An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites

Hana Habib, Yixin Zou†, Aditi Jannu, Neha Sridhar, Chelse Swoopes,
Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, Florian Schaub†
Carnegie Mellon University & †University of Michigan
{htq, ajannu, nksridha, cswoopes, acquisti, lorrie, ns1}@andrew.cmu.edu
{yixinz, fschaub}@umich.edu

Abstract

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

1 Introduction

The dominant approach for dealing with privacy concerns online, especially in the United States, has largely centered around the concepts of notice and consent [56]. Along with transparency, consumer advocates and regulators have asserted the need for consumers to have control over their personal data [22, 28, 41]. This has led some websites to offer privacy choices, 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 choices, including mechanisms created by industry self-regulatory groups (e.g., the Digital Advertising Alliance [21]) as well as those mandated by legislation, consent mechanisms appear to have failed to provide meaningful privacy protection [15, 57]. For example, many consumers are unaware that privacy choice mechanisms exist [33, 48, 60]. Additionally, past research has identified usability and noncompliance issues with particular types of opt-outs, such as those for email communications and targeted advertising [24, 35, 40, 42, 55]. Our study builds on 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.

We conducted an in-depth content 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 content analysis focused on two research questions:

1. What choices related to email communications, targeted advertising, and data deletion do websites offer?
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 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 omit-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.

ted 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.

New regulations, such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), aim to address issues with privacy choice mechanisms and include strict requirements for obtaining and maintaining consent for practices like direct marketing, targeted advertising, and disclosure or sale of personal data [25, 50]. Our study contributes a better understanding of the mechanisms websites currently use to provide choices related to these practices, and where they may fall short in helping people take advantage of available choices. Additionally, our analysis provides a foundation for future research into the development of best practices for provisioning privacy choices. These recommendations could build upon changes to the consent experience in the mobile app domain, where research showing the benefits of a uniform interface contributed to changes in permission settings implemented by the Android and iOS platforms [4]. Building new approaches for privacy choice provisioning upon practices that are already prevalent may increase the likelihood of adoption.

2 Privacy Choice Regulatory Framework

As background, we provide an overview of current legislation and industry self-regulatory guidelines related to the types of privacy choices evaluated in this study: opt-outs for email and targeted advertising and options for data deletion.

2.1 Opt-outs for Email Communications

In the United States, 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 [29]. 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. The European Union's General Data Protection Regulation (GDPR) also grants consumers "the right to object" when their personal data is processed for direct marketing purposes (Art. 21) [25]. Furthermore, the California Consumer Privacy Act (CCPA), which will go into effect in 2020, grants California residents the right to opt out of having their personal data sold to third parties, such as for marketing purposes [50].

2.2 Opt-outs for Targeted Advertising

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 [21, 38, 52]. DAA member advertisers are required to provide consumers with the choice to opt out of tracking-based targeted advertising [21]. 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 [46].

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, websites should 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). Nevertheless, the GDPR does not explicitly state that consent is required for targeted advertising, and ambiguity in Art. 6 may provide leeway for companies to claim a "legitimate business interest" and collect data for targeted advertising without obtaining explicit consent [25].

2.3 Data Deletion Choices

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) [25]. Implementations of the "right to be forgotten" vary from account deletion request forms to the ability of consumers to delete certain information related to their profile.

While no general "right to be forgotten" exists in the United States, some US federal laws contain data deletion requirements for specific 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 [30]. The CCPA will also give 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 [12].

3 Related Work

Our study builds upon prior work that (1) evaluated privacy control mechanisms; and (2) studied consumer attitudes and behaviors related to data collection and use.

3.1 Prior Evaluations of Privacy Choices

The usability of websites' privacy communications and controls has long been problematic [47, 48]. Recent work has shown that privacy policies still exhibit low readability scores [26, 44]. Additionally, most websites fail to provide specific details regarding the entities with which they share data and the purposes for which data is shared [34]. Some consumer advocates argue that current control mechanisms nudge people away from exercising their right to privacy with practices, such as creating a cumbersome route to privacy-friendly options, highlighting the positive outcome of privacy-invasive options, and incentivizing consumers to share more personal data through the framing of control mechanisms [54].

Prior studies have also revealed compliance issues related to privacy control requirements. For example, in the early 2000s the Federal Trade Commissions (FTC) found that privacy controls were not ubiquitously implemented at that time, with only 61% of surveyed websites giving consumers options regarding the collection of their personal information [27]. There is also evidence of noncompliance with the GDPR, as some major websites still deliver targeted ads to European visitors who did not consent to the use of their personal data [19].

However, it seems that companies are adjusting their privacy notice and control mechanisms in response to new legal requirements. 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 [20]. Yet, it is 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 [13].

Our analysis primarily focuses on usability issues and does not intend to analyze legal compliance (although the latter is an important direction for future work). Next we highlight key findings of prior usability evaluations regarding email communication opt-outs, targeted advertising opt-outs and data deletion choices, the three types of privacy choices on which our analysis is focused. Our study is the first to survey all three forms of privacy choices in a comprehensive manner through content analysis. Our findings provide an overview of current practices and potential usability pitfalls, with ample implications for making privacy choice mechanisms more uniform and apparent across websites.

3.1.1 Evaluation of Email Communication Opt-outs

Due to the CAN-SPAM Act, many websites offer consumers control over which email messages they receive. 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 still exist as some retailers offered broken unsubscribe links, or continued to send emails after the 10-business-days deadline [55]. 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 [53]. Our research complements these studies by examining usability issues occurring in unsubscribe mechanisms offered on websites rather than through emails, such as links in privacy policies and account settings.

3.1.2 Evaluation of Targeted Advertising Opt-outs

Existing opt-out tools for targeted advertising 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 [8]. 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, 31].

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 need to be manually installed and updated, and may be inadvertently deleted [46]. Browser extensions partially mitigate these issues but introduce other problems. Leon et al. found in 2012 that descriptions of browser extensions were filled with jargon, and participants were not effectively prompted to change their settings when the tool interfered with websites [42]. 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 [48, 60]. Moreover, when the AdChoices icon is presented on a mobile device, it tends to be difficult for people to see [33].

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 [35]. Similar noncompliance issues with the enhanced notice requirement were found by Komanduri et al. in a large-scale examination of DAA and NAI members [40]. In 2015, Cranor et al. reported that privacy policies of companies who use targeted advertising did not meet self-regulatory guidelines related to transparency and linking to personally identifiable information [16]. Our analysis complements this prior work by further highlighting practices used by websites that could make advertising opt-outs difficult to use or comprehend.

3.1.3 Evaluation of Data Deletion Choices

Comparatively, there have been fewer evaluations of data deletion mechanisms, likely due to the recency of corresponding legal requirements. The Global Privacy Enforcement Network (GPEN) reported that only half of the websites and mobile apps they evaluated provided instructions for removing personal data from the company's database in the privacy policy, and only 22% specified the retention time of inactive accounts [34]. An encouraging effort is the JustDelete.me database,[1] which rated the account deletion process of 511 web services. More than half of the websites analyzed (54%) were rated as having an "easy" process for deleting an account from the website. Yet, these ratings only apply to the specific action required to use deletion mechanisms and do not systematically analyze the full end-to-end interaction, which also includes finding and learning available mechanisms and assessing the result of the action, as we do in our study.

3.2 Programmatic Privacy Choice Extraction

Recent efforts in analyzing opt-out mechanisms have utilized automated extraction tools and machine learning. Such tools have been used to evaluate the privacy policies of US financial institutions [17] and descriptions of third-party data collection in website privacy policies [43]. Machine learning classifiers developed by Liu et al. have successfully been used to annotate privacy policy text for certain practices [45]. More directly related to privacy choice mechanisms, Sathyendra et al. and Wilson et al. developed classifiers to identify opt-out choices and deletion options in the privacy policies of websites and mobile apps [58, 62]. Ultimately, these techniques demonstrate the prospect of building tools to extract privacy choices buried in the long text of privacy policies to present them in a more user-friendly manner. However, our manual in-depth analysis of how these choices are presented by websites can identify issues and inform the design of consent mechanisms that better meet users' needs.

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

3.3 Consumer Attitudes and Behavior

Prior studies have shown that consumers are uncomfortable with certain data handling practices commonly used by websites. 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 [9]. Similarly, in another 1999 survey, 70% of respondents wanted to have the choice to be removed from a website's mailing list [18]. 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, posing difficulties for a uniform deletion interface adaptable for all services [51].

Most prior work on consumer attitudes and behavior in this area 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 [7, 39]. 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 [59]. 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 [48]. These findings are supported by qualitative work, such as Ur et al.'s 2012 interview study in which participants generally objected to being tracked [60].

Despite significant privacy concerns, consumers struggle to protect their online privacy against targeted advertising for multiple reasons [14, 42]. 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, 3, 24]. For example, many consumers may not know that ads they see may be based on their email content [48]. 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 [63]. These findings highlight the importance of improving the usability of opt-out tools and disclosures of data handling practices, as well as enhancing consumer education.

4 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 in-

cluded websites sampled across different ranges of web traffic that were registered primarily in the United States.

4.1 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 [5].

To refine the template, our research team conducted six rounds of pilot testing with 25 unique websites from Amazon Alexa's[2] 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.

4.2 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 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

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

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.

4.3 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.

4.4 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.

5 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.

5.1 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 [26]. 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 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) [32]. 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.

Privacy policies as a whole had better, but not ideal, readability, compared to privacy choice text: our analyzed privacy

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

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 [26] and for particular categories (e.g., social networking, e-commerce, and healthcare websites [23, 49]). Nevertheless, literacy research suggests materials approachable by the general public should aim for a junior high reading level (i.e., 7 to 9) [36]. 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.

5.2 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 5.3. 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 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 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 2: Summary of the availability of each type of privacy choice and websites on which they are applicable.

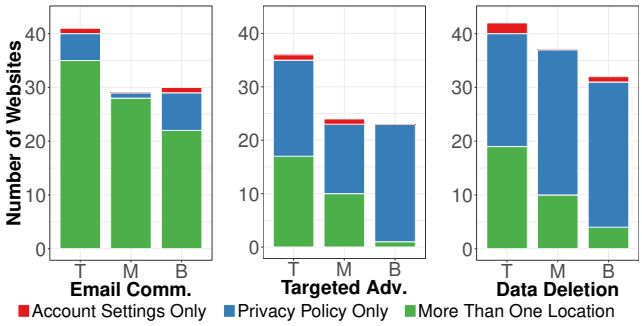

Figure 1: Location of privacy choices for top, middle, and bottom websites. Top websites offered the most privacy choices.

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 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-

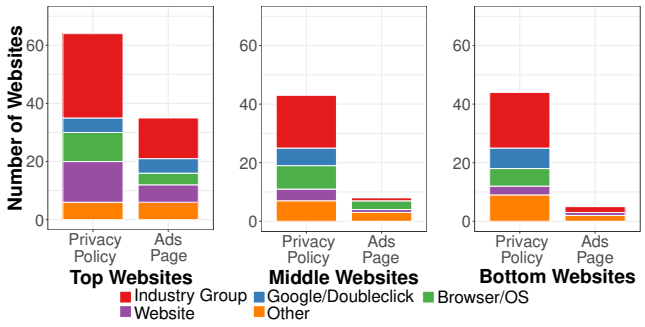

Figure 2: Distribution of different types of targeted advertising opt-outs in privacy policies and "About Ads" pages across top, middle, and bottom websites.

outs in the user account settings, 11 of which led to the same opt-out page presented in the policy.

As seen in Figure 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 [34]. 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[3] 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 [20].

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 [31]. 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) [10].

5.3 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.

There is no dominant wording for section headings. Table 3 summarizes common bigrams and trigrams in policy section headings related to privacy choices. Across policies,

[3] 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: 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.

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.

5.4 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 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

	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 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).

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.[4]

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

5.4.1 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.

6 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 [5]. It serves as a framework to highlight the cognitive and physical processes required to use choice mechanisms,

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

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

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.

6.1 Finding Privacy Choices

Use standardized terminology in privacy policies. As noted in Section 5.3, 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 [11, 61]. 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.

6.2 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 5.4. 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.

6.3 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 5.4, 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." [2, 54] 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 [37].

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.

6.4 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.

7 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.

Acknowledgments

This project is funded by the National Science Foundation under grants CNS-1330596 and CNS-1330214. We wish to acknowledge all members of the Usable Privacy Policy Project (www.usableprivacy.org) for their contributions.

References

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

[2] Alessandro Acquisti, 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 (CSUR)*, 50(3):44, 2017.

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

[4] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 787–796, 2015.

[5] 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.

[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)*, 2012.

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

[8] 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.

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

[10] California Legislative Information. Online privacy protection act of 2003 - California business and professions code sections 22575-22579, 2003.

[11] California State Government. California civ. code s. 1798.82(a), 2003. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.

[12] California State Legislature Website. SB-1121 California consumer privacy act of 2018, 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[13] 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/.

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

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

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

[17] Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur. A large-scale evaluation of U.S. financial institutions' standardized privacy notices. *Transactions on the Web*, 10(3):17, 2016.

[18] 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.

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

[20] 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 '19)*, 2019.

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

[22] Electronic Frontier Foundation. Do not track. https://www.eff.org/issues/do-not-track.

[23] Tatiana Ermakova, Benjamin Fabian, and Eleonora Babina. Readability of privacy policies of healthcare websites. In *Proceedings of Wirtschaftsinformatik*, pages 1085–1099, 2015.

[24] 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.

[25] European Commission. 2018 reform of EU data protection rules. https://ec.europa.eu/commission/

priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[26] 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, 2017.

[27] Federal Trade Commission. Privacy online: Fair information practices in the electronic marketplace, May 2000. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[28] Federal Trade Commission. Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers, March 2012. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[29] 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.

[30] 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.

[31] Roy T Fielding and David Singer. Tracking preference expression (DNT). W3C candidate recommendation, 2017. https://www.w3.org/TR/tracking-dnt/.

[32] Rudolf Franz Flesch. *Art of Readable Writing*. Harper, 1949.

[33] 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.

[34] 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.

[35] J Hernandez, A Jagadeesh, and J Mayer. Tracking the trackers: The AdChoices icon, 2011. http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon.

[36] Mark Hochhauser. Lost in the fine print: Readability of financial privacy notices, July 2001. https://www.privacyrights.org/blog/lost-fine-print-readability-financial-privacy-notices-hochhauser.

[37] Hunton Andrews Kurth LLP. CNIL fines Google €50 million for alleged GDPR violations, January 2019. https://www.huntonprivacyblog.com/2019/01/23/cnil-fines-google-e50-million-for-alleged-gdpr-violations/.

[38] 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.

[39] 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.

[40] 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.

[41] Neelie Kroes. Online privacy – reinforcing trust and confidence, June 2011. http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm.

[42] 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.

[43] Timothy Libert. An automated approach to auditing disclosure of third-party data collection in website privacy policies. In *Proceedings of the World Wide Web Conference (The Web Conference)*, pages 207–216, 2018.

[44] Thomas Linden, Hamza Harkous, and Kassem Fawaz. The privacy policy landscape after the GDPR. *arXiv preprint arXiv:1809.08396*, 2018.

[45] Frederick Liu, Shomir Wilson, Peter Story, Sebastian Zimmeck, and Norman Sadeh. Towards automatic classification of privacy policy text. Technical report, CMU-ISR-17-118R, Carnegie Mellon University, 2018.

[46] 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.

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

[48] 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)*, 2010.

[49] Gabriele Meiselwitz. Readability assessment of policies and procedures of social networking sites. In *International Conference on Online Communities and Social Computing (OCSC)*, pages 67–75. Springer, 2013.

[50] Michael Morgan, Daniel Gottlieb, Matthew Cin, Jonathan Ende, Amy Pimentel, and Li Wang. California enacts a groundbreaking new privacy law, June 2018. https://www.mwe.com/en/thought-leadership/publications/2018/06/california-enacts-groundbreaking-new-privacy-law.

[51] 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. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 329–339, 2018.

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

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

[54] Norwegian Consumer Council. Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy, June 2018. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

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

[56] 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 and Policy for the Information Society (ISJLP)*, 11:485, 2015.

[57] 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.

[58] Kanthashree Mysore Sathyendra, Shomir Wilson, Florian Schaub, Sebastian Zimmeck, and Norman Sadeh. Identifying the provision of choices in privacy policy text. In *Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2017.

[59] 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.

[60] 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.

[61] U.S. Federal Register 74. Final model privacy form under the Gramm-Leach-Bliley act, 2009.

[62] Shomir Wilson, Florian Schaub, Frederick Liu, Kanthashree Mysore Sathyendra, Daniel Smullen, Sebastian Zimmeck, Rohan Ramanath, Fei Liu, Norman Sadeh, and Noah A Smith. Analyzing privacy policies at scale: From crowdsourcing to automated annotations. *Transactions on the Web*, 13(1):1:1–1:29, 2019.

[63] 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.

A Websites Analyzed

Top Websites

adobe.com, aliexpress.com, amazon.com, ask.com, bbc.co.uk, bet9ja.com, booking.com, buzzfeed.com, cnn.com, coinmarketcap.com, craiglist.org, dailymail.co.uk, dailymotion.com, diply.com, discordapp.com, dropbox.com, ebay.com, etsy.com, facebook.com, github.com, google.com, indeed.com, mediafire.com, mozilla.org, nih.gov, nytimes.com, paypal.com, pinterest.com, providr.com, quora.com, reddit.com, roblox.com, rumble.com, salesforce.com, scribd.com, slideshare.net, spotify.com, stackexchange.com, stackoverflow.com, thestartmagazine.com, tumblr.com, twitch.tv, twitter.com, w3schools.com, whatsapp.com, wikia.com, wikihow.com, wikipedia.org, wordpress.com, yelp.com

Middle Websites

17track.net, abcnews.go.com, avclub.com, babbel.com, bbb.org, cbc.ca, colorado.edu, desmos.com, file-upload.com, funsafetab.com, furaffinity.net, gamepress.gg, huawei.com, indiewire.com, intel.com, internshala.com, kijiji.ca, ladbible.com, mit.edu, myspace.com, news24.com, openclassrooms.com, opera.com, pathofexile.com, php.net, pixiv.net, poloniex.com, python.org, qwant.com, researchgate.net, rollingstone.com, runescape.com, sfgate.com, signupgenius.com, space.com, speedtest.net, theadvocate.com, trustedreviews.com, tufts.edu, ucl.ac.uk, umd.edu, ups.com, upsc.gov.in, utah.edu, wattpad.com, wikiwand.com, worldbank.org, worldoftanks.com, yifysubtitles.com, zapmeta.ws

Bottom Websites

abebooks.com, adorama.com, artsy.net, bovada.lv, cj.com, classlink.com, coreldraw.com, dotloop.com, elitedaily.com, eurowings.com, fangraphs.com, filmapik.co, findlaw.com, fineartamerica.com, foodandwine.com, fronter.com, garena.com, gear4music.com, ghafla.com, hide.me, hsn.com, hsreplay.net, junkmail.co.za, justjared.com, kodi.tv, ldoceonline.com, letgo.com, lpu.in, majorgeeks.com, metacrawler.com, momjunction.com, mr-johal.com, ni.com, notepad-plus-plus.org, ou.edu, phys.org, playhearthstone.com, priceprice.com, rarlab.com, rice.edu, shein.in, statistic-showto.com, stocktwits.com, theathletic.com, tradingeconomics.com, uottawa.ca, uptostream.com, usgamer.net, volvocars.com, wimp.com

B Website Analysis Template

Step 1: Visit the homepage of the website

1. Please enter the name of the website (use the format "google.com").
2. Did you see a notice for consumers that is an "opt-in" to the website's privacy policy and terms of conditions (including the use of cookies)? [Yes, and it included a way to opt-out or change settings; Yes, but it did not include a way opt-out or change settings; No]
3. Is there an option on the website to create a user account? [Yes, No, Other (please specify)]

   Logic: The following two questions are displayed if Q3 = Yes

Step 2: Please create a user account for this site.

4. Do you see the option to opt out of the site's marketing during the account creation process? [Yes, No, Other (please specify)]
5. Does the website have account settings? [Yes, No, Other (please specify)]

Step 3: Look for an "about advertising" or "ad choices" related link on the home page. Click on the "about advertising" or "ad choices" link if it is there.

6. Is there an "about advertising" or "ad choices" related link on the home page? [Yes, and it works; Yes, but it's broken; No]

   Logic: The following question is displayed if If Q6 = Yes, and it works or Q6 = Yes, but it's broken

7. What was this link labeled? [Ad Choices, Something else (copy label)]

   Logic: The following three questions are displayed if Q6 = Yes, and it works

8. Where does the link direct you to? [Somewhere inside privacy policy, Somewhere inside account settings, An individual web page within the site that introduces OBA opt-outs, DAA's webpage, NAI's webpage, TrustE/TrustArc website, Other group's webpage]
9. By which parties are the advertising opt-outs on this page implemented? Include all entities that are linked to on the page. (select all that apply) [DAA, DAA of Canada (DAAC), European Interactive Digital Advertising Alliance (EDAA), Australian Digital Advertising Alliance (ADAA), NAI, TrustE/TrustArc service, The website, The browser or operating system (e.g., instructions to clear cookies or reset device advertising identifier), Google/Doubleclick, Other groups (please specify), There are no advertising opt-outs on this page]
10. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion out of all the opt-outs provided on this page?
11. What is the default setting for the opt-outs on this page (e.g., types of emails or ads already opted out of)? If none, enter 'NA'.

Step 4: Now please go back to the homepage if you are not already there.

12. Could you find the link to the site's privacy policy, or a page equivalent to a privacy policy? [Yes, and the link works; Yes, but the link is broken; No]

    Logic: The following six questions are displayed if Q12 = Yes, and the link works

Step 5: Visit the website's privacy policy, or the page equivalent to a privacy policy. Some websites may call their privacy policy something else.

13. Please copy and paste the URL for this page. Retrieve this policy through the policy retrieval tool.

14. Please copy and paste the title of the site's privacy policy.

15. Does the privacy policy (or equivalent page) have a table of contents? [Yes, No, Other (please specify)]

Step 6.1: Next, do a search for "marketing," "e-mail," "email," "mailing," "subscribe," "communications," "preference" or "opt" in the privacy policy to look for marketing opt-outs. Also skim through the policy headings to double check.

16. Does the privacy policy say that the site sends marketing or other types of communications (including email)? [Yes, the site sends communications, No, the site does not send communications, Not specified in the privacy policy, Other (please specify)]

17. Does the privacy policy have text about how to opt out of the site's marketing? [Yes, No, Not applicable (the site doesn't send marketing messages), Other (please specify)]

    Logic: The following six questions are displayed if Q16 = Yes

18. Please copy and paste the highest level heading in the policy where it describes how to opt out of the site's marketing.

19. Please copy and paste the paragraph(s) in the policy describing how to opt out of the site's marketing in the privacy policy.

20. According to the privacy policy, what types of communications can users opt out of receiving? (Make a note in the comment section if the first and third party emails are not clearly distinguished) [Newsletters, First-party marketing/promotional emails, Third-party marketing/promotional emails, User activity updates, Site announcements, Surveys, Mails, Phone calls, Text Messages/SMS, Other (please specify), None of the above]

21. According to the privacy policy, what types of communications users CANNOT opt out of? [Newsletters, First-party marketing/promotional emails, Third-party marketing/promotional emails, User activity updates, Site announcements, Surveys, Mails, Phone calls, Text Messages/SMS, Other (please specify), None of the above]

22. Does the privacy policy specify whether you can opt-out of marketing within the e-mails? [Yes, you can opt-out within the e-mails; Yes, but you can't opt-out with the e-mails; No, it wasn't specified]

23. Does the privacy policy include any links to marketing opt-outs? [Yes, there's one link to a marketing opt-out; Yes, there're multiple links to a marketing opt-out; No]

    Logic: The following four questions are displayed if Q23 = Yes, there's one link to a marketing opt-out or Q23 = Yes, there're multiple links to a marketing opt-out

Step 6.2: Next, one by one click the links to the marketing opt-out links.

24. Do any of the links in the privacy policy to the marketing opt-outs work? [Yes, they all work; Some work, but some do not; No, none of the links to the marketing opt-outs work]

25. Please copy and paste the URL(s) of the working links.

26. Please copy and paste the URL(s) of the broken links.

27. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion out of all the marketing opt-outs provided in the privacy policy?

    Logic: The following two questions are displayed if Q12 = Yes, and the link works

Step 7.1: Next, do a search for "advertising," "ads," in the privacy policy in order to find whether the site has targeted advertising and their related opt-outs. Also skim through the policy headings to double check

28. According to the privacy policy, does the website have targeted advertising? [Yes, the policy states there is targeted advertising; No, the policy states the website does not have targeted advertising; Not specified by the privacy policy]

29. Does the privacy policy page have text about how to opt out of the site's targeted advertising? [Yes, No, Not applicable (the site doesn't use OBA), Other (please specify)]

    Logic: The following seven questions are displayed if Q28 = Yes

30. Please copy and paste the highest level heading in the policy where it describes how to opt out of OBA.

31. Please copy and paste the paragraph(s) in the policy describing how to opt out of OBA.

32. According to the text of the privacy policy page, what can users opt out from related to OBA/tracking? [OBA only, Tracking, Not specified, Other (please specify)]

33. Does the privacy policy page say whether the OBA opt-outs located in the privacy policy will be effective across different browsers? [Yes, the policy says they will be effective across different browsers; Yes, but the policy says there're for current browser only; Not specified by the privacy policy; Other (please specify)]

34. Does the privacy policy page say whether the OBA opt-outs located in the privacy policy will be effective across different devices? [Yes, the policy says they will be effective across different device; Yes, but the policy says there're for current device only; Not specified by the privacy policy; Other (please specify)]

35. By which parties are the OBA opt-outs mentioned by the privacy policy implemented? Include all entities that are linked to from the privacy policy. [DAA, DAA of Canada (DAAC), European Interactive Digital Advertising Alliance (EDAA), Australian Digital Advertising Alliance (ADAA), NAI, TrustE/TrustArc service, The website, The browser or operating system (e.g., instructions to clear cookies or reset device advertising identifier), Google/Doubleclick, Other groups (please specify)]

36. Does the privacy policy page include any links to an OBA opt-out? [Yes, there is one link to an OBA opt-out; Yes, there're multiple links to different OBA opt-outs; Yes, there're multiple links to same OBA opt-out; No]

    Logic: The following four questions are displayed if Q35 = Yes, there is one link to an OBA opt-out or Q35 = Yes, there're multiple links to different OBA opt-out

    Step 7.2: Next, one by one click the links to the OBA opt-outs in the privacy policy.

37. Do any of the links in the privacy policy to the OBA opt-outs work? Note: Count links with different text and the same URL as multiple links. Include links from the privacy policy and one layer of linked pages as well. [Yes, they all work; Some work, but some do not; No, none of the OBA opt-out links work]

38. Please copy and paste the URL(s) of the working links. Place each URL on its own line.

39. Please copy and paste the URL(s) of the broken links. Place each URL on its own line.

40. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion out of all the OBA opt-outs provided in the privacy policy?

41. What is the default setting for the OBA opt-outs in the privacy policy (e.g., types of emails or ads already opted out of)? If none, enter 'NA'.

    Logic: The following question is displayed if Q12 = Yes, and the link works

    Step 8.1: Next, do a search for "delete," "deletion,""closing account," "remove" or similar terms in the privacy policy in order to find data deletion choices. Also skim through the policy headings to double check.

42. Is there any information in the privacy policy that introduces how to delete your account data? [Yes, No, Other (please specify)]

    Logic: The following eight questions is displayed if Q42 = Yes

43. Please copy and paste the highest level heading in the policy where it describes how to delete account data.

44. Please copy and paste the paragraph(s) in the policy where it describes how to delete account data.

45. According to the privacy policy, what actions can users perform related to data deletion? [Delete their account permanently, Suspend/deactivate their account (data will not be permanently deleted right away), Choose specific types of data to be deleted from their account, Not specified, Other (please specify)]

46. Please copy and paste the specific types of data indicated in the privacy policy.

47. According to the privacy policy, does the website suspend or deactivate your account before deleting it? [Yes, the policy says your account will be suspended; No, the policy says your account will be deleted after a certain amount of time; Not specified in the policy; Other (please specify)]

48. According to the privacy policy, after how long will the data be permanently deleted? [Not specified, Immediately, One week, 30 days, 60 days, 90 days, 6 months, Other (please specify)]

49. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion out of all the data deletion options?

50. Does the privacy policy include any links to delete your account data? [Yes, there's one link; Yes, there're multiple links; No]

    Logic: The following three questions are displayed if Q50 = Yes, there're one link or Q50 = Yes, there're multiple links

Step 8.2: Next, one by one click the links to the data deletion choices.

51. Does the link in the privacy policy to the data deletion choice work? [Yes, they all work; Some work, but some do not; No, they're all broken]

52. Please copy and paste the URL(s) of the working links.

53. Please copy and paste the URL(s) of the broken links.

Logic: The following five questions are displayed if Q11 = Yes, and the link works

Step 9: Next, search for "Do Not Track" or "DNT" in the privacy policy.

54. Will the website honor DNT requests? [Yes, No, Not specified in the privacy policy]

Step 10: Next, skim through the policy for things users can opt-out of. Adjust your previous answers if necessary and complete the following questions.

55. Did you find any other type of opt-outs in the privacy policy? [Yes, No]

56. What other things can users opt out from at this site as described in the privacy policy? [Device info; All first-party cookies; Location history; Profile activities/inferred interests; Sharing with third parties; Google Analytics; Other (please specify); None of the above]

57. When you are skimming through the privacy policy, could you find any other pages that aim to explain the privacy policy or the privacy and data practices of the company in general? [Yes, and the link works; Yes, but the link is broken; No; Other (please specify)]

58. Please copy and paste the URL of the link(s).

59. Did the privacy policy describe the location of a marketing or communications opt out located in the account settings? [Yes, No]

Step 11: Go to this described location in the account settings or look through the main levels of the account settings for marketing, email, or communication choices. Click links which seem to indicate user choice or preferences.

60. Is there any marketing opt-out located in the account settings? [Yes, No, Not applicable (the site doesn't send email/marketing messages), Other (please specify)]

61. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion to this marketing opt-out?

62. What is the default setting for the marketing opt-outs in the account settings (e.g., types of emails or ads already opted out of)? If none, enter 'NA'."

63. Is it the same marketing opt-out page that was presented in the privacy policy? [Yes; No, it's a different marketing opt-out page; There was no marketing opt-out described in the privacy policy; Other (please specify)]

Logic: The following question is displayed if Q63 is not "Yes"

64. What types of communications can users opt out of from in the account settings? [Newsletters, First-party marketing/promotional emails, Third-party marketing/promotional emails, User activity updates, Site announcements, Surveys, Mails, Phone calls, Text Messages/SMS, Other (please specify), None of the above]

65. Did the privacy policy describe the location of an OBA opt-out located in the account settings? [Yes, No]

Step 12: Go to this described location in the account settings or look through the main levels of the account settings for advertising choices. Click links which seem to indicate user choice or preferences.

66. Is there any OBA opt-out located in the account settings? [Yes, No, Not applicable (the site doesn't use OBA), Other (please specify)]

67. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion to this targeted advertising opt-out?

68. Is it the same opt-out page that was presented in the privacy policy? [Yes; No, it's a different OBA opt-out page; There was no OBA opt-out described in the privacy policy; Other (please specify)]

Logic: The following four questions are displayed if Q68 is not "Yes"

69. By which parties is the OBA opt-out in the account settings implemented? Include all entities that are linked to from the account settings. [DAA, DAA of Canada (DAAC), European Interactive Digital Advertising Alliance (EDAA), Australian Digital Advertising Alliance (ADAA), NAI, TrustE/TrustArc service, The website, The browser or operating system (e.g., instructions to clear cookies or reset device advertising identifier), Google/Doubleclick, Other groups (please specify)]

70. What can users opt out from related to OBA/tracking from the account settings? [OBA only (users will still be tracked), Tracking, Not specified, Other (please specify)]

71. According to the information provided, will the OBA opt-out in the account settings be effective across different browsers? [Yes; No, it's for current browser only; Not specified; Other (please specify)]

72. According to the information provided, will the OBA opt-out in the account settings be effective across different devices? [Yes; No, it's for current device only; Not specified; Other (please specify)]

73. Did the privacy policy describe the location of a data deletion choice in the account settings? [Yes, No]

Step 13: Go to this described location in the account settings or look through the main levels of the account settings for data deletion choices. Click links which seem to indicate user choice or preferences.

74. Is there any data deletion option located in the account settings? [Yes, No, Other (please specify)]

75. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion to this data deletion option?

76. Is it the same data deletion page that was presented in the privacy policy? [Yes; No, it's a different data deletion page; There was no data deletion choice presented in the privacy policy; Other (please specify)]

Logic: The following four questions are displayed if Q76 is not "Yes"

Step 14: Lastly, look through the main levels of the account settings for other types of user choices. Click links which seem to indicate user choice or preferences.

81. Did you find any other opt-outs in the account settings? [Yes, No]

77. According to the information provided, what actions can users perform related to data deletion? [Delete their account permanently, Suspend/deactivate their account (data will not be permanently deleted right away), Choose specific types of data to be deleted from their account, Not specified, Other (please specify)]

78. Please copy and paste the specific types of data it indicates. Use ";" to separate multiple items.

79. According to the information provided, does the website suspend or deactivate your account before deleting it? [Yes, there's information that says your account will be suspended; No, there's information that says your account will be deleted after a certain amount of time; Not specified within the account settings; Other (please specify)]

80. According to the privacy policy, after how long will the data be permanently deleted? [Not specified, Immediately, One week, 30 days, 60 days, 90 days, 6 months, Other (please specify)]

82. What other things can users opt out from in the account settings? [Device info; All first-party cookies; Location history; Profile activities/inferred interests; Sharing with third parties; Google Analytics; Other (please specify); None of the above]

"It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices

Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou[†], Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, Florian Schaub[†]
Carnegie Mellon University & [†]University of Michigan
{htq, spearman, jiaminw, acquisti, lorrie, ns1i}@andrew.cmu.edu
{yixinz, fschaub}@umich.edu

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

Author Keywords
Privacy; usability; privacy controls; email marketing; targeted advertising; data deletion.

CCS Concepts
•**Security and privacy** → **Usability in security and privacy;** *Privacy protections;* •**Human-centered computing** → **Empirical studies in HCI;** *Empirical studies in interaction design;* •**Social and professional topics** → *Privacy policies;*

INTRODUCTION
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 [3, 7, 40]. In part due to these regulations, privacy choices 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 [15].

However, availability does not imply usability, leaving open the question of whether these controls are actually useful to consumers. We contribute a holistic usability evaluation of the end-to-end interaction required to use common implementations of these privacy choices. Past work has found various usability problems with such controls, particularly in tools for limiting targeted advertising (e.g., [12, 21]). We expand on that work by exploring the usability of websites' own opt-outs for targeted ads. Furthermore, we examine 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.

We conducted 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 by prior work [15]. 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 and email, participants were skeptical of the effectiveness of controls provided by websites. On the nine websites studied, participants struggled most with discovering and recognizing pages with opt-out information and resorted to consulting help pages or contacting the website. Participants also expressed desire for additional controls over data sharing and deletion. Our findings suggest several implications applicable to websites similar to those in this study for making these online opt-out and deletion choices more usable and useful to consumers.

BACKGROUND & RELATED WORK
We first summarize legislation and self-regulatory industry guidelines relevant to controls for email marketing, targeted advertising, and data deletion. We then discuss prior studies on the usability of privacy controls.

CHI '20, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6708-0/20/04.
http://dx.doi.org/10.1145/3313831.3376511

Regulatory Background

The European Union's General Data Protection Regulation (GDPR) requires websites to provide several types of privacy choices for European consumers and places a special emphasis on the usability of these choices. Relevant user rights under the GDPR include the "right to object" (Art. 21) to the use of data for direct marketing purposes and the requirement for clear affirmative consent to targeted advertising (Art. 4). Such consent in practice is often implemented by cookie consent banners [4]. Moreover, the GDPR grants a "right to be forgotten," allowing consumers to request data processors to delete their personal data (Art. 17) [8].

While the United States does not have a single comprehensive privacy law, several sectoral laws pertain to the privacy controls we examined in our study. The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act requires companies to comply with consumers' wishes to opt out of receiving marketing emails, and provide a clear explanation for how to use the opt-out [10]. Other laws only apply to specific populations. For example, the Children's Online Privacy Protection Act of 1998 (COPPA) requires companies that collect data from children under 13 to honor parental requests to stop further data collection and delete already-collected data [11]. Effective in 2020, the California Consumer Privacy Act (CCPA) provides California residents rights to opt out of sales of their personal data for marketing purposes and, under certain circumstances, request deletion [3, 28].

Advertising industry organizations such as the Network Advertising Initiative (NAI), Digital Advertising Alliance (DAA), and Interactive Advertising Bureau Europe (IAB Europe) have adopted self-regulatory requirements for their online advertising practices [5, 17, 30]. Specifically, members of the DAA must provide consumers the choice to opt out of tracking-based targeted advertising [5]. In light of recent GDPR requirements, the IAB Europe also developed new guidelines for member advertisers related to transparency and consent [18].

Design of Privacy Choices

An empirical analysis of controls for email marketing, targeted advertising, and data deletion conducted by Habib et al. found that privacy choices are often presented through websites' user account settings and privacy policies. However, the terminology used in privacy policies to present these choices is inconsistent across websites, and quite often choices are not adequately described [15]. This has negative usability implications, as privacy policies still suffer from poor readability and consumers rarely read them [9]. Further exasperating this usability issue is the potential use of dark patterns and default settings, which could nudge users away from more privacy protective options [1, 13, 34, 43]. Gray et al. found that users are more likely to agree to the default option because of a belief that the product has their best interest in mind, which may not be the case with respect to data practices and privacy and could lead to unintended consequences [14].

While the goal of the GDPR is to empower consumers to have greater control over their personal data, Sanchez-Rola et al. found that numerous websites in the sample they analyzed presented misleading information about choices, and few websites provided opt-outs for ad tracking that were easy to find or effective [37]. The GDPR also led to an increase in the display of cookie consent banners, but common implementations suffer from functional and usability issues [4]. Utz et al. found that consumers often clicked cookie consents out of habit, or believed that the website would not work absent a click on the consent box [42]. On the other hand, with the implementation of the GDPR, there is also some evidence that companies are shifting towards better practices. A study by Linden et al. suggests that the GDPR was a major driving force towards significant improvements in the presentation of privacy policies inside and outside of the EU [22].

Our study expands upon this prior work by examining user expectations for privacy choices and evaluating current practices for offering choices against these expectations. It highlights additional usability issues with the design of privacy choices that make them difficult for people to use and understand.

Usability of Privacy Choices

We next present prior work examining the usability of the privacy choices that were the focus of this study: email marketing, targeted advertising, and data deletion.

Email Marketing Opt-Outs

In addition to the risk of legal penalties, businesses may also risk losing customers by using poor practices in email unsubscribe processes. Results from a study of marketing unsubscribe choices by the Nielsen-Norman group indicate that users may become annoyed with companies and report legitimate messages as spam if unsubscribe options are not clear. They recommend making unsubscribe links easy to notice and click or tap on a mobile device. They also suggest removing unnecessary feedback steps or confirmation messages and avoiding confusing checkboxes on unsubscribe pages [31].

The Internet Society's Online Trust Alliance (OTA) conducted an audit of 200 North American online retailers to assess compliance with best practices for email sign-up and unsubscribe experiences. While the vast majority of audited retailers had adopted best practices, the report highlighted room for improvement, particularly related to the visibility of opt-out links in emails. While 84% of retailer emails had clear and conspicuous unsubscribe links, a third presented the link in a smaller than recommended font size. Additionally, 29% of retailers had unsubscribe text that did not meet minimum W3C guidelines for contrast ratios, and 64% of retailers did not meet W3C's enhanced guidelines [35].

Our study provides additional insight into the usability of email opt-outs through an empirical user study and evaluates email controls other than unsubscribe links, such as those offered through account settings and privacy policies.

Targeted Advertising Opt-Outs

Prior work has shown that websites are non-compliant with self-regulatory guidelines for targeted advertising, resulting in limited transparency in opt-out choices for users [16, 20]. Opt-out tools developed by the advertising industry have also been found to be misunderstood by users. Ur et al. showed

that the DAA's AdChoices icon does not clearly communicate whether or not an ad is targeted [41]. Additionally, NAI's opt-out tool led users to believe incorrectly that they were opting out of all data collection [26]. Furthermore, these opt-out tools rely on cookies, which can cause additional issues for users. For example, when users clear their cookies their opt-out preferences will also be removed in the process, which would require them to opt out again [25].

Browser extensions that block advertising trackers only partially resolve some of these issues. Studies have found that internet users download blocking extensions for a better browsing experience but still retain a limited understanding of online tracking [24, 38]. Pujol et al. found that many users use ad-blockers with default settings, which for some extensions might not actually block all web trackers [36]. This suggests that even with blocking extensions, people are not fully aware of the ad opt-out choices they can exercise online. While users state they want more control over tracking, they are reluctant to engage deeply with respective tools [27, 39].

Prior research has largely evaluated controls for targeted advertising on the basis of compliance with industry guidelines and users' perceptions of what they do, but has not holistically examined the end-to-end interaction required to use them. Our study provides additional insights by looking more deeply into how users discover targeted advertising controls, in the context of how they are commonly presented on websites.

Data Deletion Choices

Few studies have evaluated data deletion mechanisms, and thus there are few guidelines or best practices. Murillo et al.'s 2018 qualitative study examined user understanding of online data deletion and expiration. They found that most participants were aware of a "backend" to the data deletion process (versus having an understanding completely based on user interface components such as delete buttons and trash icons), and they suggested that information about data deletion should use this understanding to explain technical constraints of data deletion and to help users understand data retention periods. They also found that participants preferred to have context-dependent control over the expiration of their data, rather than just having a fixed chronological expiration period [29].

Recent evidence indicates that the GDPR has lead to increased availability of deletion controls, which are often provided as instructions through a website's privacy policy for requesting deletion of personal data [13, 15]. The service JustDelete.me provides a database with ratings of the ease of deleting data from over 500 different websites, and compiles direct links to the deletion options on those sites. Nearly 40% of the websites listed in the database are rated as having "hard" or "impossible" deletion processes. However, this database does not provide analyses of the full user interaction required to delete data, nor does it publish its methodology for determining these ratings or suggest best practices for deletion interfaces [19].

In 2019, Habib et al. analyzed 150 English-language websites to assess the usability and interaction paths of data deletion mechanisms (as well as email and advertising opt-out mechanisms). While 74% of websites in their sample offered deletion controls, only 27 included a direct link to a tool or request form; 81 offered instructions for a data deletion request rather than providing a simple tool or form. The types of deletion and expiration options were not consistent from website to website, and the time frame in which data deletion would occur was often ambiguous. Many actions, including form fields and extraneous confirmations, were sometimes required in order to delete data. For example, 38 user actions — including filling out a form with 22 checkboxes — were required to request data deletion from the New York Times [15].

While prior work has studied users' mental models of data deletion through interviews [29], prior usability evaluations of deletion controls have relied on analysis by usability experts [15, 19]. Our study builds on this work with a user study that confirms reported usability issues and uncovers others.

STUDY DESIGN

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

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 three patterns: a user account setting, a link from the privacy policy, or text instructions in the privacy policy [15]. To

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 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.

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 1.

To minimize learning effects and prevent fatigue, we counterbalanced 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.

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 [23]. 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.

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

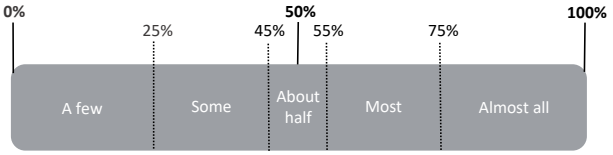

Figure 1. Terminology used to present relative frequency of themes.

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. [2] adapted Norman's theory of human-computer interaction [32] 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 [15]. 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 [6], we adopted the terminology presented in Figure 1 to provide a relative sense of frequency of major themes.

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.

PARTICIPANTS

Table 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 [23], 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.

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

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.

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 2. Participant demographics (gender, age, education, technical background) and task assignments.

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.

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

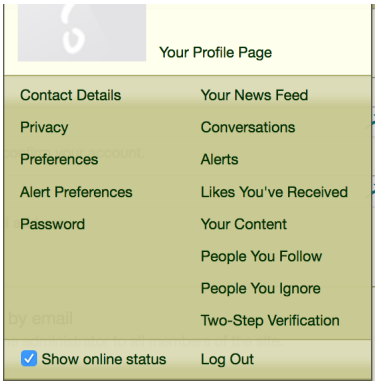

Figure 2. Screenshot of settings menu on `majorgeeks.com` where participants had difficulty finding the correct path to e-mail opt-outs.

could be found under the "privacy" or "contact details" settings pages. However, as seen in Figure 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.

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 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]

[1]This page on `runescape.com` was updated after our study. The new version partially addresses these issues by reducing the page's

Figure 3. List of data rights available on `runescape.com` which misleadingly seem clickable.

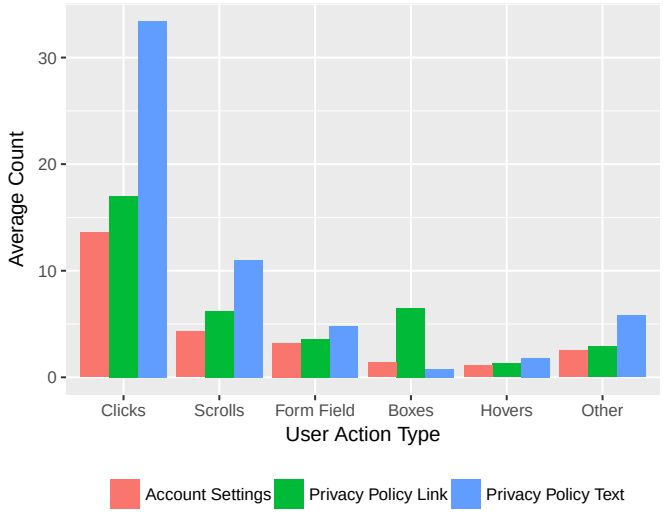

Figure 4. Number of clicks, scrolls, form fields, check boxes, hovers, and other user actions, averaged over all websites, in the participants' interaction with account settings and policy choices.

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.

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.

High level of effort exerted in exercising policy choices

Figure 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, 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

text. However, it is still unclear which privacy rights listed can be accomplished by the two mechanisms shown.

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 [15]. 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 [33]. In contrast, a warning reminded a few participants assigned to **wordpress.com** to save their changed settings.

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.

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.

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.

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.

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.

ACKNOWLEDGMENTS

This project is funded in part by the National Science Foundation (CNS-1330596, CNS-1330214), the Carnegie Corporation of New York, and Innovators Network Foundation. We wish to acknowledge all members of the Usable Privacy Policy Project (www.usableprivacy.org) for their contributions.

REFERENCES

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, and others. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 44.

[2] Terence S Andre, H Rex Hartson, Steven M Belz, and Faith A McCreary. 2001. The User Action Framework: A Reliable Foundation for Usability Engineering Support Tools. *International Journal of Human-Computer Studies* 54, 1 (2001), 107–136.

[3] California State Legislature Website. 2018. SB-1121 California Consumer Privacy Act of 2018. (2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[4] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. 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)*.

[5] Digital Advertising Alliance. 2009. Self-Regulatory Principles for Online Behavioral Advertising. (July 2009). http://digitaladvertisingalliance.org/principles.

[6] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor Into IoT Device Purchase Behavior. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*.

[7] European Commission. 2018a. Article 29 Data Protection Working Party. Guidelines on Transparency under regulation 2016/679. (2018). http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm.

[8] European Commission. 2018b. EU Data Protection Rules. (2018). https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[9] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. 2017. Large-Scale Readability Analysis of Privacy Policies. In *Proceedings of the International Conference on Web Intelligence (WI)*. 18–25.

[10] Federal Trade Commission. 2009. CAN-SPAM Act: A Compliance Guide for Business. (2009). https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

[11] Federal Trade Commission. 2017. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. (2017). https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

[12] Stacia Garlach and Daniel Suthers. 2018. 'I'm supposed to see that?'AdChoices Usability in the Mobile Environment. In *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*.

[13] Global Privacy Enforcement Network. 2017. GPEN Sweep 2017: User Controls over Personal information. (2017). https://www.privacyenforcement.net/system/files/2017%20GPEN%20Sweep%20-%20International%20Report_0.pdf.

[14] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*.

[15] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

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

[17] IAB Europe. 2011. EU Framework for Online Behavioural Advertising. (2011). https://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf.

[18] IAB Europe. 2019. GDPR Transparency and Consent Framework. (2019). https://iabtechlab.com/standards/gdpr-transparency-and-consent-framework/.

[19] JustDelete.me. 2019. A directory of direct links to delete your account from web services. (2019). https://justdeleteme.xyz.

[20] Saranga Komanduri, Richard Shay, Greg Norcie, and Blase Ur. 2011. AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements. *A Journal of Law and Policy for the Information Society* 7 (2011).

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

[22] Thomas Linden, Hamza Harkous, and Kassem Fawaz. 2018. The Privacy Policy Landscape After the GDPR. *arXiv:1809.08396* (2018).

[23] Mary Madden and Lee Rainie. 2015. Americans' Attitudes About Privacy, Security and Surveillance. (2015).

[24] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. 2018. Characterizing the use of browser-based blocking extensions to prevent online tracking. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[25] Jonathan R Mayer and John C Mitchell. 2012. Third-Party Web Tracking: Policy and Technology. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*.

[26] Aleecia M McDonald and Lorrie Faith Cranor. 2010. Americans' Attitudes About Internet Behavioral Advertising Practices. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*.

[27] William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. 2016. (Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking. *Proceedings on Privacy Enhancing Technologies* 2016, 2 (2016), 135–154.

[28] Michael Morgan, Daniel Gottlieb, Matthew Cin, Jonathan Ende, Amy Pimentel, and Li Wang. 2018. California Enacts a Groundbreaking New Privacy Law. (2018). https://www.mwe.com/en/thought-leadership/publications/2018/06/california-enacts-groundbreaking-new-privacy-law.

[29] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. 2018. "If I press delete, it's gone" - User Understanding of Online Data Deletion and Expiration. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (2018).

[30] Network Advertising Initiative. 2018. NAI Code of Conduct. (2018). https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.

[31] Nielsen Norman Group. 2018. Top 10 Design Mistakes in the Unsubscribe Experience. (2018). https://www.nngroup.com/articles/unsubscribe-mistakes/.

[32] Donald A. Norman. 1986. Cognitive Engineering. In *User Centered System Design: New Perspectives on Human-Computer Interaction*. Lawrence Erlbaum Associates, 31–61.

[33] Donald A. Norman. 1990. *The Design of Everyday Things*. Doubleday.

[34] Norwegian Consumer Council. 2018. Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy. (2018). https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[35] Online Trust Alliance. 2018. Email Marketing & Unsubscribe Audit. (2018). https://www.internetsociety.org/resources/ota/2018/2018-email-marketing-unsubscribe-audit/.

[36] Enric Pujol, Oliver Hohlfeld, and Anja Feldmann. 2015. Annoyed Users: Ads and Ad-Block Usage in the Wild. In *Proceedings of the Internet Measurement Conference*.

[37] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*.

[38] Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie Faith Cranor. 2016. Watching Them Watching Me: Browser Extensions' Impact on User Privacy Awareness and Concern. In *Proceedings of NDSS Workshop on Usable Security (USEC)*.

[39] Fatemeh Shirazi and Melanie Volkamer. 2014. What Deters Jane from Preventing Identification and Tracking on the Web?. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*.

[40] United States Congress. 1999. S.900 - Gramm-Leach-Bliley Act. (1999). https://www.congress.gov/bill/106th-congress/senate-bill/00900.

[41] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[42] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of Conference on Computer and Communications Security (CCS)*.

[43] Ari Ezra Waldman. 2019. There is No Privacy Paradox: How Cognitive Biases and Design Dark Patterns Affect Online Disclosure. *Current Opinion in Psychology* (2019).