(Un)clear and (In)conspicuous: The right to opt-out of sale under CCPA

Sean O'Connor
Pomona College
swow2015@mymail.pomona.edu

Ryan Nurwono
UC Berkeley
ryanjnurwono@gmail.com

Aden Siebel
Pomona College
amsa2017@mymail.pomona.edu

Eleanor Birrell
Pomona College
eleanor.birrell@pomona.edu

ABSTRACT

The California Consumer Privacy Act (CCPA)—which began enforcement on July 1, 2020—grants California users the right to opt-out of sale of their personal information. In this work, we perform a series of manual observational studies (conducted in July 2020, January 2021, and July 2021) to understand how websites implement this right. We find that the vast majority of sites that implement opt-out mechanisms do so with a Do Not Sell link rather than with a privacy banner, and that many of opt-out controls exhibit features such as nudging and inconvenience factors (e.g., fillable forms). We then perform a pair of user studies with 4357 unique users (recruited from Google Ads and Amazon Mechanical Turk) in which we observe how users interact with different opt-out mechanisms and evaluate how the observed implementation choices—exclusive use of links, nudging, and inconvenience factors—affect the rate at which users exercise their right to opt-out of sale. We find that these design elements significantly deter interactions with opt-out mechanisms—including reducing the opt-out rate for users who are uncomfortable with the sale of their information—and that they reduce users' awareness of their right to opt-out.

CCS CONCEPTS

• **Security and privacy** → **Privacy protections**; **Usability in security and privacy**; • **Social and professional topics** → *Governmental regulations*; • **Human-centered computing** → *Empirical studies in HCI*.

KEYWORDS

CCPA; privacy regulations; opt-out mechanisms; dark patterns

ACM Reference Format:
Sean O'Connor, Ryan Nurwono, Aden Siebel, and Eleanor Birrell. 2021. (Un)clear and (In)conspicuous: The right to opt-out of sale under CCPA. In *Proceedings of the 20th Workshop on Privacy in the Electronic Society (WPES '21), November 15, 2021, Virtual Event, Republic of Korea.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3463676.3485598

WPES '21, November 15, 2021, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-8527-5/21/11…$15.00
https://doi.org/10.1145/3463676.3485598

1 INTRODUCTION

In recent years, growing recognition of the potential for exploitation of personal data and of the shortcomings of prior privacy regimes has led to the passage of new online privacy regulations, notably the EU's General Data Protection Regulation (GDPR)—which went into effect on May 25, 2018—and the California Consumer Privacy Act (CCPA)—which began enforcement on July 1, 2020. Several pieces of work have looked at the effect of GDPR on privacy policies and data practices [22, 29, 32, 34, 40]. This work investigates implementations of CCPA requirements and their effects on user privacy, in particular their effect on users' awareness of and likelihood of invoking their right to opt-out of sale of their personal information.

As a first step, we performed a series of manual observational studies to understand how websites implement the opt-out of sale requirement imposed by CCPA. Our first observational study classified the Alexa Top 500 U.S. websites by whether and how they implemented this right immediately after enforcement of CCPA began (between July 1-15, 2020). To understand how enforcement evolved in the first year after enforcement began, we reproduced the observational study in January 2021 and July 2021.

Immediately after enforcement began in July 2020, we found that 207 (41.4%) of the Top 500 websites provided some implementation of the right to opt-out of sale on the desktop version of their site and 116 (23.2%) claimed that they did not sell personal information as defined by CCPA. 163 (33.5%) websites both failed to provide an opt-out and did not specifically deny selling information as defined by CCPA, indicating potential non-compliance with the law. Over the next year, the number of websites potentially not in compliance dropped (to 53 in January 2021 and to 30 in July 2021), with a slight increase in the number of sites that offered opt-out mechanisms (to 230) and a significant increase in sites that claimed to not sell personal information as defined by CCPA (to 238).

Among the observed opt-out mechanisms, UI elements and design choices likely to decrease interaction were common. Just 18 websites notified users of their right to opt-out of sale in banner, while most websites posted only the required homepage link (often visible only after scrolling down to the bottom of the page). Furthermore, even after clicking on a Do Not Sell link, many websites required significant additional work from users to opt-out, such as filling out forms or following directions for further steps, rather than presenting them with a single opt-out button. Finally, nudging (e.g., visually de-emphasizing the Do Not Sell button), unclear interfaces, and other *dark patterns* were common.

To understand how the observed design choices affect users' behavior (e.g., whether they invoke their right to opt-out of sale) and users' awareness of their right to opt-out, we then conducted a pair of user studies. We implemented an aggregated news website that logged how users interacted with the website—particularly how they interacted with various different implementations of a Do Not Sell opt-out mechanism. We recruited 4357 unique California users through Google Ads and Amazon Mechanical Turk, and we observed their behavior. Users recruited through Amazon Mechanical Turk also completed a follow-up survey.

In our first study, we investigated how the format of a Do Not Sell mechanism affected user privacy. We found that users assigned to the link-only condition interacted with the Do Not Sell mechanism significantly less frequently and were significantly less likely to invoke their right to opt-out of sale compared to users who were shown a banner. Among Mechanical Turk users, those assigned to the link-only condition were significantly less likely to be aware that they had a right to opt-out of sale of their personal data than users assigned to conditions with banners. Among the conditions with banners, users were generally more likely to interact with banners located at the top of the page, particularly a full-width bar banner or a banner in the top right-hand corner.

In our second study, we explored the effect of nudging and inconvenience factors (e.g., having to fill out a form or having to select multiple options) on user interactions with a Do Not Sell mechanism. We found that highlighting did not significantly affect how users interact with an opt-out banner, but that other nudging mechanisms that appeared in the wild—including presenting the opt-out option as a link rather than a button or requiring users to click on a "More Info" link to access the opt-out mechanism—had a significant impact on how many users exercised their right to opt-out. We also found that the inconvenience factors we considered all had significant negative effects on users' exercise of their right to opt-out. Conversely, we found that an anti-nudging design in which a banner contained only a single opt-out button (and no mechanism to explicitly accept the sale of personal information) significantly increased the user opt-out rate.

Overall, our findings suggest that compliance with the CCPA right to opt-out of sale is not yet universal, and that many companies who do comply with the law do so in ways that inhibit users from exercising their rights. We believe these results can serve as guidance for companies who want to enhance user privacy by following the best-practices identified in this work, and we believe they should inform any future privacy regulations.

2 BACKGROUND ON CCPA

The primary goal of the California Consumer Privacy Act (CCPA) was to give users more control over their personal information. This resulted in the introduction of four key rights:

(1) **The right to know.** Users have a right to know what personal information a business collects and how that information is used and shared. This information should be communicated in a manner that provides the user with a "meaningful understanding".
(2) **The right to delete.** Users have a right to delete personal information about them (with some exceptions).
(3) **The right to opt-out of sale.** Users have the right to opt-out of the sale of their personal information. Businesses must provide a "a clear and conspicuous link" on the homepage of their website entitled "Do Not Sell My Personal Information" that enables users to invoke their right to opt-out of sale.
(4) **The right to non-discrimination.** Businesses cannot deny a service, degrade the quality of service, or change the price of a service just because a user exercises their rights under CCPA.

CCPA also broadened the definition of personal information to include any information "that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household". This definition explicitly includes information about online activities (e.g., a user's interactions with a website) and any inferences drawn from personal information.

3 OPT-OUT MECHANISMS IN THE WILD

To investigate how websites implement the CCPA right to opt-out of sale, we conducted a series of three observational studies. Each study comprised of a manual analysis of the Alexa Top 500 U.S. websites (as listed July 1, 2020); the first manual study was conducted immediately after enforcement of CCPA began (July 1-15, 2020), the second manual study was conducted six months later (January 1-February 26, 2021), and the third one year later (July 1-24, 2021). In each manual study, we collected information about whether the website sold personal information (as defined under CCPA) and about whether the website included an opt-out of sale link. We also qualitatively coded the design and implementation of the opt-out mechanism (if provided).

3.1 Methodology

Prior to beginning our manual observational studies, we developed a coding book based on a preliminary analysis of 50 websites (desktop and mobile); these codes included presence/absence of opt-out link (and visibility without scrolling or clicking), presence/absence of banner (and location), format of the opt-out mechanism (buttons, sliders, form, etc.), number of options in the opt-out mechanism, and presence and type of nudging.

For each of the manual observational studies, one author visited each of the Top 500 U.S. websites (as listed by Alexa on July 1, 2020) from a California IP address. For each website, we recorded whether we were able to reach the website (i.e., whether the site returned a valid, English-language HTML page), whether the website claimed to sell user data as defined under CCPA, and whether the website contained an opt-out of sale link on their home page. If the website claimed to sell user data and did not have an opt-out of sale link on their home page, we checked whether there was an opt-out mechanism available in their privacy policy. If the website claimed to sell user data and had an opt-out mechanism, we qualitatively coded elements of the opt-out mechanism's design, such as how it was displayed and whether it employed nudging. Borderline cases were resolved through discussion with a second author.

To determine whether each website sold user information as defined under CCPA, we scanned through its privacy policy. We looked for a specific statement regarding the sale of user data with

Sale of Data	**07/2020**		**01/2021**		**07/2021**	
Sells Data	207	(41.4%)	228	(45.6%)	230	(46.0%)
Unspecified	163	(32.6%)	53	(11%)	30	(6.0%)
Does not Sell Data	116	(23.2%)	208	(41.4%)	238	(47.6%)
Website Unreachable	14	(2.8%)	11	(2.0%)	2	(0.4%)
Opt-out of Sale	**07/2020**		**01/2021**		**07/2021**	
Banner	18	(3.7%)	18	(3.7%)	18	(3.6%)
Of sells data	18	(8.7%)	18	(7.9%)	18	(7.8%)
Valid Link on Homepage		-	184	(37.6%)	193	(28.8%)
Of sells data		-	182	(79.8%)	193	(83.9%)
Any Link on Homepage	174	(35.8%)	196	(40.1%)	204	(41.0%)
Of sells data	173	(83.6%)	195	(85.6%)	204	(88.7%)
Any opt-out Mechanism	207	(42.6%)	228	(46.6%)	230	(46.2%)
Of sells data	201	(97.1%)	226	(99.1%)	230	(100.0%)
No opt-out Mechanism	279	(57.4%)	261	(53.4%)	268	(53.8%)
Of sells data	6	(2.9%)	2	(0.9%)	0	(0.0%)

Table 1: Evolution of CCPA opt-out of sale mechanisms among the Top 500 U.S. websites between July 2020 and July 2021.

regard to CCPA, as we noticed many websites made general statements denying data sale only to later admit in a CCPA-specific section that they engaged in sales as defined by the law. Websites that made no CCPA-specific statement about sale of data were coded as "unspecified".

To determine whether websites had an opt-out of sale link on their home page, we performed a thorough manual check of each site's homepage. First, we searched each homepage for CCPA-related phrasing ("sell", "info", "CCPA", "California", and "CA"). We also manually checked any parts of the site where links were present, including any expandable page elements. If the website claimed to sell personal data but did not have an opt-out link on the home page, we proceeded to search the site's privacy policy and, if applicable, CCPA umbrella page for instructions related to opting-out of sale of personal information.

For websites where an opt-out mechanism was present, we additionally performed qualitative coding of UI design elements in its implementation using the pre-defined coding book.

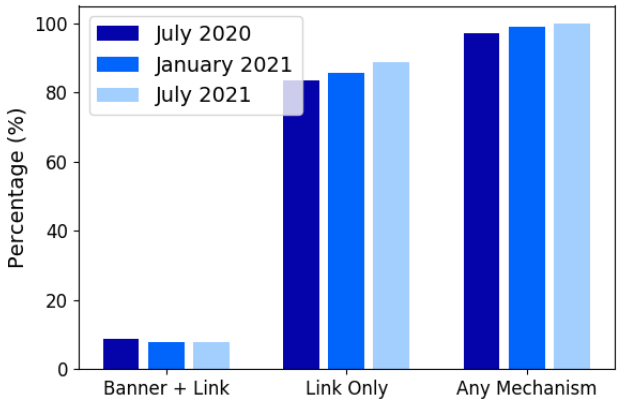


Figure 1: Prevalence of opt-out of sale mechanisms in Top 500 U.S. websites that sell personal information.

3.2 Data Sale and Compliance

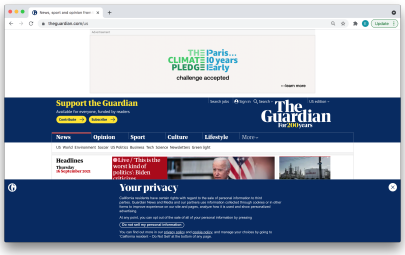
While we did not attempt to definitively judge any website's compliance with CCPA, our results outline the evolving landscape of CCPA compliance in the year after enforcement began. These results are summarized in Table 1.

In our first manual study, we found that 41.4% of the Top 500 websites explicitly acknowledged that they sold personal information as defined under CCPA, 23.2% of those websites specifically stated that they did not sell user personal information, and 32.6% of those websites made no definitive statement either way. The remaining 14 websites returned errors when we attempted to reach them.[1] We also observed that there were significant differences in companies' interpretations of what constitutes a sale under CCPA. Notably, some companies assert that providing data to third-party tracking or targeted advertising tools does not constitute a sale despite the current consensus that this sort of transaction does constitute a sale of personal information under CCPA.[2]

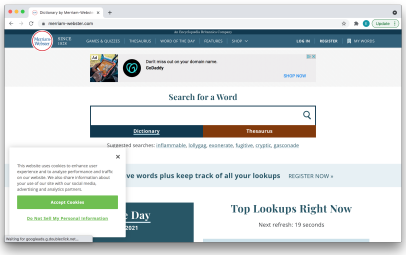
In the second and third observational studies—conducted six months and one year after enforcement of CCPA commenced—we observed a decrease in the number of websites that failed to specify whether or not they sold personal information (to just 6% in July 2021). Most of this change appears to be due to websites that do not sell personal information now explicitly saying so (47.6% of websites in the third study), although an additional 23 websites stated that they sold personal information in July 2021 compared to July 2020.

[1]Upon subsequent inspection, we found that the majority of these sites returned errors because the website actually used a non-standard subdomain and returned an error to requests made to the domain name listed by Alexa and to the www subdomain; those sites were included in the July 2021 study. Two of these sites appear to have been temporary sites serving malware or adware that had been taken down prior to the date we attempted to visit them.

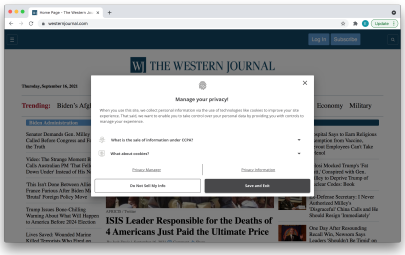
[2]Note that during our first manual study, regulatory guidelines from the California Office of Attorney General were still under development and did not take effect until August 14th, 2020.



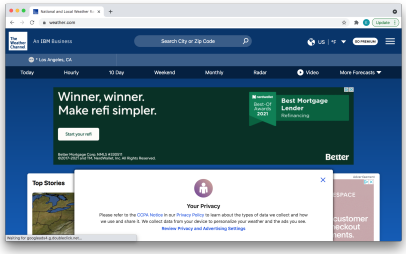
(a) Example website with bottom bar and single in-banner Do Not Sell link.



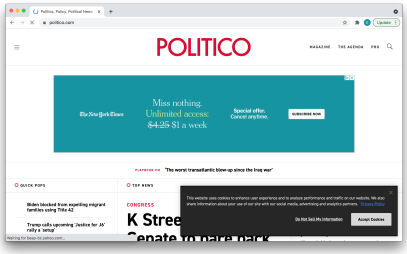
(b) Example website with bottom left banner and two options.



(c) Example website with center banner, two options, and blocking.



(d) Example website with bottom center banner and opt-out link.



(e) Example website with bottom right banner and two options.

Figure 2: Example opt-out of sale banners observed in manual observational studies.

These results suggest that an increasing awareness of CCPA—and increasing effort to comply with its requirements—evolved over the year after enforcement began.

To understand how websites implement the CCPA opt-out of sale requirement, we focused on the subset of websites that sell personal information as defined under CCPA. In our first observational study, we found that 97.1% of websites that explicitly acknowledge selling personal information provide some sort of opt-out of sale mechanism, however only 83.6% of such websites provide on opt-out link on their home page as required by CCPA. We did observe improved compliance in our second and third observational studies; by July 2021, 100% of websites that were confirmed to sell personal information provided some sort of opt-out of sale mechanism, and 88.7% provided an opt-out of sale link on their homepage (although only 83.9% of such websites provided a link with the precise wording required by CCPA). These trends are summarized in Figure 1. We observe, however, that actual compliance may be somewhat lower, as it is likely that some websites that do not specify their practices or that claim not to sell information actual do sell personal information as defined by CCPA and therefore should be providing an opt-out of sale mechanism.

3.3 Form of Opt-out Mechanisms

Among the Top 500 websites that implemented some form of opt-out of sale mechanism (207 websites in July 2020, 228 websites in January 2021, 230 websites in July 2021), we observed that websites commonly adopt design and implementation choices that appear to violate the spirit of the CCPA, which states that opt-out links should be "clear and conspicuous" on the homepage.

Location	07/2020	01/2021	07/2021
Bottom bar	77.8%	72.2%	77.8%
Bottom left box	0.0%	5.5%	5.5%
Bottom center box	5.5%	5.5%	5.5%
Bottom right box	11.1%	11.0%	5.5%
Centered	5.5%	5.5%	5.5%

Options in Banner	07/2020	01/2021	07/2021
Link to Mechanism	83.3%	77.7%	83.3%
Single Do Not Sell button	5.5%	5.5%	0.0%
Two or more buttons	11.1%	16.7%	16.7%

Blocking	07/2020	01/2021	07/2021
Blocking	5.5%	5.5%	5.5%
No blocking	94.4%	94.4%	94.4%

Table 2: Properties of CCPA opt-out of sale banners

3.3.1 CCPA Banners. After the adoption of GDPR in the European Union, consent notices—banners that provide information about data collection practices and give the user an opportunity to consent—became pervasive [15]. Substantial percentages of users are willing to engage with such notices, although factors such as position, options available, wording and nudging can mitigate the impact of such banners [40]. We expected to see a similar rise in CCPA banners after enforcement began in July 2020, but our observational studies found that very few websites actually implemented opt-out mechanism in banner or provided a link to their opt-out

mechanism in a banner. In July 2020, just 18 of the Top 500 websites provided a banner relating to opting-out of sale; this number remained unchanged through July 2021. Moreover, many of the banners we observed adopted design choices that have previously been found to decrease engagement [40]: locating the banner as a bar along the bottom of the page or in the bottom right, allowing the user to interact with the page before interacting with the banner (no blocking), and linking to the opt-out mechanism rather than providing the mechanism directly in the banner. In one case, the banner was only visible after scrolling to the bottom of the page. Examples of the types of banners we observed are shown in Figure 2, and precise statistics from each observation study are given in Table 2.

3.3.2 Opt-out Links on Homepage. CCPA mandates that opt-out of sale links must be "clear and conspicuous". However, we found that many opt-out links were implemented in a manner likely to negatively impact usability. Our findings are summarized in Table 3.

In July 2020, we found that 98.7% of these links were located at the bottom of the page and that 97.4% required scrolling down (often many screen-lengths) before they were visible, factors which likely contributed to users being unable to locate Do Not Sell links in a prior study [30]. The fraction of links that required scrolling was slightly lower in January 2021 and July 2021, but the difference was primarily due to an increase in the number of hidden links (i.e., links that were visible only after opening a menu or otherwise interacting with the page); only 4 websites (2.1%) had opt-out links that were visible without scrolling or clicking in July 2021. Moreover, links were often displayed among lists of other links and were typically in a smaller font size than the rest of the page. Some links were also displayed in low-contrast font colors (e.g., light gray). All of these factors have been found to impair link usability in other contexts [16].

CCPA requires that opt-out links be titled "Do Not Sell My Personal Information" or "Do Not Sell My Info". However, deviations from these mandated phrasings were common. In July 2020, we documented 12 unique phrasings, most of which served to obfuscate the purpose of the link. 8 of these phrasings did so by omitting words (e.g., "Do Not Sell"), which has been shown to be ineffective in communicating sale opt-out to users [13]. 6 did so by adding technical or legal language to the link phrasing (e.g., "Cal. Civ. Code §1798.135: Do Not Sell My Info"). The importance of clear and consistent link names to enhance privacy choice usability has been demonstrated in other contexts [10, 16, 22, 27], so these deviations seem likely to inhibit users' ability to utilize opt-outs. In July 2021, we categorized all websites according to whether their opt-out of sale link followed the legally-mandated wording; we found that 11 websites (4.8%) used non-compliant language for their opt-out of sale link.

8 of the link-based pages in July 2021 (down from 18 in July 2020) also displayed an unrelated privacy or cookie banner, which contained no information on CCPA. These banners might direct privacy-inclined users away from opt-out mechanisms and instead toward general privacy policies or cookie settings; the presence of multiple privacy-related headings on a site has been shown to impair privacy choice usability as users struggle to select the correct page from a site's navigation menu [22]. These banners also frequently blocked the bottom of the screen in a way that made the opt-out link (usually located at the very bottom of the page) impossible to see without first dismissing the banner; in a prior study, the presence of such an occluding cookie banner was noted to contribute to users being unable to find a site's DNS link when searching for it [30].

Location	**07/2020**	**01/2021**	**07/2021**
Top	1.28%	0.6%	0.5%
Left	0.0%	0.6%	0.5%
Right	0.0%	0.6%	1.0%
Bottom	98.7%	98.3%	98.0%
Visibility	**07/2020**	**01/2021**	**07/2021**
Scrolling required to see	97.4%	92.6%	94.2%
Hidden under clickable	1.9%	9.0%	9.0%
Initially Visible	1.3%	2.8%	2.1%

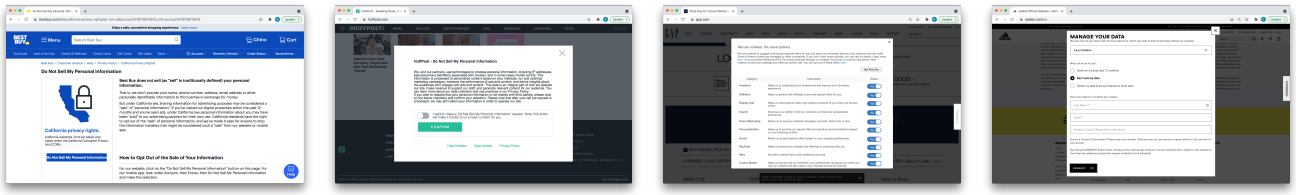
Table 3: Properties CCPA opt-out of sale links on homepages

3.3.3 Opt-out Links in Privacy Policies. In addition to the websites that provided an opt-out link on their homepage, a few websites (33 in the July 2020 study, 32 in the January 2021 study, 26 in the July 2021 study) provided an opt-out mechanism that was only accessible from the site's privacy policy. This implementation is not compliant with the requirements of CCPA—which states that an opt-out link must be provided on the homepage of the website. Moreover, prior work has consistently found that users do not read or look at privacy policies [4, 24, 38], so providing a mechanism that is only accessible from that page—and that is often embedded within long, legalese text—is likely to deter users from discovering or invoking their right to opt-out of the sale of their personal information.

3.4 Opt-Out Controls

Among both banners and links, the vast majority of homepage opt-out notices we observed (approximately 98% in each study) linked to a Do Not Sell page that required further action to opt-out. We therefore also analyzed the design choices implemented by the opt-out controls that were reached after clicking on this link. We identified 8 classes of controls for opting-out of sale of personal information:

(1) **One option (Do Not Sell)**. A single clickable element that opts the user out of the sale of their personal information.
(2) **Two option**. A two-state control that sets opt-out entirely on or entirely off. This took the form of a toggle switch, a checkbox, or a pair of buttons ("Accept" and "Do Not Sell").
(3) **Multi-option**. Fine-grained options to control information sale beyond entirely enabled/disabled. In most cases, these options allowed the author to authorize or disallow sale for different purposes or to different third parties.
(4) **Fillable form**. A form requiring the user to input personal information in order to opt-out. This information ranged from just an email address, to full name, address, and more.



(a) One option (Do Not Sell). (b) Two options. (c) Multiple options. (d) Fillable form.

Figure 3: Example websites exhibiting different categories of opt-out mechanisms. The other four classes of mechanism constitute written directions.

These were frequently seen on shopping and subscription-based websites.

(5) **Directions for contacting company**. Instructions to contact the company to make an opt-out request, usually through email or a customer service portal. Excludes instructions that provide a fillable form.
(6) **Directions for dealing with other third party(s)**. Directions to opt-out by using controls on third-party websites, usually industry-provided targeted advertising opt-out sites.
(7) **Directions for adjusting account settings**. Seen on websites where users have an account, these sites directed users to sign in and utilize privacy settings within their account to control sale of their information.
(8) **Directions for adjusting browser settings**. Directions to opt-out of information sale by adjusting browser settings, usually either disabling cookies or enabling a "Do Not Track" setting on mobile devices.

The first three classes of mechanisms were classified as *direct* mechanisms, since those mechanisms enable users to opt-out directly on that webpage; the other five classes of mechanisms, which gave instructions or mechanisms for adjusting settings, contacting the company, or contacting various third parties, were classified as indirect mechanisms.

Overall, 41.1% of the Top 500 who provided an opt-out mechanisms in July 2020 provided some sort of direct mechanism; 9.2% of sites provided a single Do Not Sell button, 23.7% provided a two-option mechanism, and 9.2% provided a multi-option mechanism. By July 2021, the fraction of opt-out mechanisms that provided some form of direct mechanism had risen slightly (to 44.0%), and the fraction of mechanisms that provided a single Do Not Sell button had risen significantly (to 17.3%). Although indirect mechanisms were the most common class of mechanism observed in both studies, we observed drops in the prevalence of fillable forms (from 42.0% to 36.1%) and in directions for adjusting browser settings (from 12.6% to 5.1%) between July 2020 and July 2021. The complete categorization of opt-out controls observed in our two manual observational studies is shown in Figure 4.

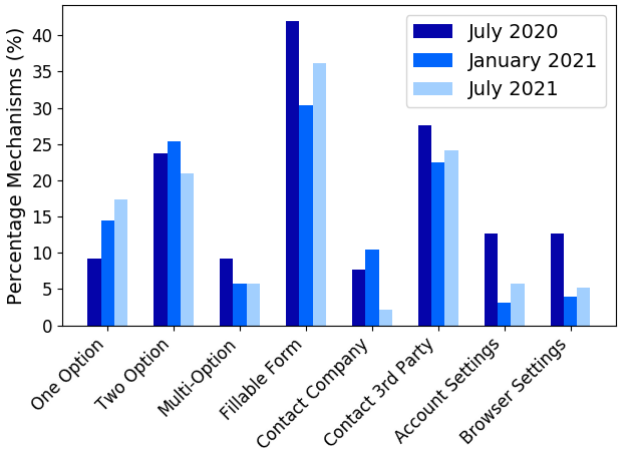


Figure 4: Prevalence of different CCPA opt-out controls in our observational studies. One Option, Two Option, and Multi-Option designs are considered to be direct mechanism. The other five classes of controls are indirect mechanisms.

3.4.1 Nudging in Direct Mechanisms. Most implementations of direct mechanisms offered two or more options; for these mechanisms we observed whether the website used some for of *nudging* to decrease user opt-out rates. To develop a codebook for nudging, we looked for dark patterns that had been previously identified as issues among GDPR consent banners. Prior work identified five classes of nudging that were prevalent among cookie consent mechanisms:

(1) **Defaulting [40].** The allow option is pre-selected in the opt-out mechanism.
(2) **Highlighting [40].** The allow option is made visually more prominent than the opt-out option using different colors.
(3) **Asymmetric UI [40].** The allow option is made visually more prominent than the opt-out option using different classes of element (e.g., an allow button and an opt-out link, possibly inlined in other text).
(4) **Confirmshaming [6].** Users who select the opt-out option are then required to confirm their choice, requiring additional clicks compared to the accept option.
(5) **Asymmetric Difficulty [34].** Accepting sale of personal data was easier than opting out (e.g., immediately accessible with one click, while opt-out required toggling multiple options and/or visiting a separate opt-out page) in a manner other than requiring confirmation to opt-out.

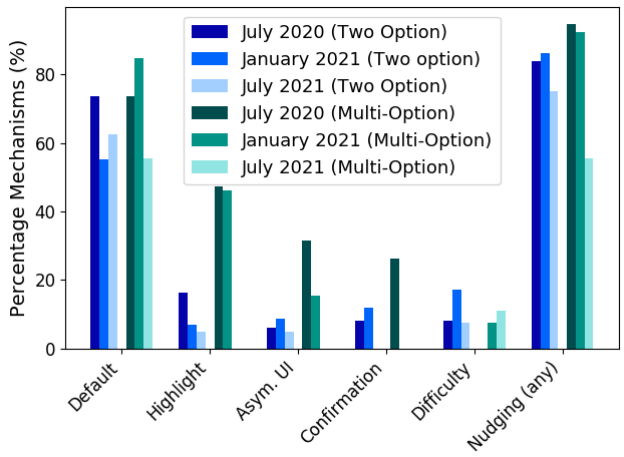


Figure 5: Prevalence of nudging in direct opt-out mechanisms with two or more options, by study. Data for mechanisms with 2 options (e.g., two buttons or a slider) are shown in blue, and data for multi-option mechanisms are shown in gray.

We found that nudging was prevalent among direct opt-out mechanisms with two options. This was largely due to the predominance of toggles that were set to allow sale of personal information by default (even though the mechanism was accessed only after a user had clicked on an opt-out of sale link), but highlighting, asymmetric UI, and asymmetric difficulty were also common in multi-option mechanisms. Between July 2020 and January 2021, nudging was also very common among multi-option mechanisms, but that frequency decreased significantly (to 55.6%) by July 2021. These results are summarized in Figure 5.

3.4.2 Usability of Indirect Mechanisms. The majority of opt-out mechanisms in each study (55-58%) were an instance of some class of indirect mechanism: directions for adjusting account settings, a fillable form or other instructions for contacting the company, or directions for dealing with browser settings or other third parties. Many of these implementations raise inherent usability concerns.

Prior work has shown that users cannot or will not complete opt-outs on multiple third-party sites, suggesting directions for dealing with multiple third parties may be effectively unusable [27]. Even when users were required to utilize only one such site, opt-out sites for targeted advertising have been found to have significant usability issues [20, 22, 27] and instructions about how to opt-out once on the third-party site were often vague or missing. It is also unclear whether opting-out on these sites fully prevents the sale of personal information; in one study, half of the behavioral advertising opt-out sites studied continued to track users after the opt-out had been invoked [35]. As such, providing directions to third parties as an opt-out of sale mechanism might not be sufficient to comply with CCPA.

Directions to adjust account settings also might not comply with CCPA, which forbids companies from requiring users make an account to submit an opt-out. Moreover, such directions often lacked specific information about which settings needed to be changed (and how) in order to opt-out of sale. Instead, many websites simply directed users to general browser information pages about adjusting cookie settings.

Directions for contacting the company raised concerns due to past work showing the difficulties users have with such directions. A prior study of Do Not Sell found that users contacting companies for an opt-out request are frequently met with slow responses, requests for invasive or difficult-to-provide information, and unclear instructions in company responses [30]. Another study of other privacy opt-outs found that, in addition to increasing the number of required actions, directions for contacting the company left users struggling to know what information to include in such requests [22].

Multi-step instructions generally were of such length and complexity to raise usability concerns. These instructions typically contained ambiguous and poor directions that were missing key information, such as which steps were required to completely opt-out. Some contained contradictory instructions: for instance, one site told the user to both keep cookies enabled in order to store an opt-out cookie, and to disable cookies entirely. Some also entailed individually visiting an extensive number of third-party sites and independently navigating their opt-out processes (as many as 16 for one website).

Finally, fillable forms—the most common type of opt-out mechanism—often requested excessive personal information from users. While some user information might be needed to fully implement an opt-out, we documented examples of information request that seem unlikely to be necessary. Several websites required an email address to create a verifiable request, even when the user did not have an account on the site. One website also required the user's full physical address to confirm California residency. Such practices both require additional effort by the user in order to invoke their right to opt-out and also raise concerns about how the information collected in the form will be used, turning the opt-out process itself into a potential privacy threat. In at least one previously documented case, a company used an email address provided during CCPA sale opt-out to sign a user up for a marketing list, despite the law explicitly prohibiting such behavior [30].

4 THE IMPACT OF CCPA DESIGN CHOICES

To evaluate the effect of the observed design choices on privacy, we conducted a user study in which we observed how people interacted with different opt-out of sale mechanisms. This study evaluated two primary research questions: (1) What is the impact of link-only mechanisms compared to banner mechanisms? and (2) What is the impact of nudging? We evaluated the impact of these design factors on how likely users were to opt-out of the sale of their personal information and the impact on how aware users were that they had a right to opt-out of sale.

4.1 Methodology

To conduct this study, we implemented a news aggregation site to serve as our example website. We chose this context because it provides a credible privacy threat even for a brief, one-time visitor:

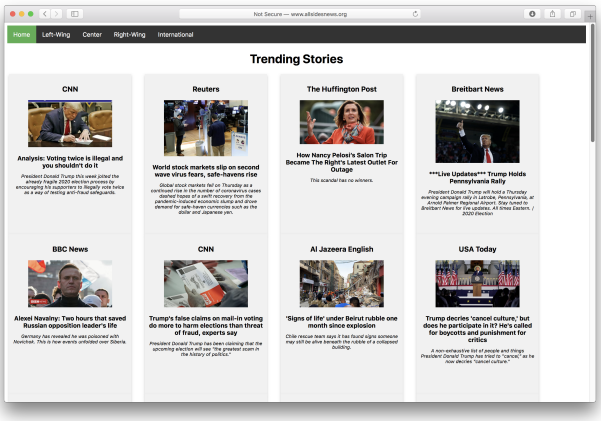


Figure 6: News aggregation site used in user studies.

a user's browsing pattern on such a site can expose sensitive information such as political beliefs and interests that are commonly sold to third-party aggregators. A screenshot of our website in shown in Figure 6. For each experiment, we implemented several different versions with different opt-out mechanisms; each study participant was pseudo-randomly assigned to a condition based on their current IP address. The details of the individual conditions are described in Sections 4.4 and 4.5.

For each user who visited the site, we logged how that user interacted with the site. Logged actions were associated with a unique identifier constructed by hashing the user's IP address; no personally-identifiable information was stored. Logged actions included various ways of interacting with the opt-out mechanisms, including clicking on the opt-out link, clicking on individual buttons in a banner, or closing a banner. We also logged general interactions with the site: which pages the user visited and which links they clicked on. Finally, we logged a heartbeat message whenever the webpage was in focus on the user's device to enable us to calculate how long each user spent on the site.

At the bottom of each page (adjacent to the opt-out link) we provided a link to our privacy policy, which stated that this was an academic study exploring how users interact with Do Not Sell mechanisms, and that no personal information was collected; the privacy policy also included a button that users could click to opt-out of the study and have their log entries deleted.

Users were recruited by two methods: through Amazon Mechanical Turk and through Google Ads. To avoid biasing the results, none of the participants were informed upfront that they were participating in a study about CCPA or privacy.

To recruit participants through Amazon Mechanical Turk, we advertised the task as, "5 min - Beta Test Aggregated News Website". Users were asked to visit our site and interact however they normally would with a webpage; they then completed a follow-up survey containing questions about the sale of data on the page, as well as demographic information (detailed in Appendix A). Recruitment was limited to workers with at least a 95% approval rate and at least 50 accepted HITs who were located in California. Each

Figure 7: The Google Advertisement displayed to users.

worker was compensated $1.00 USD for their participation, and the study ran from July 16-27, 2020.

One potential concern among MTurk users, however, was the possibility that their interactions might not accurately reflect the way users interact with CCPA mechanisms on real sites, due to their knowledge the site was part of a study and the paid motivation behind their visit. To mitigate this concern, we recruited a second group of users through a Google Ads campaign run between August 15-18, 2020; the ad was placed for search terms relating to news, and was targeted at California users through the Google Ads network (see Figure) with an average cost per click of 33 cents. A copy of the recruiting ad is shown in Figure 7.

Our cleaned dataset included log records from 4357 unique users: 1726 users participated in Experiment 1 (1295 recruited through Google ads and 431 recruited through Amazon Mechanical Turk) and 2531 users participated in Experiment 2 (2233 recruited through Google ads and 398 recruited through Amazon Mechanical Turk). 53.3% of our users visited the desktop version of the site and 47.7% visited from a mobile browser.

4.2 Analysis Plan

The primary goal of our user study was to determine whether there were differences in how users interacted with the website differed based on the condition to which they were assigned. We therefore evaluated all hypotheses using Chi-squared contingency tests to test for differences in behavior and responses between study participants assigned to the different conditions. Due to the number of statistical tests, we applied a Holm-Bonferroni multiple comparison correction; all results that are reported as statistically significant are significant after the correction was applied.

4.3 Ethical Considerations

The majority of our study participants (3528/4357) were users recruited through Google Ads. To assure data validity, these users were not aware they were participating in a research study; this omission of prior informed consent inherently raises ethical issues.

To minimize the risk to our users, no personally-identifiable information was collected. Log entries were associated with a unique identifier defined by a hash of the user's IP address; no IP addresses or other identifiers were stored. Information collected was used only for research purposes; no information was actually sold.

Users recruited from Amazon Mechanical Turk were informed of our data collection practices in advance and were given the opportunity to opt-out prior to beginning the user study. The privacy policy for our website also clearly stated that this was an academic study exploring how users interact with Do Not Sell mechanisms, and that no personal information was collected or sold; the privacy policy also included a button that users could click to opt-out of the study and have their log entries deleted.

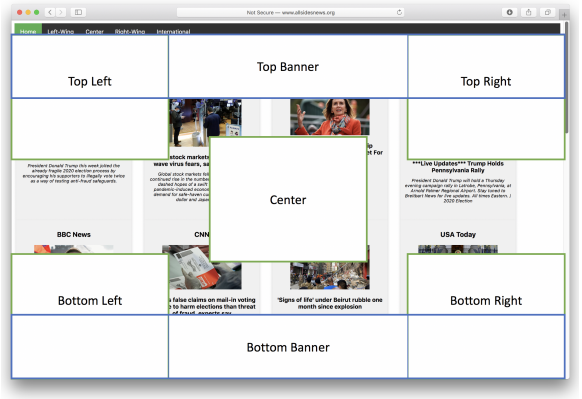


Figure 8: A schematic diagram of the banner locations used in Experiment 1.

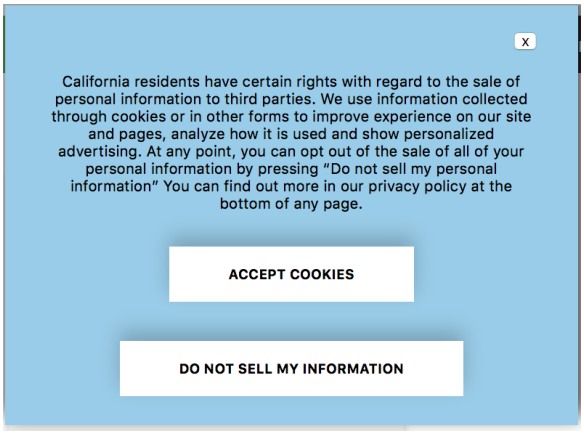


Figure 9: Example pop-up banner used in Experiment 1.

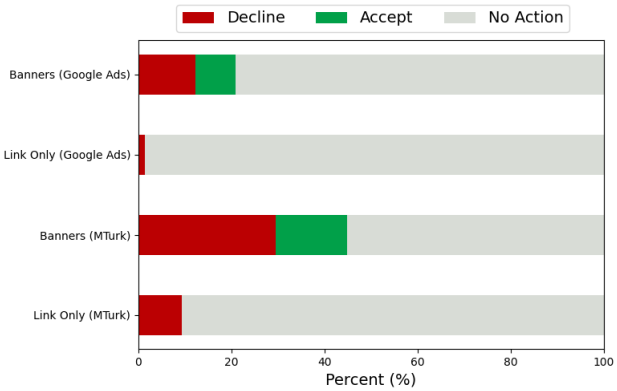


Figure 10: The effect of format (banner vs. link-only) on opt-out interaction rates on the desktop version of the site.

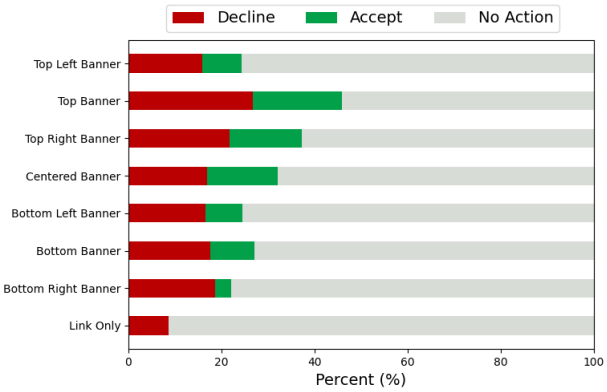


Figure 11: The effect of banner location on opt-out interaction rates on the desktop version of the site.

This research received an IRB exemption approval from the institutional ethics review board (IRB) at our institution.

4.4 Experiment 1: Links vs. Banners

Our first experiment investigated how users interact with opt-out links compared to how users interact with opt-out mechanisms contained in pop-up banners in a between-subjects study. Prior work has found that user actions with banners vary significantly depending on the location of the banner [7, 17, 34, 40], so we considered a variety of different banner locations. On the desktop version of the site, we used seven different banner locations: a pop-up banner in each of the four corners, a pop-up banner in the center of the page, and full-width banners at the top and bottom of the page. Each subject was assigned one condition at random when they first visited the page, with 106-188 participants assigned to each condition. A diagram of the different banner locations is provided in Figure 8. A screenshot of the banner used in the corner and center conditions of this experiment is provided in Figure 9; the full-width banner used in the top and bottom conditions (also used as a baseline in Experiment 2) is shown in Figure 12b.

Unsurprisingly, users interacted with the opt-out link significantly less frequently than with banners ($p < .001$). An average of 19.3% of desktop users who were shown a banner opted out of sale; among desktop users who were shown the link-only website, just 8.6% of users opted out of the sale of their data. We found that users recruited on Amazon Mechanical Turk interacted with opt-out mechanisms at significantly higher rates than users who visited the site after clicking on an ad, perhaps because the task was advertised as Beta testing a website, which some users might consider to include testing all the links. We expect the behavior of users recruited through ads—who did not realize they were participating in a user study—to be representative of normal user behavior online; among users recruited through Google Ads, 12.2% of users in banner conditions opted out of sale whereas just 1.4% of users in the link-only condition opted out of sale ($p < .001$). These results are summarized in Figure 10.

We note that these interaction rates are somewhat higher than interaction rates with cookie banners by European users [40]; the distinction may be due to users having stronger options about sale of personal information than about use of cookies, or it may be

due to the different population of users. California users see and interact with banners less frequently than European users, so less banner-fatigue might currently result in higher interaction with banners on websites that have them.

To further understand the effect of opt-out links on privacy, we compared follow-up survey responses from MTurk users to the condition they were assigned. We found that only 54.5% of users assigned to the link-only case were aware that they had the ability to opt-out of the sale of their personal data on our website compared to 71.1% of users who were assigned to one of the conditions with banners ($p = .019$). This suggests that the predominant link-only implementation of CCPA's right to opt-out of sale is significantly less effective at informing users of their rights than banner designs.

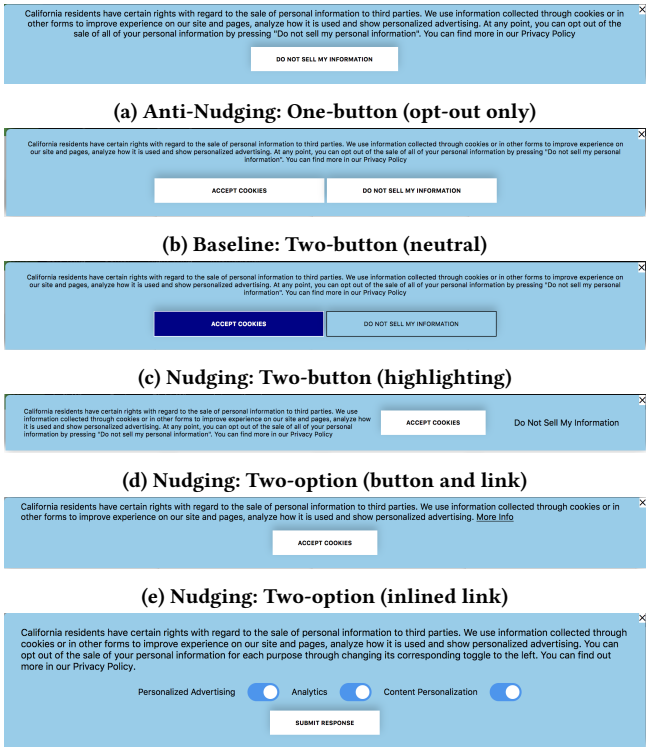
We also evaluated the effect of banner placement on interaction rates by users; we found that users recruited through Google Ads generally interacted more frequently with banners located at the top of the page than with banners at the bottom of the page. The banner that ran across the full width of the top of the page exhibited the highest interaction rates: 20.5% of users exercised their right to opt-out and 12.8% explicitly accepted the sale of their personal information. This rate of interaction was significantly higher than the bottom-left ($p = .005$) and bottom-right ($p = .027$) locations, but it was not significantly higher than the other banner locations. All banner locations individually resulted in significantly higher interaction rates that the link-only design. These results are summarized in Figure 11.

4.5 Experiment 2: Nudging

In our second experiment, we evaluated the effect of nudging and inconvenience factors on user interactions with the Do Not Sell mechanism. Drawing on inspiration from example implementations we saw in the wild, we generated three different banner designs with nudging: one in which the "Accept" button was highlighted (and the opt-out button was the same color as the background), one in which the opt-out button was replaced with a link, and one in which the opt-out button was replaced with a "More info" link inlined with the text. We compared these designs to a neutral design with no nudging and to an anti-nudging design in which the banner contained only a single opt-out button. To maximize data collection, all banners were implemented as full-width banners located at the top of the page; these banner designs are shown in Figure 12.

We also tested three designs incorporating commonly seen inconvenience factors. First, we implemented a banner requiring the user to separately toggle off three different categories of information sale, instead of a single opt-out button (Figure 12f). We also tested an indirect version of this design, where users were first presented with the baseline banner design (Figure 12b), but clicking "Do Not Sell My Information" led to a second dialogue that presented them with the three-toggle mechanism to complete the process. Finally, we tested another indirect banner that required users clicking the opt-out button to subsequently fill out a form with their email address.

We found that eliminating the "Accept" button (our anti-nudging design) reduced the overall interaction rate but significantly increased the opt-out rate from 20.5% to 31.2% ($p < .001$). The nudging design with highlighting did not significantly affect the interaction



(a) Anti-Nudging: One-button (opt-out only)

(b) Baseline: Two-button (neutral)

(c) Nudging: Two-button (highlighting)

(d) Nudging: Two-option (button and link)

(e) Nudging: Two-option (inlined link)

(f) Inconvenience: Multi-option (direct)

Figure 12: Banner designs used in Experiment 2

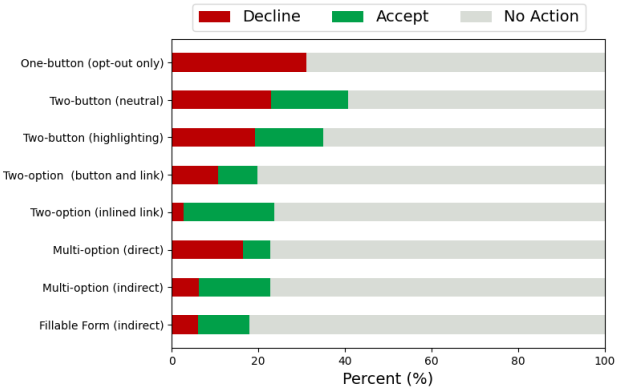


Figure 13: The effect of nudging and inconvenience on opt-out interaction rates.

rate ($p = .555$). However, replacing the opt-out button with an opt-out link in the same location or replacing the opt-out button with an inline "More Info" link both significantly reduced the interaction rate and precluded any users from exercising their right to opt-out of sale ($p < .001$).

We found that all three inconvenience factors significantly reduced interactions with the opt-out mechanism ($p < .001$). If users

were asked to individually opt-out of sale of data for different purposes (e.g., personalized ads, analytics, and content personalization), only 16.6% exercised their right to opt-out of sale for one or more purposes (compared to the baseline opt-out rate of 20.5%). The condition in which users had to fill out a form in order to exercise their right to opt-out—a relatively common design in the wild—had a particularly low rate of users opting-out at just 6.2%. These results, summarized in Figure 13, are consistent with prior work on the effect of nudging on GDPR consent notices [40].

5 DISCUSSION

Our results provide insight into the impact of various implementation choices for opt-out mechanisms under CCPA; these results can therefore offer guidance for websites that want to voluntarily improve user privacy. Our findings confirm that companies can enhance user privacy by adding a pop-up banner on their homepage in addition to a link; ideally, this banner would located either at the top of their homepage or in another location of high visual importance, but any banner design is likely to enhance privacy relative to a link-only mechanism. We also recommend avoiding designs that place additional work on users—such as indirect mechanisms and multi-option mechanisms—to the maximum extent possible; instead, we recommend utilizing a banner with a single in-banner button that allows users to entirely opt out in one click. If information needs to be collected from users during opt-out, we recommend minimizing the number and granularity of data collected.

Our findings also provide guidance for how to write more effective future privacy regulations. First, we recommend that regulations expand to regulate opt-out mechanisms beyond requiring a link. Regulations should require that information collection be minimized, and users should never have to input information that the company doesn't already have. When no additional user information is needed to implement the opt-out, opt-out should be possible with a single click; navigating to separate pages, requiring users to opt-out for different purposes separately, and displaying vague lengthy disclosures should not be part of the opt-out process. Users should also not have to opt-out for multiple purposes separately; opt-out should be universally completed in one step. To be fully effective, regulations should require that opt-out can be completed directly within the site, rather than directing users to a third-party page, telling them to change their browser settings, or requiring them to contact the company to file a request.

Second, our results suggest that regulators need to empower a robust enforcement agency to enforce standards such as the "clear and conspicuous" requirement for Do Not Sell links. Our observational studies found numerous examples of websites with missing, incorrectly placed, incorrectly worded, or broken Do Not Sell links. Moreover, many websites that do have correct links adopt a design that appears to violate the spirit of the "clear and conspicuous" requirement. For example, links are not currently required to be immediately visible, an issue we found for an overwhelming majority of opt-out links. Other issues currently unaddressed by CCPA include links being hidden in menus, displayed in small fonts, or shown in low-contrast colors. As we have seen in response to revised GDPR guidelines [29], companies are likely to respond to modified regulations by creating new deceptive designs; effective enforcement of CCPA will therefore depend on robust, flexible, and active litigation to enforce the requirements of CCPA and to develop relevant case law about what constitutes a clear and conspicuous opt-out mechanism. Allowing direct action and class action lawsuits would be one possible mechanism for improving compliance.

Finally, our results suggest that privacy regulations that depend on individual opt-out might be inherently flawed. Across all conditions in our user studies, most participants who expressed discomfort with our example site selling their data did not actually utilize the opt-out mechanism on our site. This reinforces prior findings that opt-out mechanisms discourage engagement, a problem that is exacerbated in the online ecosystem due to the large number of individual sites and data brokers that collect personal information about users (for example, there are over 200 data brokers registered in California [30], in addition to the potentially hundreds or thousands of websites with which a user has direct relationships). To completely opt-out from the sale of their information, consumers would have to separately file opt-out requests with each these companies; based on our observations, completely preventing the sale of one's data is currently infeasible. As such, efforts that go beyond the implementation of CCPA's sale opt-out, such as the adoption of Do Not Sell browser signals or future legislation to limit data sale, will be critical for enhancing user privacy at scale.

6 RELATED WORK

Recent privacy regulations, notably CCPA and GDPR, have given rise to questions about how these regulations impact user privacy and how future regulations might further enhance privacy. This line of work takes place within the context of a larger body of work that has explored how aspects of user design affect user engagement in general and interactions with privacy mechanisms in particular.

6.1 Privacy Regulation Compliance in the Wild

Due to the recent adoption of CCPA, previous work studying the implementation of CCPA has been limited. A Consumer Reports study [30] asked users to attempt to opt-out of sale on 216 websites from the California Data Broker registrar (all of whom sell data and are subject to CCPA). They found that 11.1% of data broker websites lacked a CCPA-required homepage Do Not Sell link, and they documented examples of difficult, unclear, and time-intensive opt-out processes. However, they did not perform a comprehensive analysis of top websites or study how CCPA-compliance has evolved longitudinally; to the best of our knowledge, this work is the first to provide a comprehensive, longitudinal analysis of how websites implement CCPA in the wild.

Prior work has also considered similar questions about the impact of earlier privacy regulations, notably GDPR. An observational study conducted in May 2018 found that 62.2% of top European websites displayed cookie notices [15]; however, in 2019 more than 95% of banners failed to meet GDPR requirements by offering users no or insufficient choices [36, 40], and in 2020 just 11.8% of banners analyzed met minimal GDPR requirements [34]. Observational studies found that most notices were implemented as bottom bar banners [40], and that the use of dark patterns in GDPR notices to nudge users towards consent is common [34, 40]. Our work conducts an analogous series of observational studies for CCPA.

6.2 Usability of CCPA Opt-out Mechanisms

Cranor et. al. performed a series of studies examining how different taglines and icons influence user comprehension and recall of Do Not Sell links [11–14]. They found that most participants failed to notice Do Not Sell links in an image of a website, that users expect links to opt them out in a single click, and that an overwhelming majority of participants were unaware of CCPA and/or misunderstood what kinds of personal information were included in Do Not Sell—all findings that are consistent with our results. They recommended the adoption of standardized icons and placement, along with enforcement of the existing requirement for standardized language for opt-out links. However, their work did not compare the usability of current links or privacy icons with opt-out banners, and it did not consider the impact design choices after the initial opt-out link on usability.

The Consumer Reports study [30], which asked users to attempt to opt-out of sale on data broker websites, also studied the usability of opt-out mechanisms. In their study, three users were asked to attempt to opt-out of sale of their personal data on each site. They found that 31.4% of the sites studied displayed their link in such a manner that at least one out of three users was unable to find it, that more than a third of participants spent over five minutes opting out (with a maximum time of over an hour), and that 14% were unable to successfully complete the process. However, the limited sample size (3 users per website) and the differences in design choices adopted by each site precluded any statistically significant results about the impact of the observed designs on users' awareness of (and likelihood of invoking) their right to opt-out of sale.

Earlier work also consistently found that opt-out mechanisms were hard for users to understand and use [22, 23, 27, 40]. However, those studies were conducted prior to the adoption of CCPA and focused on the usability of opt-out mechanisms under earlier laws, such as the CAN-SPAM Act and GDPR.

6.3 Effect of UI on Privacy Notice Usability

A large body of work has explored the effect of user interface design on interactions with privacy notices and options.

Banner Position. A large-scale experiment varying the position of GDPR cookie consent notices found that users were significantly more likely to interact with banners in the lower left corner and less likely to interact with banners at the top of the page [40], a result that is inconsistent with our finding that users interact more with banners located at the top of the page. However, that study focused on European users (who frequently encounter consent notice banners and may be trained to look for them in particular locations). The different results might also be due to differences in time spent on the page (that study used an ecommerce site where most users stayed for only a few seconds whereas our study used a news site where the average users visited for 47 seconds) or due to difference in banner size and design (the effect of banner position has been extensively studied in the context of advertising banners, with inconsistent results [3, 7, 17, 19, 28, 33]).

Blocking. Blocking the underlying website has been shown to increase user interaction with cookie banners by a factor of 3.8 [34], a result consistent with prior work on browser phishing warnings [18]. We found that blocking mechanisms were uncommon in the wild, so we did not evaluate its effect on engagement with CCPA opt-out mechanisms.

Nudging. The use of design elements to prevent the user from making privacy-friendly choices is part of a broader literature on web design dark patterns [9]. Substantial work has gone into developing a taxonomy for dark patterns [5, 6, 8, 21], which exists within a larger literature on nudging [1]. Prior work has found that dark patterns are commonly used by ecommerce sites to encourage users to make more purchases and disclose more information [31]; our work extends this finding by observing the prevalence of various types of nudging among CCPA opt-out mechanisms.

Prior work has consistently found that nudging and dark patterns effectively influence user behavior, including causing users to share more information on social networks [25], and that defaults in particular cause users to accept more cookies [34, 40]. In recognition of these effects, GDPR (unlike CCPA) bans specific anti-privacy designs in cookie consent notices, such as preselected checkboxes [34]. However, some privacy advocates have argued that nudging should be used to nudge users towards privacy-protecting choices [2, 37]. This work extends these CCPA opt-out mechanisms by finding that certain forms of nudging can either increase or decrease the rate of user opt-out.

Inconvenience Factors. Studies have also found the effort required by privacy choices can pose a barrier to users. A study of Data Deletion and Targeted Advertising Opt-Out Choices [27] found that opt-out implementations frequently required excessive work from users (26.1-37.5 actions on average). They found that users had difficulty completing some task, such as writing an email request to opt-out, and that no users were willing to utilize multiple third-party opt-out pages in order to opt-out. Among direct mechanisms, users are less likely to interact with fine-grained mechanisms than with binary choices in cookie notices [40]; fine-grained privacy settings for social network increase users' regret about their choices and decrease user satisfaction [25, 26], although fine-grained privacy settings for location can make users feel more comfortable, suggesting the effect of granularity depends on context [39]. This work is the first to study the effect of inconvenience factors (including fine-grained vs. binary mechanisms) on user engagement with CCPA opt-out mechanisms.

7 CONCLUSION

The California Consumer Privacy Act (CCPA) has been celebrated as ushering in a new era of privacy protections in the United States. This paper identifies how CCPA's right to opt-out of sale has been implemented among top US websites, and how implementation has evolved over the first year of enforcement. We also describe a pair of user studies that evaluate the effect of these implementation choices and find they negatively impact user privacy. These results demonstrate the importance of regulations that provide clear guidelines backed by robust enforcement agencies in order to empower users to exercise their privacy rights.

REFERENCES

[1] 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):1–41, 2017.

[2] Alessandro Acquisti, Idris Adjerid, and Laura Brandimarte. Gone in 15 seconds: The limits of privacy transparency and control. *IEEE Security & Privacy*, 11(4):72–74, 2013.

[3] Pegie Stark Adam, Sara Quinn, and Rick Edmonds. *Eyetracking the news: A study of print and online reading*. Poynter, 2007.

[4] Manon Arcand, Jacques Nantel, Mathieu Arles-Dufour, and Anne Vincent. The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*, 31(5):661–681, 2007.

[5] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016(4):237–254, 2016.

[6] Harry Brignull. Dark patterns. *Dark Patterns*, 2019.

[7] Virginio Cantoni, Marco Porta, Stefania Ricotti, and Francesca Zanin. Banner positioning in the masthead area of online newspapers: an eye tracking study. In *Proceedings of the 14th International Conference on Computer Systems and Technologies*, pages 145–152, 2013.

[8] Gregory Conti and Edward Sobiesk. Malicious interface design: exploiting the user. In *Proceedings of the 19th International Conference on World Wide Web*, pages 271–280, 2010.

[9] Norwegian Consumer Council. Deceived by design, how tech companies use dark patterns to discourage us from exercising our rights to privacy. *Norwegian Consumer Council Report*, 2018.

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

[11] Lorrie Faith Cranor. Informing California privacy regulations with evidence from research. *Communications of the ACM*, 64(3):29–32, 2021.

[12] Lorrie Faith Cranor, Hana Habib, Yixin Zou, Alessandro Acquisti, Joel Reidenberg, Norman Sadeh, and Florian Schaub. CCPA opt-out icon testing - Phase 2. *Submitted to California Office of Attorney General*, 2020.

[13] Lorrie Faith Cranor, Hana Habib, Yixin Zou, Alessandro Acquisti, Joel Reidenberg, Norman Sadeh, and Florian Schaub. Design and evaluation of a usable icon and tagline to signal an opt-out of the sale of personal information as required by CCPA. *Submitted to California Office of Attorney General*, 2020.

[14] Lorrie Faith Cranor, Hana Habib, Yixin Zou, Alessandro Acquisti, Joel Reidenberg, Norman Sadeh, and Florian Schaub. User testing of the proposed CCPA do-not-sell icon. *Submitted to California Office of Attorney General*, 2020.

[15] 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. *arXiv preprint arXiv:1808.05096*, 2018.

[16] Jayati Dev, Emilee Rader, and Sameer Patil. Why Johnny can't unsubscribe: Barriers to stopping unwanted email. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

[17] Kim Doyle, Anastasia Minor, and Carolyn Weyrich. Banner ad location effectiveness study. *University of Michigan*, 1997.

[18] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1065–1074, 2008.

[19] Mario R Garcia, Pegie Stark, and Ed Miller. *Eyes on the News*. Poynter Institute for Media Studies St. Petersburg, FL, 1991.

[20] Stacia Garlach and Daniel Suthers. I'm supposed to see that? AdChoices usability in the mobile environment. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[21] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2018.

[22] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "It's a scavenger hunt": Usability of websites' opt-out and data deletion choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

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

[24] Carlos Jensen, Colin Potts, and Christian Jensen. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1):203–227, 2005.

[25] Bart Piet Knijnenburg and Alfred Kobsa. Increasing sharing tendency without reducing satisfaction: Finding the best privacy-settings user interface for social networks. 2014.

[26] Stefan Korff and Rainer Böhme. Too much choice: End-user privacy decisions in the context of choice proliferation. In *10th Symposium On Usable Privacy and Security*, pages 69–87, 2014.

[27] Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie 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*, pages 589–598, 2012.

[28] Raymond W. Lim and Michael S. Wogalter. The position of static and on-off banners in www displays on subsequent recognition. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 44, pages 420–423. SAGE Publications Sage CA: Los Angeles, CA, 2000.

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

[30] Maureen Mahoney. California Consumer Privacy Act: Are consumers' digital rights protected? *Consumer Reports Digital Lab*, 2020.

[31] Arunesh Mathur, Gunes Acar, Michael J Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–32, 2019.

[32] Célestin Matte, Nataliia Bielova, and Cristiana Santos. Do cookie banners respect my choice? Measuring legal compliance of banners from IAB Europe's transparency and consent framework. In *2020 IEEE Symposium on Security and Privacy*, pages 791–809. IEEE, 2020.

[33] Jakob Nielsen. Banner blindness: Old and new findings. *Retrieved November*, 11:2014, 2007.

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

[35] Takahito Sakamoto and Masahiro Matsunaga. After GDPR, still tracking or not? Understanding opt-out states for online behavioral advertising. In *2019 IEEE Security and Privacy Workshops*, pages 92–99. IEEE, 2019.

[36] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. Can i opt out yet? GDPR and the global illusion of cookie control. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pages 340–351, 2019.

[37] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security*, pages 1–17, 2015.

[38] H. Jeff Smith, Tamara Dinev, and Heng Xu. Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4):989–1015, 2011.

[39] Karen Tang, Jason Hong, and Dan Siewiorek. The implications of offering more disclosure choices for social location sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 391–394, 2012.

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

A FOLLOW-UP SURVEY QUESTIONS

In this Appendix, we provide the complete set of questions asked in the follow-up survey provided to study participants recruited through Amazon Mechanical Turk after they had interacted with our example website.

(1) "Did the website you visited track your behavior and sell this information to third parties?" (Yes / No / Unsure)
(2) "Did the website you visited give you an option to opt-out of the sale of your personal data?"(Yes / No / Unsure)
(3) "If this website tracked your behavior and sold this information to third parties, how comfortable would you be with it?" (Very Comfortable / Somewhat comfortable / Neutral / Somewhat uncomfortable / Very uncomfortable)
(4) "Are you aware that California law requires websites that sell your data to allow you to opt-out?" (Yes / No)
(5) "How often have you noticed websites you visit giving you an option to opt-out of the sale of your data?" (Never / A few times / Sometimes / Often / Always)
(6) "How often do you opt-out of the sale of your data on websites you visit?" (Never Have / Have a few times / Sometimes / Usually / Always)
(7) "What is your current age?" (18-24 / 25-34 / 35-44 / 45-59 / 60-74 / 75+)
(8) "What is your gender?" (Man / Woman / Non-binary person / Other)
(9) "Choose one or more races that you consider yourself to be:" (White / Black or African American / American Indian or Alaska Native / Asian / Pacific Islander or Native Hawaiian / Other)
(10) "Do you consider yourself to be Hispanic?" (Yes / No)
(11) "How would you describe your political views on social issues?" (Very socially liberal / Somewhat socially liberal / Neither socially liberal nor socially conservative / Somewhat socially conservative / Very socially conservative)
(12) "How would you describe your political views on economic issues?" (Very economically liberal / Somewhat economically liberal / Neither economically liberal nor economically conservative / Somewhat economically conservative / Very economically conservative)
(13) "In which state do you currently reside?" (<50 States> / D.C. / Puerto Rico / Not in US)