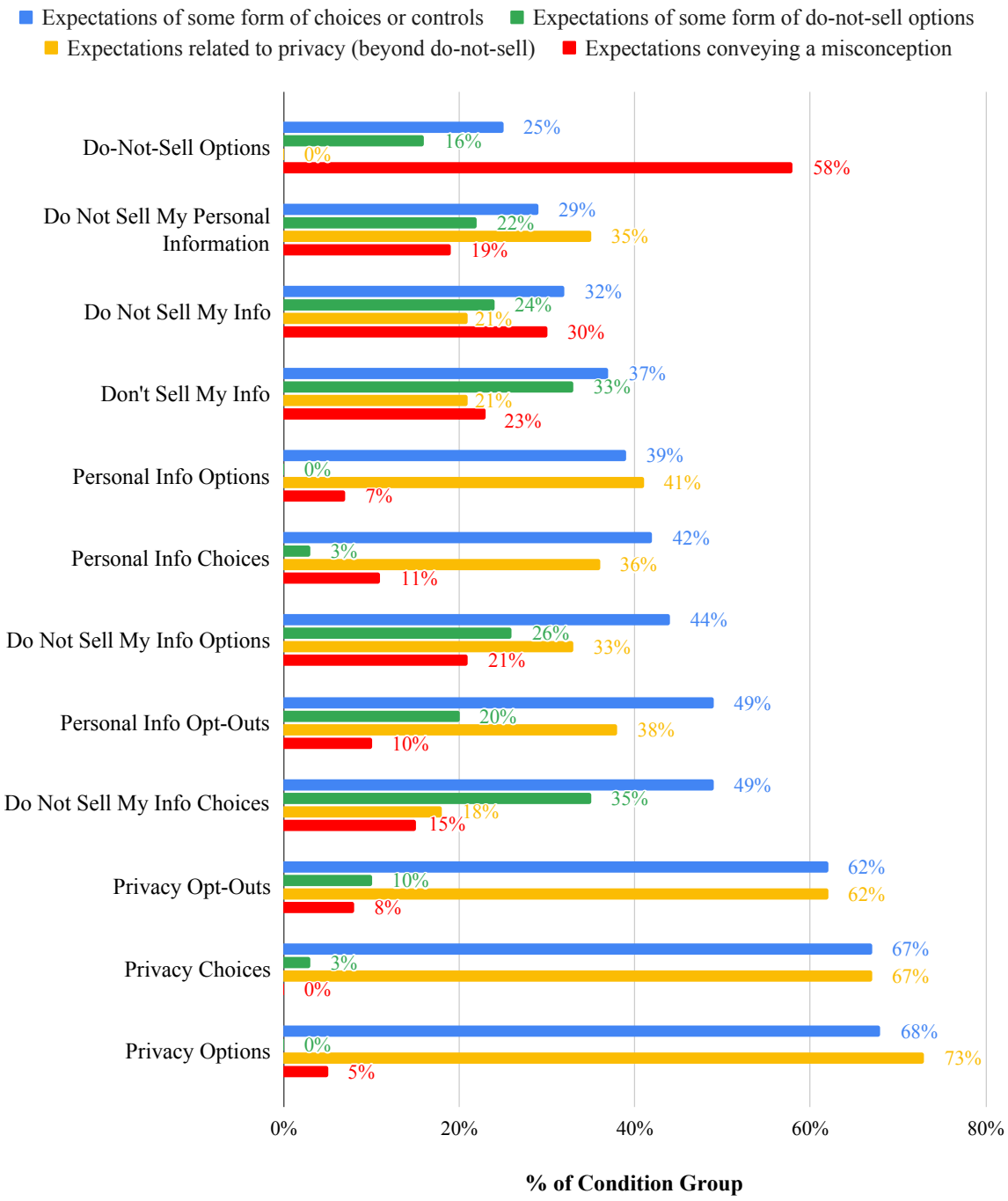


Figure 5.5: Distribution of expectations in response to “What do you think would happen if you clicked on this [link]?” in our link text pre-study.

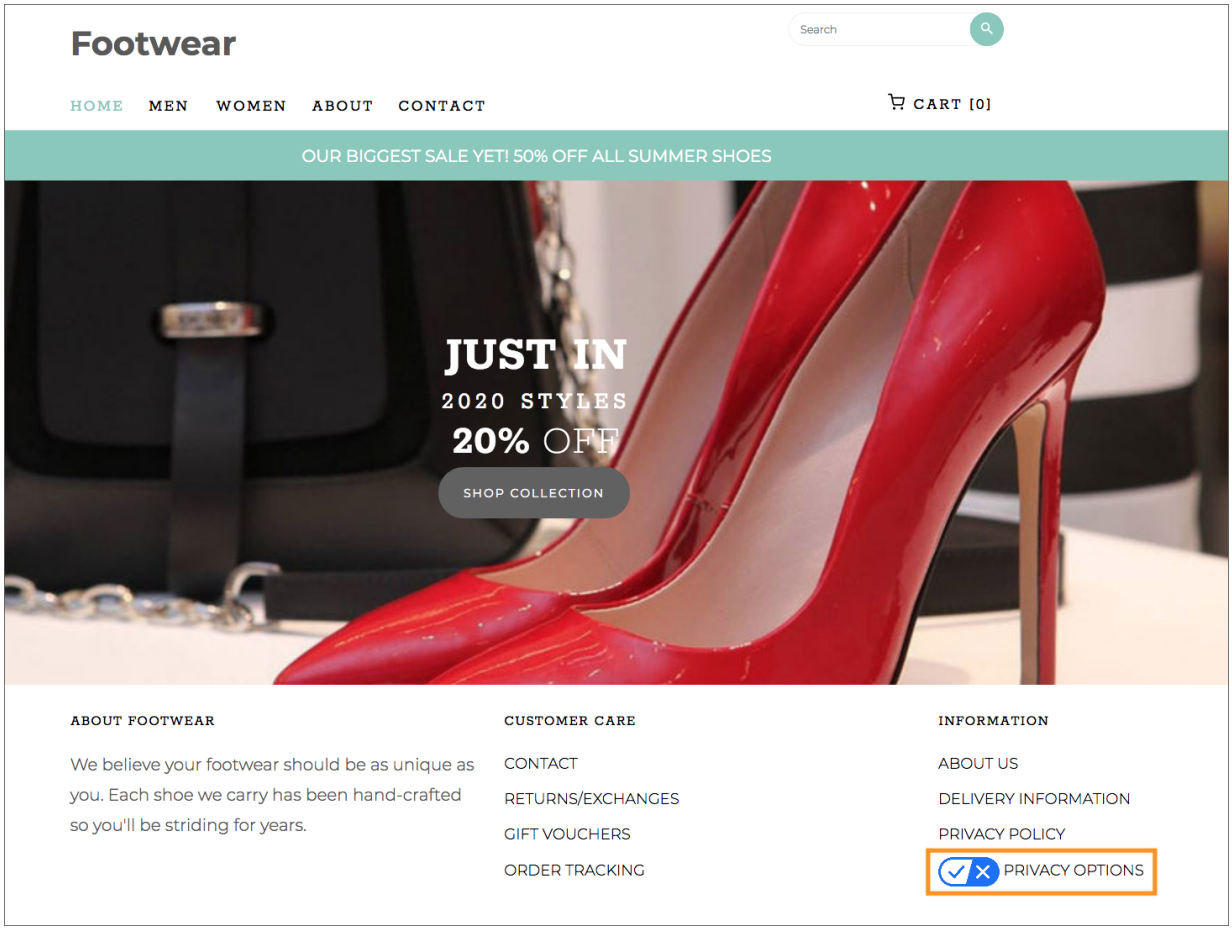
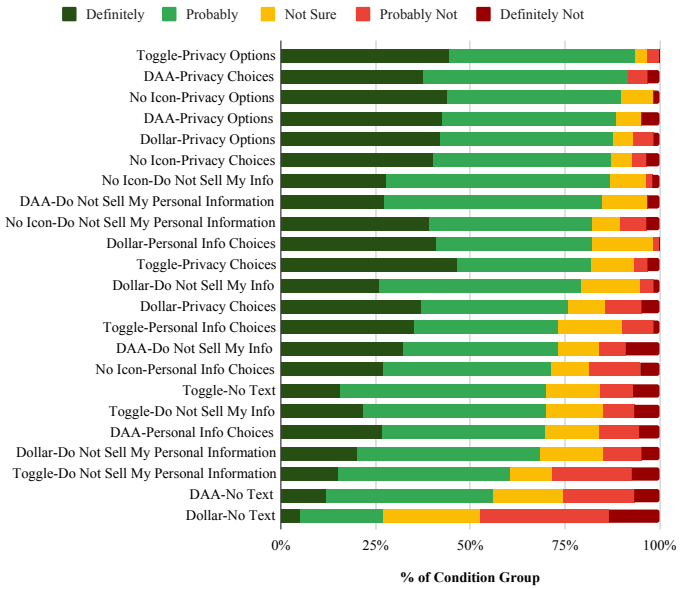
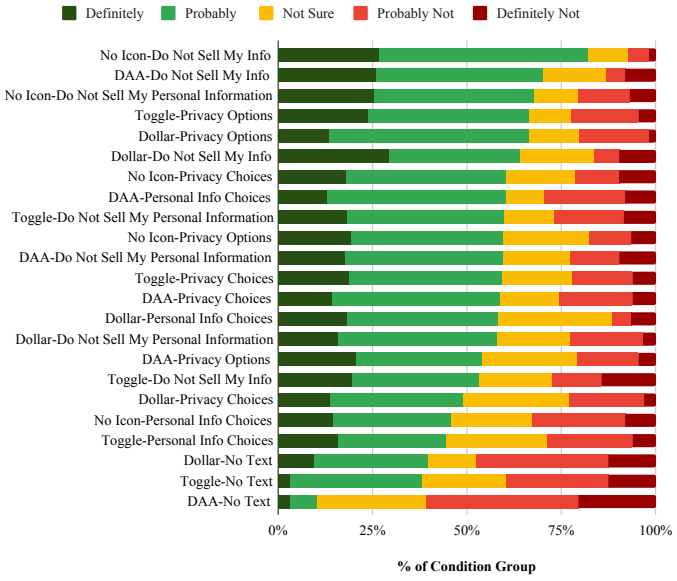


Figure 5.6: Icon and link text presented on a fictitious online shoe retailer webpage used in the icon-text combination evaluation. The icon and link text were highlighted with an orange rectangle to attract participants' attention. Shown is the condition combining *Stylized-Toggle* (icon) and "Privacy Options" (link text).



(a) "It [the symbol/phrase] will take me to a page with choices about how my personal information is used and shared by the website."



(b) "It [the symbol/phrase] will take me to a page with choices about the sale of my personal information."

Figure 5.7: Distribution of Likert responses across conditions in icon-text combinations evaluation.

Figure 5.8: Our stylized toggle, OAG's proposed opt-out button, its variant, and the iOS switch button.

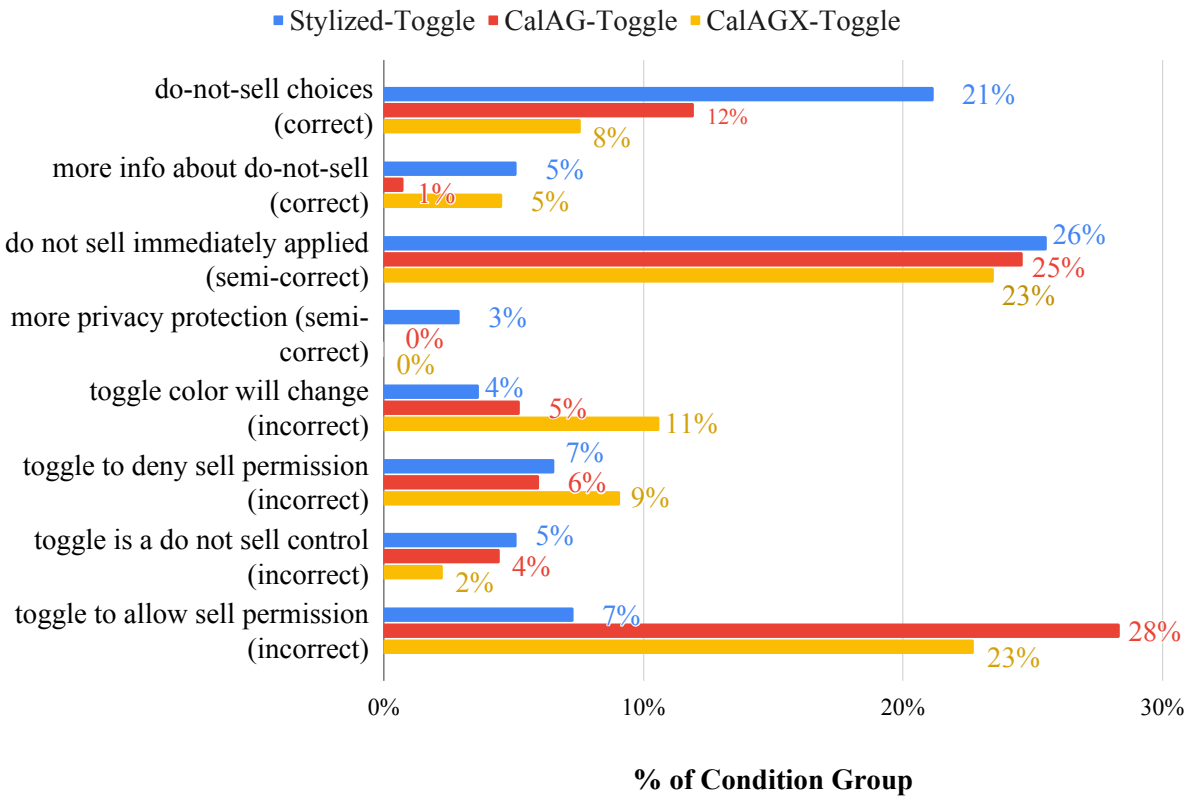


Figure 5.9: Common expectations of what would happen after clicking based on open-ended responses in conditions with *Stylized-Toggle* (n=137), *CalAG-Toggle* (n=134) and *CalAGX-Toggle* (n=132).

Chapter 6

Identifying User Needs for Advertising Controls on Facebook

The research previously presented in Chapters 3 and 4 primarily focused on consumers' ability to find, comprehend, and use different types of privacy choice mechanisms. Chapter 5 presented a potential solution for more effectively communicating the availability of privacy choice mechanisms. The research described in this chapter focuses on another aspect of usability: whether privacy choice mechanisms actually align with user needs. This is studied in the context of controls for online behavioral advertising (OBA) available on Facebook

OBA, an integral part of how many free online services operate, generates over $100 billion of revenue each year, primarily profiting major tech companies, such as Google and Facebook, that serve targeted ads [**?**]. Facebook allows advertisers to target ads to users based on rich behavioral data including demographics, location data, interests, similarities to other groups of individuals, activities on Facebook such as clicking ads or interacting with business pages, and activity on other websites or apps [**? ?**]. These practices may help advertisers reach interested audiences, and allow consumers to use services without a fee while potentially receiving more relevant ads. However, many argue that OBA can cause privacy harm to users [**? ? ?**]. Prior work has found that while consumers have some understanding of the data collected about them, they do not have a complete understanding of companies' advertising practices and sometimes find them creepy [119**? ?**]. Furthermore, users may not be sufficiently equipped to make informed decisions about the use of their data for OBA [2].

Facebook has considerably expanded its user privacy settings over the past several years, and now offers numerous controls related to users' advertising experience. Previous work has examined Facebook's privacy settings, primarily in the context of whether they address user needs for privacy from other Facebook users [**? ?**]. What is missing is an understanding of user needs related to Facebook's data collection and advertising practices. This chapter fills this gap through a survey and remote usability study exploring what Facebook users want to control about their advertising experience, and specific concerns that shape their needs related to advertising

This chapter is a lightly edited version of a paper in submission as: 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 Conference on Computer-Supported Cooperative Work and Social Computing (CSCW). ACM, 2021[63].

controls. Additionally, this study contributes a better understanding of the usability barriers presented by current implementations of such controls on Facebook. Our results highlight how different design choices can impact the usability of advertising controls, providing insights for platforms beyond Facebook.

Our survey identified some Facebook advertising controls that participants were already using for both privacy-related as well as user experience reasons, and others that participants had not yet discovered but seemed likely to address their needs. Participants in our remote usability study struggled to find and navigate available advertising controls, but controls directly accessible from an advertisement were perceived to be more usable. Furthermore, while participants exhibited a reasonable comprehension of granular controls related to specific ads, advertisers, or personal information used in targeting, they struggled to understand controls related to the use of list-based audiences and data aggregation from third-parties. We also found that participants had differing needs and priorities related to advertising controls, which could be categorized into four groups according to their sentiments toward targeted advertising and concerns related to data collection.

This chapter makes the following contributions:

- Demonstration of where Facebook's ad controls fall short in terms of usability and where they seem to meet user needs.
- A set of functional requirements to address a wide range of user objectives related to targeted advertising, spanning from a desire for less data collection to a desire for ads that are even more relevant to their interests.
- Discussion of how the usability findings and functional requirements may be helpful for improving the usability of ad controls on other platforms beyond Facebook.

6.1 Online Survey

We conducted an online survey to gain preliminary insights into users' strategies for controlling their advertising experience as well user needs that are unmet by existing controls. Our findings suggest that Facebook users have different goals related to the ads they see on the platform, including some that are already addressed by current controls. However, there seems to be a lack of awareness of these controls, suggesting issues of discoverability. These results helped inform the design of our remote usability study tasks.

6.1.1 Survey Methods

We ran our survey on two crowdsourcing platforms. Prior to the survey, participants completed a consent form approved by our IRB.

Survey Design

Participants answered up to 28 multiple-choice and open-ended survey questions. To capture background information related to participants' Facebook experience, we first asked multiple-choice questions regarding frequency of Facebook usage, frequency of encountering Facebook ads, and device preference when using Facebook. We then asked open-ended, multiple choice,

and Likert-scale questions to learn more about participants' sentiments toward the ads they see on Facebook, drawn from prior work [**?**]. To capture information about the use of specific types of ad controls, the survey then presented opportunities to describe any past experience attempting to control the amount or topics of ads they saw on Facebook, which advertisers were able to show them ads on Facebook, and/or which information was used to target them with ads on Facebook. To further probe participants' past experiences with Facebook's ad controls, we next asked participants to recall whether they had ever seen an ad on Facebook they did not want to see, and if so, what (if anything) they did about it. Similarly, participants were then shown screenshots of the desktop and mobile versions of Facebook's Ad Preferences (as it appeared in June 2020) and were asked to recall any past experience with it: whether they had ever changed their settings using that page, and if they had, what settings they changed and why. To better understand user objectives related to advertising that may not have been captured by the previous questions, we asked another open-ended question: "Are there any aspects of advertising on Facebook that you would like to control or change but haven't yet been able to? If so, please describe." Additionally, to learn more about the use of other types of ad control strategies participants were asked to select which, if any, strategies or software they currently use to control ads on the device they use the most. Last, participants answered demographic questions about their age, gender, and race or ethnic identity. The full survey is presented in Appendix **??**.

Survey Analysis

We used thematic analysis to categorize the free responses. Two researchers worked collaboratively to build the codebook, using affinity diagramming to create categories for questions about users' attitudes and reasons for their behaviors. The data was coded by one of the two researchers. To ensure consistency, the two coders reviewed each other's work. We also performed an additional round of higher-level coding that incorporated responses to multiple questions to generate two lists: one of goals users had described related to controlling ads and another of Facebook advertising controls that each user had mentioned using at any point in the survey. We primarily report on this higher-level coding as this most directly impacted the remote usability study.

6.1.2 Recruitment & Demographics

Participants were recruited from Amazon Mechanical Turk (MTurk) and Prolific in July 2020. We required participants to be at least 18 years old, live in the United States, and speak English. MTurk participants were required to have least a 97% approval rating and 50 previously approved HITs. MTurkers completed a short screening survey and then were invited to complete our main survey if they reported using Facebook within the past year. Participants from Prolific were filtered for Facebook use using Prolific's pre-screening tool.

We collected 29 MTurk responses and 150 Prolific responses.[1] Survey responses were evaluated holistically for quality based on reCAPTCHA scores, Qualtrics bot flagging, completion

[1]We began survey recruitment on both platforms, but due to low MTurk data quality completed recruitment on Prolific.

time (at least one minute spent), and manual review of free responses to determine whethey they were intelligible. One Prolific response was discarded because the participant reported no Facebook use in the past year in our survey's frequency-of-use question. From MTurk, we recruited 48 participants to take the screening survey, 29 of whom met eligibility requirements and completed the main survey. Of those 29 responses, one was discarded because the same MTurker completed the task twice due to a technical error, and four were discarded due to extremely low-quality free response answers (e.g., blocks of text copied and pasted from Wikipedia). In total, we used data from 173 participants, 149 from Prolific and 24 from MTurk.

Most participants completed the survey in under 10 minutes. Respondents were compensated $2.00 for their participation (equivalent to about $12.00/hr). Among participants, 52.0% identified as men, 45.7% as women, and 2.3% non-binary or agender. Our sample was 71.3% white. Participants' age ranged from 18 to 76 with a median age of 31. 63.6% of our participants reported being daily Facebook users, 32.4% reported using Facebook less than every day but more than once a week, and 4.0% used Facebook less than once a week but more than once a month. The vast majority of participants performed at least some of their Facebook use on mobile devices. 61.8% used it on both phones and laptop or desktop computers, 32.4% only on phones, and 5.8% only on computers. Among these 163 Facebook mobile users, 56.4% used Android phones, 44.2% used iPhones, and 16.0% used iPads or other tablets. 63.4% reported that they normally used the Facebook app rather than visiting the Facebook website through their mobile browser.

6.1.3 Survey Results

We present survey results related to participants' goals and previous experiences in using Facebook's ad controls. Participants described a variety of desired ad controls, many of which are already provided by Facebook. We observed that the objectives described by participants reflected both privacy and user experience-related motivations. However, low engagement with these controls suggest an issue of discoverability, particularly for controls in the Ad Preferences page.

User Goals Related to Ad Controls

Participants described a variety of goals related to their Facebook advertising experience. While many are already addressed by existing controls, other goals articulated by participants are not currently implemented by Facebook features and were perceived to require a dramatic shift in Facebook's revenue model (marked with a $*$).

Limiting Collection/Use of Third-Party Data. Of the goals that can be addressed by existing controls, controls related to data collected from third-party websites and apps were mentioned most frequently. In response to the question of what they would like to change about advertising on Facebook, one participant wanted Facebook to "...stop tracking me when I use other sites that aren't even Facebook." The collection and use of some types of third-party data can be controlled through the Off-Facebook Activity and Data from Partners controls, respectively.

Adjusting Ad Relevance. Another frequently mentioned type of desired control pertained to the relevance of ads. Specifically, participants described wanting control over the topics used for ad targeting to make ads more relevant to them. In explaining their past use of the Interest Categories menu within Ad Preferences, one participant wrote, "I didn't really care for beauty salons and I prefer my ads to be tailored to me."

Blocking Ads or Advertisers. Participants also commonly described wanting controls to block specific ads or advertisers that they found annoying or repetitive, both of which are available through an ad's contextual menu. As one participant described, "I get a lot of repeats for the same written advertisement with different pictures and I want to get rid of it. "

Other Goals Met by Existing Controls. Some participants desired greater transparency about what data Facebook has about them and how ads are funded and targeted to users, which may be at least partially addressed by the data access tool and "Why am I seeing this ad?" feature. A few wanted to control the quantity or type of political ads that they were shown. A control for this (Ad Topics: Social Issues, Elections or Politics within Ad Preferences) became available to U.S.-based users in June 2020 just prior to us running this survey [**?** **?**]. Additionally, a couple of participants wanted to control visibility of social actions such as liking or commenting on ads, which can be done with "Ads that include your social actions" within Ad Preferences.

∗**Limiting the Number of Ads.** The most common goal related to their Facebook advertising experience participants mentioned was reducing the number of ads they encountered or removing ads from the platform altogether. Some mentioned being willing to pay to use Facebook if it meant an ad-free experience. However, many participants recognized that this type of control was unlikely given their (sometimes incorrect) perception of Facebook's business model. One participant stated, "I would prefer if there were no ads whatsoever on Facebook, but I am aware that they bank on selling our information to third parties who then display personalized ads on our pages."

∗**Limiting Facebook Tracking and Targeting.** Participants also expressed general privacy concerns about tracking and ad targeting that suggested interest in broader controls to disable these practices. Similar to participants who desired reducing the number ads they experience on the platform, participants recognized that Facebook's tracking and ad targeting is what generates revenue for the platform. Some also mentioned being willing to pay for the service if it led to greater control over the collection and use of their data.

∗**Moderating Ads.** In describing desired controls or changes to their advertising experience, many participants mentioned concerns about clickbait, scams, and disinformation in ads. Though Facebook does allow users to report individual ads for these reasons and has a review process for ads [**?**], participants expressed that Facebook should play a larger role in ad moderation and quality control. As one participant articulated, "I wish the Facebook would act more like a old school publisher and establish standards and practices and not publish content (ads or other content) that does not conform to those standards."

Previous Engagement with Ad Controls

Despite participants' concerns and desired changes related to their advertising experience, relatively few had reported using Facebook's advertising controls even when coming across an unwanted ad. However, non-Facebook strategies for controlling online ads appeared to be widely used in our sample.

Reactions to Unwanted Facebook Ads When prompted about their prior experiences with Facebook ads, 49 participants (28.3%) recalled seeing an ad on Facebook in the past month that they did not want to see. Fifteen of those participants said they did nothing about it, or simply scrolled past it. Of the 21 respondents who said they did take action about an unwanted ad, a majority (18 participants) used the contextual menu directly on the ad itself to hide or report the ad or advertiser. Only one participant went to the Ad Preferences interface and adjusted their Interest Categories in response to a specific unwanted ad. Two other participants took actions outside of Facebook in response to unwanted ads, such as using the "adaware button" or starting to use private browsing mode, and one of the participants who hid the ad from the contextual menu also "disable[d] cookies on websites I visit." The remaining thirteen did not clearly articulate what they did, and just described what they did not like about the ad.

The Ad Preferences Page Only 33 participants (19.0%) reported having used the Ad Preferences page before, which suggests possible discoverability problems with this page. About half (16) did not clearly state what type of change they made, but among those who recalled what they did, most changed settings limiting the use of third party data or relating to interests. While 19 participants reported a desire to control the collection or use of third-party app data, only four recalled having used the Data from Partners setting. In addition, while 16 participants reported a desire to manipulate ad topics or interests, only nine participants had removed Interest Categories from their profile via Ad Preferences. We also asked participants about their motivation for visiting Ad Preferences. Some gave responses that corresponded to their general attitudes toward Facebook ads, such as finding ads annoying, irrelevant, or creepy. Several also noted that they visited Ad Preferences because someone they knew suggested it, and one said that they visited Ad Preferences due to a prompt that appeared when they were hiding an ad using contextual controls.

Contextual Menu Controls Participants who reported a desire to control specific ads or advertisers appeared to be relatively successful in finding these controls within an ad's contextual menu. Of the 28 participants who mentioned wanting to hide a specific ad at some point in the survey, 22 had reported using the contextual Hide Ad control. Nine participants also reported using contextual Report Ad controls. Similarly, six of nine participants who wanted to hide ads from an advertiser reported using this option within an ad's contextual menu.

Other Ad Controls While reported usage of Facebook ad controls was overall low, the majority of participants did take actions to control ads on the internet in general. 69.9% of participants

reported taking some step, such as using an ad blocker, private browsing mode, or antivirus software, to try to control online advertising on their devices.

6.2 Remote Usability Study

Based on results from our survey, we designed a remote usability study to further explore user needs for and the usability of Facebook's advertising controls.

6.2.1 Remote Usability Study Design

We used our survey findings to identify study tasks. Sessions were held remotely and participants used their own Facebook accounts. We analyzed the empirical and qualitative data on how participants performed tasks and viewed the ad controls they encountered.

Study Tasks Selection

To facilitate and anchor an in-depth discussion about the usability and usefulness of 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. No controls appeared to map to the fourth area (relatively high reported usage and low reported desirability).

The controls we included in our study tasks are listed in Table 6.1. The *Hide Ad* control had both a relatively high desirability and reported usage, and is available through a contextual menu on an advertisement. The *Manage Future Activity* and *Data About Your Activity from Partners* controls both address concerns reported in the survey about data from outside of Facebook being used to target ads but did not appear to be frequently used. The *List Usage* controls, which determine whether a particular advertising list containing information shared from third parties can be used to both show and exclude users from seeing particular ads, appear to be controls that were neither frequently used nor address a frequently reported concern. However, prior work suggests that the use of advertising lists in online advertising is not well-known and causes user concern, thus settings to control advertising lists may be of interest to users [145]. In addition to tasks involving these four controls, we also included a task to more directly measure the discoverability of the Ad Preferences page.

Study Session Components

Each session consisted of a semi-structured interview portion followed by tasks conducted on the participant's device. Sessions were recorded and transcribed using Zoom's cloud recording

Control	Description	Location	Reported Desirability	Reported Usage
Hide Ad	"Never see this specific ad again"	Contextual	High	High
Data from Partners	"Personalized ads based on your activity on other websites, apps or offline"	Ad Preferences	High	Low
Manage FutureActivity	"Choose whether your off-Facebook activity is saved with your account"	Your Facebook Information	High	Low
List Usage	"You can choose whether lists [company name] uploaded can be used to show you/exclude you from seeing ads."	Ad Preferences	Low	Low

Table 6.1: Facebook controls used in study tasks, how they are described by Facebook, where they are located on the platform, and survey participants' reported level of desirability and usage.

features, and were attended by at least two members of the team. After the completion of each task, we asked questions about their experience.

Pre-task Questions We began the session with questions about participants' perceptions of Facebook advertising. First, we asked participants what information they thought Facebook collects about them, whether Facebook has access to their interaction with other websites or apps, along with how this sharing works, and what Facebook might do with this information. Next, we asked about the ads participants see on Facebook, including how relevant they are to their interests, how repetitive ads seem, the overall amount of advertising, and how ads on Facebook compare to the ads they see on other services. We further explored participants' perceptions of how personalized ads occur by asking them to recall a targeted ad on Facebook. To learn more about participants' previous behaviors related to Facebook advertising, we asked them to recall a recent time they saw an ad on Facebook that they did not want to see and followed up with questions about why they did not want to see the unwanted ad and if they took actions in response. We further asked if they had tried changing settings related to advertising on Facebook, their awareness of advertising lists or audience-aware advertising on Facebook, and if there are any aspects of advertising on Facebook that they would like to control but have not yet been able to.

Study Tasks Participants were assigned to one of two groups of study tasks using balanced assignment to ensure device diversity for each task group. Tasks were grouped to mitigate learning effects and ensure consistent session durations. Due to the remote nature of the study, participants used their own Facebook accounts and were asked to share their screens over Zoom to

enable richer discussions of their interactions while completing the study tasks. Each task was described as a scenario and participants were encouraged to think aloud while completing the tasks. Participants were given a hint if they indicated they were not sure what to do next in their task.

Group 1 (Hide Ad, Ad Preferences Discoverability, List Usage): For the *Hide Ad* task involving the Hide Ad control in the contextual menu, we first asked participants to scroll through their News Feed to locate an ad. We then described the scenario as: "Imagine that you do not like this ad and do not want to see this specific ad in the future. How do you think you could remove the ad from your News Feed right now?" For the *Ad Preferences Discoverability* task, participants were prompted: "Could you show us what you would try to do if you were looking to change your Facebook settings related to advertising?" For the *List Usage* scenario, we had participants review the information on the Audience-based advertising page within Ad Preferences and then asked: "What would you do to manage how a particular company could use an advertising list on Facebook?"

Group 2 (Hotel Deals): For the *Hotel Deals* task, we described the scenario as: "Imagine you went to a few travel websites, and you don't like that the ads you're now seeing on Facebook are all related to hotel deals. How would you stop this from happening in the future with your other browsing activity?" To complete this task, participants needed to utilize either the Data from Partners or Manage Future Activity controls, as both controls relate to the use of data about off-Facebook activities for advertising.

Task Follow-up We followed up each task with questions about the usability of the control. We also asked participants about their understanding of how the control would impact the ads they see both on and off Facebook. To learn more about the utility of these controls, we also asked whether the control was something they would like to use, and about their past experiences with the scenario. We also asked similar questions about other controls in the menu (i.e., Report Ad and Why Am I Seeing This Ad? in the contextual menu and Clear Off-Facebook History in the Off-Facebook History settings page). Participants who were assigned to the Hotel Deals task were directed to the other control related to the scenario (i.e., to the Manage Future Activity control if they initially found the Data from Partners control and vice versa). They were then asked to summarize both controls and describe their similarities and differences.

After completing their group-assigned study tasks, participants were directed to Ad Preferences and given time to explore the available advertising controls. We then asked about the usability and their past experience with this page and other ad controls that they might have changed on Facebook in the past. We also asked participants which study tasks they found easier, and why. Lastly, we inquired as to what participants would want a Facebook "magic button" to do related to advertising, as well as what other controls regarding their personal data that they wished Facebook offered.

Data Analysis

We analyzed the empirical and qualitative data captured in the study session transcripts (corrected by the research team), researcher notes taken during the session, and screen recordings of the session tasks. We developed an analysis template that allowed us to systematically record

empirical metrics about the study tasks such as the pages the participants visited while finding the control, whether and how long participants took to find the control, whether they required a hint to complete the task, and if they navigated away from the control related to study task. To ensure consistency in the data analysis, two researchers independently completed the template for five of the 25 study sessions. Though we observed low disagreement (¡10% of analyzed metrics) in the analysis, all disagreements were discussed and reconciled. The remaining participant sessions were reviewed by one researcher.

We also conducted a thematic analysis of the qualitative data. One researcher developed an initial codebook after the first stage of interview recruitment. We iterated on our codebook as we completed and coded additional interviews until we observed no additional meaningful codes being added. Members of the study team involved in coding jointly coded one session to ensure a shared understanding of the codebook. The remaining sessions were distributed among the research team and coded by one researcher. Researchers conferred with each other throughout coding to ensure consistency and updated previously coded data. Last, one researcher conducted affinity diagramming of the thematic coding, grouping participants with similar viewpoints. A second researcher verified these groupings.

Research Ethics

The study protocol was approved by the IRB at our institution. Prior to scheduling a study session, participants completed a consent form that described the study procedure, including that participants would use their own Facebook accounts and that sessions would be recorded. These aspects of the consent form were also reviewed with participants at the beginning of the study session. Participants were told that turning their camera on was optional, but that their video would appear in the recording if enabled. We also notified participants that we could edit the recording to remove anything that they were uncomfortable with us storing long-term.

Given the virtual nature of the interview and use of participants' personal Facebook accounts, we also included measures in our protocol to minimize collection of personal information that was unnecessary for our study goals, especially from non-consenting individuals. In the screening survey used in recruitment for our remote usability study, we only collected contact email addresses from eligible participants. At the beginning of the sessions, we confirmed that participants were in a quiet and private location. We also informed participants that we could pause the recording if needed, such as if someone appeared in the background. Participants joining the session from their mobile device were encouraged to enable "Do Not Disturb" mode so that notification previews would not be recorded. Those using a laptop or desktop computer were encouraged to share only the browser window with Facebook through Zoom, rather than their entire desktop. Additionally, if a password prompt appeared during the session, participants were asked to pause their screen share; if they had difficulty doing so, the interviewer paused the session recording. After completing our analysis, we used the blur tool in Adobe Premiere Pro to obscure participants' personal information as well as any information about the participants' friends from the screen recordings, and edited this information from the audio.

6.2.2 Recruitment and Demographics

Prior to recruiting participants, we conducted four pilot study sessions to refine our study protocol and determine study length and compensation.

Participants were recruited through Craigslist postings advertising a 60-90 minute virtual study about Facebook settings, compensated with a $25 Amazon gift card. We recruited participants from four cities in the mid-West and mid-Atlantic regions of the US. Potential participants completed a screening survey (provided in Appendix **??**) that asked about their Facebook usage and perceptions, technical knowledge and skill, and demographics. To be eligible for the study, participants were required to be Facebook users over the age of 18, located in the US, and fluent in English. We conducted purposive sampling, balancing our sample for device type, age, race, technical education, and perceptions of Facebook advertising. To capture perspectives of those who are most likely to struggle with advertising controls, we also prioritized recruitment of individuals who were over 65 or demonstrated low technical knowledge or skill. We conducted recruitment in three stages, after which we observed saturation in the data.

In total, we conducted study sessions with 25 participants between October 2020 and January 2021. Twelve participants were assigned Group 1 tasks and 13 were assigned Group 2 tasks.[2] Given our sample size and purposive sampling criteria, we aimed for demographic diversity rather than a representative sample. Eleven participants identified as male and 14 as female. Participants ranged in age from 21 to 66 years old, with a mean age of 37. Eighteen participants identified their race as white, four as black or African American, and three as Asian. Our participants reported a mixed background related to technical knowledge and skill. Seventeen participants reported not having a a formal education in a computer-related field, such as computer science or IT. While 24 participants correctly identified the definition of a cookie (in the context of the Internet) on the screening survey, five participants reported that they would ask for help if they did not know how to do something on their phone or computer. Our participants were fairly active Facebook users, with all participants reporting using the platform at least once a week and 22 reporting using it every day. Fifteen participants conducted the task portion of the study session from their desktop or laptop computer, five used an Android device, and five used an iPhone or iPad. The median length of study sessions was 61 minutes (min: 38 minutes, max: 117 minutes).

6.2.3 Remote Usability Study Results

While participants exhibited some understanding of Facebook's advertising practices, they did not fully understand the mechanisms enabling data sharing and 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. Throughout the session, participants described various objectives related to the ads they see on Facebook, which we observed were related to their overall opinions about Facebook ads, and could be categorized into four groups.

[2]Three participants in Group 1 were not able to complete the List Usage task due to technical difficulties with Facebook.

Perceptions & Behaviors

Understanding of Facebook advertising When describing their previous experiences with Facebook ads, participants discussed receiving ads based on activities they performed on Facebook, as well as outside of Facebook. Participants in our sample were generally aware that Facebook had access to data about users' activities on websites and apps that are not affiliated with Facebook, in addition to user activities on the platform or other Facebook-owned services. When describing how data collection from third-parties occurred, participants believed that apps or companies could directly share user data with Facebook as well as through Facebook tracking technologies collecting data from these other websites or apps. While this suggests some awareness of Facebook's capabilities to collect data from third parties, participants had difficulty describing the exact data sharing practices or mechanisms used in this data collection. This is unsurprising given the complexity and lack of transparency about Facebook's advertising ecosystem. Participants surmised two primary uses for the data Facebook collects about its users: the personalization of Facebook content such as ads, and a misconception that the data is sold to other companies.

Past experiences with controlling ads Most participants had taken actions related to the advertising they experience online, particularly on Facebook. Participants frequently recalled using the Hide Ad control from the contextual menu. We observed that although some participants had settings other than the default on their Ad Preferences page, most of these participants did not recall having made changes to the Ad Preferences settings. Less common was previous experience clearing off-Facebook activity associated with the account using the Off-Facebook Activity settings. Participants described experiences using advertising controls on other platforms as well, such as those available through contextual menus on the corner of an ad or ad settings provided by a website or app. The use of ad blockers was also common, though participants did not believe they impacted Facebook ads or data collection, or were not sure. Other strategies participants mentioned for managing their advertising experience included using private browsing mode or private web browsers such as Brave, using the opt-out tool implemented by the Digital Advertising Alliance, enabling VPNs, and clearing their browsing history.

Usability of Facebook Ad Controls

Participants struggled with most session tasks, particularly with finding and understanding available Facebook controls. While they provided suggestions on how Facebook could improve its advertising controls, many suspected that Facebook's motivations in providing these controls were not in users' best interests.

Location of controls In locating task-related controls, participants had least difficulty finding the contextual Hide Ad option. In finding Ad Preferences, participants easily completed the first three steps of the interaction (clicking the down arrow in the main navigation bar, then Settings & Privacy, then Settings) but had difficulty locating the Ads link to Ad Preferences in the navigation menu. Many required a hint to keep scrolling through the menu, as it was the eighteenth link on the desktop version of the Facebook website and twenty-first on mobile. Participants spent

the most time on the Hotel Deals task; an average of 7.8 minutes (min: 3 minutes, max: 24 minutes). Only one participant found the Manage Future Activity setting in the Off-Facebook Activity page, while others attempted to identify appropriate controls within Ad Preferences.

Despite many participants having visited the page before, Ad Preferences was generally perceived to be difficult to find. Participants complained that there were too many options to look through on the Settings page. As one participant explained: "I got into it by sheer luck. I don't know if I could do it again if I wanted to." Others thought that the interaction path to get to Ad Preferences is too long, saying, "You got to go through mazes to get to it." There were participants who considered Ad Preferences intuitive to find. One participant explained their process as: "I know I'm trying to do advertisements. So then I kind of just went through [the Settings page] and just found words that associate with advertisements and it took me a minute." No participant reported that the Manage Future Activity control was easy to find. One participant described the interaction as "I had to...like open the door to open another door to open another door, that was ridiculous."

Participants suggested ways to make Ad Preferences easier to find. This included providing it as an option earlier in the current interaction, such as in the Settings & Privacy menu or main Settings drop-down menu, rather than a link from the Settings page. Another suggestion was to have it as an option in an ad's contextual menu (currently it is linked from the Why Am I Seeing this Ad? option). Other suggestions would make Ad Preferences even more prominent, such as an icon in the main navigation bar (i.e., next to the Notifications icon) or a link in the Your Shortcuts section (located on the left side of the page on Facebook's desktop site). One participant noticed the AdChoices link and icon, required for Digital Advertising Alliance members [34], and suggested that it or one next to it could lead to Ad Preferences rather than the current informational page.

Layout of controls In addition to considering the Hide Ad control easy to locate, participants also thought it was easy to use. While most participants assigned this task had used this control before, even those who had not used it before reported similar sentiments. Participants suggested one way to simplify the feature even more would be to remove the prompt requesting a reason for hiding the ad to make it a single-step process, similar to how the feature is implemented on other services.

The interaction required to manage the use of advertising lists did not appear to be obvious to some participants, even when starting from within the Audience-based advertising menu in Ad Preferences. During this task, one participant followed a Facebook help page linked from the Audience-based advertising menu, which included instructions for adjusting the Data from Partners setting instead of usage of advertising lists. Most commonly, participants needed prompting to click on a specific advertiser from the list of advertisers that appears in the Audience-based advertising menu. One participant described the interface as "really clunky...to be required to click through to like this list usage section and then go through and click like 'do not allow' [for individual companies]." Multiple participants suggested that a single opt-out related to the usage of advertising lists would greatly simplify the current interface.

Participants expressed mixed opinions about the layout of controls within the Ad Preferences page. Some thought it was too time consuming to go through all the settings menu, or reflected

the sentiment that there were "too many options in too many different places." In contrast, others found Ad Preferences easy to navigate. Suggestions for improving the current layout of controls included consolidation, such as centralizing controls to one menu, or having a single button or opt-out to disable existing controls related to data sharing. Others recommended more radical changes to Ad Preferences, such as reducing advertising controls to user defined topics or allowing users to indicate what topics of ads they would be interested in seeing and to block types of ads they do not want to see. One participant defined a simple hierarchy of toggle switches: a top-level option to specify whether or not Facebook could show ads, then a toggle for whether or not those ads could be personalized to a users' interests, and a third toggle related to whether ads could be targeted based on data collected from outside of Facebook (rather than just Facebook activity).

Understanding controls Participants in the Ad Preferences Discoverability task correctly identified the page as related to advertising settings but expressed differing views related to how understandable the page was. For example, one participant appreciated that there was a short explanation of each control on the page, while another complained: "it looks like there's a lot of wording that doesn't make it simple so you don't want to click on something and like break Facebook." Others thought it was difficult to distinguish how the available controls differ from one another.

During the session tasks and participants' exploration of Ad Preferences, we observed that some controls were understood better than others. Specifically, most participants were able to determine how granular controls related to specific ads, advertisers, or information used for targeting would impact the ads they see. An exception is the Ad Topics controls which allow users to mark "see fewer" for a standard list of advertising topics. Participants commonly believed that those topics were customized to the user through the interests Facebook inferred from their activity. Also less clear were controls for how the data collected through different advertising practices could be used. For example, participants thought controls related to the use of advertising lists would block ads from a particular advertiser or prevent them from sharing information with Facebook. Similarly, some participants had a misconception that disabling the Manage Future Activity and Data from Partners controls would lead to ads that were not personalized, rather than just personalized with Facebook activity. Participants also did not comprehend how these two controls differed; the former being related to the *collection* of off-Facebook activity and the latter the *use* of off-Facebook activity for advertising.

Speculation about Facebook's ad controls Participants offered much speculation related to how and why Facebook implemented its advertising controls in the way it did. Many felt that Facebook made the controls intentionally hard to find or use. As one participant suggested, "I'm sure they did it on purpose to make it difficult for you to find this [the Ad Preferences page]. Obviously because they don't want to lose the revenue." Others suggested that the controls do not actually do what they claim to do. One participant stated that they preferred extremely granular controls related to the types of data used in advertising and practices related to data collection so they would have more confidence that the control actually functions as described. There were also participants who believed that Facebook was lying about a stated practice or

	Ad Opinions	Privacy Concern	Engagement w/ Controls	Primary Goal(s)
The Privacy Concerned	Creepy	High	High	Prevent tracking Less personalization
The Advertising Curators	Sometimes helpful	Low	High	More personalization
The Advertising Irritated	Annoying	Low	Medium	See fewer ads Stop repetitive ads
The Advertising Disengaged	Resigned Ignore them	Medium	Low	Various

Table 6.2: Summary of user groupings related to participants' opinions about advertising, level of privacy concern, willingness to engage with advertising controls, and goals related to advertising.

being misleading in their explanations of their practices.

Participants expressed conflicting opinions related to how committed Facebook is to offering user controls. One participant stated, "I definitely think there's an attempt at least by Facebook to try and be somewhat transparent about their practices, and what they're sharing, and what they're collecting." On the other hand, others felt that Facebook provided ad controls only to avoid scrutiny from regulators or users. Some expressed a sense of futility in using Facebook's ad controls: "I mean, does it make a difference? No, not really. They still know everything they need to know. They still have the information of billions of people. But I guess it gives me the illusion of having a little more privacy."

User Goals Related to Facebook Ads

We identified four groupings of users who shared overall common sentiments about their ad experience and ad controls, which are summarized in Table 6.2.

The Privacy Concerned Six participants expressed primarily negative opinions about the ads they see on Facebook and found them creepy. As one participant described, "I always get upset when I see tailored ads because because it always feels like an invasion of privacy and that somebody's watching what you do." Relative to the other groups, this group had a higher level of concern related to Facebook tracking. Their primary goals related to their Facebook advertising experience included preventing cross-site tracking and receiving generic ads. Participants seemed willing to use controls and had past experiences with Facebook's ad controls. Some had also used other mechanisms to control ads, including private browsing mode and advertising settings on other apps or websites. Participants expressed a desire for controls and transparency related to Facebook tracking, such as being able to opt-out of tracking entirely and the ability to erase the personal data held by third-party advertisers.

The Advertising Curators In contrast to other groups, a group of six participants stated that they did not mind the ads they saw on Facebook and sometimes found them helpful. Participants in this group also seemed willing to use advertising controls, and many used controls in the past. Their primary goals for controlling their advertising experience included being able to adjust ad personalization so that ads are personalized even more to their interests, such as by hiding specific ads or advertisers. Participants also indicated wanting greater control over the topics of the ads they see on Facebook, such as by being able to directly indicate topics related to their interests as well as topics that are not related to their interests. For example, one participant who used the Clear Off-Facebook History feature during their session explained, "I'm just thinking that they had all this information on me . . . and I just wanted to get rid of it and start from scratch because my preferences may change over time." Concerns related to tracking or privacy were rarely mentioned by participants in this group.

The Advertising Irritated This group of seven participants had negative opinions about Facebook advertising. Rather than privacy concerns, participants' primary complaint was that ads on the platform were annoying. Participants' annoyance with ads was related to the the number of ads they see on the platform, as well as the ads they see being too repetitive. They appeared to be somewhat less willing to engage in Facebook ad controls, but some had used ad controls on the platform in the past. Participants in this group primarily wanted to be able to stop repetitive ads, or have some way to limit the amount of advertising they see on Facebook (which they recognized would be against Facebook's monetary interests). In their explanation of why they were not likely to use the Hide Ad feature in the future, one advertising-irritated participant described, "Because I don't really care so much what ads I see. I just want to see less of them. So, you know, until they introduce that option, which I don't think they ever will, then I just don't care that much."

The Advertising Disengaged Another group of six participants was disengaged with the advertising they experienced on Facebook. Some said that they ignored the ads that they see, while others expressed a resigned acceptance that targeted ads and data collection practices that enable them are just the way the Internet functions, even if they found them privacy-invasive. As one participant summarized, "I totally believe that all these companies have so much information on us at this point, and it's just, it is what it is, you know. I can just choose not to use it. But I do. So I kind of just have to accept the consequences of that." Many had previous experience with using ad blocking extensions or ad controls on Facebook and other services but expressed a low willingness to further engage with them. When prompted about the desired functionality of ad controls, participants described more of a variety of goals compared to other groups. Some described desired controls related to tracking, such as a setting to indicate that only the "minimum" information required for targeted advertising could be collected by the platform, and a way to select what information Facebook could collect. Others described controls related to personalization of ads, such as being able to select which advertisers could serve them ads.

6.3 Discussion

Our study explored user needs for advertising controls on Facebook, finding that users have differing goals related to the management of their advertising experience. While some goals were motivated by privacy concerns, others were more related to user experience on the platform. We found that the implementations of Facebook's existing advertising controls fell short of users' needs and expectations in some regards, but aligned well in others. Our results have implications for the design of advertising controls on Facebook as well as other platforms.

6.3.1 Limitations

While our study provides insight into user needs, it is not without its limitations. In both our survey and remote usability study we focused primarily on advertising controls implemented by Facebook, and not those available through third-parties such as the Digital Advertising Alliance (DAA). While we collected some data about participants' past experience with external ad controls, such as browser extensions and private browsing, we did not explore the usability or utility of those mechanisms in detail.

The timing of our study may have influenced some of our findings. Because our study was conducted shortly before and after the 2020 US Presidential election, participants had been seeing more election-related ads than they might normally see, and this appeared to influence participants' opinions about Facebook advertising. Furthermore, due to the COVID-19 pandemic, we conducted what would have been an in-person lab study in a virtual setting, with both benefits and drawbacks. While it allowed us to recruit participants outside of our immediate geographic area, we may have introduced a self-selection bias of only participants who were comfortable with using Zoom teleconferencing. Additionally, the virtual nature of the session may have led participants who primarily use Facebook on their mobile device to join their study session using their laptop or desktop computer, where they might have been more familiar with Zoom but less familiar with Facebook's settings. Our remote usability study explored the opinions and experiences of 25 participants. While we believe this provided a reasonable sampling of US Facebook users' experiences with ad controls, a larger study would likely have uncovered other experiences, and perhaps additional user groups. Additionally, while we attempted to mitigate priming effects with neutral questions (e.g., "What do you think about the ads you see on Facebook?") during initial discussion of advertising, it is possible that discussion of data collection by Facebook may have primed participants to think about privacy more than they would have otherwise.

6.3.2 Do Current Facebook Ad Controls Meet User Needs?

In terms of usability, current Facebook advertising controls had mixed results in meeting user needs. A major obstacle for participants in completing most study tasks was finding the Ad Preferences page. Though participants were able to complete the first two steps of the interaction, they struggled to find the Ads link from the navigation menu in the main Settings page, which only appeared after several scrolls. Participants seemed to be overwhelmed by the number of links in the menu. During their exploration of Ad Preferences, participants felt that the

current structure was too time-consuming and required too much effort to click through to access the different controls. In contrast, participants were able to find the Hide Ad control within the contextual menu accessible from an ad easily. Though it is unclear exactly how hiding a specific advertisement would impact Facebook's advertising algorithms, participants exhibited a relatively better understanding of this feature and other granular controls related to specific advertisers and interest categories, compared to their understanding of controls related to the use of Facebook collected data (e.g., the Data from Partners setting).

Similar to prior work that grouped Facebook users based on their privacy needs and behaviors related to other platform users [**?**], we were able to group users with different types of needs related to the functionality of ad controls. The available Facebook advertising controls meet the needs of some types of users more than others, particularly those who want ads to be more personalized to their interests. For example, controls related to removing interest categories, particular advertisers, and hiding specific ads are well aligned with user goals described by the *Advertising Curators* and *Advertising Irritated*. Additional controls that allow users to customize topics of interest could be offered. Considering the misconceptions related to the Ad Topics portion of Ad Preferences, repurposing this interface to allow users to select topics of ads they want to see and topics to block would benefit these users.

Current Facebook controls for advertising fall short of meeting the needs of the *Privacy Concerned* and *Advertising Disengaged*, who expressed a greater level of privacy concern. These participants were interested in preventing data sharing and tracking, rather than the use of shared data. Of the available controls, those in the Off-Facebook Activity menu best met the needs of these users. Facebook's description of these tools states that they pertain to data shared through Facebook's "business tools" and discloses only some of what these tools may be [**?**]. It is likely that the Off-Facebook Activity controls do not entirely prevent the cross-platform data sharing that is concerning to many users.

6.3.3 How Can Current Facebook Ad Controls Be Improved?

In considering user needs related to advertising controls, Facebook and other platforms should first and foremost consider the discoverability of controls. As many of Facebook's controls are centralized to Ad Preferences, it is vital that users are able to easily access this page. Participants provided several suggestions for simplifying the interaction required to reach this page. This included providing a link to Ad Preferences in either the Settings or Settings & Privacy drop-down menus that occur in the first two steps of the current interaction. Another suggestion was to include a link to the Ad Preferences page directly in the contextual menu available from an ad rather than requiring the additional step of first clicking "Why Am I Seeing This Ad?"

It is also important for platforms like Facebook to implement controls that meet the needs of different types of users. In addition to needs related to the functionality of controls, interface needs should also be considered. Our findings suggest that some users prefer very granular advertising controls such as the Hide Ad control, while others would prefer coarser controls that would stop all tracking or targeting. Furthermore, controls that required several interactions to change the setting such as the Manage Future Activity and List Usage controls were perceived to be particularly cumbersome. Similarly, some participants in our study appeared to be dissatisfied with the multi-layer design of the controls within Ad Preferences. Thus, to make current controls

more usable, Facebook should consider alternate designs. For example, the current multi-layer design could be improved by providing coarse controls over targeted practices directly on the Ad Preferences landing page and then more granular controls within sub-menus. Alternatively, a hierarchical layout might help to guide users through available options and thus reduce the effort required to engage with advertising settings.

Our study also highlighted the importance of fostering and maintaining user trust. Participants were cognizant of Facebook's tumultuous history with privacy and other social issues. This appeared to impact their confidence in the advertising controls they encountered during the study and their perceptions of Facebook's motivations for providing these controls. Such skepticism could affect how likely users are to engage with the controls. Thus, it is important for companies to follow practices that respect user values and needs, such as disclosing why they provide some controls but not others, as well as how they process user data, even when it is not being used for direct advertising on the platform.

6.3.4 Design Implications for Platforms Beyond Facebook

While Facebook's extensive data collection capabilities and public controversies may result in some privacy concerns specific to Facebook, we believe this study offers findings that can inform the design of advertising controls on other platforms as well.

Assess User Needs Our results highlight that users have differing goals related to their advertising experience on Facebook, such as making it more tailored to their interests or trying to minimize privacy invasion. Designers of advertising controls should examine the diverse needs of their users even when they are in conflict with each other: a "one-size-fits-all" approach will likely result in some users' needs being unmet. Furthermore, designers should be cognizant of the tension between providing users with meaningful control and overwhelming them. Simply implementing a plethora of advertising-related controls on a platform will also result in unmet needs. As demonstrated in our study, users may struggle to understand the difference between controls when presented with a large number of options. This highlights the necessity of following user-centered design practices and thoroughly understanding user needs prior to the deployment of an interface. While our study design provides an example of how such a needs assessment could be conducted once there is at least a high-fidelity prototype of an interface, other types of formative studies could be conducted earlier in the design process [87]. Designs should also be rigorously tested with large populations of users to ensure that they can meet diverse needs.

Make Controls Findable Many of our findings regarding users' expectations related to locating and using advertising controls would also likely apply to other platforms. For example, in our study, participants who were assigned to locate advertising settings correctly began their interaction with the Settings drop-down menu. Other platforms should follow this standard practice in UI design so that users can easily find advertising and privacy controls. Furthermore, our results suggest contextual menus located directly within an advertisement can effectively supplement advertising controls within settings pages. Our study participants frequently reported

using the Hide Ad feature within this type of contextual menu when discussing their past experiences with advertising controls. Providing advertising and other privacy controls within such a contextual menu enables users to make in-the-moment decisions related to their advertising experience and potentially other uses of their data. Such contextual menus could also provide a direct link to advertising and privacy controls located within settings pages so that they are more easily accessible if users want to further engage with the platform's privacy features.

Align Functionality with Expectations Controls that have unexpected functionality have poor usability and fall short of meeting users' needs. For example, participants in our study expected the list of topics in the Ad Topics menu to be customized to the user rather than to be a global list for all users. This global list lead to confusion, as some participants felt that the topics presented were not at all related to their interests. Considering the extensive amount of data collection and personalization of content elsewhere on the platform, the misconception that the Ad Topics menu is customized to users is understandable. Potentially compounding this confusion is that Facebook does allow users to remove "Interest Categories" from their profile, which is a list of topics that is customized to each user based on topics Facebook has inferred the user is interested in. However, this menu is much less prominent within the Ad Preferences page, requiring two more additional clicks within the Ad Settings tab. The Ad Topics menu is just one example of how controls could be misaligned with user expectations, but there may also be other controls that do not match user expectations. Thus, another important reason to conduct usability testing of privacy controls before implementation is to ensure that they are aligned with user expectations.

6.4 Conclusion

We conducted a two-part study to explore user needs for advertising controls on Facebook. We first ran a survey on Mechanical Turk and Prolific, which identified existing controls that seemed aligned with user goals related to controlling their Facebook advertising experience. Then we conducted a remote usability study to explore user goals in more detail and identify usability barriers with existing Facebook controls. Our results highlight that users have varying objectives and opinions related to Facebook ads. Some of Facebook's existing controls, particularly those related to controlling specific ads, advertisers, or information used in targeting, aligned well with user needs. However, the discoverability of some controls was low, and controls related to the use of collected data were poorly understood and did not appear to fully address participants' concerns related to tracking.

Chapter 7

Guidelines for Evaluating Privacy Choice Interfaces

Historically, companies have had economic motivation to encourage users to share their data through consent and privacy choice mechanisms, and may not have exerted more than minimal effort in testing the usability of such interfaces. On the other hand, the poor usability of such interactions, including the use of dark patterns which may make privacy-protective options less usable than other options, 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 [22]. Moreover, designers are not privacy experts and thus may not be familiar with methods to evaluate the effectiveness of consent and privacy choice experiences. Privacy choice interfaces require different considerations than other types of interfaces. Typically, users make privacy decisions when trying to accomplish a different goal (e.g., browse a website) which impacts how they interact with the privacy choice interface and the metrics by which these interfaces are considered usable. 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.

This chapter synthesizes the approaches used in the previous chapters of this thesis, as well as prior evaluations of privacy choice interfaces, into comprehensive guidance that can inform organizations about how to evaluate their privacy choice interfaces and also justify why resources should be allocated to conduct such usability evaluations. These guidelines are proposed to be a set of best practices when testing privacy choice interactions. Furthermore, regulators can use these guidelines as a means to hold companies accountable to rigorous usability testing of their privacy choice and consent processes.

The goal of these evaluation guidelines is to help increase the usability of privacy choice and consent interfaces. These guidelines may be beneficial to designers without privacy expertise, as well as privacy practitioners who do not have much usability experience. 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. Proposed frameworks for more usable privacy choice and consent include AI agents to help automatically facilitate privacy choice consent decisions based on a user's prefer-

ences [95], as well as standardization of consent and privacy choice interfaces. These guidelines could be used in such efforts to ensure that proposed AI-assisted decision-making interfaces and standardized implementation guidelines are actually usable. However, until such frameworks are widely adopted, these evaluation guidelines could help companies improve the usability of their unique privacy choice and consent interfaces.

This chapter first identifies seven high-level usability objectives, identified through a review of both general and privacy choice-specific definitions of usability. It then highlights different research methods and study designs that can be used to perform usability evaluations of privacy choice interfaces, and provides guidance for organizations on selecting an appropriate evaluation method. Next, the chapter proposes a set of comprehensive guidelines that can be used by practitioners to evaluate the usability of privacy choice interface designs. These guidelines are structured according to the seven high-level goals of privacy choice interface usability evaluations. For each guideline, example prompts and metrics that address the high-level evaluation goals are provided. These are drawn from classic approaches to usability testing, prior work in privacy choice evaluations, and normative perspectives related to dark patterns [99]. The guidelines highlight how to apply different 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, are described. Furthermore, the guidelines highlight prior studies that align with particular high-level study objectives and different research methods.

This chapter makes the following contributions:

- Definition of seven high-level usability objectives relevant to privacy choice interactions.
- An overview of research methods and study designs for evaluating the usability of privacy choice interfaces.
- Guidance pertaining to selecting an appropriate usability evaluation approach.
- A set of comprehensive guidelines, including suggested metrics and question prompts, to evaluate again each high-level usability objective.

7.1 Evaluation Objectives

To consider the holistic usability of privacy choice interfaces, it is important to first identify aspects of usability that are relevant to the privacy choice experience. Privacy choice interactions differ from other interactions in that users are typically not trying to achieve a privacy goal when they interact with a system. Thus, the way they interact with privacy choice interfaces will be heavily impacted by their primary goal. Furthermore, when evaluating privacy choice interfaces it is important to consider that users' behaviors and attitudes toward such interfaces are heavily influenced by their past experiences with similar privacy choices. As a result, it may be necessary to overcome habituation to achieve meaningful privacy choice for a particular context. A review of different definitions of usability resulted in seven high-level objectives for usability evaluations, which provide an organizing structure for the guidelines.

This section first provides an overview of the usability definitions referenced, which were

primarily selected from textbooks in HCI and privacy. Following is a description of how components of the definitions were grouped, resulting in the seven high-level objectives.

7.1.1 Previous Usability-Related Definitions

Feng et al. [49] provide a definition of usable privacy choice interactions, which include components related to usability more generally as well as those more specific to privacy choice interfaces. They describe the concept of meaningful privacy choice which "extend beyond traditional usability considerations to include several facets that are more specifically tied to supporting users in making privacy decisions that capture their true privacy preferences." According to Feng et al.'s definition, components of meaningful privacy choice include:

- *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
- *Neutrality*: whether privacy choice interfaces exhibit dark patterns, particularly those that make exercising privacy-protective options more difficult to use than other available options

Schaub and Cranor [127] explain that "meeting legal and regulatory obligations is not sufficient to create privacy interfaces that are usable and useful for users." Components they consider required for effective privacy interfaces include:

- *Findability*: people can find provided privacy information and controls
- *Understandability*: people can understand provided privacy information and controls
- *Usability*: people can successfully use provided privacy information and controls
- *Usefulness*: privacy information and controls align with users' needs with respect to making privacy-related decisions and managing their privacy

The International Organization for Standardization (ISO) 9241 [?] provides a definition of usability that is generalizable to users' interactions with any computerized system. The standard considers usability as the effectiveness, efficiency and satisfaction with which users achieve specified goals in particular environments. It defines these three components as:

- *Effectiveness*: the accuracy and completeness with which specified users can achieve specified goals in particular environments
- *Efficiency*: the resources expended in relation to the accuracy and completeness of goals achieved
- *Satisfaction*: the comfort and acceptability of the work system to its users and other people affected by its use

Quesenbery [?] extends ISO's definition of usability and describes the "5 Es" of a usable interface as:

- *Effective*: how completely and accurately the work or experience is completed or goals reached

- *Efficient*: how quickly this work can be completed
- *Engaging*: how well the interface draws the user into the interaction and how pleasant and satisfying it is to use
- *Error tolerant*: how well the product prevents errors and can help the user recover from mistakes that do occur
- *Easy to learn*: how well the product supports both the initial orientation and continued learning throughout the complete lifetime of use

Nielsen [?] defines usability as a "quality attribute that assesses how easy user interfaces are to use." The five "quality components" of usability include:

- *Learnability*: How easy is it for users to accomplish basic tasks the first time they encounter the system?
- *Efficiency*: Once users have learned the system, how quickly can they perform tasks?
- *Memorability*: When users return to the system after a period of not using it, how easily can they reestablish proficiency?
- *Errors*: How many errors do users make, how severe are these errors and how easily can they recover from the errors?
- *Satisfaction*: How pleasant is it to use the system?

Morville's UX Honeycomb [?] is commonly referred to in web design and explains the "qualities of user experience that web designers must address." These qualities include whether interfaces are:

- *Useful*: Does the interface actually allow users to do something that has utility for them?
- *Desirable*: Is the interface attractive or lead to users having positive emotions
- *Valuable*: Does the interface do something of value to the organization (e.g., advance the group's mission, contribute to the bottom line)
- *Usable*: Can users perform the action they intend to perform?
- *Findable*: Can users locate the control that they need?
- *Credible*: Do users believe that the control does what it is supposed to do, what it says it does?
- *Accessible*: Is this control usable to people who do not have specialized knowledge or expertise? Is this control usable by users with disabilities?

7.1.2 Grouping Usability Definition Components

Table 7.1 highlights the overlap between the referenced usability definitions, as well as where they differ. Comparing these definitions resulted in seven high-level groups, which correspond to different objectives of usability evaluations. Definitions of these objectives for the context of privacy choice interfaces are provided in this section.

1. User Needs: Whether a privacy choice interface allows the intended users to accomplish a privacy goal that has utility for them. Also includes accuracy and completeness of the interface in addressing the goal.

Components from previous definitions: **Effectiveness** (Feng et al. [49], ISO [**?**], Quesenbery [**?**]), **Useful** (Schaub and Cranor [127], Morville UX Honeycomb [**?**])

2. User Ability & Effort: Whether a privacy choice interface allows the intended users to accomplish a particular privacy goal and with minimal effort.

Components from previous definitions: **Efficiency** (Feng et al. [49], ISO [**?**], Quesenbery [**?**], Nielsen [**?**]), **Usable** (Schaub and Cranor [127], Morville UX Honeycomb [**?**]), **Accessible** by "non-experts" (Morville UX Honeycomb [**?**])

3. User Awareness: Whether the intended users are aware that a particular privacy choice exists within a privacy choice interface, and if they are able to find it.

Components from previous definitions: **User awareness** (Feng et al. [49]), **Findable** (Schaub and Cranor [127], Morville UX Honeycomb [**?**]), **Easy to learn** - initial orientation (Quesenbery [**?**], Nielsen [**?**])

4. User Comprehension: Whether the intended users understand what a particular privacy choice does and the implications of their decisions.

Components from previous definitions: **Comprehensiveness** (Feng et al. [49]), **Understandability** (Schaub and Cranor [127]), **Easy to learn** - continued learning (Quesenbery [**?**])

5. User Sentiment: Whether the intended users are satisfied with a privacy choice interface and options it provides. This includes whether users have faith that the privacy choice will be honored.

Components from previous definitions: **Satisfaction** (ISO [**?**], Nielsen [**?**]), **Engaging** (Quesenbery [**?**]), **Desirable** (Morville UX Honeycomb [**?**]), **Credible** (Morville UX Honeycomb [**?**])

6. Decision Reversal: Whether a privacy choice interface allows the intended users to correct an error or change their decision. This also includes the effort required to do so.

Components from previous definitions: **Error tolerant** (Quesenbery [**?**], Nielsen [**?**])

7. Nudging Patterns: Whether the design of a privacy choice interface leads the intended users to select certain choices in the interface over others. In contrast to the other high-level objectives which are applicable to almost any type of user interface, evaluating for nudging patterns is especially relevant to contexts in which users are asked to give up something, such as their personal data to the benefit of the company

Components from previous definitions: **Neutrality** (Feng et al. [49])

7.2 Research Methods

This section describes different research methods and study designs that can be applied to evaluate how well privacy choice interfaces meet the desired usability objectives. While this may not

	Related to user needs	Related to ability & effort	Related to awareness	Related to comprehension	Related to sentiment	Related to decision reversal	Related to nudging patterns
Feng et al. [49]	Effectiveness	Efficiency	User awareness	Comprehensiveness			Neutrality
Schaub & Cranor [127]	Usefulness	Usablity	Findability	Understandability			
ISO [?]	Effectiveness	Efficiency			Satisfaction		
Quesenbery [?]	Effectiveness	Efficiency	Easy to learn (initial use)	Easy to learn (continued used)	Engaging	Error tolerant	
Nielsen [?]		Efficiency			Satisfaction	Error tolerant	
Morville UX Honeycomb [?]	Useful	Usable, Accessible	Findable		Desirable, Credible		

Table 7.1: Components of the referenced usability definitions grouped according to different usability aspects.

be a comprehensive list of all possible evaluation techniques, it demonstrates a wide breadth and diversity of approaches.

7.2.1 Expert Evaluation Methods

Inspection-based approaches can be adapted to evaluate the usability of privacy choice and consent interfaces. While the usability of privacy choice interfaces overlap with the usability of other types of interfaces overall, a key difference is analyzing the impact of any potential nudging patterns that may appear in the design. Below is a brief description of five inspection-based methods that could be used in evaluating for different usability objectives. Additional information about these approaches can be found in the HCI literature (e.g., [147]).

Perspective-based UI Inspection: One or more people evaluate the privacy choice interface from the perspective of a particular type of user (super-user, less-tech savvy, person with disability) or through the lens of a specific normative value, in this case privacy.

Individual Expert Review: One or more experts in HCI, the privacy choice domain, or the product conducts a review to find usability problems in a privacy choice interface according to the usability objective(s).

Cognitive Walkthrough: An expert interacts with a privacy choice interface to identify usability issues that primarily impact its learnability. This method is based on the theory that users learn through exploration.

Heuristic Evaluation: An individual or team evaluates a privacy choice interface design against a list of UX principles (e.g. Nielsen Heuristics) or other pre-defined criteria (e.g., regulatory requirements).

Formal Usability Evaluation: Trained inspectors conduct coordinated, individual usability assessments of a privacy choice interface (similar to formal code inspections). This may include collecting information about the shortest path to complete a privacy choice task, the minimum number of actions required to complete it, or the time taken to complete the task.

7.2.2 User Study Designs

User studies can complement inspection-based evaluations with perspectives from individuals who are more likely to represent the opinions and behaviors of end-users of the privacy choice interface. User study evaluations of privacy choice interfaces could be implemented through different research methods and study designs. Some may involve assigning participants to a task involving a privacy choice interface, with questions being asked before or after task completion (or both). In lieu of a task, participants may be asked about their previous experiences with a

privacy choice interface if it has already been deployed. It is also possible for studies to combine these elements to explore whether the privacy choice interfaces meet a particular usability objective.

No Task Assigned

- **Research methods:** *surveys, interviews, focus groups*

Qualitative Prompts: Participants' are asked about their desires relating to privacy or past experiences with a privacy interface. However, a limitation of asking about past experiences is that participants may not fully recall the interface or their interactions.

- **Research method:** *field study*

Quantitative Metrics: This study design involves measurement of users' behavior when interacting with a deployed privacy choice interface, for example average amount of time spent before making a choice and percentage of users who click each button. While measurement studies provide insight into how users are interacting with an interface, they do not typically provide an explanation as to why users interact with it in the way that they do, unless paired with an interview or survey.

Participants Assigned Privacy Task

- Research methods: *online survey, online experiment, lab usability study*

Participant Inspection: Participants are shown a privacy choice interface and are encouraged to fully engage with it prior to answering questions (e.g., about what choice they would make or to measure their awareness or comprehension). Typically, participants are allowed to reference the interface while they are answering questions.

Participant Quick Review: Participants are shown a privacy choice interface but are only allowed a short period to engage with it (e.g., 3 seconds). Typically, participants are not allowed to reference the interface while they are answering questions.

Hypothetical Scenario: Participants are given a realistic scenario which motivates a privacy choice-related task, and are asked how they would complete the task or use a privacy choice interface according to what was described in the scenario.

Make Personal Privacy Choices: Participants are shown a privacy choice interface and are asked how they would interact with it according to their own personal privacy preferences.

Participants Assigned Distraction Task

- **Research methods:** *online experiment, lab usability study*

Considering that privacy/security are often secondary priorities when users interact with a system, simulating this in a user study might require assigning participants a "distraction task". Examples of distraction tasks might include shopping for a particular item, or finding information on a website. Participants should encounter the privacy choice interface or an indicator leading to it along their interaction during the distraction task.

Privacy Choice Prompt Appears: Participants are asked to complete a task that is unrelated to the privacy choice interface being evaluated, but are exposed to the privacy choice interface at some point in the study.

Participant Seeks Out Privacy Settings: Participants are asked to complete a task that is unrelated to privacy but as part of the interface they can see the current privacy settings. During the course of task completion they may choose to change their privacy settings according to their preferences.

7.2.3 Selecting Evaluation Methods

When selecting research methods and study designs to use in privacy choice interface evaluations, it is important to consider several factors related to the organization conducting the evaluation and particular interface being evaluated. These factors may impact the suitability of different research methods. Here we describe a few of these practical considerations, though there may be others that impact a given privacy choice interface assessment.

Design Stage of the Privacy Choice Interface

An important factor that impacts what types of usability evaluations of a privacy choice interface are suitable is where in the design process the evaluation is being conducted. Ideally, the usability of a particular design will be assessed throughout the different stages of design, with multiple research methods. These usability assessments should build on each other. For example, a usability assessment in the ideation design phase may involve using qualitative methods, such as interviews or focus groups, to better understand users' needs in the context of a privacy choice interface. Expert evaluations, online surveys, experiments, and lab usability studies may be conducted with prototypes of the privacy choice interface to assess how well users' needs are met, as well as to what extent other usability objectives, including ability & effort, awareness, and comprehension, are achieved. Once a privacy choice interface is deployed, expert evaluations and field studies may be used to confirm that the usability of the final design is similar to results from previous usability testing.

Data Needed for Organizational Decisions

When considering the scope of possible research methods for assessments of privacy choice interfaces, it is necessary to prioritize which and what type of data are most important to capture from an organizational perspective. For example, some organizations may have additional requirements related to privacy choice that must be examined through a usability evaluation and thus focus more on a subset of the described usability objectives. Furthermore, organizations may differ in how they weigh and use different types of data in design decision-making. User studies that involve empirical data, such as field studies, online experiments, or lab usability studies, typically provide the best representation of how users may perceive or react to a particular design once it is deployed. However, other types of user studies involving self-reported data may still provide enough of this insight to help organizations move forward with certain decisions. Expert evaluations can also play an important role in organizational decision-making, particularly in contexts where user feedback may not be helpful (e.g., new technologies where the average user may not be aware of all possible interaction paths).

Availability of Resources for Usability Testing

Another important consideration in planning usability evaluations is the resources available, in terms of time, budget, and skill set of the evaluation team. While inspection-based evaluations are typically less costly than user studies in terms of time and budget, they require one or more evaluators with specific legal, design, or privacy expertise. User studies involving primarily quantitative data, such as surveys, can be deployed to a large number of participants (e.g., through online crowd-sourcing platforms) and analyzed in a short amount of time but may require a larger testing budget. Qualitative user studies can be run with a smaller budget but may require more time for both data collection and analysis.

7.3 Evaluation Guidelines

The evaluation guidelines are organized according to the seven identified high-level usability evaluation goals. It is important to note that acceptable thresholds for meeting these guidelines are not universal, but rather depend on the context of the privacy choice interface. Many factors, including intended user groups, complexity of options, and devices used to display the privacy choice interface, influence whether a given privacy choice interface is sufficiently usable. For each guideline we include:

- A description of measures or example prompts. We refer to established usability metrics and heuristics when appropriate, or specific components of existing usability scales that are applicable to the privacy choice context.
- Additional details for implementing the guideline in an evaluation study.
- Research methods or study designs most appropriate for implementing the guideline
- What types of privacy choice interfaces the guideline applies to, in terms of the Timing component of the privacy choices design space [49]: *all* (any type of privacy choice interface), *on-demand* (privacy settings pages that the user seeks out), or *interruptive* (privacy

choice interfaces that appear at setup, just-in-time, are context-aware, are periodic, or are personalized.
- Citation(s) for prior evaluations of privacy choice interfaces demonstrating the guideline (if applicable). These examples were selected to illustrate concepts in this document but is not a complete list of prior privacy choice interface evaluations. A summary of the methods used in these cited studies is provided in Appendix **??**.

7.3.1 User Needs

Ideally, the design team would have completed a needs assessment during the design phase using qualitative approaches such as interviews/focus groups, diary studies, and qualitative surveys. These guidelines pertain to evaluating whether the interface is aligned with the identified needs and how well/completely it addresses them. If privacy choice interfaces are being used in contexts where it is unlikely that users already know their privacy needs, the choice interface should help users identify privacy goals they may have when using the system. Furthermore, evaluating interruptive privacy choice interfaces for User Needs may require special considerations in user studies since making privacy-related decisions will likely not be users' primary goal when they encounter it. Such evaluations could involve instructing participants to pay attention to any privacy-related options that appear, drawing their attention to a general area of a website or app containing the choice interface, or providing an opportunity to review the privacy choice interface with more focused attention.

Users' privacy objectives related to their use of a system

- Example prompts:
  - What settings or controls related to [domain of privacy choice] would you like to have available to you, if any? [for initial exploration into user needs prior to designing the privacy choice interface]
  - What other settings or controls related to [domain of privacy choice] would you like to have available to you, if any? [for further exploration into user needs related to an existing privacy choice interface design]
  - What would you like to change about [domain of privacy choice] that you haven't yet been able to? [for further exploration into user needs related to a deployed or prototyped privacy choice interface design]
- Similar prompts may have been used in the initial needs assessment, but can also be used again afterwards to reflect on whether the implemented interface meets users' goals. This prompt assumes that participants have experience using the system, but not necessarily the privacy choice interface being evaluated.
- Methods: survey, interview, focus group
- Timing: all
- Prior work: [**?**]

Users' intentions when interacting with a privacy choice interface

- Example prompt: What were you trying to achieve when you [interaction with privacy choice interface]?
- This prompt should get participants to reflect on what their goals were in a past interaction with a privacy choice interface, which could be privacy related (e.g., trying to prevent a certain type of data collection) or more practical (e.g., to continue to the main website). This prompt assumes that participants had experience with the privacy choice interface being evaluated, for example through a study task.
- Methods: survey, interview, online experiment, lab usability study
- Timing: all

How completely does the implemented interface achieve users' needs?

- Example heuristics:
  - Does the interface meet the needs of different types of users (including those who may have conflicting goals)?
  - Does it allow users to achieve all of their stated objectives, or only some of them?
- This requires having some knowledge of users' objectives through a user study, and could be done in conjunction with 7.3.1.
- Methods: perspective-based UI inspection, individual expert review
- Timing: all

How accurately does the implemented interface achieve users' needs?

- Example heuristics:
  - Does the interface do what users would like it to do?
  - How does it help users accomplish their goals?
- This requires having some knowledge of users' intentions when using a privacy choice interface, and could be done in conjunction with 7.3.1.
- Methods: individual expert review
- Timing: all

7.3.2 User Ability & Effort

This is a part of what most usability testing guidelines cover, and primarily involves quantitative measures that estimate the effort involved in using the interface. These metrics can be used to compare interfaces (e.g., a previous version of the interface, alternate designs, or the interface of a similar product). For user studies, measuring ability and effort usually involves assigning participants to complete a task involving the interface. Much of the effort involved in using a choice interface will likely be in finding where it is, but users could possibly make other errors such as forgetting to save their privacy choices or toggling a choice in the wrong direction.

Percentage of participants able to complete a privacy choice task without aid; type and extent of assistance required

- Example prompts & metrics:
  - What would you do if you wanted to [complete privacy choice task]?
  - Given a task that requires using a privacy choice interface, were participants able to complete it on their own?
  - In moderated studies, what were the hints/aid required to help participants complete their task?
- Methods: Online experiment, lab usability study
- Timing: all
- Prior work: [62**?**]

Time taken to complete a privacy choice task

- Example metrics:
  - Given a task that requires using a privacy choice interface, how long did it take for participants to complete this task?
  - Alternative time-based metrics include time-based efficiency and overall relative efficiency [**?**]
- Methods: Online experiment, lab usability study
- Timing: all
- Prior work: [**?**]

User actions required to complete a privacy choice task

- Example metrics:
  - Given a task that requires using a privacy choice interface, how many user actions (e.g., clicks, hovers, form fields) did it take for participants to complete this task?
  - What common errors did users make in completing the task?
- Methods: Online experiment, lab usability study
- Timing: all
- Prior work: [62]

Perceived effort in completing the privacy choice task

- After completing a task that requires using a privacy choice interface, participants can be asked questions related to the perceived ease or difficulty of their experience. Alternatively, these questions can be asked about participants' prior experiences with a privacy choice interface outside of the study environment.
- Commonly used prompts that measure perceived effort on a Likert scale include [**?**]:
  - The Single Ease Question (SEQ)
  - Items 2, 3, 4, and 8 on the System Usability Scale (SUS)
- Methods: Online experiment, lab usability study
- Timing: all

- Prior work: [62**?**]

Estimated ability and effort required to complete a privacy choice task

- Example heuristics:
  - A set of design heuristics specific to the privacy choice interface
  - Established usability heuristics (e.g., items 1-3, 7, 8 of Nielsen heuristics [**?**])
  - How does the ability and effort of an "expert" with prior knowledge of the interaction compare to those of user study participants to complete a privacy choice task? This could be done in conjunction with 7.3.2 and 7.3.2.
- Methods: Heuristic evaluation, formal usability evaluation
- Timing: all
- Prior work: [61]

7.3.3 User Awareness

In the context of what the user is actually doing, we want to ensure that they recognize that the privacy choice(s) exist and that they are able to find them. This is probably the most difficult aspect of users' interaction with a privacy choice interface and may be measured together or separately from User Ability & Effort (Section 7.3.2). Testing for user awareness may be less important for privacy choice interfaces that interrupt the user, compared to on-demand privacy settings pages that users must seek out. Furthermore, for step-wise privacy choice interfaces, in which privacy choices are incrementally revealed, it may be sufficient to evaluate whether users are aware of the general types of options available to them, rather than every option offered in the interface.

Percentage of participants aware the privacy choice exists

- Participants can be shown a privacy choice or be exposed to one while completing a distraction task. Evaluators can ask participants follow-up questions including:
  - Whether participants recall the specific privacy choice interface or options available to them related to privacy
  - Whether participants realize they were asked to make a privacy choice and are able to identify which choice they made
  - What participants can recall from the privacy choice interface
- Methods: Survey, online experiment, lab usability study
- Timing: all
- Prior work: [**?**]

Percentage of participants able to find the privacy choice

- Example metrics:
  - Given a task that requires using a privacy choice interface, were participants able to find it on their own?

    - In moderated studies, what were the hints/aid required to help participants find the privacy choice?
- Methods: Online experiment, lab usability study
- Timing: On-demand privacy choices
- Prior work: [62**?**]

Time taken to find the privacy choice

- Example metrics:
    - Given a task that requires using a privacy choice interface, how long did it take for participants to find the correct privacy choice?
    - How did this compare to the time it took an "expert" with prior knowledge of the system to find it?
- Methods: Online experiment, lab usability study
- Timing: On-demand privacy choices
- Prior work: [**?**]

Path taken while trying to find the privacy choice

- Example metrics:
    - Given a task that requires using a privacy choice interface, how long did it take for participants to find the correct privacy choice?
    - How did this compare to the interaction path of an "expert" with prior knowledge of the system to find it?
- Methods: Online experiment, lab usability study
- Timing: On-demand privacy choices
- Prior work: [**?**]

Perceived difficulty in finding the privacy choice

- Example prompts:
    - After completing a task that requires using a privacy choice interface, participants can be asked questions related to the perceived ease or difficulty in finding the privacy choice.
    - Alternatively, these questions can be asked about participants' prior experiences with a privacy choice interface outside of the study environment.
- Methods: Online experiment, lab usability study
- Timing: On-demand privacy choices
- Prior work: [**?**]

Estimated difficulty in finding the privacy choice

- Inspection-based approaches can be used to estimate the difficulty of finding a privacy choice. This can be accomplished through a cognitive walkthrough of the system or identifying a set of heuristics.

- Example heuristics:
  - A set of design heuristics specific to the privacy choice interface
  - Established usability heuristics (e.g., items 4 and 6 of Nielsen heuristics [**?**])
  - How does the ability of an "expert" with prior knowledge of the system compare to those of user study participants to find the privacy choice interface? This could be done in conjunction with 7.3.3 and 7.3.3.
- Methods: Heuristic evaluation, cognitive walkthrough
- Timing: On-demand privacy choices
- Prior work: [61]

7.3.4 User Comprehension

In order for a privacy choice to be effective, it is important to ensure that users actually understand what the interface does, or if there are common misconceptions about its functionality. When evaluating for comprehension, it is important to keep in mind that users may not have a thorough understanding of the technologies that the privacy choice interface is about. It is more important to evaluate whether users understand the options that are available to them and the implications of their decision, given their (often) incomplete technical knowledge.

Objective knowledge when users' attention is focused on a privacy choice interface

- Example prompts & heuristics:
  - What would you expect to happen when [description of privacy choice decision]?
  - Do participants understand the privacy benefits and risks associated with different options?
  - If applicable, can participants recognize whether a privacy choice is optional or mandatory?
- Methods: Survey, online experiment, lab usability study
- Timing: all
- Prior work: [62, 64**?**]

Objective knowledge when users' attention is not focused on a privacy choice interface

- Example heuristics:
  - Given their normal interaction with a system, do participants understand what the privacy choice interface does and the implications of a decision?
  - How well does their objective knowledge compare to those of users' who had focused attention on the privacy choice interface?
- Similar to measuring awareness of a privacy choice, this measure might require assigning participants to a distraction task.
- Methods: Online experiment, lab usability study
- Timing: Interruptive

Perceived difficulty in learning or comprehending the privacy choice interface

- After completing a task that requires using a privacy choice interface, participants can be asked questions related to the perceived ease or difficulty in learning or comprehending the privacy choices.
- Commonly used prompts that measure perceived learnability include:
  - What (if anything) they found difficult to understand about the privacy choice interface.
  - Items 5, 6, 7 and 10 on the System Usability Scale (SUS) [**?**]
- Alternatively, these questions can be asked about participants' prior experiences with a privacy choice interface outside of the study environment
- Methods: Survey, online experiment, lab usability study
- Timing: all
- Prior work: [62**?**]

Estimated difficulty in learning or comprehending the privacy choice interface

- Inspection-based approaches can be used to estimate the difficulty of learning or comprehending a privacy choice interface. Example heuristics may include:
  - Item 10 of Nielsen heuristics [**?**]
  - What, if any aid, might be required
  - Whether particular types of users might have greater difficulty in learning or comprehending what the choice interface does
- Methods: Heuristic evaluation, cognitive walkthrough, or perspective-based UI inspection
- Timing: all
- Prior work: [61]

7.3.5 User Sentiment

Likert measures and qualitative prompts can be used to gauge users' satisfaction with a privacy choice interface after they have had some experience using it, such as through a study task.

Users' perceptions of transparency and control after interacting with a privacy choice interface

- Example prompts:
  - To what extent do you feel this [privacy choice interface] provides sufficient control over your data?
  - How transparent do you feel that this [privacy choice interface] is related to the use of your data?
- These could be measured using a Likert scale with a follow-up qualitative prompt to explore further.
- Methods: Survey, online experiment, lab usability study
- Timing: all

Subjective knowledge after interacting with a privacy choice interface

- Example prompts:
  - To what extent do you feel informed about your choices related to [privacy choice domain]?
  - How capable do you feel in making a decision related to [privacy choice domain]?
  - How confident are they in their privacy choice (e.g., item 9 of SUS [**?**])?
- These could be measured using a Likert scale with a follow-up qualitative prompt to explore further.
- Methods: Survey, online experiment, lab usability study
- Timing: all

Users' comfort and trust in the privacy choice interface

- Example prompts:
  - How comfortable or uncomfortable do you feel about how your data will be used?
  - To what extent do you feel that your [privacy choice decision] will be honored?
- These could be measured using a Likert scale with a follow-up qualitative prompt to explore further
- Methods: Survey, online experiment, lab usability study
- Timing: all

Users' self-reported investment in their privacy choice

- Example prompts:
  - How carefully did you consider your [privacy choice]?
  - Imagine that you saw this [privacy choice interface], how likely would you be to engage with [the privacy choice interface]?
- These could be measured using a Likert scale with a follow-up qualitative prompt to explore further.
- Methods: Survey, online experiment, lab usability study
- Timing: all Prior work: [**?**]

7.3.6 Decision Reversal

Users need to be able to change their privacy choice decision, both immediately after an interaction with a privacy choice interface and, if applicable, at a later time through user settings offered through the website or app. This allows for users to correct an error they may have made in their initial privacy choice as well as circumstances in which users change their mind about how their data is used or collected. The measures under User Ability & Effort related to making an initial privacy choice can be adapted to measure users' ability and effort in reversing their privacy decision (both immediately after making an initial decision and at a later point in time in which the choice interface or a settings page must be revisited). Similarly, those related to User Awareness and User Comprehension can be utilized to ensure that users can find and understand the information and processes that a part of reversing their privacy decision. In this case, the privacy

choice task assigned to participants would be to undo or modify their initial privacy choice. This aspect of usability is applicable to the entire privacy choice design space.

7.3.7 Nudging Patterns

Privacy choice interfaces often exhibit dark patterns that nudge users to less privacy-protective outcomes to the benefit of the company. This usually occurs when privacy-protective options are made less salient or more cumbersome to use than the alternatives. Furthermore, regulations such as the GDPR and CPRA make the use of dark patterns in privacy choice interfaces, particularly those related to consent, illegal. As such it is important for designers to be aware of the way they are nudging consumers and evaluate whether this nudging would be considered a dark pattern. In some contexts, it may even be appropriate for interfaces to nudge users to privacy-protective choices. To evaluate privacy choice interfaces for dark patterns, we should consider the four normative perspectives described by Mathur et al. with regards to privacy [99].

Impact of the privacy choice interface on individual welfare

- Mathur et al. suggest measuring a "welfarist conception of privacy" [99]. Example metrics include:
  - Calculating the financial value of the data disclosed because of a design pattern
  - Examining the proportion of users whose needs were not satisfied because of a dark pattern
- These metrics could also highlight whether individual welfare could be improved with nudges toward privacy-protective choices
- Methods: Survey, field study, online experiment
- Timing: all
- Prior work: [110]

Impact of the privacy choice interface on users' trust

- Privacy choice interfaces should be evaluated on whether they are detrimental to the collective welfare. In the context of privacy choice interfaces, dark patterns may result in a loss of trust or skepticism (e.g., in the company, in companies using similar privacy choice interfaces)
- Example prompts:
  - Prompts related to User Sentiment (e.g., 7.3.5 and 7.3.5) could also be used to evaluate a privacy choice interface's impact on user trust
- Similarly, they could be applied to evaluate whether nudges toward privacy-protective choices improve trust
- Methods: Survey, field study, online experiment
- Timing: all

Unintended societal consequences caused by the privacy choice interface

- Another aspect of collective welfare is analyzing whether the privacy choice interface could lead to unintentional disclosure of personal information, and whether this could have negative societal-level impact. A prominent example is Facebook users unknowingly consenting to their data being shared with Cambridge Analytica, which used the data to influence global elections [**?**].
- Methods: Individual expert review
- Timing: all
- Prior work: [**?**]

How well the privacy choice interface aligns with regulatory objectives

- Both GDPR and CCPA/CPRA have provisions related to the usability of privacy choice interfaces, particularly to the consent of data collection. Prior empirical evaluations of consent notices have identified dark patterns that likely violate the spirit of GDPR and could potentially lead to regulatory penalties. Particularly Nowens et al. and Soe et al. provide a list of design criteria for cookie consent notices to evaluate for the presence of dark patterns and potential violations of the GDPR [110, 132]. This includes that consent be explicit (e.g., require a click from the user), consent must be as easy to withdraw or refuse as it is to give, and the privacy choice interface contain no pre-selected boxes for non-necessary purposes [110]. Other potentially violating design patterns are the absence of actual choices in the interface (e.g., instructions to change privacy choices are simply described in a notice text), choice toggles that are unlabelled, and not using antonyms of the consent option to label the option denying consent [132] .
- Methods: Heuristic evaluation, individual expert review
- Timing: all
- Prior work: [110, 132**?**]

How well the privacy choice interface enables individual autonomy

- Mathur et al. [99] suggest evaluating to what degree an interface interferes with "users' ability to make independent decisions," which would require comparing interfaces with nudging patterns with a neutral design. This could be measured through measures that align with other evaluation objectives including:
  - If a privacy choice interface design seems to nudge users to a particular option (i.e., what options do users select under different designs?)
  - If an option that aligns with their preferences is available (see 7.3.1)
  - If they are able (and effort required) to choose their preferred option (see 7.3.2, 7.3.2, 7.3.2)
  - Whether users are aware of all options available to them (see 7.3.3)
  - If they can comprehend available options (see 7.3.4 and 7.3.4)
  - Users' perceptions of autonomy (see 7.3.5 and 7.3.5)
- Similarly, in some contexts it may be beneficial to evaluate whether interfaces utilizing reflective design better enable individual autonomy, as suggested by Terpstra et al [**?**].

- Methods: Survey, online experiment, lab usability study
- Timing: all
- Prior work: [110]

7.4 Discussion

This document contributes a guide that organizations can use to evaluate the usability of their privacy choice interfaces. First, it identifies seven high-level objectives that are aligned with the usability of privacy choice interfaces, based on the HCI and privacy choice literature. Next is an overview of research methods and study designs that could be utilized in evaluations of privacy choice interfaces. For each of the seven usability objectives, the document describes several evaluation guidelines utilizing these research methods as well as corresponding example measures and prompts.

These guidelines are intended to allow evaluators of privacy choice interfaces to uncover a breadth of potential usability issues. While organizations can apply these guidelines to a privacy choice interface that is already in use, ideally these guidelines would be incorporated into an iterative design process so that usability issues can be addressed prior to the interface being deployed. To evaluate privacy choice interfaces thoroughly, it is likely that multiple, complementary evaluations will be necessary utilizing different research methods and study protocols. At least one evaluation should be conducted with study participants interacting with the privacy choice interface in a realistic context, as this approach is most likely to mirror how users would interact with the interface once it is deployed. The data collected from this evaluation could be used to confirm potential usability issues identified through other approaches, such as through expert evaluation.

It is important to recognize that better design of privacy choice interfaces, particularly those that allow users to decline data sharing just as easily as to agree to it, may be at odds with revenue-generating goals of a company. Though mounting consumer pressure should encourage companies to better privacy practices, it is still unclear whether this will translate to better consumer privacy protection. Privacy choice requirements in new regulation, which include general requirements for usability, provide further incentive for companies to evaluate their privacy choice interfaces. While these guidelines could help organizations meet such usability requirements, and regulators to hold organizations accountable to better design practices, it is possible that interface designs that perform best in terms of meeting usability objectives (such as those that bundle certain privacy choices) would not be in full compliance with legal requirements in a particular jurisdiction. Conversely, it is likely that not all lawful designs of privacy choice interfaces would perform well in meeting the usability objectives described in these guidelines.

The evaluation guidelines listed in this document could also be used in contexts other than evaluating the usability of a single privacy choice interface. The same measures and prompts described could be applied in studies that compare multiple privacy choice interface designs to identify which design elements are beneficial or detrimental to different aspects of usability. As such, the evaluation guidelines provided are an initial step towards implementation guidelines that would standardize privacy choice interfaces for certain contexts. While adoption of new frameworks, including automated decision-making and standardized privacy choice interfaces,

are necessary to further reduce the burden of privacy-decision making from users, these guidelines provide immediately actionable guidance for organizations in how to improve consent and privacy choice interfaces for users.

Chapter 8

Applying the Evaluation Guidelines to Cookie Consent Interfaces

Chapter 7 proposed a comprehensive set of guidelines that can be used to evaluate privacy choice interfaces in different contexts. While these guidelines included example metrics and prompts for each high-level usability objective, it may be difficult for organizations that have less experience with usability testing to understand how to appropriately utilize them when evaluating their privacy choice interfaces. To demonstrate the application of the guidelines in a particular privacy choice context, we conducted a usability evaluation of cookie consent interfaces.

While the guidelines could have been demonstrated in other privacy decision-making contexts, we chose to focus on cookie consent notices for several reasons. First, interfaces related to the use of cookies are prevalent on websites and apps, particularly after a 2009 amendment to the EU's ePrivacy Directive [72]. These interfaces have become vital to organizations as they are used to meet legal requirements for notice and consent to data collection and processing under the GDPR and CCPA [42, 115]. As such, internet users encounter these interfaces daily. While existing privacy regulation stipulates that these interfaces be usable, there are no standards for usable cookie consent interfaces. As a result, organizations use a wide range of design practices in their implementations, some of which have been highlighted in prior work as dark patterns [60, 110]. Dark patterns — design practices that nudge users toward less privacy-protective options — within cookie consent interfaces could lead to users unknowingly consenting to data collection or failing to exercise their preferred privacy choices. Beyond dark patterns, it is important to consider other usability aspects of cookie consent interfaces, such as user awareness and comprehension of choices, as interfaces with poor usability could lead to privacy fatigue in users, described as "the tendency of consumers to disclose greater information over time when using more complex and less-usable privacy controls" [79].

We based our evaluation of cookie consent notices on those implemented through Consent Management Platforms (CMPs). These services have emerged to help organizations manage consent flows on their websites and apps in compliance with regulatory requirements. According to a report by the ad-tech company Kevel, approximately 52% of the top 10,000 US websites that serve ads have a CMP-implemented cookie consent interface, with five CMPs capturing the majority of the market share [83]. While some design aspects of the consent interface are standardized for each CMP, there are others that organizations can choose to customize for their

particular website or app. Considering the prevalence of CMPs and consolidation of the space into a handful of services, improvements in the usability of CMP-implemented cookie consent interfaces would have widespread impacts.

We conducted a two-stage evaluation to demonstrate the application of the guidelines provided in Chapter 7. This work builds on research by Utz et al [140] and Nouwens et al. [110] with a more comprehensive usability assessment of user interactions with consent interfaces. First, we conducted an inspection-based evaluation of 191 cookie consent interfaces implemented through five major CMP services, using an approach informed by three standard HCI methods: heuristic evaluation, cognitive walkthrough, and independent expert review [147]. We evaluated each interface for several dark pattern heuristics identified in prior work as well as other potential usability barriers. Our inspection-based evaluation yielded a list of design parameters that appear to be customizable through CMPs. In the second stage of our evaluation, we drew on our findings from our inspection-based evaluation to further investigate seven design parameters (listed in Section 8.2.1 of this chapter) that may impact the usability of consent notices. We conducted a between-subjects online experiment with 1,109 participants to evaluate the usability of 12 consent interface designs, utilizing the metrics and prompts provided in the evaluation guidelines. Participants in the experiment were asked to complete a shopping task on a prototype of a fictitious online retailer, where they encountered one of the consent interface design variants. Following task completion, participants answered survey questions related to the usability of the consent notice.

Our analysis of participants' interactions with the prototype website and survey responses highlighted significant differences in terms of usability between the design variants tested. We found that prominence of the consent interface impacted participants' awareness of available choices. Additionally, both the presentation of cookie consent choices as a link within the consent interface text as well as the inclusion of text highlighting negative outcomes of not allowing optional cookies appeared to impact participants' comprehension of which choices were being recommended by the website. Our results also indicate that the absence of in-line cookie options within the initial screen of the interface appeared to have reduced participants' investment in their consent decision.

This chapter makes the following contributions:

- Demonstration of the application of the evaluation guidelines provided in Chapter 7 to the domain of cookie consent interfaces.
- A summary of dark pattern heuristics identified in our inspection-based evaluation of cookie consent interfaces implemented through CMPs.
- Quantification of the usability impact of seven design parameters through a user study evaluation of 12 cookie consent interface designs.
- Identification of design choices that organizations could make, or that could be incorporated into a standardization effort, that would improve the usability of cookie consent interfaces.

8.1 Inspection-Based Evaluation of Cookie Consent Interfaces

As an initial step in our evaluation of design practices used in CMP-implemented cookie consent interfaces, we conducted an inspection-based evaluation of such interfaces across a wide range of websites. We developed a standardized procedure for our evaluation, informed by independent expert review, cognitive walkthrough, and heuristic evaluation approaches [147]. Utilizing the results of this expert review, we identified design parameters for consent interfaces that seem to be customizable through CMPs and may have an impact on usability.

8.1.1 Inspection Procedure

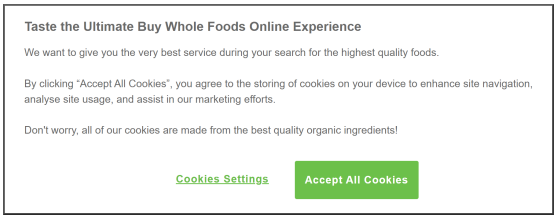
To conduct our inspection-based evaluation of CMP-implemented interfaces, we first identified five services that are in widespread use through a review of prior work in this space [69, 110]: Cookiebot, Crownpeak, OneTrust, QuantCast, and TrustArc. We built upon Nouwens et al.'s dataset of 680 popular UK websites [110] and compiled a diverse set of 932 websites that have consent interfaces that are implemented through these CMPs. To diversify our website sample, we developed a web scraper using webXray, a tool for analyzing webpage traffic [92], which looked for domain requests to any of the CMPs identified. We ran our scraper on 1,000 websites, randomly sampled from Tranco's list of top 10,000 global websites [88] (as of June 21, 2021) and stratified for web popularity. This yielded another 251 websites for our sample set of websites using CMP-implemented notices. We also referred to any reported client organizations included on each service's website, but only found one instance of a consent interface implemented through a CMP.

In total, we evaluated 191 websites drawn from our list of websites that contain a consent interface implemented through one of the five CMPs. We evaluated at least ten interfaces implemented through each CMP and attempted to identify distinct interface designs within the group of websites using each service, particularly which cookie options were provided, where and how they were presented to users, and the content of the interface text. Thus our sample includes a wide variety of interfaces but is not representative of the frequency with which each type of interface appears.

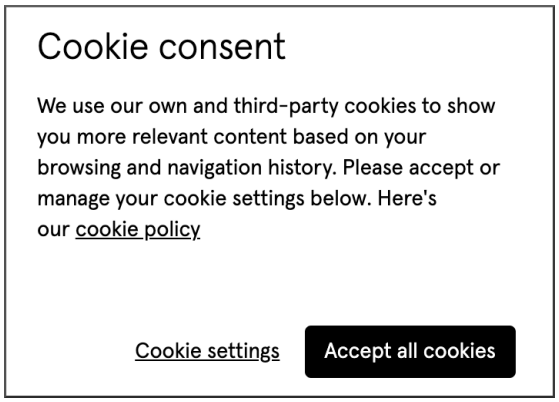
For each website, one member of the research team visited the desktop version of the website from a computer with a US-based IP address using private browsing mode to mitigate impact of the researcher's prior cookie consent decisions. The researcher first evaluated the interface based on a set of dark pattern heuristics identified in prior work, including design patterns that may lead to unintentional data disclosure or be considered illegal under the GDPR or CCPA [99, 110, 132]. Specifically they identified whether the consent interface:

- did not actually provide choices related to the use of cookies (see Figure 8.1a)
- used "confirmshaming' which is wording that guilts or shames users to influence their decision [15] (see Figure 8.1b)
- had unequal interaction paths for the most and least privacy-protective options (see Figure 8.1c)
- had default options that were not privacy-protective (see Figure 8.1d)
- had unintuitive placement of buttons for confirming users' cookie preferences and allowing all cookies (see Figure 8.1e)

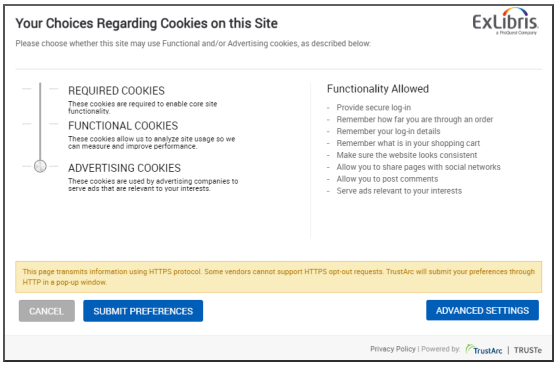
(a) Example of a cookie consent notice that does not provide users with actual choices related to cookies. The privacy policy simply describes the use of cookies.



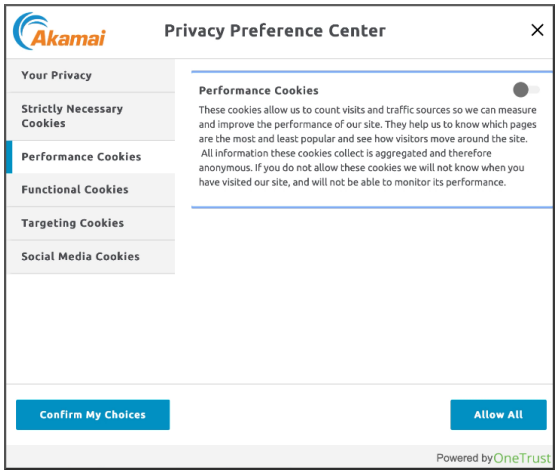
(b) Example of a type of confirmshaming where it is implied that users do not want "the very best service" or appreciate "the best quality organic ingredients" if all cookies are not accepted.



(c) Example of a consent notice where the option to "Accept all cookies" is a prominent button in the interface but more privacy-protective options are provided through a less conspicuous "Cookie settings" link.



(d) Example of a cookie preferences page within a consent interface where the default setting ("Advertising Cookies") is the least privacy-protective.



(e) Example of a cookie preferences page where the placement of the "Allow All" and "Confirm My Choices" buttons is confusing as save or submit buttons typically appear on the bottom right.

Figure 8.1: Examples of cookie consent interfaces found during our inspection-based evaluation for each dark pattern heuristic.

After evaluating the interface against these heuristics, the researcher conducted a cognitive walkthrough of the cookie consent interface by clicking on available options and links within the interface, observing any potential usability barriers. Finally, the researcher made any additional notes about aspects of the consent interface that may confuse users based on their knowledge of usability and dark patterns. The researcher's observations were recorded in a database, along with screenshots or screen recordings of the analyzed cookie consent interface.[1]

8.1.2 Inspection Evaluation Results

Dark pattern heuristics and other usability issues were prevalent in the CMP-implemented consent interfaces we evaluated. We then identified a list of ten design parameters that appear to be customizable through CMPs and may impact the usability of consent interfaces.

Summary of Dark Pattern Heuristics & Usability Barriers

As shown in Table 8.1, the vast majority of the consent interfaces (88.0%) reviewed exhibited a dark pattern heuristic. The most prevalent, observed on 150 (78.5%) websites, was having a simpler interaction path for less privacy-protective cookie options (i.e.,"accept all cookies") than for more privacy-protective options. Forty-nine (25.4%) of consent interfaces in our sample also had pre-selected or default options that were less protective of users' privacy than other available options. This dark pattern heuristic occurred relatively more frequently in consent interfaces implemented through OneTrust or TrustArc, but as our sample is not representative, this may or may not reflect trends across all websites using these CMPs.

Some consent interfaces also exhibited usability barriers, beyond potential dark patterns, that were uncovered during a cognitive walkthrough of the interfaces. One example was a consent interface that contained an "Options" button on the cookie options page that did not appear to do anything but dismiss the consent interface.[2] This would likely impact users' comprehension of the interface, as well as sentiment towards the company. Another interface contained a "Confirm My Choices" button within the cookie options page but no choices were actually present on the page.[3] The absence of choices on an interface where users would expect them to be present is highly likely to impact users' ability to effectively make decisions related to cookies on the website.

Design Parameters for CMP-Implemented interfaces

We used our recorded observations to compare consent interfaces implemented through the same CMP. In doing so, we identified design parameters that we hypothesized would have an impact on the usability of the consent interface and that appear to be customizable through CMPs. We enumerated ten such parameters related to specific components of the cookie consent interface (such as the interface text or interface buttons) or the user interactions involved in the consent decision, as well as possible implementations of the parameter that we observed (listed in Table 8.2).

[1]The database of our observations is available at `https://airtable.com/shrnbTJ0ZIPl9OMm6`.
[2]This particular consent interface was on `friday-ad.co.uk` and implemented through Quantcast.
[3]This particular consent interface was on `sketchup.com` and implemented through OneTrust.

CMP (n)	Unequal paths	"Bad" defaults	Confusing buttons	No choices	Confirmshaming	Other barriers	None
OneTrust (70)	60	33	21	4	1	5	6
Quantcast (69)	55	0	0	7	1	1	7
CookieBot (20)	9	5	0	2	0	5	8
TrustArc (19)	14	9	0	2	1	0	2
CrownPeak (13)	12	2	1	2	0	1	0
	150	**49**	**22**	**17**	**3**	**12**	**23**

Table 8.1: Counts of the dark pattern heuristics and other usability barriers identified during our inspection-based evaluation of consent interfaces implemented through five CMP services. (n = number of consent interfaces evaluated for a particular CMP)

8.2 User Study Evaluation of Consent Interface Designs

To further investigate the usability impact of design choices that organizations can make when implementing their cookie consent interfaces, we conducted a large-scale online user study in which 1,109 participants were each randomly assigned to visit and interact with a fictitious e-commerce website implementing one of 12 cookie consent design variants.

8.2.1 User Study Design

We enumerated possible design choices for each design parameter we identified through our inspection-based evaluation of consent interfaces in Table 8.2 based on the practices we observed in the design of the consent interfaces we looked at in our inspection-based evaluation. As it was infeasible to study all of the possible design choices, we ranked the design parameters according to what was likely to have the most impact on usability and prioritized design choices for which there has not yet been much research or established best practice in UX design. Along these criteria, we decided not to explore the placement of button options within the consent interface (for which there are established best practices [52]) and the granularity of choices offered (for which there has been prior research that shows that users may be overwhelmed by having too many choices [14]). Similarly, we did not include a study variable explicitly exploring the number of clicks required to reach a choices interface from the initial screen of the consent notice, as prior research has shown that choices are most usable when presented on the initial screen of the interface [110]. Our study also did not explore accessibility issues, such as those related to color contrast and size of button components within the interface, which also have established guidelines [142].

The remaining seven design parameters corresponded to variables in our study. We developed the following hypotheses for these variables:

H1. *Prominence of the consent interface*: User awareness of cookie consent options would be better for a fully-blocking consent interface (i.e., "consent wall"), compared to a non-blocking consent banner or "Cookie Preferences" button at the bottom of a webpage (a design option for OneTrust).

H2. *Path to a cookie options interface*: User awareness of cookie consent options would be better for "in-line" cookie options provided on the initial screen of the interface (a design

Design Parameter	Possible Implementations	Usability Objective(s)
Prominence of the consent interface	persistent "Cookie Preferences" button, non-blocking banner, consent wall	User awareness
Path leading to a cookie options interface (where options to allow/deny cookies are presented)	link embedded in text, equally weighted interface button, in-line options in initial screen	User awareness
How/whether the notice text described the presence of choices	loss aversion text present, text mentions that options are available	User awareness, User sentiment
Readability of the notice	fonts, colors, contrasts, text layout (bulleted vs. paragraph)	User comprehension
Text within button options	generic ("Okay," "Submit"), detailed ("Allow selected cookies," "Allow all cookies")	User comprehension
Placement of button options	"Allow all" option shifts with user actions, "All all" remains in place	User ability & effort
Format of choices interface	choices separated in multiple tabs, all choices on same page	User ability & effort
The number of clicks required to reach the choices interface from the notice	2 or more clicks, 1 click, no clicks (in-line options)	User ability & effort
The granularity of choices offered	cookie-level, category-level	User ability & effort
The process for changing or revoking a consent decision	none (clear browser cookies), link in cookie policy, persistent "Cookie Preferences" button	Decision reversal

Table 8.2: List of design parameters that appear to be customizable through CMPs, possible implementations for each (in order of the least to best option for usability based on our expert knowledge), and the corresponding usability objectives that we hypothesized could be impacted.

option for CookieBot), compared to a link to a cookie choices page embedded within the text of the interface or a button leading to a choices page.

H3. *Loss aversion framing describing the presence of choices:* The presence of text highlighting negative outcomes of not accepting optional cookies would exploit a cognitive bias called loss aversion, where people prefer to avoid a loss compared to gaining something equivalent, creating a nudging effect towards accepting all cookies and impacting user sentiment.

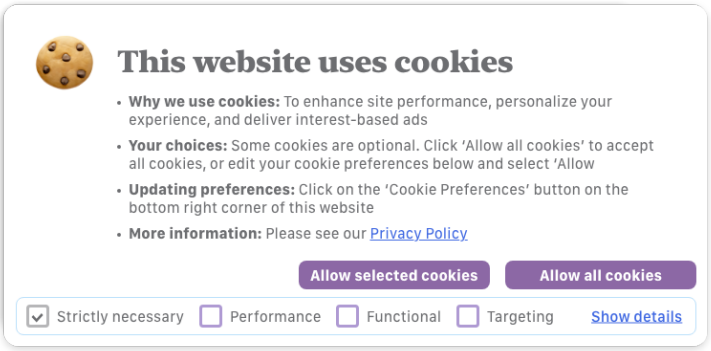
H4. *Layout of the notice text:* User comprehension of the cookie consent decision would be better for a bulleted format of the text, compared to paragraph format.

H5. *Text within button options:* User comprehension of the cookie consent decision would be better if the button options detailed the action of the button (i.e., "Allow selected cookies" and "Allow all cookies"), compared to more generic text (i.e.,"Submit" and "Okay").

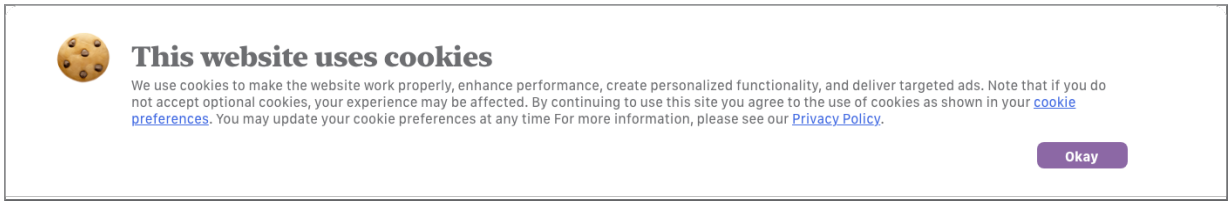
H6. *Layout of cookie choices page:* A cookie choices page with all options on one screen (i.e., "single-page" layout), would make it easier for users to change choices with less effort, compared to a choices page comprised of tabs for different categories of cookies used on the website (i.e., "multi-page" layout).

H7. *Process for changing or revoking a consent decision:*

(a) Decision reversal would be better facilitated by a persistent "Cookie Preferences" (a design option for OneTrust), compared to a website's cookie and privacy policy.



(a) "Best practices" cookie consent interface design variant used as a baseline for comparison which incorporated the design choices that we considered as most privacy-protective or beneficial to usability.

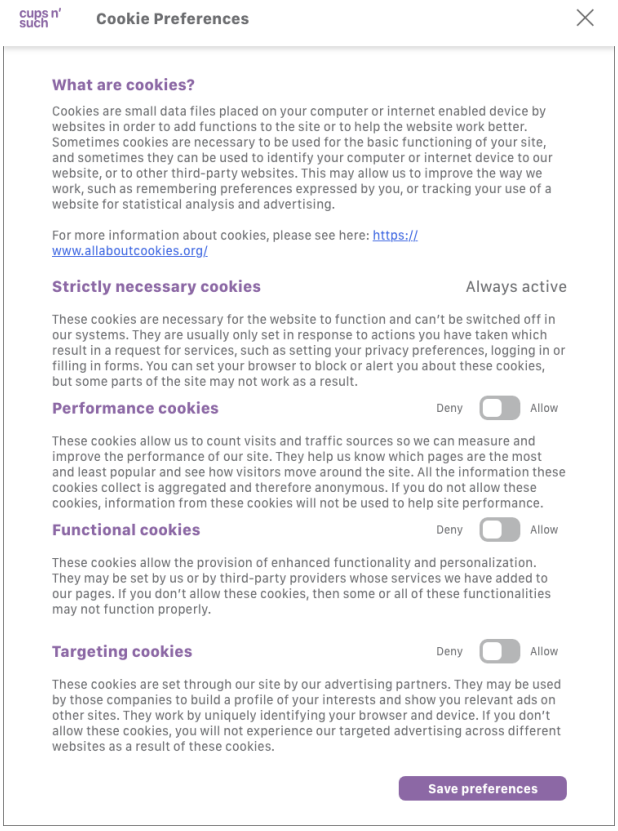


(b) "Worst practices" cookie consent interface design variant which incorporated the design choices that we considered as least privacy-protective or most detrimental to usability.

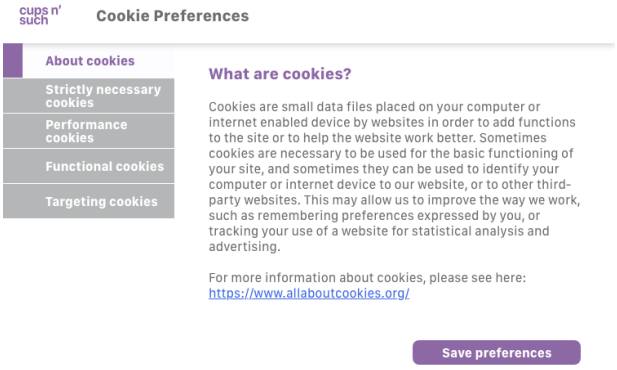
Figure 8.2: Two consent interface design variants that demonstrate the design choices for each parameter explored in our study.

(b) Decision reversal would be better facilitated if the process for changing or revoking a consent decision is stated in the notice text.

We developed 12 design variants of cookie consent interfaces to explore our study variables and test our stated hypotheses. So that we could isolate the effect of each design choice, one design variant was composed of what we considered as "best practices": what we hypothesized as the most privacy-protective or usable options for each study variable (see Figure 8.2a). Ten of the design variants manipulated just one study variable such that they differed from the "best practices" baseline in only one aspect of the interface design. A twelfth design variant explored the combination of design choices that we considered were the least privacy-protective or usable, which we refer to as "worst practices" (see Figure 8.2b). The design variants included a link to a single-layer "Cookie Preferences" page (shown in Figure 8.3a) or a multi-layer version of the page (Figure 8.3b), which included information about cookies and four different cookie categories (strictly necessary, performance, functional, and targeting) as well as toggles to enable/disable the later three categories. Table 8.3 provides an overview of the design variants explored in our study and their values for the seven study variables.



(a) Single-layer "Cookie Preferences" interface linked from the cookie consent interface in ten of the design variants.



(b) Multi-layer "Cookie Preferences" interface linked from the cookie consent interface in the *layout-multilayer* and *worst-practices* design variants.

Figure 8.3: The two styles of the"Cookie Preferences" linked through the cookie consent interface design variants explored in our study.

Condition Name	Interface Prominence	Options Path	Loss Aversion	Text Layout	Button Text	Choices Layout	Decision Reversal
best-practices	fully-blocking	in-line	absent	bulleted	detailed	single-page	persistent button
prominence-cornerButton	non-blocking button	n/a	n/a	n/a	n/a	single-page	persistent button
prominence-banner	non-blocking banner	in-line	absent	bulleted	detailed	single-page	persistent button
options-embeddedLink	fully-blocking	embedded link	absent	bulleted	detailed	single-page	persistent button
options-interfaceButton	fully-blocking	interface button	absent	bulleted	detailed	single-page	persistent button
text-lossAversion	fully-blocking	in-line	present	bulleted	detailed	single-page	persistent button
text-layoutParagraph	fully-blocking	in-line	absent	paragraph	detailed	single-page	persistent button
button-generic	fully-blocking	in-line	absent	bulleted	generic	single-page	persistent button
layout-multilayer	fully-blocking	in-line	absent	bulleted	detailed	multi-page	persistent button
reversal-noInstructions	fully-blocking	in-line	absent	bulleted	detailed	single-page	no instructions (button present)
reversal-cookiePolicy	fully-blocking	in-line	absent	bulleted	detailed	single-page	cookie policy
worst-practices	non-blocking banner	embedded link	present	paragraph	generic	multi-page	no instructions (cookie policy)

Table 8.3: Overview of the 12 cookie consent interface design variants and their values for the seven design parameters explored in our online experiment.

8.2.2 User Study Data Collection & Analysis

Experimental Protocol

We conducted an online experiment utilizing a between-subjects protocol to test our hypotheses. To explore the impact of the different design parameters in a realistic context, we presented our consent notice designs in the context of a fictitious e-commerce website that sold cups, mugs, and other drinkware. We implemented the parts of an e-commerce website relevant to the cookie consent experience or basic shopping functionality, including a cookie consent interface (varied per condition), privacy policy, cookie policy, product catalog, and product detail pages using Adobe XD. We implemented the prototypes only in a desktop version of a website to maximize the chances of participants being able to read and interact with the consent notice. In order to capture participants' interactions with the website as well as timing data, we utilized a usability testing platform called Useberry. After completing the study consent form and verifying their eligibility, participants in our study were assigned one of the study conditions at random and directed to Useberry. To prevent participants from overly fixating on the consent notice, participants were give a distraction task — to add a product from the store catalog to their cart. Participants were instructed to interact with the prototype as they would a real website and perform whatever action they would take the first time they visited a real e-commerce website. After the initial instruction screens, participants were exposed to a cookie consent interface design according to their assigned condition. Once participants completed the study task, or indicated that they give up on the task, they were directed to a follow-up survey implemented on Qualtrics.

The survey (provided in Appendix **??**) included questions for evaluating the different high-level usability objectives provided in the evaluation guidelines described in Chapter 7. Partici-

pants first answered questions related to user awareness and unfocused comprehension based on their recall of the consent notice. After completing this portion of the survey, participants were provided an opportunity to refer back to the consent interface and prototype of the e-commerce website as they answered additional questions.

Our protocol was approved by our university's Institutional Review Board. While participants consented to their interactions with the prototype website being captured, we did not collect any personal information from participants.

Participant Recruitment

To prevent priming potential participants, we described the study as a study requesting feedback about an e-commerce website. As cookie consent interfaces and users' experiences with them may differ across legal jurisdictions, we only recruited US-based participants. Additionally, participants were required to be over 18 years old, fluent in English, and have access to a tablet or computer to complete the study (to properly render the prototypes). Median completion time for our study was 15 minutes and 48 seconds, and participants were compensated $5.00.

Based on a power analysis for our planned statistical tests, at least 66 participants per condition (786 participants total) would be needed to detect a moderate effect size with at least 80% power. In total, 1,316 participants from Prolific completed our study between July 28 and July 30, 2021.

Data Analysis

Our analysis includes data from 1,109 participants. We did not include responses from 127 participants who were inadvertently exposed to two different versions of our consent notice due to a technical issue with Useberry prior to completing the survey.[4] We also removed responses from 42 participants who were detected using a mobile device by Useberry, as our prototypes were designed for tablet or desktop viewing. Last, we removed 38 participant responses for which a valid Useberry session (sessions in which we could confirm participants saw a consent notice either through successful task completion or reviewing their interaction data) was not recorded. A few participants completed the study twice, so we retained only their first submission.

We analyzed user interaction and timing metrics collected through Useberry, as well as participants' survey responses. Since Useberry could not be configured to record participants' exact consent decision in a format appropriate for such large-scale analysis, we analyzed participants' self-reported consent decision from the survey. Participants first indicated which cookie options they selected in the recall portion of the survey, and answered the same question after reviewing the consent interface. A researcher reviewed a recording of a participant's interactions with the prototype captured by Useberry to verify their consent decision if there was a discrepancy in their response to these two questions, or if they indicated selecting an unavailable option (i.e., "Allow social media cookies" or "Allow no cookies"). Approximately 20% of participants' consent decisions were reviewed in this manner.

[4]Due to the same technical issue with Useberry, another 342 Prolific workers attempted to participate in our study but were unable to complete it. These participants were compensated $1.00 for their time.

Gender		Age (Years)		Race/Ethnicity		Education		Income		Tech Expertise	
Agender	0.45%	18-24	64.9%	Am. Indian/Alaska Native	1.0%	High school or less	15.0%	<$10k	8.6%	Yes	17.0%
Female	79.8%	25-34	26.3%	Asian	8.7%	Some college	30.7%	$10k to $49,999	31.2%	No	83.0%
Male	15.1%	35-44	5.6%	Black	5.1%	Associates/Bachelors	40.7%	$50k to $99,999	29.5%		
Non-binary/Genderqueer	4.1%	45-54	2.4%	Hispanic/Latinx	3.2%	Graduate/Professional	13.6%	$100k to $149,999	14.5%		
Self-described	0.36%	55-64	0.63%	Hawaiian/Pacific Islander	0.26%	No response	0.09%	$\geq$ $150k	9.8%		
No response	0.27%	>65	0.0%	White	79.7%			No response	6.4%		
		No response	0.45%	Self-described	1.1%						
				No response	1.1%						

Table 8.4: Summary of participant demographics. Participants were allowed to select multiple options for race/ethnicity so percentages are greater than 100. Those who reported having a formal education or work experience in a computer-related field were counted as technical experts.

In our reporting of statistics, we include both p-values and an effect size for the appropriate statistical test. Since our study was powered to detect at least moderate effect sizes with at least 80% for our planned analysis, we note any significant results for which a smaller effect size was observed. P-values from any post-hoc pairwise comparisons were adjusted with a Bonferonni correction to be able to correct for additional comparisons with categorical data. We conducted a thematic analysis of qualitative survey questions. One member of the research team developed an initial codebook based on a subset of 10% of responses drawn at random. Two researchers then independently coded another random subset of 20% of the data, achieving a Cohen's κ inter-rater agreement of 0.84 (averaged over all questions), which is considered as high agreement [**?**]. Any conflicts in the coding were resolved and the codebook was accordingly modified in collaboration. The remaining survey responses were coded by a single researcher using the modified codebook.

8.2.3 Participant Demographics

Table 8.4 provides a demographics summary of our study population. While our participant sample was diverse, it was not representative of the US population, skewing more female, white, and younger than the general population [138]. It is likely that our study was impacted by an influx of new registrations on Prolic by young females that occurred in July 2021 due to a viral video on TikTok [21]. We report on the impact of age and gender in our analysis of participants' consent decision, awareness of available cookie options, comprehension of the interface, and investment in decision-making. The vast majority of our participants (85.8%) reported shopping online at least once a month, and only four participants indicated that they never shop online. This suggests that participants in our sample likely had prior experiences with websites similar to our prototype which may have influenced their interactions during our study.

8.2.4 User Study Results

Our study results highlight that several design parameters that we explored significantly impacted the usability of consent interfaces. We found that the absence of in-line options within the initial screen of the interface impacted participants' consent decision, comprehension of available cookie options, as well as sentiment toward the consent interface. Additionally, we observed that awareness of available cookie options was impacted by the prominence of the consent interface

and that the presence of loss aversion text in the notice influenced participants' comprehension of which cookie options were being recommended. Furthermore, a persistent "Cookie Preferences" button improved participants' ability to change their initial consent decision.

User Needs

The majority (72.7%) of our participants who made a consent decision selected the "Allow all cookies" option in the interface, 24.4% selected "Allow only strictly necessary cookies," and another 2.9% allowed some custom combination of strictly necessary, performance, functional, or targeting cookies. As shown in Figure 8.4, participants' cookie consent decision significantly differed across conditions ($p < 0.001$, $V = 0.29$). Participants in all four conditions that did not include in-line options were significantly more likely to consent to all cookies, compared those in *best-practices*. We did not observe significant impact of age or gender on participants' consent decision.

About half of participants who selected "Allow all cookies" (50.2%) described that their goal was to dismiss the consent notice (e.g., "I wanted to get that pop up off my screen so I could browse the site"), suggesting that participants may have become habituated into clicking this option when available. Others who allowed all cookies described more specific goals, such as enabling specific features of the website (e.g.,"Ease of use when I return to the website in remembering my information"), allowing for full functionality of the website (e.g., "To gain full access to the website and all its features"), or improving the performance of the website (e.g.,"For the website to run as smooth as possible"). In contrast, the majority of those who only allowed strictly necessary cookies (57.9%) described privacy-related goals, including limiting the amount of personal data that is collected (e.g., "Bare minimum private information collected") or web tracking that may occur which could lead to targeted ads ("I don't want my actions to be tracked unnecessarily, especially for targeting ads."). Some participants who selected this option expressed that they wanted to limit the number of cookies because of an incomplete understanding of web cookies (e.g.,"I do not really understand cookies, but I think that they clog up your computer so I wanted to avoid this."). These results highlight the importance of providing cookie options that align with specific goals.

In assessing user needs related to the consent interface, we also asked participants to describe what, if any, additional options related to cookies they would like have. While the majority of participants did not articulate any additional choices they would like to have, most commonly participants suggested providing an option for denying all cookies (which would be infeasible for an e-commerce website given current web technology). Others suggested providing "cookie options" for other privacy or security-related features (e.g., "Cookies that will help keep passwords and logins safe."), or an option for cookies not to persist beyond the browsing session (e.g., "Option to clear cookies when done browsing"). In lieu of additional options, some participants desired additional information, such as definitions for the term cookies and different cookie categories or how the website would behave if not all cookies were allowed.

User Ability & Effort

In the survey participants were provided an opportunity to review the consent notice again and were explicitly asked to select what their preferred consent decision would be for the website. In their response, 40.1% indicated they would want to allow all cookies, 29.7% preferred to allow only strictly necessary cookies, 25.2% indicated a custom combination of cookie categories, and 5.1% preferred that the website not use any cookies at all. There was no significant difference between conditions in participants' preferred consent decision. Excluding participants who reported that they would prefer not to allow any cookies (a preference that could not be selected in any condition), only about half of participants (52.6%) actually selected their preferred consent decision during their interactions with the website. A Pearson's chi-squared test found that this significantly differed across conditions ($p = 0.04$, $V = 0.14$), but no conditions were significantly different from *best-practices* in pairwise comparisons. However, the majority of participants (74.0%) felt that it was very easy or somewhat easy to make their preferred consent decision, which did not significantly differ across conditions. Taken together, these results suggest that while most users didn't find it difficult to use any of the consent interfaces, only about half bothered to use the interface to make their preferred decision, regardless of interface variant.

Participants spent an average of 1 minute and 28 seconds with 9.1 clicks to complete the study task (i.e., adding a product to the shopping cart), which was not found to significantly differ across conditions. This suggests that the effort required to complete a consent decision was similar across conditions. In our analysis of participants' interactions with the prototype website, we observed that 24.0% of participants in *worst-practices* and 19.8% of participants in *prominence-nonblockingBanner* went directly to the catalog without making a consent decision. No participants in *prominence-cornerButton* were observed indicating their cookie preferences at any point during their interactions with the website. This implies that a substantial portion of users are likely not to indicate their cookie preferences if not blocked from using other parts of the website.

Beyond making a consent decision with a button option, we observed 99 additional interactions with other components of the cookie consent interface, seven interactions with one of the links to the website's privacy policy (located within the consent interface or in the footer of the website), and no interactions with the website's cookie policy. Figure 8.5 provides a summary of participants' engagement with cookie-related options, which we observed appeared to impacted by our some of our study variables. Fewer participants made changes to the toggles corresponding to different cookie categories in the single-page options layout of the cookie choices interface in *options-interfaceButton* than in the multi-page layout in *layout-multilayer*, suggesting that the increased effort required to change choices in the multi-layer design may have deterred participants from exercising available options. However, this difference was not found to be statistically significant.

User Awareness

About two-thirds of participants (66.6%) recalled making a privacy decision on the prototype website, nearly all of whom remembered it being about the use of cookies on the website. A Fisher's exact test found that recall of making a privacy decision significantly differed across

conditions ($p < 0.001$, Cramer's V = 0.37), with participants in the *prominence-cornerButton* and *worst-practices* conditions reporting significantly less awareness of a privacy decision in follow-up pairwise comparisons compared to those assigned to *best-practices*. Three-quarters of participants in *best-practices* recalled making a privacy decision, compared to half of *worst-practices* participants and only 2.9% of *prominence-cornerButton* participants.

In their recall of options related to specific categories of cookies, participants correctly recalled between three and four categories out of seven listed (two of which were not actually available on the website). A Kruskal-Wallis test found that participants' recall of the options related to specific cookie categories was significantly different across conditions but with a small effect size ($p < 0.001, \eta = 0.053$). Similar to recall of making a privacy decision, participants in *prominence-cornerButton* (2.7 options correct on average) and *worst-practices* (2.8 correct) had significantly worse recall of available cookies options, compared to those in *best-practices* (3.5 correct) – not surprising as it appears that none of the participants in this condition made a cookie consent selection and likely did not even view the options. Kruskal-Wallis tests found that recall of cookie options was also significantly impacted by age ($p = 0.005$, η =.006) and gender ($p < 0.001$, $\eta = 0.010$) though with small effect sizes. Those aged 35 and older had better recall of available options (3.6 correct) than those younger 35 (3.2 correct). Compared to females (3.2 correct), males were found to have significantly better recall (3.6 correct).

Our analysis of interactions with the website prototype (reported in Figure 8.5) also provides evidence that user awareness of cookie options was impacted by our study variables. While the "Cookie Preferences" button in the bottom corner of the webpage was used in almost all of the other design variants, it seemed to go ignored in *prominence-cornerButton*, suggesting that a fully-blocking or banner-style consent notice led to greater awareness of available cookie choices. Though participants engaged with the "Edit cookie preferences" button in *options-interfaceButton* relatively more than the in-line options in *best-practices*, a smaller percentage of participants in *options-embeddedLink* clicked on the link within the text to the cookie choices interface. While this suggests that the embedded link was not prominent and contributed to lower user awareness of choices, these differences were not found to be statistically significant.

User Comprehension

To gauge participants' comprehension of their cookie-related choices, the survey included five multiple-choice questions in which participants were asked to select the correct definitions for the term "cookies" (in the context of the internet) and each of the four cookie categories included in the interface. On average, participants correctly answered between two and three questions, based on their recall of the website and consent interface when their attention likely was not focused on available cookie choices. Participants' unfocused comprehension was not found to significantly differ across conditions. Less than half of participants (47.6%) selected the correct definition for "performance cookies" and only 16.0% selected the correct answer for "functional cookies," suggesting that these two labels for cookie categories are not very intuitive. Most commonly, participants thought functional cookies were those that were needed for the website to work properly – the correct definition for "strictly necessary cookies." Kruskal-Wallis tests did find significant differences with small effect sizes by age ($p = 0.01$, $\eta = 0.005$), as well as gender ($p < 0.001$, $\eta = 0.01$). Those younger than 35 correctly answered 2.7 questions, compared to

3.1 questions for those 35 and older, while females answered 2.6 questions correctly on average, compared to 3.1 questions for males.

A Friedman test found a significant improvement in comprehension ($p < 0.001$, Kendall's W = 0.59) by about one question when participants answered the same five comprehension questions again after being able to review the consent interface. Unlike participants' unfocused comprehension, there was a significant difference across conditions in focused comprehension ($p < 0.001, \eta = 0.08$). Compared to those in *best-practices*, participants in *options-embeddedLink*, *options-interfaceButton*, and *layout-multilayer* answered more of the comprehension questions correctly after reviewing the consent interface. This may be because participants in these conditions were not exposed to the different cookie category terms through in-line options and instead saw them on the Cookie Preferences page where they were defined. When asked which aspects of the consent interface they referred to when answering the survey questions, a larger percentage of participants in these conditions did report referring to the Cookie Preferences page, compared to those in *best-practices*. While there was not a significant difference by gender in focused comprehension, a Kruskal-Wallis test did find a significant impact of age with a small effect ($p < 0.001$, $\eta = 0.01$). Unlike unfocused comprehension, those younger than 35 exhibited better comprehension than older participants, answering 3.7 questions correctly compared to 3.3.

After reviewing the consent interface, participants were asked how easy or difficult they thought the consent interface was to understand. Over two-thirds (68.0%) reported that it was somewhat easy or very easy to understand, which was was not significantly different across conditions. The survey also asked participants about their comprehension of which cookie consent option was being recommended by the interface, reported in Figure 8.6. A Pearson's chi-squared test did find that participants' interpretations did significantly differ across conditions ($p < 0.001$, V = 0.15). The majority of participants in *worst-practices* (60.0%) and *options-embeddedLink* (50.0%) thought that the interface was recommending to allow all cookies, compared to only 38.6% of those in *best-practices*, highlighting the impact of the absence of an equally weighted interface button leading or corresponding to other possible cookie options. The majority of participants in *text-lossAversion* (51.7%) also thought that the website was recommending to allow all cookies, indicating a possible outcome of including such text in the consent interface.

Participants were also asked to indicate the likelihood of five different scenarios if a cookie consent decision was not made on the website. The most common expectations were "all cookies would be allowed and the entire website would still work" and "no cookies would be allowed by some parts of the website would still work," rated as "probably yes" or "definitely yes" by 68.3% and 56.0% of participants respectively. This highlights that ambiguity that exists in current implementations of cookie consent interfaces, as both of these scenarios are technically feasible. Pearson's chi-squared tests found that expectations for both scenarios significantly differed across conditions (p = 0.02, V = 0.13 and p = 0.003, V = 0.14 respectively) but in follow-up pairwise comparisons no conditions significantly differed from *best-practices*.

User Sentiment

To gauge participants' level of investment in making a cookie consent decision, we asked participants who indicated that they made a consent decision on the prototype website two multiple-

choice questions and one Likert scale question related to their decision-making process. Pearson chi-squared tests found that there was a significant different across conditions in participants' strategies for selecting their cookie preferences ($p < 0.001$, V = 0.18), as well as their engagement with the interface text ($p < 0.001$, V = 0.23). Similarly, a Kruskal-Wallis test found that participants' ratings for how carefully they made their consent decision also differed across conditions but with a small effect size ($p < 0.001$, $\eta = 0.051$). Significantly more participants in *options-embededLink* (83.3%, p.adj = 0.006) reported choosing the "easiest option" when making their consent decision and were more likely to report that they made their decision "not at all carefully" (73.4%, p.adj = 0.04), compared to participants in *best-practices* (55.7% and 46.6% respectively reported the same). Similarly, significantly more participants in *worst-practices* than *best-practices* made their decision "not at all carefully" (75.6%, p.adj = 0.01) and reported skipping over the interface text (59.0%, p.adj = 0.001). Those in *layout-multilayer* were also significantly more likely to report choosing the "easiest option" (80.7%, p.adj = 0.04). This suggests that the absence of in-line options within the initial screen of the consent interface may have reduced participants' investment in their consent decision.

Pearson chi-squared tests and a Kruskal-Wallis test comparing responses to these three questions also revealed significant differences in decision-making investment with age and gender. Compared to those 35 years or older, younger participants were more likely to report choosing the "easiest option" ($p < 0.001$, V = 0.16), skipping over the notice text (p = 0.001, V = 0.11), and making their decision "not at all carefully" ($p < .001$, $\eta = 0.051$ [small effect]). Relative to males, females reported less investment in their decision-making, being more likely to choose the "easiest option" ($p < 0.001$, V = 0.20), skipping over the notice text (p = 0.002, V = 0.10), and making their decision "not at all carefully" ($p < 0.001$, $\eta = .065$).

Participants also answered several questions to assess their subjective knowledge related to the consent interface. Across all conditions, 92.2% felt "moderately" or "extremely" informed about their choices related to cookies. A Kruskal-Wallis test found that there was an overall difference between conditions with a small effect size ($p < 0.001, \eta = 0.026$), but in follow-up pairwise comparisons no significant differences were found between *best-practices* and other conditions. Similarly, 95.3% reported feeling "moderately" or "extremely" capable of making a cookie decision, which did not significantly differ across conditions. A smaller percentage (79.5%) of those who made a consent decision were "moderately" or "extremely" confident that their consent decision was the right choice for them, which also did not significantly differ across conditions. This supports that there was some degree of misalignment between participants' actual consent decisions and their preferred decisions.

We also asked participants several questions related to other aspects of user sentiment toward the consent interface. Overall, 92.2% of participants felt "moderately" or "extremely" informed about data collected by cookies on the website. While a Kruskal-Wallis test found that there was an overall difference between conditions with a small effect size ($p < 0.001, \eta = 0.039$), no conditions were found to be significantly different from *best-practices* in post-hoc comparisons. The overwhelming majority of participants (93.8%) also reported feeling that the interface provided the cookie choices that they wanted, which was not found be be significant across study conditions. Compared to their perceptions of transparency and control, participants reported slightly lower levels of comfort and trust in their actual consent decisions; 80.0% were "moderately" or "extremely" comfortable about the use of cookies on the website given their consent decision

and 83.4% were "moderately" or "extremely" trustful that their cookie consent decision would be honored by the website. These sentiments were also not found to differ significantly across conditions suggesting that there may be some aspect of the consent process overall rather than a particular aspect of the interface design that is impacting user sentiment.

Decision Reversal

A Pearson's chi-squared test found that participants in the *best-practice* condition that contained a persistent "Cookie Preferences" button in the bottom right corner of the page were significantly more likely than those in *reversal-cookiePolicy* which did not contain this button to recognize a correct method to change their initial cookie consent decision ($p = 0.001$, $V = 0.28$). The vast majority (81.8%) of *best-practices* participants stated that they would use this button to change their decision, while 45.3% of participants in *reversal-cookiePolicy* stated they would visit the website's cookie policy (as instructed in the notice text). We found that the presence of reversal instructions did not have a significant impact on participants' ability to reverse their initial consent decision.

When asked how they would reverse their preferences if there was no "Cookie Preferences" button, only 16.1% of participants in the conditions that contained this button described an effective alternative method for revising their consent decision for the website, such as the website's privacy or cookie policy, deleting browser cookies, using a different browser or device, or visiting the website in private browsing mode. This suggests that after being exposed to the "Cookie Preferences" button its absence had a much greater impact than if participants had not seen it at all. Along these lines, 42.2% said that they would give up trying to change their consent preferences or just leave the website. Over a fifth (22.9%) described other strategies that could potentially lead them to a correct decision reversal path, such as changing browser settings, looking through the settings or other parts of the website, contacting the website, or searching for instructions using a search engine. A small portion of participants (10.4%) described an incorrect strategy such as refreshing the page or revisiting it in another tab, and another 6.3% were not sure what they would do to reverse their consent decision.

8.3 Discussion

In this section, we first describe limitations of our evaluation of cookie consent interfaces. We then discuss nudging patterns with regards to our consent interface designs, the final aspect of the evaluation guidelines described in Chapter 7 and revisit our initial hypotheses for the design parameters we evaluated. Last we compare the inspection-based and user study evaluation approaches used in this study.

8.3.1 Limitations

While our study provides valuable insights into the usability of consent notices, it is not without its limitations. Our inspection-based evaluation of consent notices was based on those implemented by CMPs which yielded a list of ten design parameters. It is possible that consent

notices that are not implemented through CMPs incorporate other design parameters that were not uncovered in our inspection-based evaluation. Furthermore, our user study only explored a subset of the identified design parameters and implementations corresponding to these parameters. Though prior research and best practices exist with regard to the three parameters we did not include (placement of button options, number of clicks required to reach the cookie choices interface, and granularity of the choices offered), these should be further explored in the context of cookie consent interfaces. Our study also did not evaluate the accessibility of cookie consent interfaces, which should be implemented according to standardized accessibility guidelines to ensure that they are usable by a larger population of internet users [142].

Though our user study evaluated our cookie consent interface designs in a realistic context, participants were aware that they were interacting with a prototype website through Useberry which may have impacted their interactions and impressions of the consent interface. Additionally, while Useberry allowed us to capture interaction data related to the time and number of clicks participants spent on the study task, we were unable to analyze these metrics specifically for the consent interface. Considering that no participants in the *prominence-cornerButton* condition indicated their cookie preferences and that the time and click metrics captured did not significantly differ across conditions, it is reasonable to assume that none of our design variants required significantly more effort for users to make a consent decision.

Our results may also be impacted by the relatively poor gender and age diversity of our user study sample. While we did not find that gender or age significantly impacted participants' consent decision, we did observe differences in user awareness, comprehension, and sentiment. Female-identifying participants and those under the age of 35 had less awareness and comprehension of available cookie options and were less invested in their decision-making, on average, compared to male-identifying participants or those older than 35. Technical literacy more generally is likely to differ with gender and age, as 10.5% of females under 35 in our study sample reported having a degree or working in a computer-related field, compared to 78.7% of males older than 35. Given that our sample was dominated by participants with less investment in in their decision-making and lower comprehension of available cookie options, we expect we may have failed to detect some differences in conditions that might be detectable in a more representative study. Future work evaluating the usability of consent interfaces should be conducted with a study population that is more representative of the internet population overall.

8.3.2 Evaluating for Dark Patterns

Next we apply the guidelines provided in Section 7.3.7 to evaluate our consent interface designs for the presence and impact of dark patterns.

Alignment With Regulatory Objectives

Our inspection-based evaluation confirms the work of Nowens et al. and Soe et al. which found that the majority of consent interfaces users interact with may not meet the requirements of GDPR [110, 132]. None of the cookie consent design variants explored in our study, including *best-practices*, completely meet the design criteria this prior work has proposed for meeting GDPR requirements. Our results suggest that non-blocking cookie consent interfaces, such

as those tested in our *prominence-cornerButton*, *prominence-banner*, and *worst-practices* conditions, would not immediately meet requirements for consent to be explicit since many participants in those conditions did not make a consent decision during their interaction with the website. In order to satisfy this requirement with a non-blocking interface, a website or app would need to be implemented in such a way that data collection did not occur until the user made a consent decision. While the three design variants that did not include in-line options — *options-embeddedLink*, *options-interfaceButton*, and *worst-practices* — did not require significantly more effort to make a consent decision, refusing consent to all cookies appeared to require more effort than consenting to all cookies as significantly more participants in those conditions consented to all cookies compared to *best-practices*. None of our design variants explored a label for the option allowing only strictly necessary cookies that was the exact antonym of "Allow all cookies" (such as "Deny optional cookies") which is recommended practice to make it easy for users to deny consent for some purposes but not others [132]. However, considering our *best-practices* variant included in-line options with check-boxes next to different cookie categories, using the word "Deny" next to a check box may make it confusing as to whether checking the boxes would allow or deny those categories.

Impact on Individual Autonomy & User Trust

Our results indicate that the design parameters we explored had a significant impact on individual autonomy. As reported previously, without the presence of in-line cookie options available in the initial screen of the interface, participants seem to be nudged towards allowing all cookies. Our results indicated that our design variants included cookie options that aligned well with participants' preferences, but only about half of participants actually selected the cookie option for their reported preference. Considering that no condition significantly differed from *best-practices* in this regard, it is likely that factors external to the design of the consent interface, such as participants' past experiences with cookie consent interfaces and a desire to continue to the shopping task, influenced participants' decision-making which is reflected in participants' reported goals. Our results also indicate that individual autonomy with regards to awareness and comprehension of available cookie options may be impacted by the prominence of the choice interface and absence of in-line options. While participants in conditions with a less prominent interface exhibited lower awareness of available consent options compared to those in *best-practices*, participants in conditions without in-line options had better comprehension of these options when revisiting the consent interface (presumably because a larger portion of them visited the "Cookie Preferences" screen), suggesting a need for more information in the initial layer of the consent screen. We also observed that the absence of in-line options impacted participants' perceptions of autonomy, as participants in these conditions reported a lower level of investment in their decision-making compared to those in *best-practices*. In contrast to our findings related to individual autonomy, we did not find that the design parameters we explored significantly impacted user's trust in the privacy choice interface, as participants reported similar perceptions of transparency and control and levels of comfort across conditions.

Consequences to Individual Welfare & Society

While our study did not specifically focus on the impact to individual welfare or societal consequences, our results provide some insights into these aspects of dark patterns in the context of cookie consent interfaces. Considering that users must make consent decisions on each website or app they use, aggregated together the cost of reading these notices, comprehending available options, and making a decision is likely not trivial. Future work could more thoroughly explore this impact to individual welfare, using an approach similar to McDonald and Cranor's estimate of the cost of reading privacy policies [101], and could quantify specific costs associated with different consent interface design parameters. It is likely that users have formed coping strategies to manage the burden of cookie consent decisions, considering that over half of participants in our *best-practices* condition reported selecting the "easiest option" when making their consent decision.

In addition to impact to individual welfare, cookie consent decisions also have societal-level consequences. Cookies, among other technologies, enable web tracking which feed into big data aggregation. This data aggregation is used to train algorithms that aid humans in different decision-making contexts that are critical to society, such as consumer credit ratings, employment decisions, admissions to higher education institutions, and criminal punishments [43]. Our study found that those who consented to only the use of strictly necessary cookies largely did so for privacy-related reasons, including to limit the amount of data aggregation and web tracking that occurs. This suggests that cookie consent interfaces that make it difficult for users to opt out of optional cookies have an overall negative impact on society as they contribute to seemingly limitless data aggregation against the desire of many consumers.

8.3.3 Design Implications

We found that several of the design parameters we explored had a significant impact on the usability of the consent interface. Table 8.5 provides a summary of our findings related to each of our initial hypotheses. Among the seven design parameter we explored, we find that the prominence of the consent interface, presence of in-line options within the initial screen of the interface, and presence of a persistent "Cookie Preferences" button for enabling changes to the initial consent decision had the greatest impact on usability. These results are in line with prior work which suggest that more salient privacy information and options yield better usability outcomes (e.g., [36, 140]). Other parameters, such as loss aversion framing and layout of a cookie preferences page, also had some influence on participants' comprehension of and engagement with available cookie options. While our *best-practices* variant incorporates the design choices that performed best for nearly all of the usability facets we explored, it is interesting that it performed worse compared to conditions in which in-line options were absent in participants' comprehension of choices when explicitly instructed to revisit the consent interface. This suggests that providing definitions of cookie categories within the in-line options, such as through a tooltip, may help with comprehension of choices and better enable user decision-making, although this idea should be tested empirically.

Hypothesis	Result	Summary
H1. Prominence of the consent interface	Supported	Compared to *best-practices*, participants in *prominence-cornerButton* had less awareness of a privacy decision and available cookie options.
H2. Path to a cookie options interface	Not supported	While there no significant impact on awareness, we did find that the absence of in-line options impacted focused comprehension and investment in decision-making.
H3. Loss aversion framing describing the presence of choices	Not supported	While there was no significant impact on participants' consent decision or sentiment, we did observe that participants in *text-lossAversion* were more likely to comprehend the recommended option as "allow all cookies" compared to those *best-practices*.
H4. Layout of the notice text	Not supported	No significant impact on comprehension or other usability aspects were observed between *text-layoutParagraph* and *best-practices*.
H5. Text within button options	Not supported	No significant impact on comprehension or other usability aspects were observed between *button-generic* and *best-practices*.
H6. Layout of cookie choices page	Partially supported	Though only a small number of participants visited the "Cookie Preferences" page in either condition, fewer participants in *layout-multilayer* changed toggles for cookie options compared to those in *options-interfaceButton*
H7a. Process for changing or revoking a consent decision: persistent button	Supported	Compared to *best-practices*, participants in *reversal-cookiePolicy* were significantly less likely to report a correct method for changing their consent decision.
H7b. Process for changing or revoking a consent decision: no instructions	Not supported	No significant impact on participants' reporting of a correct method for changing their consent decision was observed between *reversal-noInstructions* and *best-practices*.

Table 8.5: Summary of findings related to our initial hypotheses for the seven design parameters explored in our study.

8.4 Conclusion

To demonstrate the evaluation guidelines proposed in Chapter 7 we conducted a two-part study of cookie consent interfaces, finding that the design of these interfaces significantly impact the high-level objectives described in the guidelines. We first conducted a inspection-based evaluation of consent interfaces implemented through consent management platforms (CMPs) which identified design parameters that organizations can customize for their websites or apps. To explore which design choices for these parameters result in better usability, we conducted a large-scale between-subjects experiment on Prolific evaluating 12 cookie consent design variants. We find that several design choices, such as a "consent wall" implementation of the consent interface, in-line options corresponding to cookie categories, and a persistent "Cookie Preferences" button enabling decision reversal yielded significantly better usability outcomes. Our comprehensive usability assessment of cookie consent interfaces provides an example of how the evaluation guidelines described in this thesis can result in actionable design implications for a specific privacy choice context.

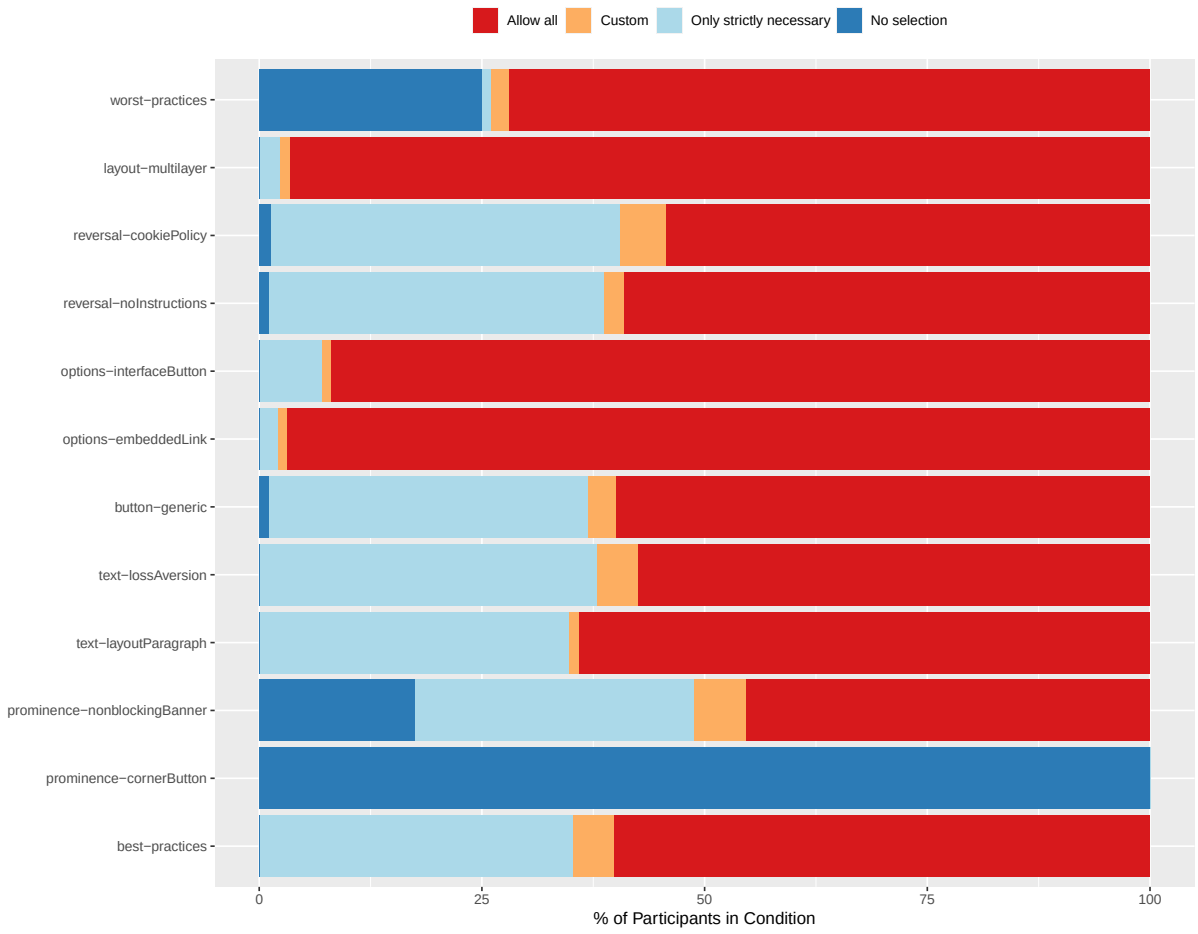


Figure 8.4: Participants' cookie consent decisions in their interactions with the prototype website where "custom" refers to any combination of strictly necessary, performance, functional, or targeting cookies. Three participants who saw blocking consent notice (in the *reversal-cookiePolicy*, *reversal-noInstructions*, and *button-generic* conditions) bypassed making a consent decision by clicking on other links within the consent notice, which dismissed the notice in the prototype.

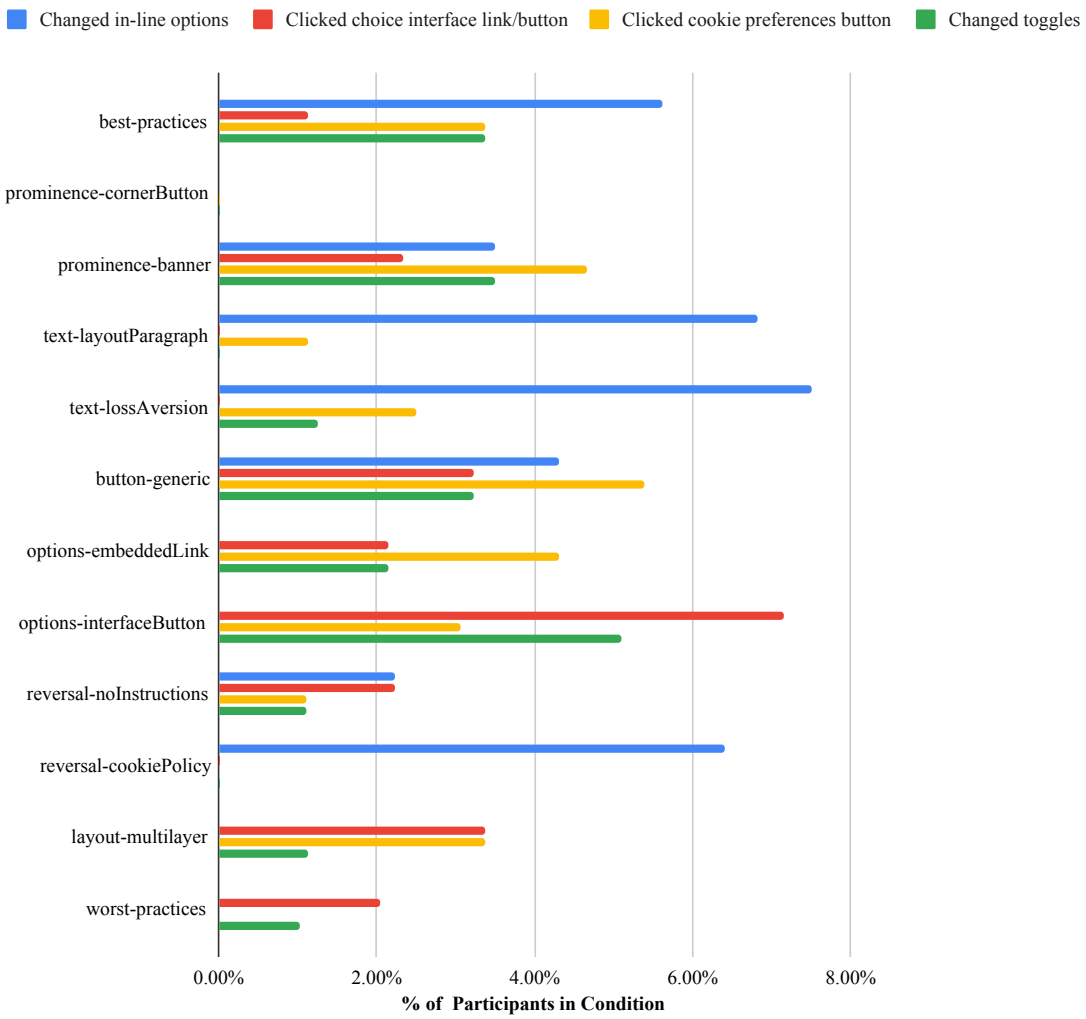


Figure 8.5: A summary of participants' engagement with the cookie consent interface beyond selecting one of the button options. Specifically, we noted (if applicable to the study condition) whether participants changed any of the in-line options in the interface, clicked on the link or button leading to the cookie choices interface, clicked the persistent cookie preferences button, or changed any toggles within the cookie choices interface.

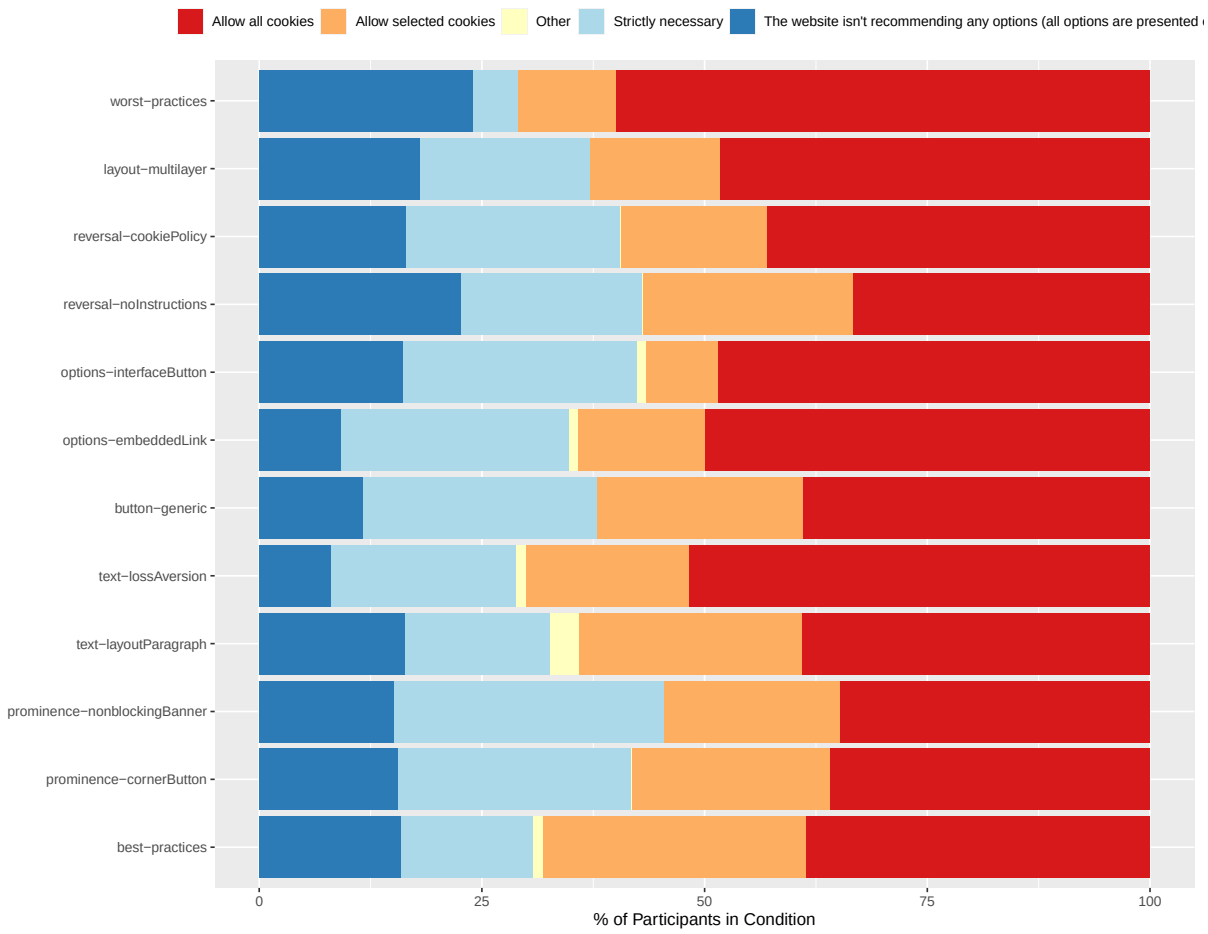


Figure 8.6: Participants' comprehension of what (if any) cookie consent options the website seemed to be recommending.

Chapter 9

Conclusion

This dissertation explores usability issues associated with different privacy choice mechanisms, and provides comprehensive guidance for conducting evaluations of interfaces through which privacy choice mechanisms are provided. A heuristic-based empirical evaluation of privacy choices related to email marketing, targeted advertising, and data deletion identified several aspects of these privacy choices that may lead to poor user awareness and comprehension (Chapter 3). These usability issues were further explored through a lab usability study which evaluated common implementations of these three types of privacy choices and provided actionable guidance for improving the usability of these privacy choice mechanisms (Chapter 4). A third study aimed to address issues user comprehension of privacy choice mechanisms through an iterative evaluation of new icons and accompanying text descriptions that communicate the presence of available controls finding that a stylized toggle icon was most effective in this regard (Chapter 5). Beyond awareness and comprehension, another aspect of usability explored in this dissertation is whether privacy choice mechanisms address user needs. This was studied through a remote usability study in the context of advertising controls available on Facebook which identified several aspects in how current controls fall short addressing users' privacy goals (Chapter 6). To aid privacy and design practitioners in conducting evaluations of their own privacy choice interfaces, the approaches used in these usability evaluations, as well as prior research, were synthesized into a set of comprehensive guidelines which address seven high-level usability objectives (Chapter 7). Lastly, this dissertation demonstrates the application of this guidance through a two-part evaluation of cookie consent interfaces which provided insights into the specific usability impact of different design choices (Chapter 8).

9.1 Privacy Choice Interface Evaluation Approaches

Table 9.1 details the evaluation methods utilized in the studies described in this thesis and maps them to the high-level usability objectives outlined in the evaluation guidelines presented in Chapter 7. One of the studies described focused on a single high-level usability objective, three explored multiple, while the last evaluated against all seven. This demonstrates that in applying the guidelines, evaluation studies can be scoped to explore specific usability objectives related to a privacy choice interface.

Study	Evaluation Method	Usability Objective(s)
An Empirical Analysis of Data Deletion and Opt-Out Choices (Chap. 3)	Heuristic evaluation	Awareness, Ability & effort, Comprehension
The Usability of Websites' Opt-Out and Data Deletion Choices (Chap. 4)	Interview, Lab usability study, formal usability evaluation	Awareness, Ability & effort, Comprehension
How to (In)Effectively Convey Privacy Choices with Icons and Link Texts (Chap. 5)	Online experiments	Comprehension
Identifying User Needs for Advertising Controls on Facebook (Chap. 6)	Survey, Interview, Remote usability study	User needs, Awareness, Ability & effort, Comprehension
Applying to Evaluation Guidelines to Cookie Consent Notices (Chap 8)	Heuristic evaluation, Cognitive walkthrough, Independent expert review, Online experiment	Awareness, Ability & effort, Comprehension, User needs, User sentiment, Decision reversal, Nudging patterns

Table 9.1: Overview of the evaluation methods discussed in this thesis and their mapping to the high-level usability objectives described in the evaluation guidelines.

The studies described in Chapters 3 and 4 demonstrate how inspection-based usability evaluations and user studies can complement each other. The research discussed in Chapter 3 utilized a heuristic evaluation method based on a custom set of heuristics identified by the research team, while the user study reported in Chapter 3 incorporated interview questions and privacy choice tasks in which participants were described hypothetical scenarios. This study also included a formal usability evaluation in which a researcher collected data related to the user actions required to use the privacy choice mechanisms to compare against the user actions in participants' interactions. The results of both studies were discussed through the lens of the User Action Framework [4] which corresponds to the user awareness, ability & effort, and comprehension objectives of the evaluation guidelines. Both studies yielded in a similar set of design recommendations, including for privacy regulation to include explicit usability requirements for privacy choice mechanisms.

As reported in Chapter 5, a series of online experiments utilizing participant inspection approach was used to evaluate user comprehension of new icons and link texts for conveying the presence of privacy controls. This study demonstrates an iterative approach to conducting an in-depth exploration of a single usability objective. While the initial experiments explored icons and link texts without any additional context to capture participants' unprimed impressions, the final evaluation study placed the combination of icons and links in the context of a fictitious online retailer. Follow-up work to this study used a similar approach to explore the impact of these icons on user awareness and sentiment by assigning participants a distraction task to draw attention to the area of the website containing the privacy choice mechanism [31]. This highlights that evaluation approaches can often be quickly retooled to explore additional high-level usability objectives.

Chapter 6 describes a two-part study which primarily focused on user needs for advertising controls on Facebook. The preliminary survey relied on participants' recall of past experiences with advertising controls which allowed for the collection of user study data at scale, but at the potential cost of participants incorrectly remembering their previous interactions. However, this survey identified groups of advertising controls that were incorporated into a second usability evaluation. This follow-up evaluation, conducted as a remote usability study instead of an in-

person laboratory study due to the COVID-19 pandemic, utilized an approach similar to that described in Chapter 4. In addition to privacy tasks described through hypothetical scenarios, this study included a participant inspection of Facebook's Ad Preferences interface which yielded additional usability findings related to user ability & effort and comprehension.

The research reported in Chapter 8 combined approaches used in the previous studies to conduct a comprehensive usability evaluation of cookie consent interfaces. A heuristic evaluation, similar to that described in Chapter 3, was first conducted to identify design parameters associated with cookie consent interfaces implemented through CMPs. This was followed by an online experiment, conducted in a similar manner as the final experiment described in Chapter 5. An important difference between the approaches used in the two studies was that participants were exposed to a cookie consent interface via an interactive prototype of an online retailer's website rather than a static image, which allowed for a better evaluation of user ability & effort. To evaluate for user awareness of available choices, user needs, and unfocused comprehension of cookie options, this study assigned participants a distraction task to more closely replicate how users interact with consent interfaces on actual websites. A follow-up participant inspection of the consent interface allowed for an evaluation of other aspects of comprehension, as well as user sentiment and decision reversal.

While the studies described in this thesis demonstrate a variety of methods for conducting usability evaluations of privacy choice interfaces, not all of the methods described in Chapter 7 were utilized. None of the studies used a perspective-based UI inspection, which may be better than other approaches for evaluating a consent interface through the lens of a particular user group (e.g., users of screen-reading technologies) or privacy as a normative value (e.g., [60]). These studies also did not include any field studies which can be used to evaluate several usability objectives for privacy choice interfaces that have already been deployed (e.g., [8]). The user study approaches described in this thesis did not include evaluations based on a participant quick review of the interface which may be useful for evaluating user awareness and unfocused comprehension of available privacy choice mechanisms. Additionally, none of the user studies described included a distraction task in which participants would seek out privacy settings, an approach that would that relate best to evaluating user ability & effort and user needs.

Bibliography

[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. 2.4

[2] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, 2005. 2.4, 6

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, 50(3):1–41, 2017. 1, 2.4, 3.3.3

[4] 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. 2.6, 3.1.1, 3.3, 4.1.3, 5.6.2, 9.1

[5] Apple Inc. App privacy details on the app store. `https://developer.apple.com/app-store/app-privacy-details/`, 2021. 2.5

[6] 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. 2.4

[7] 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. 2.6

[8] Vinayshekhar Bannihatti Kumar, Roger Iyengar, Namita Nisal, Yuanyuan Feng, Hana Habib, Peter Story, Sushain Cherivirala, Margaret Hagan, Lorrie Cranor, Shomir Wilson, et al. Finding a choice in a haystack: Automatic extraction of opt-out statements from privacy policy text. In *Proceedings of The Web Conference*, pages 1943–1954, 2020. 2.5, 5, 9.1

[9] Carol M Barnum. *Usability Testing Essentials: Ready, Set...Test*. Morgan Kaufmann, 2011. 2.6

[10] Paola Benassi. TRUSTe: An online privacy seal program. *Communications of the ACM*, 42(2):56–59, 1999. doi: 10.1145/293411.293461. 2.5, 5

[11] 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. doi: 10.1109/RE.2016.20. 2.5

[12] Alexander Bleier and Maik Eisenbeiss. The importance of trust for personalized online advertising. *Journal of Retailing*, 91(3):390–409, 2015. 2.3

[13] 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. 2.4

[14] Dirk Bollen, Bart P Knijnenburg, Martijn C Willemsen, and Mark Graus. Understanding choice overload in recommender systems. In *Proceedings of the Conference on Recommender Systems*, pages 63–70. ACM, 2010. 8.2.1

[15] Harry Brignull. Types of dark patterns: Confirmshaming. `https://www.darkpatterns.org/types-of-dark-pattern/confirmshaming`. 8.1.1

[16] Harry Brignull. Dark patterns: Deception vs. honesty in UI design. *Interaction Design, Usability*, 338, 2011. 2.4

[17] 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. doi: 10.1145/3404983.3405518. 2.5

[18] Bloomberg Businessweek. Business Week/Harris Poll: A Growing Threat. page 96, 2000. 2.3

[19] 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. ISSN 03029743. doi: 10.1007/11423409_20. 2.5

[20] Fred H Cate. The limits of notice and choice. *IEEE Security & Privacy*, 8(2):59–62, 2010. 1

[21] Nick Charalambides. We recently went viral on tiktok - here's what we learned, August 2021. `https://blog.prolific.co/we-recently-went-viral-on-tiktok-heres-what-we-learned/`. 8.2.3

[22] 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. ISBN 9781450356312. doi: 10.1145/3197391.3205417. URL `https://doi.org/10.1145/3197391.3205417`. 7

[23] 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. 2.4

[24] 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/`. 2.2

[25] Norwegian Consumer Council. Deceived by design: How tech companies use dark pat-

terns to discourage us from exercising our rights to privacy. Technical report, 2018. 1, 2.2

[26] 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. 2.6

[27] Lorrie Faith Cranor. Can users control online behavioral advertising effectively? *IEEE Security & Privacy*, 10(2):93–96, 2012. 2.4

[28] Lorrie Faith Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications & High Technology Law*, 10:273, 2012. 1, 2.1, 3, 5, 5.6.2

[29] 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. 2.3

[30] 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. 1, 2.2

[31] Lorrie Faith Cranor, Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Joel Reidenberg, Norman Sadeh, and Florian Schaub. Ccpa opt-out icon testing – phase 2, May 2020. `https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/dns-icon-study-report-052822020.pdf`. 9.1

[32] 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-id` 1, 2.2

[33] 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. 2.2, 2.5, 3.2.2, 5

[34] Digital Advertising Alliance. Self-regulatory principles for online behavioral advertising, July 2009. `http://digitaladvertisingalliance.org/principles`. 1, 2.1, 3, 5.2.2, 6.2.3

[35] Disconnect, Inc. Disconnect privacy icons, 2014. `https://github.com/disconnectme/privacy-icons`. 2.5, 5

[36] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, 2021. 8.3.3

[37] 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. 2.5, 2.6

[38] 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. doi: 10.1145/2702123.2702251. 2.5, 5

[39] 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. 2.5, 2.6, 4.1.3

[40] 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. doi: 10.1109/sp40000.2020.00043. 2.5, 2.6, 5

[41] 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. 2.4, 3

[42] 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`. 1, 2.1, 5, 8

[43] Executive Office of the President. Big data: A report on algorithmic systems, opportunity, and civil rights. Technical report, The White House, May 2016. 8.3.2

[44] 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. 2.4, 3.2.1, 3.2.1, 5

[45] 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`. 2.6

[46] 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`. 1, 2.1

[47] 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`. 2.1

[48] 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. 2.5, 5.2.1

[49] 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. 2.6, 7.1.1, 7.1.2, 7.1.2, 7.1.2, 7.1.2, 7.1.2, **??**, 7.3

[50] 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. ISBN 978-1-4503-5620-6. doi: 10.1145/3173574.3173627. URL https://doi.org/10.1145/3173574.3173627. 2.3

[51] 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. 2.5, 5.4, 5.6.2

[52] Say fo Maksim. Buttons alignment policy, February 2020. https://uxplanet.org/buttons-alignment-policy-a26de4ce0c70. 8.2.1

[53] 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. doi: 10.1145/506443.506577. 2.5

[54] Lothar Fritsch. Privacy dark patterns in identity management. In *Proceedings of the Open Identity Summit (OID)*, 2017. 2.4

[55] 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. 2.4, 2.5, 3, 4

[56] Ghostery. Ghostery: Homepage, 2017. https://www.ghostery.com. 2.5, 5

[57] 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. doi: 10.1145/1143120.1143137. 2.5, 5

[58] 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. 2.4, 3.2.2

[59] 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. 2.4

[60] 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. 2.4, 8, 9.1

[61] 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. 1, 0, 5.6.2, 7.3.2, 7.3.3, 7.3.4

[62] 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. 1, 0, 7.3.2, 7.3.2, 7.3.2, 7.3.3, 7.3.4, 7.3.4

[63] 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 Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)*. ACM, 2021. 1, 0

[64] 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. 1, 0, 7.3.4

[65] Munawar Hafiz. A collection of privacy design patterns. In *Proceedings of the Conference on Pattern Languages of Programs (PLoP)*. The Hillside Group, 2006. 2.4

[66] 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`. 2.2, 3

[67] Morten Hertzum. Usability testing: A practitioner's guide to evaluating the user experience. *Synthesis Lectures on Human-Centered Informatics*, 13(1):i–105, 2020. 2.6

[68] 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`. 2.1

[69] Maximilian Hils, Daniel W Woods, and Rainer Böhme. Measuring the emergence of consent management on the web. In *Proceedings of the Internet Measurement Conference (IMC)*, pages 317–332. ACM, 2020. 8.1.1

[70] Paul Hitlin and Lee Rainie. Facebook algorithms and personal data. Technical report, Pew Research Center, 2019. 2.3

[71] 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. doi: 10.1007/978-3-642-20769-3_27. 2.5, 5

[72] Horizon 2020 Framework Programme of the European Union. Cookies, the gdpr, and the eprivacy directive. 8

[73] William K Horton. *The Icon Book: Visual Symbols for Computer Systems and Documentation*. John Wiley & Sons, Inc., 1994. 2.5, 5.4, 5.6.2

[74] 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. 2.1

[75] 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. 2.5, 5

[76] 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. 2.5

[77] 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. 2.5

[78] 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. 2.5

[79] Mark J Keith, Courtenay Maynes, Paul Benjamin Lowry, and Jeffry Babb. Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In *Proceedings of the International Conference on Information Systems (ICIS)*, 2014. 8

[80] 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. doi: 10.1145/1572532.1572538. 2.5, 5

[81] 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. doi: 10.1145/1753326.1753561. 2.5, 2.6, 5

[82] 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. 2.5, 2.6

[83] Kevel. Consent management platform (cmp) 2021 tracker, July 2021. https://www.kevel.co/cmp/. 8

[84] 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. 2.3

[85] 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. 2.2, 3

[86] Steve Krug. *Don't make me think!: A common sense approach to Web usability*. Pearson Education India, 2000. 2.6

[87] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, 2017. 2.6, 5.2.1, 6.3.4

[88] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. Tranco: A research-oriented top sites ranking hardened against manipulation. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019. doi: 10.14722/ndss.2019.23386. 8.1.1

[89] 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. 1, 2.4, 3

[90] Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users? In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*, pages 19–30. ACM, 2012. 4, 5.2.3, 5.6.2

[91] Chris Lewis. *Irresistible Apps: Motivational design patterns for apps, games, and web-based communities*. Springer, 2014. 2.4

[92] Timothy Patrick Libert. *Track The Planet: A Web-Scale Analysis Of How Online Behavioral Advertising Violates Social Norms*. PhD thesis, University of Pennsylvania, Philadelphia, PA, 2017. 8.1.1

[93] 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. doi: 10.1145/1978942.1979244. 2.5

[94] 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. 2.4

[95] 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. 7

[96] 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. doi: 10.2478/popets-2020-0037. 2.5

[97] 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`. 2.2

[98] Manfredo Massironi. *The Psychology of Graphic Images: Seeing, Drawing, Communicating*. Psychology Press, 2001. 2.5

[99] 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. 2.6, 7, 7.3.7, 7.3.7, 7.3.7, 8.1.1

[100] 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. 2.1, 2.4

[101] 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. 2.4, 2.5, 5, 8.3.2

[102] 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. 2.3, 2.4, 2.5, 3

[103] 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. 2.5

[104] 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. 2.5

[105] Mozilla. Privacy icons, February 2020. `https://wiki.mozilla.org/Privacy_Icons`. 2.5, 5

[106] 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. ISBN 9781931971454. 2.3

[107] Network Advertising Initiative. NAI code of conduct, 2018. `https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf`. 1, 2.1

[108] Nielsen Norman Group. Top 10 design mistakes in the unsubscribe experience, April 2018. `https://www.nngroup.com/articles/unsubscribe-mistakes/`. 2.4, 5.6.2

[109] 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. 1

[110] 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. ISBN 9781450367080. doi: 10.1145/3313831.3376321. URL `https://doi.org/10.1145/3313831.3376321`. 2.4, 2.5, 7.3.7, 7.3.7, 7.3.7, 8, 8.1.1, 8.2.1, 8.3.2

[111] 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. doi: 10.1080/1369118X.2018.1486870. 2.5

[112] 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. 2.2

[113] 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. 2.1, 5, 5.3.1, 5.5.2

[114] 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. 2.1

[115] 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. 1, 2.1, 8

[116] Online Trust Alliance. Email marketing & unsubscribe audit, December 2017. https://otalliance.org/system/files/files/initiative/documents/2017emailunsubscribeaudit.pdf. 1, 2.2, 3

[117] 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. doi: 10.1145/2702123.2702164. 2.5

[118] PrivacyGrade.org. Privacygrade.org, 2020. http://privacygrade.org/home. 2.5, 5

[119] 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. 2.3, 6

[120] 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. doi: 10.15779/Z384K33. 2.5

[121] 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. 1, 3

[122] 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. 2.5, 5

[123] 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. 2.5, 5, 5.2.1, 5.4, 5.6.1, 5.6.2

[124] 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. 1, 3

[125] 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. 2.6

[126] Elizabeth B-N Sanders. Converging perspectives: Product development research for the 1990s. *Design Management Journal*, 3(4):49–54, 1992. 2.6

[127] 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. 2.5, 2.6, 5.6.3, 7.1.1, 7.1.2, 7.1.2, 7.1.2, 7.1.2, **??**

[128] 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. doi: 10.14722/usec.2016.23017. 2.4

[129] 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. doi: 10.1109/SP.2007.35. 2.5

[130] Mark Scott and Laurens Cerulus. Europe's new data protection rules export privacy standards worldwide. *Politico*, January 2018. `https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-` 2.1

[131] Robert H Sloan and Richard Warner. Beyond notice and choice: Privacy, norms, and consent. *Journal of High Technology Law*, 14:370, 2014. 1

[132] 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. ISBN 9781450375795. URL `https://doi.org/10.1145/3419249.3420132`. 1, 2.2, 7.3.7, 8.1.1, 8.3.2

[133] Daniel J Solove. Privacy self-management and the consent dilemma. *Harvard Law Review*, 126:1880, 2012. 1

[134] Stanford Legal Design Lab. Icons for legal help, 2020. `https://betterinternet.law.stanford.edu/design-guide/icons-for-legal-help/`. 2.5

[135] 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`. 2.1

[136] Janice Y Tsai, Serge Egelman, Lorrie Faith Cranor, and Alessandro Acquisti. The effect of online privacy information on purchasing behavior: An experimental study. *Information*

Systems Research, 22(2):254–268, 2011. doi: 10.1287/isre.1090.0260. 2.5, 2.6

[137] 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. 2.3

[138] United States Census Bureau. 2020 demographic analysis estimates press kit, December 2020. https://www.census.gov/newsroom/press-kits/2020/2020-demographic-analysis.html. 8.2.3

[139] 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. 2.3, 2.4, 2.5, 3, 5.6.2, 5.6.3

[140] 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. doi: 10.1145/3319535.3354212. 2.4, 2.5, 5, 8, 8.3.3

[141] W3C Policy Languages Interest Group. Platform for privacy preferences (P3P) project, 2018. https://www.w3.org/P3P//. 2.1

[142] W3C Web Accessibility Initiative. Web content accessibility guidelines (WCAG) 2.1, 2018. https://www.w3.org/TR/WCAG21/. 2.6, 8.2.1, 8.3.1

[143] W3C Working Group. Tracking preference expression (DNT), 2019. https://www.w3.org/TR/tracking-dnt/. 1, 2.1, 3.2.2

[144] Ari Ezra Waldman. Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, 31, 2020. 1

[145] 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. 2.3, 6.2.1

[146] 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. doi: 10.1080/014492999119129. 2.5, 5.4

[147] Chauncey Wilson. *User Interface Inspection Methods: A User-Centered Design Method*. Newnes, 2013. 2.6, 7.2.1, 8, 8.1

[148] Michael S Wogalter. Communication-human information processing (C-HIP) model. *Handbook of warnings*, pages 51–61, 2006. 2.6

[149] 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. 2.3

[150] 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. 2.6

Appendix A: An Empirical Analysis of Data Deletion...

A.1 Websites Analyzed

A.2 Website Analysis Template

Appendix B: The Usability of Websites' Opt-Out...

B.1 Interview Script

B.2 Codebook

Appendix C: How to (In)Effectively Convey Privacy Choices...

C.1 Survey Questions

C.2 Participant Demographics

C.3 Codebooks

C.4 Regression Outputs

Appendix D: Identifying User Needs for Advertising Controls...

D.1 Facebook Ad Controls

D.2 Survey Questions

D.3 Survey Codebooks

D.4 Remote Usability Study Screening Questions

D.5 Remote Usability Study Interview Script

D.6 Remote Usability Study Codebooks

Appendix E: Applying the Evaluation Guidelines...

E.1 Cookie Consent Design Variants

E.2 Survey Questions

E.3 Codebooks