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

Hana Habib, Yixin Zou, Aditi Jannu, Chelse Swoopes,
Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, Florian Schaub

May 4, 2018

Abstract

Many websites provide users with mechanisms to exercise control over their online privacy. The manner in which these mechanisms are implemented can significantly affect users' behaviors and privacy outcomes, as the technical and regulatory landscape related to online data collection continues to evolve. Therefore, it is important to understand how websites offer privacy choices to their visitors, and evaluate whether individuals can make adequate use of these mechanisms. We presented the results from an analysis of data deletion choices and opt-outs for email communications and targeted advertising, and present results from 59 websites. We find that although privacy choices are being offered by a majority of websites, exercising these choices may be difficult or confusing for users in multiple ways, both due to technical implementation and lack of detail in privacy policies. By pinpointing such issues, results from our analysis can improve the overall user experience for expressing these types of privacy controls.

1 Introduction

Many companies send marketing emails to consumers to promote products and services. Targeted advertising is another popular marketing mechanism, in which customized advertisements are delivered to consumers based on preferences and/or interests inferred from data collected using tracking tools. When these marketing strategies are implemented, some companies offer consumers the choice to opt out of receiving marketing emails, targeted ads, or have their accounts and related data removed from the companies' databases.

These marketing, targeted advertising, and data deletion choices often fall under some form of regulatory regime. Within the United States, the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003 [3] established rules for marketing emails, such as requiring businesses to stop sending consumers marketing emails after 10 business days once an opt-out request is made. Industry groups such as the Digital Advertising Alliance (DAA) set self-regulatory standards to make targeted advertising opt-outs available to users [2]. Furthermore, the recent the General Data Protection Regulation (GDPR), adopted by the European Union but are expected to have a worldwide impact, enforces stringent compliance with simple privacy controls for consumers [5], with a special focus on data deletion choices. Under the GDPR, companies must obtain clear consent from users prior data collection, and allow users to withdraw their consent, or opt out, at any time (Articles 7 and 15). Another "right to be forgotten" requirement in GDPR (Article 17) grants users the right to request websites to delete their personal data.

Empirical studies, however, suggest usability and noncompliance issues with these opt-outs [17,19]. Internet users are quite concerned with companies' data collection practices [24], but they struggle to understand and navigate opt-out choices [15]. While ear-

lier studies examined the usability issues of particular types of opt-outs [4,31], we lack resent, large-scale examinations of different opt-outs that have evolved over time in accordance to the change of regulatory regimes.

As part of the Usable Privacy Policy Project [26], we conducted an analysis of Internet privacy choices that are required by laws and available to users today. In our analysis, we collected empirical metrics about data deletion options and opt-out mechanisms for email communications and targeted advertising. Our primary research goals were to better understand current practices used by websites to offer privacy choices, and to inform the design of a better consent and opt-out experience.

Our results suggest that privacy choices related to data deletion, email communications, and targeted advertising are commonly offered, primarily through the website's privacy policy. However, there are multiple reasons users may find them difficult to use and understand. Privacy policies typically omit important details about the privacy choices, such as whether a targeted advertising opt-out would stop all tracking, or a time frame in which a request for account deletion would be completed. Some policies also contain opt-out links that directed the user to an unexpected page, or referred to non-existent privacy choices.

Though it is important for users to have these privacy choices, it is equally important for websites to ensure they are usable. This study lays the groundwork to conduct further evaluations of these choices.

2 Regulatory Framework

In this section, we provide an overview of current legislation and industry self-regulatory guidelines related to our evaluated privacy choices: opt-outs for email and targeted advertising and data deletion options.

Pertaining to email communications, the United States' Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 establishes national standards for companies in the United States that send any form of electronic commercial messages to consumers [3]. It specifically requires that companies must 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, the company must be able to process recipients' opt-out requests for at least 30 days, and any opt-out request must be honored (meaning no longer receive commercial message) within 10 business days. Additionally, the CAN-SPAM Act provides other consumer protections, such as banning the use of false or misleading header information (i.e., the source, destination, and routing information attached to the beginning of an e-mail message) and deceptive subject lines, requiring a clear disclosure when the message is an advertisement, and mandating the inclusion of the sender's physical postal address.

In the early 2000s, industry organizations in the U.S. and Europe, such as the Network Advertising Initiative (NAI), Digital Advertising Alliance (DAA), and Interactive Advertising Bureau Europe (IAB Europe) started formulating sets of principles related to practices used in targeted, or online behavioral advertising [2, 6]. The *Self-Regulatory Principles for Online Behavioral Advertising*, for example, has seven key principles centering on user education, data transparency, opt-out choices, data security, material changes in practices, sensitive data, and accountability of compliance [2]. Specifically, member advertisers are required to provide consumers with the choice to opt out of tracking-based targeting advertising. The scope covers data collected and used by the company, as well as those transferred to other non-affiliated entities. However, it only covers data used for delivering tailored ads, which means data collected for other purposes are not affected [22].

The more recent General Data Protection Regulation (GDPR) in the European Union, however, makes obtaining active agreement from users for data collection related to targeted advertising and other purposes mandatory and no longer voluntary (Article 29). This active agreement must comprise an affirmative action and is not satisfied with pre-checked boxes or idleness from the user (Article 4). It also requires that users be allowed to withdraw their con-

sent at any time (Article 7). Moreover, specific consent for each data processing operation must be provided in an easily acceptable form using simple, clear language and visualization if need be. If the user is a child, the language must be understandable by a child. The GDPR also restricts processing of some categories of personal data, despite having obtained explicit consent (Article 9) [5].

With respects to data deletion, the GDPR also grants European Union residents the "right to be forgotten," which stipulates that, under certain circumstances, companies must comply with requests from users to erase their personal data (Article 17). Examples of these circumstances include when the personal data are no longer needed for their original purposes, when users withdraw their consent, and when the data are illegally processed. One implementation of the "right to be forgotten" would be through account deletion requests, or the ability for users to delete certain information related to their profile [5].

With regards to the United States, there has not been any federal law enforcing the "right to be forgotten", but the State of California does have a similar law pertaining to state residents under 18 years old (minors) (CA Bus & Prof Code Section 22580 in 2013 [7]). This law requires websites, mobile applications, and other online services to provide registered minor users with the choice to remove their public data. Nevertheless, there are several exception circumstances, such as when the information is anonymized, required to be retained by the federal law, or the minor has received respective compensation for providing the information [25].

Our analysis aims to explore the landscape of deletion choices and email and advertising opt-outs, within this regulatory context.

3 Related Work

Prior to our study, others have evaluated available privacy control mechanisms against current regulatory requirements. Previous research has also studied user awareness and attitudes towards these opt-outs, as well as companies' data collection and management practices in general.

3.1 Prior Opt-out Evaluations

Following the passage of the CAN-SPAM Act [3], websites have started offering consumers increased controls for the email messages they receive. A recent audit of top North American retailers by the Online Trust Alliance found that 92% of the websites surveyed offered "unsubscribe" links within the message. However, the study also revealed that some retailers were in violation of the CAN-SPAM Act. [4].

Existing opt-out tools for targeted advertising range from manually blocking third-party cookies in web browsers, installing browser plug-ins, to placing opt-out cookies through industry self-regulatory websites. However, their effectiveness in terms of limiting targeted advertising varies. Many opt-out options, for example, prevent tailored ads from being displayed but do not opt users out of web tracking [11]. Certain browser plug-ins (e.g., Ghostery and Abine Taco) and cookie-based tools were found to be helpful in limiting targeted text-based ads on Google, but the "Do Not Track" [16] option in browsers was relatively ineffective [9].

An additional issue with targeted advertising opt-out tools is noncompliance with self-regulatory guidelines. A study by Hernandez et al. [17] revealed that among Alexa's top 500 websites in the U.S., only about 10% of third-party ads had the required AdChoices icon required to be in compliance with industry self-regulatory principles, and even fewer with the related text. Similar noncompliance issues were found by Komanduri et al. [19] in a large-scale examination of DAA and NAI members in 2011, in which over 80% of members were in full or partial compliance with the privacy notice requirement, but less than half were in compliance with the enhanced notice requirement [19]. They also found several problems with regards to opt-out cookie settings. For example, the two opt-out mechanisms provided by the DAA and NAI set different cookies, but neither functioned in Apple Safari with default settings.

Furthermore, prior evaluations on targeted advertising opt-out tools have revealed numerous usability issues, which impose a heavy burden on users. For instance, the usage of opt-out cookies were found to be cumbersome because they are fragile (i.e., can

easily be modified by third-party companies), and they need to be manually installed and updated [22]. Browser extensions such as TACO partially mitigate these issues, but they have their own usability issues as well [20]

The graphical user interfaces for the tools offered by industry self-regulatory groups also suffer from usability issues. A study by McDonald and Cranor demonstrated the unintuitive nature of the NAI's opt out page: only about 10% of surveyed participants were able to tell that the purpose of the page was to help users opt out of targeted advertising, rather than tracking or ads from specific companies [24]. An in-lab user evaluation conducted by Leon et al. on nine different targeted advertising opt-out tools found that most users could not complete the opt-out without guidance, or spent a significant amount of time exercising privacy preferences, and no users had a clear idea about the consequence of opting out [20].

Recent efforts in opt-out analysis have moved towards the utilization of automatic extraction tools to enhance the scale and accuracy of analysis. For instance, Cranor et al. [14] developed an automated parsing program to extract and evaluate the privacy policies of U.S. financial institutions, and provided valuable insights about the state of compliance with federal standards, as well as variances among different institutions. In another work conducted by Sathyendra et al. [27], classification models were adopted to identify opt-out choices in websites' and mobile apps' privacy policies, offering implications for developing relevant systems to help users learn about their choices. Ultimately, these techniques demonstrate the prospect of automating manual analysis, and building tools to extract opt-out choices buried in the long text of privacy policies, and present them in a user-friendly manner.

Our work will build off these prior findings to evaluate different types of privacy choices, such as data deletion mechanisms and opt-outs for email communications, which may suffer from similar usability issues as opt-outs for targeted advertising. It also aims to test the usefulness of automated extraction tools in helping users exercise available privacy choices.

3.2 User Attitudes and Awareness

Internet users consider targeted advertising as a double-edged sword [18]. On one hand, targeted advertising is favored when it is perceived to be personally relevant to consumers, and empirical evidence suggests it stimulates purchase behaviors [10,18]. On the other hand, it triggers significant privacy concerns, particularly centering on the large amount of sensitive data being collected, shared, and used in a nontransparent way [18].

A line of research has examined users' objection to targeted advertising as being privacy invasive. Turow et al. conducted a nationwide survey and revealed that more than 70% of respondents reported they did not want marketers to collect their data and deliver ads, discounts, or news based on their interests [30]. Similarly, McDonald and Cranor found that 55% of survey participants preferred not to see interest-based ads [24] . These findings are supported by qualitative work, such as Ur et al.'s interview-based study in which participants expressed a general objection to their data being tracked and monitored [31].

Based on the controversies surrounding targeted advertising, Tene and Polenetsky suggested that the focus of the debate should be whether targeted advertising creates more societal values and economic efficiency over their harmful impacts on individuals' privacy, and moreover, the burden of privacy control should be placed on businesses to follow better privacy practices, rather than individuals to make sense of privacy notices [29]. This view also emerged in Turow et al.'s study in which 38% of respondents expressed the view that companies should devote efforts to consumer privacy protection [30].

Despite being concerned about the privacy implications of targeted advertising, consumers struggle to protect their online privacy for multiple reasons [12, 20]. Estrada-Jiménez et al. summarized three aspects that limit users' capabilities in dealing with targeted advertising [15]. First is a lack of awareness, such as being unaware of being tracked until seeing strong evidence suggesting the leakage of personal information (e.g., embarrassing ads [8]). The second is the power asymmetry between individual consumers and entities in the targeted advertising

ecosystem (e.g., ad networks, ad platforms, and data aggregators), so that user preferences and concerns are not strictly enforced. The third issue identified is bounded technical knowledge to fully understand and utilize privacy-enhancing technologies [15].

The last point, specifically, has been supported by a body of empirical work on user knowledge of targeted advertising mechanisms and related opt-out tools. For instance, McDonald and Cranor found that the majority of users know about the existence of customized ads based on visited websites, but only 39% of participants knew that ads they see can also be based on their email content [24].Yao et al. found common misconceptions among participants' mental models of targeted advertising. Some participants considered trackers as hackers or viruses, and others speculated that trackers access local files and reside locally on one's computer [32].

Moreover, users show little awareness and poor understanding of opt-out tools for targeted advertising. For example, Ur et al.'s study showed that many participants did not recognize the DAA's AdChoices icon used to signify that an ad is a result of targeted advertising, and misinterpreted its purpose [31]. McDonald and Cranor demonstrated that participants held misconceptions about how cookies function and the methods offered to opt out of tracking cookies [24]. They also found that participants misunderstood the text description of opt-out cookies provided by the ad industry [23, 24]. This suggests that the adoption of opt-out tools faces significant barriers, and demonstrates the importance of user education, as users cannot be expected to be able to make an informed decision about targeted advertising when they cannot understand the mechanisms they can use to opt out [24].

4 Manual Annotation

We developed an annotation template to standardize the procedures for analyzing each website. Using this template, we annotated the privacy choices available on 59 websites. We found that privacy choices, particularly opt-outs for email communications and targeted advertising, were widely available. However, our annotations also revealed several reasons exercising these choices may be difficult for online users.

4.1 Methodology

We iteratively developed an analysis and annotation template which we implemented Qualtrics[1] to collect metrics about the data deletion, email, and targeted advertising choices offered by websites. For the purpose of our analysis, we considered data deletion mechanisms as a means through which users could delete their account or information related to their account, including via an email to the company. We defined opt-outs for email communications as mechanisms that allowed users to request that a website stop sending them any type of email message (e.g., marketing, surveys, newsletters). Any link to an advertising industry website or opt-out tool, as well as advertising related settings implemented by the website were considered as opt-outs for targeted advertising.

In an annotation of a website, researchers visited different pages of the website and answered the relevant questions in the template related to data deletion choices and opt-outs for email communications and targeted advertising. For all choices, we recorded information such as where the privacy choice is located, the shortest path to it as measured by number of user actions required to exercise the choice, and other information about it described in privacy policy. To prevent the researchers' browser cookies or cookie settings from altering the content displayed by a website, annotations were done in private browsing mode. Annotators were asked to:

1. Visit the homepage of the website
2. Create a user account for the website
3. Annotate any opt-outs for targeted advertising on a page linked from the homepage that explains the website's advertising practices (e.g., "AdChoice")
4. Extract the HTML of the website's privacy policy for our automated analyses

[1] Qualtrics: https://www.qualtrics.com/

5. Annotate any opt-outs for email communications in the privacy policy
6. Annotate any opt-outs for targeted advertising in the privacy policy
7. Annotate any data deletion mechanisms in the privacy policy
8. Note whether the privacy policy mentions Do Not Track
9. Note any other privacy choices in the privacy policy
10. Annotate any opt-outs for email communications in the user account settings
11. Annotate any opt-outs for targeted advertising in the user account settings
12. Annotate any data deletion mechanisms in the user account settings
13. Note any other privacy choices in the user account settings

The full annotation template is provided in Appendix B.

To refine the template, our research team conducted six rounds of piloting with 25 unique websites between September 2017 and March 2018 from Amazon Alexa's[2] ranking of top 50 U.S. websites. For every round of piloting, two researchers independently annotated a small set of websites. The researchers then reconciled disagreements in the annotations, and collaboratively revised the questions in the template to ensure that there was a mutual understanding of the metrics being collected.

For our full analysis, we annotated 59 websites sampled from Alexa's ranking of global top 10,000 websites (as of March 2018). Our analysis excludes adult-content websites, websites that are not in English, and websites that require personal information (such as a social security number) or organization affiliation for account registration. Annotations for the full analysis were all conducted in April 2018, and annotations from our pilot rounds are not included in our full analysis. Due to GDPR, many websites were releasing new versions of their privacy policies during the period of our data analysis. As seen in Table 1, the majority of the websites analyzed were registered in the United States, based on their ICANN "WHOIS' record. The full list of websites can be found in the Appendix.

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

Region	# of Websites
United States	38
Europe	11
Canada	5
India	3
China	2

Table 1: The number of websites located in each region, based on their ICANN "WHOIS" record.

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. Figure 1 plots the reach against rank of the top 10,000 websites. We selected two thresholds at which the reach of websites level off: rank 200 and rank 5,000. Thus, we categorized the websites as: *top websites* (ranks 1 - 200), *middle websites* (ranks 201 - 5,000), and *bottom websites* (ranks $>$ 5,000).

Our analysis included 19 *top*, 21 *middle*, and 19 *bottom* websites. Annotations were completed in stages, such that researchers annotated websites contained in one category at a time. To ensure that annotations were thorough and consistent, two researchers independently coded nine (15%) websites sampled from each category. Cohen's kappa was averaged over 50 questions that were considered to be the primary data points for our analysis, resulting in $\kappa = 0.52$. Some of these questions only appeared based on responses to previous questions, resulting in a relatively low agreement. All disagreements in annotations were reviewed and reconciled, prior to the remaining websites in that category being annotated by a single researcher. Researchers completed annotations of a website in a range of 5 to 50 minutes, with an average of 25 minutes spent per website.

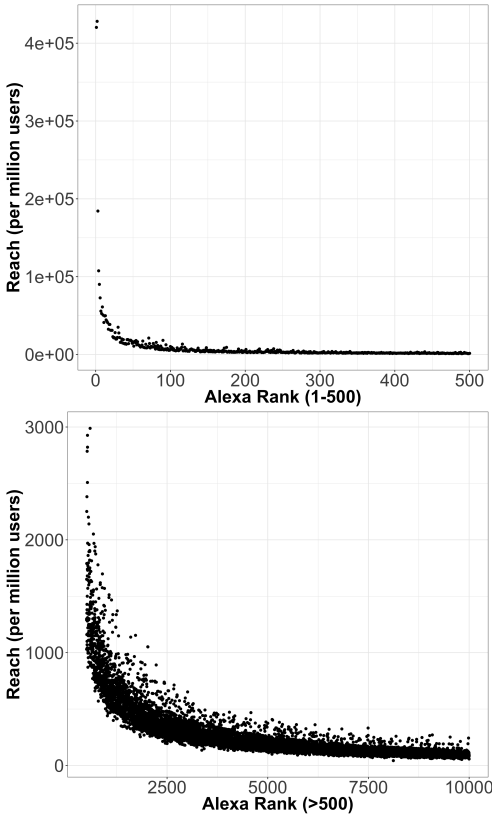

Figure 1: Reach per million users plotted against rank of the top 10,000 websites. The top graph includes ranks above 500, while the bottom includes the rest. We picked ranks 200 and 5,000 as the dividing thresholds for our categories.

4.2 Results

Using our annotation template, we recorded data points from each website related to the presence, privacy policy description, and usability of privacy choices. We found that privacy choices were commonly available on the websites analyzed. However, our annotations indicate that not all of these choices offered are usable due to both technical errors and vague policy text.

4.2.1 Presence of Privacy Choices

Out of the 59 websites analyzed, 53 had privacy policies. Of these 53 websites, 45 (85%) stated in their privacy policy that the website sends marketing communications, and 34 (64%) notified users in their privacy policy that the website uses targeted advertising. At least one opt-out for marketing communications was provided by 39 of the 45 (87%) websites that sent marketing communications, and 31 of the 34 (91%) websites with targeted advertising offered at least one opt-out on the website for targeted ads. Thirty-one websites (53%) in our analysis provided some form of data deletion mechanism to users.

The location of privacy choices across top, middle, and bottom websites is displayed in Figure 2. Top websites provided the most privacy choices out of the three categories, though middle and bottom websites were not significantly behind. Opt-outs for email communications were most frequently offered through more than one means. Thirty-nine websites presented opt-outs for email communications in the privacy policy, 30 stated in the privacy policy that users could unsubscribe within emails, 22 had an opt-out in the account settings, and 12 websites provided an opt-out during account creation.

Websites relied more heavily on their privacy policy to provide opt-outs for targeted advertising. All 31 websites which offer at least one opt-out for targeted advertising provided them through the website's privacy policy. Five websites also included opt-outs in the user account settings, and five websites had an "Ad Choices" page linked from the home page that described the website's advertising practices and presented opt-out choices. As seen in Figure 3, many websites solely used opt-out tools provided by the advertising industry. Top websites were the most likely to have implemented their own opt-outs.

Three websites of the 59 displayed a cookie consent notice, which alerts users that cookies are being used on the website and get consent to place cookies in the user's browser. One of these websites was registered in Europe, while the other two were U.S.-based. Only two offered a means to opt-out or change cookie related settings.

Mechanisms to delete data were the least present

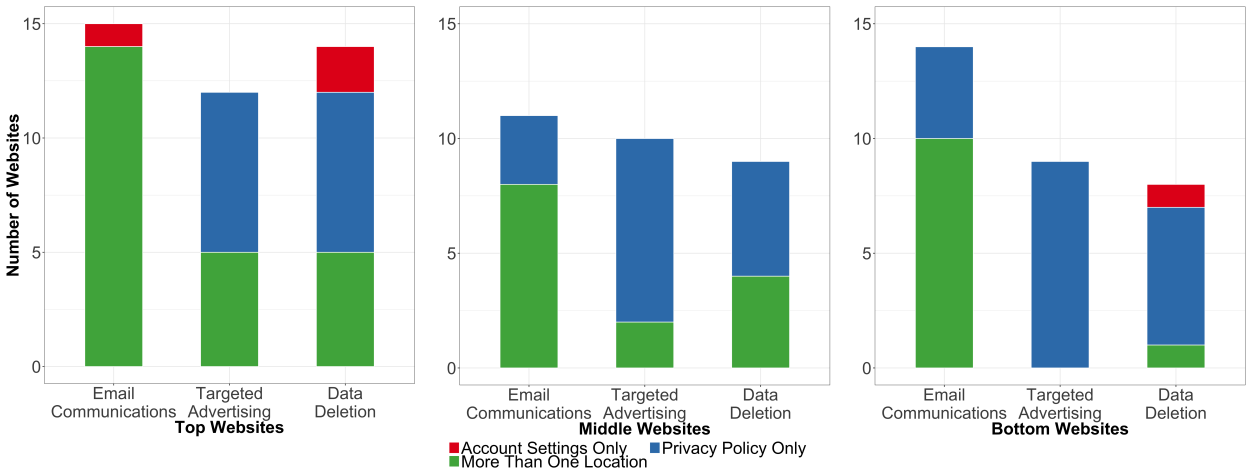

Figure 2: Location of privacy choices across top, middle, and bottom websites. Top websites had the most privacy choices available to users.

on the websites analyzed, especially on bottom websites. This is of note as the GDPR requires websites to offer these mechanisms if the website handles personal data of citizens from the European Union. Of the 59 websites, 29 provided data deletion choices through the privacy policy and 13 displayed them in the user account settings. Most commonly, users were presented the option to have their account permanently deleted, as was offered by 22 websites. Fourteen websites also provided mechanisms to select certain types of information to be removed from the account, while four allowed users to temporarily suspend or deactivate their account.

4.2.2 Privacy Policy Descriptions of Choices

Our annotations of websites also included information provided to users related to different privacy choices in the privacy policies. Of the 59 websites analyzed, 53 (90%) provided users with a privacy policy linked from the home page. Our annotations did not note policies located elsewhere on the website, as those policies would likely not be easily discovered by an average user.

Section Headings: Table 2 summarizes the keywords used to present privacy choices to users. Terms related to "personal information or personal data" and "preference or choice" were commonly used in the headings of sections containing any type of privacy choice. Other keywords were more directly related to the privacy choice contained in the section. For example, 12 policies used either "email" or "communications" to describe opt-outs for email communications, and 13 used the terms "ads" or "advertising" for targeted advertising related opt-outs. Data deletion options were presented in sections described using both terms pertaining to "personal information" and "control" or "access" (e.g.,"How you can access and control the information we collect").

Email Communications: Opt-outs related to email communications were largely for marketing or promotional email from the website, as indicated by 25 policies. Thirteen policies stated users could opt-out of receiving website announcements and updates. Other less common forms of emails sent by websites included newsletters, notifications about user activity, and surveys. Some websites offered opt-outs for different types of communications, in conjunction with email opt-outs. Three websites also allowed

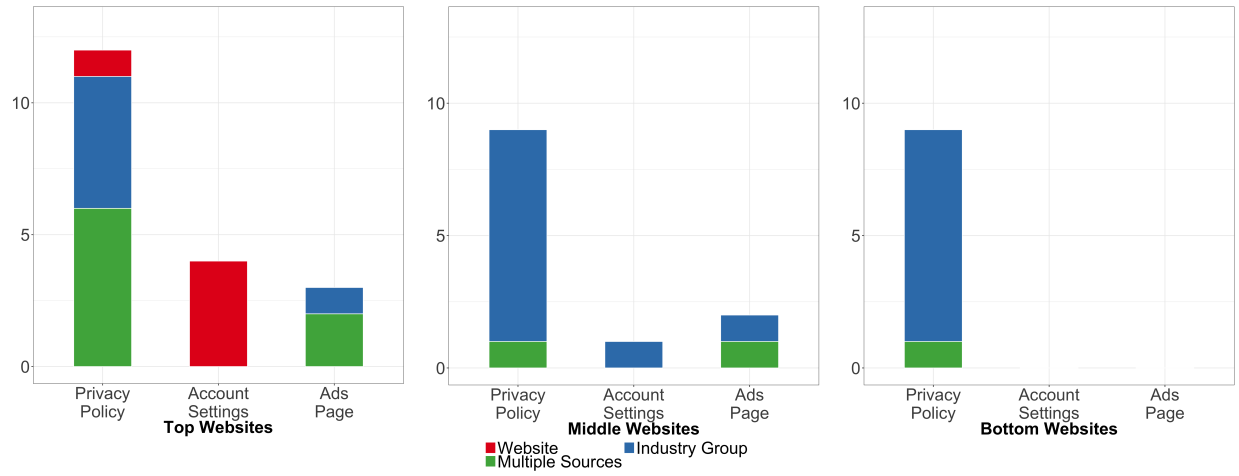

Figure 3: The distribution of different types of targeted advertising opt-outs across top, middle, and bottom websites.

users to opt out of SMS communications, and two offered opt-outs for commercial phone calls from the website.

Targeted Advertising: For the most part, privacy policies did not describe whether users were opting out of tracking entirely or just the display of targeted advertisements. Only seven of the 31 websites that offered opt-outs for targeted advertising made this distinction within the policy text. Similarly, 26 of these websites' policies did not specify whether the opt-out would be effective across different devices, and 24 did not clarify whether the opt-out applied across all the browsers a user has installed.

Data Deletion: Similarly, not much information was provided about data and account deletion mechanisms. Of the 28 websites providing these choices in their privacy policy, 25 (89%) did not describe a time frame in which a user's account would be permanently deleted. Three websites stated that the information related to a user's account would be deleted within 30 days of the user deleting their accounts. One website stated it would take up to one year to remove all of a user's information. Related to a user's right to access, users were charged a fee to access their personal information, as allowed by the GDPR, on two of the websites analyzed [5].

Other Privacy Choices: Though less common than opt-outs for email communications and targeted advertising, and data deletion choices, some websites offered other types of privacy related opt-outs to users. As seen in Table 3, the most common of these was opt-outs for the sharing of personal information with third parties, offered by seven websites.

Of the 53 policies analyzed in our sample, only one specified that it would honor Do Not Track (DNT), a mechanism that allows users to express that they wish not to be tracked by websites [16]. Another 34 did not specify whether or not they would respect the DNT header, while five explicitly stated that the website will not honor it.

4.2.3 Usability of Privacy Choices

Our annotations also included how many steps users had to take to exercise a privacy choice. We counted user actions as the number of clicks, hovers, or form boxes encountered during the process of applying a privacy choice, from the home page up until the point of applying the privacy choice. Table 4 displays summary statistics related to the shortest path available

Key Words	Example	Email Communications	Targeted Advertising	Data Deletion
Personal Info/Data	*How We Use Your Data*	15	6	18
Preference/Choice	*What Choices Do I Have?*	12	8	9
Email/Communications	*Electronic newsletters policy*	12	0	0
Marketing	*Marketing Purposes*	5	0	0
Control/Access	*Information and Access*	4	0	13
Opt Out	*Opt-Out Rights*	3	2	2
Account	*Accounts and User Profiles*	1	0	5
Deletion	*How Can I Delete My Account?*	1	0	6
Ads/Advertising	*Internet-Based Advertising*	0	13	0
Cookies/Tracking	*How to manage or refuse cookies*	0	7	0
Other		4	4	2

Table 2: A summary of the keywords used in privacy policy section headings containing privacy choices. Counts are the number of policies in which terms related to a particular keyword were used in the section heading containing a privacy choice. Some policies described the same privacy choice under multiple headings, or used multiple keywords in the section heading.

Opt-Out Type	# of Websites
Third-Party Sharing	7
Google Analytics	6
All First-Party Cookies	5
Location History Tracking	5
Inferred Interests	5
Collection of Device Identifiers	4

Table 3: Other forms of privacy choices available to users on the websites analyzed.

to exercise choices of each type provided on the website. Opt-outs for email varied widely, while those for targeted advertising and data deletion mechanisms required a similar number of user actions. The variation in opt-outs for email communications could be because some websites send multiple types of commercial messages, such as updates and recommendations.

	Min	Max	Mean	Median	SD
Email Communications	2	10	4.3	3	2.5
Targeted Advertising	1	5	3.2	3	0.92
Data Deletion	3	5	3.9	4	0.86

Table 4: Summary statistics for the minimum number of user actions required to exercise privacy choices, counted from the home page until the action recording the choice (i.e., "save/apply" button).

While completing annotations, we noted several points of confusion in policies related to privacy choices. For example, some websites mentioned user accounts in the privacy policy but no mechanisms to create a user account were observed on the website. In some cases this was because the policies were outdated, while in others the policy available covered a family of websites in which some websites did have user accounts. In other instances, text in the policy referred to an opt-out elsewhere, but that opt-out did not exist. On two websites, the privacy policy stated that users could opt-out of marketing messages by emailing them, but the email address was missing from the text. A few of the opt-out links analyzed directed users to pages that were not related to the opt-out, such as the website's home page, the account settings for a parent website, or, as in one case, Facebook's developer documentation.

Another common issue was that some websites had policies that were difficult to navigate due to confusing navigation menus or placement of policies in small pop-up boxes. Websites also sometime provided different privacy statements for different platforms, providing users different privacy choices for their mobile device than for their laptop or desktop computer. Conversely, a one website made additional efforts to make their privacy policy more accessible to users by providing users with a short video introducing their privacy practices.

5 Programmed Analysis

We plan to scale certain metrics from our manual analysis, such as whether opt-out or data deletion choices exist in the privacy policy, by leveraging tools developed by the Usable Privacy Policy Project [21, 27, 28, 33]. This is still work in progress.

6 Discussion

We conducted an empirical analysis of privacy choices related to email communications, targeted advertising, and data deletion on 59 websites. Overall, we found that privacy choices are available on websites, largely through privacy policies. However, the terms used in privacy policies to present privacy choices vary from website to website. Our analysis uncovered several issues that impact the usability of privacy choices, such as broken links. Lastly, our findings confirm those from prior work which demonstrated that policies typically lack meaningful information related to privacy choices that would aid user understanding [13].

6.1 Limitations

While our study provides important insight into the current landscape of privacy choices available to users, our findings have limitations. One major limitation is that our sample only included English-language websites, which may not be reflective of websites in other languages. Another limitation related to our particular sample of websites is that we only included websites from Alexa's list of top 10,000. Websites with lower rankings may offer a different distribution of privacy choices compared to that observed in our sample.

Additionally, while we noted other privacy choices available to users in privacy policies, we did not annotate these choices with the same depth as we did data deletion mechanisms and opt-outs for email communications and targeted advertising opt-outs. Though there are likely interesting findings related to other privacy choices, we believe our focus on these more common choices provides us with a better understanding of how privacy choices are generally offered by websites.

Another factor which may impact our findings is that our annotations were conducted four to seven weeks prior to the GDPR going into effect on May 25, 2018. Some privacy policies in our analysis may have been recently updated for GDPR, while others might not have been. As GDPR mandates some of the privacy choices we analyzed for websites that collect information from citizens of the European Union, we may have observed extremely recent changes to privacy choice offerings.

Lastly, since our annotations were conducted using IP addresses based in the United States we may not have observed privacy choices available to residents of other jurisdictions that have other legal privacy requirements. In particular, the European Data Protection Directive (which is being replaced by GDPR) was in effect at the time of data collection. Our analysis thus only reflects privacy choices available to U.S.-based consumers.

6.2 Design Implications

Our findings indicate that there are likely several reasons users may find exercising privacy choices difficult or confusing, making these choices potentially ineffective. Companies may be able to improve the usability of their privacy choices by addressing these issues.

Umbrella Privacy Policies: Some of the points of confusion highlighted in Section 4.2.3 can be attributed to the use of one policy for a family of websites. This lead to issues such as links from the policy being directed to unrelated pages on a parent company, and references to account settings even when the website did not offer mechanisms to create user accounts. While maintaining one policy may be easier for parent companies, this places the burden on users to figure out what policies apply for a particular website, which may not be possible for them to do. To mitigate such issues privacy policies need to be reviewed to ensure that the information provided is applicable to all the websites on which the policy is used.

Confusing Terminology: As noted in Section 4.2.2, there was variation in the keywords used in the headings of privacy policy sections in which privacy choices were described. 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 Choices" in others. Even more confusing, some policies contained multiple titles similar to both of these. This inconsistency from policy to policy may make finding specific privacy choices harder for users. Standardizing section headings, as was done for privacy notices provided by U.S. financial institutions [1], might be a step toward making privacy choices more usable.

Multi-Step Processes: Another way expressing privacy choices may be frustrating for users is that they typically require multiple steps. As described in Section 4.2.3, the privacy choices annotated required an average of three to four user actions prior to pressing a button to apply the choice, assuming the user knew which pages to navigate to beforehand. On the extreme end, opting-out of email communications from Spotify required 10 user actions as the interface required users to uncheck several boxes related to different communication types. Though this type of interface allows users to have greater control over the messages they receive, to minimize user effort websites should also have a "one-click" opt-out box visible to users without scrolling. Additionally, privacy choices should be registered with the website once a user selects or unselects an option, as pressing a "save" or "apply" button may not be intuitive, especially if it is not visible to the user without scrolling. This would avoid situations in which a user thinks they have completed an opt-out, but their choice was not registered by the website.

Different Opt-Out Options: Our analysis also revealed that sometimes websites offer different opt-out choices on different pages of the website, for the same opt-out type. For example, Kijiji (a subsidiary of eBay) provided links to opt-outs implemented by eBay and three advertising groups (DAA, DAAC, and EDAA) in a "AdChoice" page linked to the home page, but only opt-outs implemented by eBay in the privacy policy. By looking at just the privacy policy, where websites most frequently present privacy choices, a user would miss other opt-outs available to them as described by the website. Additionally, a user who did see all four opt-outs on the "AdChoice" might not know which ones to use. Providing all privacy choices in a centralized location, such as a privacy choices page, could help users locate privacy choices more easily.

6.3 Future Work

We plan to continue our analysis with an additional 200 websites from the Alexa global top websites. The results of this study could inform the design of a user study to highlight further design and implementation issues with opt-outs. This study could also explore whether these opt-outs are conceptualized and utilized differently by individual end-users with different backgrounds and characteristics, such as those with cybersecurity knowledge or higher level of privacy concern. Another direction would be to examine whether these opt-outs are functioning in the way as claimed by the website or third-parties from a technical perspective. The findings from our analysis, as well as such further evaluations of privacy choices, could be used to develop a more usable opt-out platform for websites to adopt.

Acknowledgements

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] Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 2009.

[2] Self-Regulatory Principles for Online Behavioral Advertising, Jul 2009. http://digitaladvertisingalliance.org/principles.

[3] CAN-SPAM Act: A Compliance Guide for Business, Mar 2017. https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

[4] Email Marketing & Unsubscribe Audit, Dec 2017. https://otalliance.org/system/files/files/initiative/documents/2017emailunsubscribeaudit.pdf.

[5] Home page of the european union general data protection regulation (gdpr), 2017. https://www.eugdpr.org/eugdpr.org.html.

[6] NAI Code of Conduct, 2018. https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.

[7] Privacy Rights for California Minors in the Digital World, 2018. https://law.justia.com/codes/california/2013/code-bpc/division-8/chapter-22.1/section-22580/.

[8] Lalit Agarwal, Nisheeth Shrivastava, Sharad Jaiswal, and Saurabh Panjwani. Do not Embarrass: Re-Examining User Concerns for Online Tracking and Advertising. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, page 8. ACM, 2013.

[9] Rebecca Balebako, Pedro Leon, Richard Shay, Blase Ur, Yang Wang, and Lorrie Faith Cranor. Measuring the Effectiveness of Privacy Tools for Limiting Behavioral Advertising. In *Proceedings of the Web 2.0 Security and Privacy Workshop (W2SP)*. IEEE, 2012.

[10] Alexander Bleier and Maik Eisenbeiss. The Importance of Trust for Personalized Online Advertising. *Journal of Retailing*, 91(3):390–409, 2015.

[11] Sophie C Boerman, Sanne Kruikemeier, and Frederik J Zuiderveen Borgesius. Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3):363–376, 2017.

[12] Lorrie Faith Cranor. Can Users Control Online Behavioral Advertising Effectively? *IEEE Security & Privacy*, 10(2):93–96, 2012.

[13] 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 (ISJLP)*, 11:325, 2015.

[14] 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 (TWEB)*, 10(3):17, 2016.

[15] 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.

[16] Roy T Fielding and David Singer. Tracking Preference Expression (DNT). W3C Candidate Recommendation, 2017. https://www.w3.org/TR/tracking-dnt/.

[17] 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.

[18] 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.

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

[20] 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 SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2012.

[21] Frederick Liu, Shomir Wilson, Peter Story, Sebastian Zimmeck, and Norman Sadeh. Towards Automatic Classification of Privacy Policy Text. Technical report, 2017.

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

[23] Aleecia M McDonald and Lorrie Faith Cranor. An empirical study of how people perceive online behavioral advertising. Technical report, CMU-CyLab-09-015, Carnegie Mellon University, 2009.

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

[25] Susan Ross. California Enacts "Right to be Forgotten" for Minors.

[26] Norman Sadeh, Alessandro Acquisti, Travis D Breaux, Lorrie Faith Cranor, Aleecia M McDonald, Joel R Reidenberg, Noah A Smith, Fei Liu, N Cameron Russell, Florian Schaub, et al. The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About. Technical report, CMU-ISR-13-119, Carnegie Mellon University, 2013.

[27] 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)*. SIGDAT, 2017.

[28] Peter Story, Sebastian Zimmeck, and Norman Sadeh. Which Apps have Privacy Policies? Technical report, 2018.

[29] Omer Tene and Jules Polenetsky. To Track or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law Science & Technology*, 13:281, 2012.

[30] 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.

[31] 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.

[32] 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.

[33] Sebastian Zimmeck, Ziqi Wang, Lieyong Zou, Roger Iyengar, Bin Liu, Florian Schaub, Shomir Wilson, Norman Sadeh, Steven M Bellovin, and Joel Reidenberg. Automated Analysis of Privacy Requirements for Mobile Apps. In *Proceedings of the Network and Distributed System Security (NDSS) Symposium*, 2017.

A Websites Analyzed

17track.net, abebooks.com, adobe.com, adorama.com, artsy.net, avclub.com, booking.com, bovada.lv, buzzfeed.com, coinmarketcap.com, craiglist.org, dailymail.co.uk, dailymotion.com,

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)

desmos.com, discordapp.com, ebay.com, eurowings.com, fangraphs.com, file-upload.com, findlaw.com, furaffinity.net, gamepress.gg, github.com, google.com, hsn.com, kijiji.ca, ladbible.com, letgo.com, lpu.in, metacrawler.com, mit.edu, momjunction.com, myspace.com, notepad-plus-plus.org, opera.com, ou.edu, php.net, phys.org, playhearthstone.com, reddit.com, researchgate.net, rumble.com, salesforce.com, shein.in, signupgenius.com, slideshare.net, space.com, spotify.com, stackexchange.com, theathletic.com, trustedreviews.com, tufts.edu, tumblr.com, ucl.ac.uk, uottawa.ca, upsc.gov.in, volvocars.com, wattpad.com, wordpress.com

B Website Annotation 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)]
   - ☐ 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?

    Step 4: Now please go back to the homepage if you are not already there.
11. 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 Q11 = 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.
12. Please copy and paste the URL for this page. Retrieve this policy through the policy retrieval tool.
13. Please copy and paste the title of the site's privacy policy.
14. 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.

15. 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)

16. 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

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

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

19. 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 up-

dates
- ☐ Site announcements
- ☐ Surveys
- ☐ Mails
- ☐ Phone calls
- ☐ Text Messages/SMS
- ☐ Other (please specify)
- ☐ None of the above

20. 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

21. 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

22. 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 Q22 = Yes, there's one link to a marketing opt-out or Q22 = 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.

23. 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

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

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

26. 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 Q11 = 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

27. 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

28. 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

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

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

31. 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)

32. 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)

33. 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)

34. 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
- ☐ The website
- ☐ The browser or operating system (e.g., instructions to clear cookies or reset device advertising identifier)
- ☐ Google/Doubleclick
- ☐ Other groups (please specify)

35. 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.

36. Do any of the links in the privacy policy to the OBA opt-outs work?

- ○ Yes, they all work
- ○ Some work, but some do not
- ○ No, none of the OBA opt-out links work

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

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

39. 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?

    Logic: The following question is displayed if Q11 = 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.

40. 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 Q40 = Yes

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

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

43. 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)

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

45. 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)

46. 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)

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

48. 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 Q48 = Yes, there're one link or Q47 = Yes, there're multiple links

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

49. 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

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

51. 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.

52. 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.

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

54. 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

55. 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)

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

57. 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.

58. 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)

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

60. 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 Q60 is not "Yes"

61. 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

62. 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.

63. Is there any OBA opt-out located in the account settings?

- ○ Yes
- ○ No
- ○ Not applicable (the site doesn't use OBA)
- ○ Other (please specify)

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

65. 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 Q65 is not "Yes"

66. 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)

67. 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)
68. 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)
69. 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)
70. 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.

71. Is there any data deletion option located in the account settings? [Yes, No, Other (please specify)]
72. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion to this data deletion option?
73. 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 Q73 is not "Yes"

74. 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)
75. Please copy and paste the specific types of data it indicates. Use ";" to separate multiple items.
76. 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)
77. 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)

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.

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

79. 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

80. Please add any comments in the section below.