Pomona College
Department of Computer Science

A Step Forward and More of the Same: Global Privacy Control and California Privacy Law

Jan Charatan

April 28, 2023

Submitted as part of the senior exercise for the degree of
Bachelor of Arts in Computer Science

Professor Eleanor Birrell, advisor

Abstract

Citizens of California have a right to opt out of the sale of their personal information under the California Consumer Privacy Act (CCPA). The California Privacy Rights Act (CPRA) explicitly clarifies that browser-based opt out signals like Global Privacy Control (GPC) are a valid way to exercise this right. This legal enforceability under California privacy law makes GPC different from previous attempts at privacy signals like DNT or P3P that lost traction because companies had little incentive to respect them. Through a longitudinal measurement study, we show that while GPC adoption among the top 25,000 websites is increasing, there are still many websites that are not compliant with the specification. Additionally, we show through a user study that GPC banners can have an impact on user understanding and attitudes. Among other things, our research reaffirms the need for enforcement of California privacy laws and for specificity in privacy laws.

Acknowledgments

I would like to thank my advisor Dr. Eleanor Birrell, without whom this project would not have been possible. I would also like to thank my family and friends for their support during my college years. I would especially like to thank my brother, David, for his help debugging Python code during the measurement study portion of this project and for his feedback on draft versions of this thesis.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Our activity on the internet can paint a surprisingly accurate picture about us. Details about our browsing habits like the websites we visit and how we interact with them can be used to accurately predict demographic information like gender, age, location, and political orientation [HJ18]. As a result of the value that can be derived from our browsing data, it has become a valuable commodity—the websites that we regularly visit sell our information to other companies and data analysis firms to use in marketing, sales, product development and user experience.

Under the 2018 California Consumer Privacy Act (CCPA), Californians gained the right to opt out of the sale of their personal information. Despite this being a great victory for privacy advocates in theory, the actual implementation of this right has left much to be desired. Many companies use design strategies known as dark patterns to subtly nudge users away from exercising their right to opt out sale [ONSB21] or do not design their websites in CCPA-compliant ways [VNW22]. Beyond this, a practical concern with opt out of sale is that it is very difficult for users to opt out of sale on the many sites they visit. A 2008 paper by McDonald and Cranor estimated that U.S. internet users visit 1462 unique websites per year [MC08]—it would be unreasonable to expect any normal individual to opt out of sale using a different mechanism on each of these sites.

One alternative for exercising opt out of sale rights are opt out signals, which are digital representations of privacy preferences that are sent to a site on behalf of a user via mechanisms like HTTP headers or cookies. The obvious benefit of such signals is that they lower the burden on the user since privacy preferences can be automatically expressed without any potential for nudging. Unfortunately, previous attempts at opt out signals such as

Do Not Track (DNT) or the Platform for Privacy Preferences (P3P) failed due to lacking legal enforceability. One emerging opt out signal that has the potential to be more successful is Global Privacy Control (GPC). This signal expresses that a user wants to opt out of the sale on a site through HTTP headers or the DOM and unlike P3P and DNT, it is legally enforceable in the state of California. Former California attorney general Xavier Becerra confirmed via Twitter that GPC is a valid way to opt out of sale under the CCPA [Bec21]. The California Privacy Rights Act (CPRA), which will begin to be enforced on July 1, 2023, explicitly codifies that opt out signals are a valid way to opt out of sale into law.

As a result of GPC's legal enforceability under California privacy law, it has much more potential for success than previous opt out signals. However, for it to be truly effective it must be accessible to average users. This can be done by implementing it in easy-to-use browser extensions or ideally, directly into browsers as has been done with Firefox, DuckDuckGo and Brave. Additionally, California must continue to enforce that websites are actually respecting GPC signals as they did when they fined Sephora $1.2 million for not properly respecting GPC signals [oAGRB22].

The first portion of this thesis focuses on measuring current adoption of GPC. We conduct a longitudinal measurement study which involved scraping the top 25,000 websites from the Tranco research list across multiple months with the goal of seeing if the number of companies that comply with and mention GPC is increasing. The results of this measurement study are promising—we find that websites are increasingly opting users out of sale when they send GPC signals and that generally, the rate at which GPC is being mentioned in privacy policies is growing. At the same time, we still find that there are some issues with compliance.

The second portion of this thesis involves a user study where we investigate the impact of GPC displays on user attitudes and understanding. We find that depending on their type, displays can help users better understand that they are being opted out of sale. Similarly, displays can have an impact on user attitudes affecting things like whether users feel like their privacy is being protected. Additionally, during our user study we investigate current understanding of, adoption of and interest in GPC.

Following this introduction, Chapter 2 briefly discusses related work in this area of research and background about relevant laws. Chapter 3 discusses the methodology, results and limitations of our measurement study and chapter 4 discusses the methodology and results of our user study. Finally, Chapter 5 summarizes our results and discusses our recommendations for lawmakers, companies and citizens of California based on these results.

Chapter 2

Background & Related Work

2.1 CCPA

The passage of the 2018 California Consumer Privacy Act (CCPA) [oCLC18] made California the first state in the United States to sign a comprehensive piece of consumer privacy legislation into law. Within this law, there are four main rights that are granted to Californians—the right to know about the data being collected about you, the right to delete data about you, the right to non-discrimination for acting upon CCPA rights, and the right to opt-out of the sale of your personal information. The latter right—which allows users to opt out of the sale of their personal information—can be exercised in a variety of ways. Most commonly, users can exercise this right by finding a link labeled "Do Not Sell My Personal Information" (DNSMPI) in a website's footer that leads them to some sort of mechanism where they can express their preference to opt out of the sale of their personal information.

There is a lot of research that shows that there are serious problems with current opt out mechanisms. O'Connor et al. find that privacy-eroding designs are widespread among CCPA opt out mechanisms [ONSB21]. The authors also investigate how users interact with various common opt-out mechanisms and find that the design of the mechanism has significant impacts on consent rates—for example, putting the option to opt-out as an inline link or in a form makes it so that almost no users opt-out. Van Nortwick and Wilson research CCPA compliance rates by examining the state of DNSMPI links on almost 500,000 websites [VNW22]. They find that only about 2% of websites have such links and that only about 40% of these links meet the minimum standards of readability. Another issue with current opt out mechanisms is that users have to go through a separate process for opting out on each site. Although there is no research that estimates the amount of time CCPA opt out mechanisms take users per year, research by McDonald et al. provides a useful frame of reference [MC08]. They find that average American internet users visit 1462 unique websites per year. Given how much current mechanisms vary between sites, it would take an extremely long time for a user to opt out of sale on every site they visit.

Based on these problems with current opt out mechanisms, some researchers have looked at ways that opting out could be made easier. Siebel et al. find that standardized, visible banners increase opt-out rates and satisfaction [SB22]. Bannihatti et al. find opt out statements in privacy policies using heuristics and machine learning and put them into a browser extension [BKIN+20]. Zimmeck et al. attempt to standardize Do Not Sell by creating a browser extension called OptMeOwt that automatically places Do Not Sell cookies on sites and sends Do Not Sell headers [ZA20].

There is also research related to the CCPA that does not focus on opt out of sale. Chen et al. focus on the right to know and show that even if websites are legally required under the CCPA to disclose certain data practices, variance and vagueness in definitions can lead to confusion among users [CFN+21]. Other research related to the CCPA has investigated how to best convey privacy choices. Cranor et al. propose an icon that could help signal to users that they can exercise CCPA privacy choices [CHZ+20]; they suggest that this icon works best when it is accompanied by the text "Do Not Sell My Personal Information." Habib et al. point to the importance of accompanying icons with text and standardization [HZY+21].

2.2 CPRA

The California Privacy Rights Act (CPRA) [oCLC20] is a privacy bill that passed into law on November 3, 2020. The law became fully effective on January 1, 2023 and enforcement is scheduled to begin on July 1, 2023. The CPRA expands upon the privacy protections granted by the CCPA by giving Californians two new rights—the right to correct inaccurate personal information and the right to limit the use and disclosure of sensitive personal information. In addition, it creates the California Privacy Protection Agency, which will be tasked with enforcing the rights of Californians under the CCPA and CPRA.

Beyond this, the CPRA also strengthens existing rights like the right to opt out of sale. The law explicitly reaffirms that opt out preference signals are a valid way to opt out of sale. Although a tweet by California attorney general Xavier Becerra confirmed that this was already the case under the CCPA [Bec21], this demonstrates that California lawmakers are aware of the deficiencies with existing opt out of sale mechanisms and are seeking to make it easier for Californians to exercise their privacy rights.

2.3 Privacy Preference Signals

Historically, there have been numerous efforts to create technologies and frameworks to help aid users in making privacy choices. The first such effort happened during the late 1990s with the development of the Platform for Privacy Preferences (P3P) specification, which encodes human-readable privacy policies into machine-readable XML files [p3p]. Using P3P, users can define privacy preferences that can then be checked against a website's policy. Although various studies found that P3P privacy policies existed on several thousand sites in the early 2000s, the specification ultimately fizzled out since it was not legally enforceable [HWB21]. Another issue was that many sites intentionally misconfigured P3P since any sort of mistake in the setup meant that users agreed to everything.

In response to the failure of P3P, the Do Not Track (DNT) signal was created. This signal simply sends an HTTP request with a `DNT: 1` header indicating that the user does not wish to be tracked. DNT was implemented in a variety of browsers, but could only be turned on through external add-ons. Like previous attempts at privacy signals, DNT was never widely adopted by websites because of a lack of legal enforcement [HWB21]. Under the California Online Privacy Protection Act (CalOPPA) [oCLC13], companies in California are legally required to state in their privacy policies whether they respect DNT, but are not required to acknowledge the signal. The result of this is many companies simply having a disclaimer in their privacy policy that they don't acknowledge the signal.

As a result of government pressure, AdTech vendors founded a self-regulatory body called the Network Advertising Initiative (NAI) in 2000. As part of this initiative, they came up with the idea of opt-out cookies to help users express privacy preferences online. To do this, users would have to visit the NAI site and then they could go through a list of participating ad companies and express that they do not want to be tracked by each of these companies. The problem with this initiative is that the definition of tracking is very narrow and that the number of companies that participate is very small (75 as of January 2021) [HWB21].

Global Privacy Control (GPC) [gpc] is an opt-out signal that is sent via HTTP headers or the DOM that follows naturally from DNT. It is similar to DNT in that it is a signal that sends only a single bit value, but it is different in that it is a do not sell (DNS), rather than a do not track (DNT) signal. This much more closely reflects the wording of recent privacy laws like the Europe's General Data Protection Regulation (GDPR) and the CCPA, so it has more of a legal basis for enforcement. As it stands currently, GPC is implemented in some browsers, including Firefox, DuckDuckGo and Brave and it is used by over 50 million users. Zimmeck et al. conduct a user study to understand whether there is a need for GPC, create a browser extension that analyzes whether websites are respecting GPC, and conduct a measurement study to analyze GPC compliance among a small subset of top websites [ZWA+23]. They find that usable software is important for GPC adoption and that transparency about whether the signal is being respected is crucial for GPC to be effective.

A final privacy preference is signal is Advanced Data Protection Control (ADPC) [adp], which is essentially a modern version of P3P. As is the case with GPC, it is communicated through HTTP headers and the DOM. However, it can also be communicated through JavaScript APIs. It is bidirectional and can be initiated by both the user and the vendor to express privacy preferences or decisions. It is a much more granular and extensible signal than GPC. Human et al. provide a comparison between GPC and ADPC [HPM+22]. As it stands currently, ADPC is much less popular than GPC.

2.4 Consent Banners

Consent banners represent the opposite of opt out signals since the user has to manually make a choice each time they visit a website. Consent banners are widespread in Europe under the Transparency and Consent Framework (TCF) [tcf]. This framework defines what users consent to when they select certain options in consent dialogues and how third parties exchange consent signals. There is a large body of research that points out problems with TCF. Kulyk et al. find that users often click away from the consent dialogues without paying attention to them [KGHV20]. The same study also finds that users who have been exposed to consent dialogues for longer became more likely to accept them and less concerned about their privacy. Nouwens et al. finds that these dark patterns are very widely used and that only 11.8% of the websites meet the minimum standards that are outlined in the European Union's data privacy law. Additionally, they find that design decisions can have a significant impact on the amount of people that opt out [NLV$^+$20]. The findings of Utz et al. are similar. They observe that seemingly minor decisions about how GDPR-compliant consent banners are implemented have large effects on consent [UDF$^+$19]. Matte et al. find issues with how TCF is implemented. Among a crawl of 28,257 websites, they find that 41 websites illegally register positive consent even if the user has not made their choice, 236 websites nudge the users towards accepting consent by pre-selecting options, and 27 websites store a positive consent even if the user has explicitly opted out [MBS20].

Chapter 3

Prevalence of GPC in the Wild

To evaluate the prevalence of Global Privacy Control in the wild, we conducted a longitudinal web-scraping measurement study that evaluated two primary research questions:

(1) Do websites actually opt users out of sale when a GPC signal is sent?

(2) What information do websites provide about their GPC compliance?

3.1 Methodology

3.1.1 Scraping Infrastructure

To answer the above questions, we created a Selenium [sel] web scraper that used a GeckoDriver [gec] browser engine. This scraper was run on the top 25,000 websites from the October 29, 2022 Tranco top websites list [VLPJ] six times between mid-November 2022 and mid-April 2023. To combat some of the problems inherent to web scraping, such as websites temporarily being unavailable, the scraper was run twice each time a sample was collected. All of the data collection was done on AWS EC2 c6i.8xlarge instances that were located in a California data center (us-west-1) so that any CCPA functionality hidden behind geofencing would be shown to our scraper. Using the Python multiprocessing library, we ran the scraper on 32 websites at a time. This resulted in our scraper being able to run a complete sample in about 10 hours. Every time a new website was visited or a new link was opened on a website, we added a manual delay of five seconds to allow the website to open and the content to load.

3.1.2 Data Collected

For each website that was visited, our scraper logged the following:

- Whether a Do Not Sell My Personal Information link is found on the website's homepage. This is determined by looking for phrases that are a slight variation of *do not sell my personal information.* The full list of phrases we looked for is taken from Van Nortwick & Wilson's paper [VNW22] and includes the following: "do not sell my personal information", "do not sell my information", "do not sell my info", "do not sell my personal info", "do not sell or share my personal information", "do not sell or share my information", "do not sell or share my info", "do not sell or share my personal info".

- The state of the US Privacy String when GPC is off and when it is on. The US privacy string is an encoded 4 character string that describes signals regarding user privacy and choice under the CCPA. It is accessed using the US Privacy User Signal Mechanism (USP API). Most notably, the string encodes whether the user has opted out of the sale of their personal information on this website. When collecting the US Privacy String data, we also collect the version of the USP API that we are fetching the data from.

- Whether the privacy policy contains GPC-related language. To do this, we use a simple heuristic to attempt to find the privacy policy. We begin by looking on the homepage of the site for a link labeled either "Privacy Policy" or "Privacy Statement." If there is a matching link, we click it and search it. If there is no such link, we look for a link that contains the word "Privacy." If there is no "Privacy" link, we do not continue further and assume that there is no privacy policy easily accessible from the homepage. If there is such a link, however, we click on the first one and again look for either "Privacy Statement" or "Privacy Policy." If we find such a link, we stop and search it. If there is no link that explicitly points to a privacy policy, we simply search the "Privacy" link instead. When we search a link, we simply look for the following regexes:

  - **Regex 1:** `opt(-| )out( preference)? signals?( honored)?`
  - **Regex 2:** `global privacy control`
  - **Regex 3:** `browser(-based( standard)?)? signals?`

When we find one or more instances of any of these regexes, we save the source of the page we scraped.

- The content of `/.well-known/gpc.json` if it exists. To be compliant with the GPC specification, websites are supposed to have a `gpc.json` file within the `/.well-known` directory of their website that contains a value of `true` for a property `gpc`.

3.1.3 Data Conflict Resolution

As mentioned above, each time we ran the scraper, we collected two samples on separate instances. If there was conflicting information, we used the following heuristics to figure out the data for our overall run:

- If a DNSMPI link was found on one of two runs, we report true for the overall run.

- For the US Privacy Strings and US API version, we first prefer complete data. That means if one run is 0,0,1YYN,1 and one run is 1YNN,1,1YYN,1, we prefer the latter run. If the runs are both complete and still different, we prefer the more recent run. If we have one run that only has the string and version for GPC off and another which only has the string and version for GPC on, then we stitch the runs together to produce a complete run.

- If we have conflicting data for privacy policies, we prefer the results in this order: privacy policy on home → privacy policy layer down → privacy link → no privacy link → error. If we two searches that happened on the same layer and conflicting numbers, we prefer the run with more occurrences of regexes.

- For the results of `GPC.json`, we prefer a run where the `GPC.json` is found and if there is a conflict between the contents, we prefer the more recent run.

3.2 Results

3.2.1 Do websites actually opt users out of sale when a GPC signal is sent?

To answer this question, we examine the effect of sending the GPC signal on the US Privacy String. The `N → Y` category is most useful for doing this

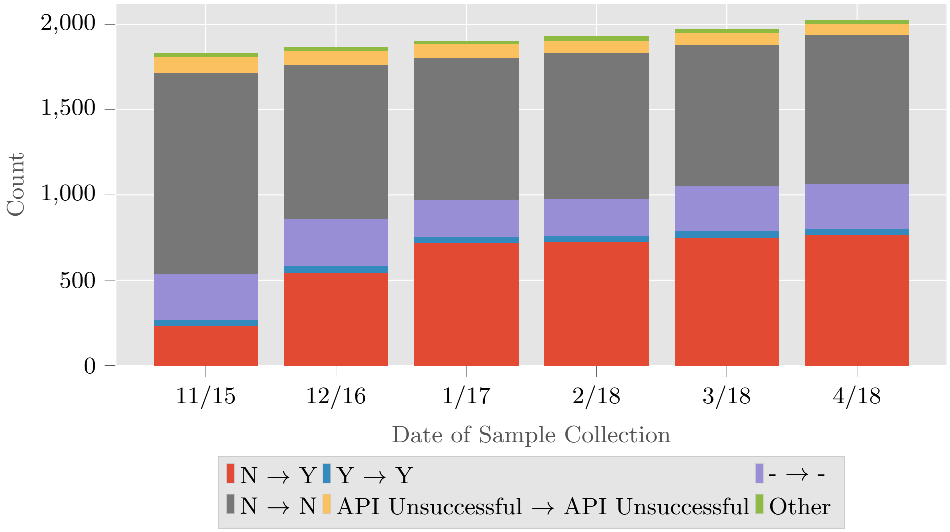


Figure 3.1: Effect of sending GPC signal on US Privacy String's opt-out of sale value

since these are sites where the scraper was not being opted out of the sale without GPC and was being opted out with the signal. Figure 3.1 shows there is an increasing number of sites that fall into this category. In absolute numbers, we went from 235 websites falling into this category of websites that appear to be respecting the GPC signal during November to 751 sites in March. On the flipside, the `N` → `N` category represents sites that are not opting users out of their sale even when the GPC signal is being sent. Within this category, the number of sites has decreased from 1173 to 829 during the course of our study. Although the reduction is promising, these 829 websites are all potentially not compliant with the GPC specification. A small number of sites fall into the `-` → `-` category. These are sites that claim that the requirements of CCPA do not apply to them. Additionally, some sites are in the `Y` → `Y` category; these are sites that opted our scraper out of sale even before we sent the GPC signal. Finally, there is a category for API call failures and there is the `Other` category which includes less common values such as `-` → `Y` and `N` → `-`.

Although the US Privacy String is designed for CCPA compliance and thus many websites that implement it are likely legally required to respect the CCPA, it is possible that some of the websites in Figure 3.1 are not required to follow the CCPA. To better understand the effect of CCPA on the US Privacy String for websites that are required to respect CCPA, we

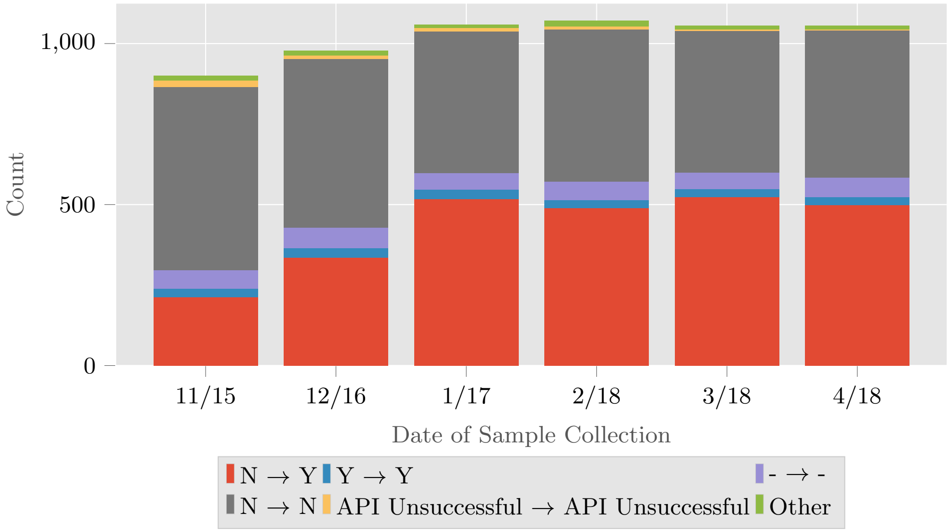


Figure 3.2: Effect of sending GPC signal on US Privacy String's opt-out of sale value on websites with a DNSMPI link

can look at Figure 3.2, which shows the subset of the data from Figure 3.1 where the homepage has a DNSMPI link. These websites are more likely to have to follow the CCPA since they are already following the requirement to provide a clear and conspicuous DNSMPI link. From this data, we see the same general trend that we saw in Figure 3.1 where the size of the `N → Y` category is increasing and the size of the `N → N` category is decreasing. Thus, the 440 websites that fall into the `N → N` category on Figure 3.2 are likely to be not CCPA-compliant since they are not opting users out of sale when GPC is sent.

3.2.2 What information do websites provide about their GPC compliance?

To understand the which information websites provide about their CCPA-compliance, we first examined whether sites had a `gpc.json` file located within the `/.well-known` directory. According to the GPC specification, websites can indicate that they are complying with the specification by having this file and by setting the `gpc` property in this file to `true`. Figure 3.3 shows that only a small number of websites have this file properly set up. Although the number is slightly increasing, in absolute terms it is still very low with the number of websites with valid files being 18 in November and

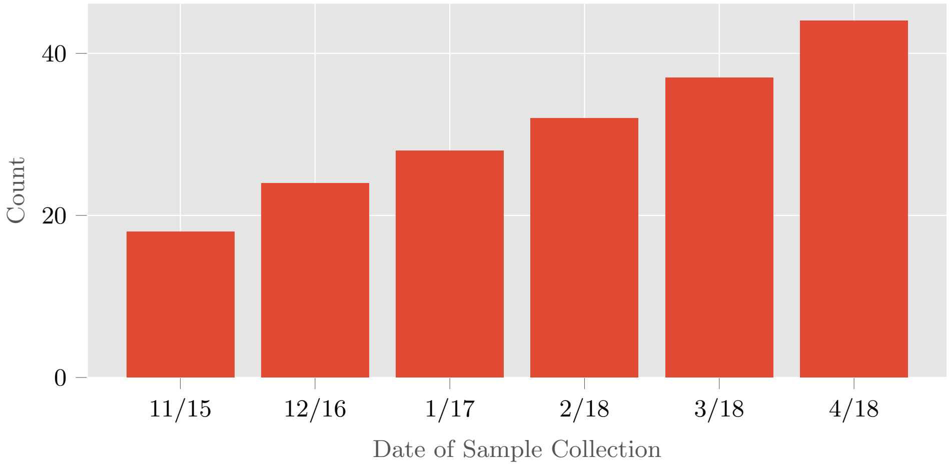


Figure 3.3: Websites with `GPC.json` files with GPC property set to `true`

44 in April.

Next, we examined the frequency at which GPC-related language is found in privacy policies. As mentioned above, we used very simple heuristics to find the privacy policies from the homepage of the website and we looked for the following three regexes:

- **Regex 1:** `opt(-| )out( preference)?  signals?( honored)?`
- **Regex 2:** `global privacy control`
- **Regex 3:** `browser(-based( standard)?)?  signals?`

As shown by Figure 3.4, we can see that over time, the number of websites with GPC-related language in their privacy policies has increased from 257 to 859. It is important to note, however, that not all of these mentions are referring to GPC since regexes 1 or 3 could also exist when there is a discussion of Do Not Track signals or other browser based signals. Figure 3.5 shows the number of privacy policies where only the second regex that explicitly references GPC is found. Here, it is evident again that the number of mentions of GPC is increasing, going from 76 in November to 613 in March. Thus, the privacy policy data also shows a clear trend of adoption of GPC increasing among websites.

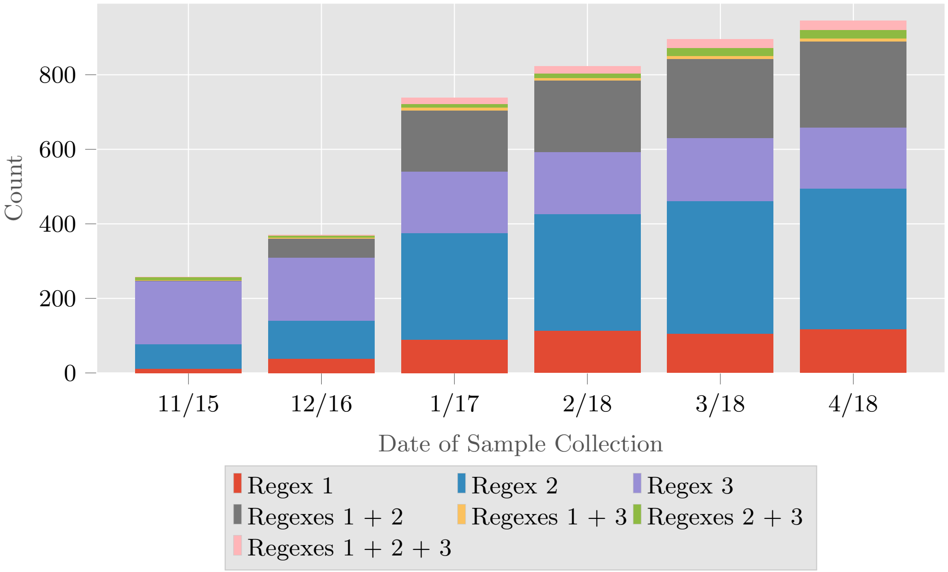


Figure 3.4: Websites with GPC-related language in their privacy policy

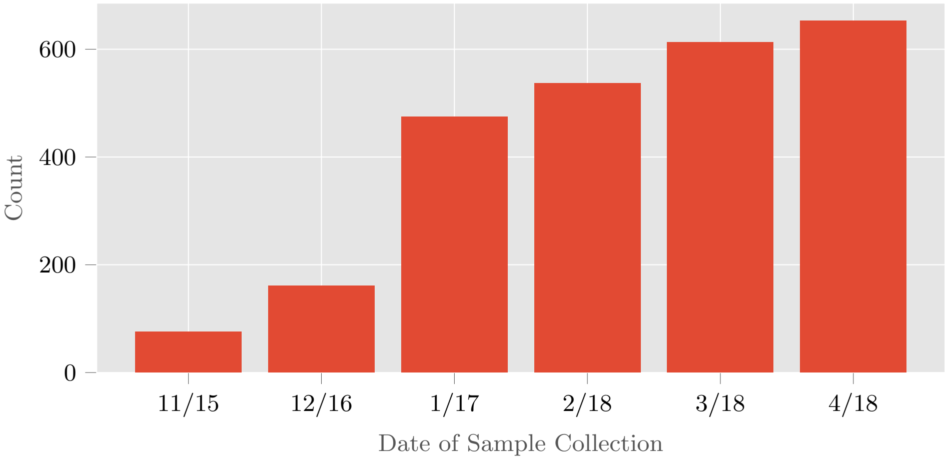


Figure 3.5: Websites with regex 2 (global privacy control) in their privacy policy

3.3 Limitations

There are a number of possible limitations with our methodology in this measurement study. For one, some websites can recognize web scrapers—as a result, they may send a different version of the website or require that a CAPTCHA is solved before the website can be entered. This may result in our scraper collecting incorrect data for some websites. Additionally, by its nature, scraping is imperfect. For example, depending on the speed of the server handling our requests, it is possible that the site would not have been loaded by the time we are searching for something. Although we attempted to mitigate this issue by adding in manual delays and running the scraper twice for each sample, it is still important to note that these inherent issues will inevitably impact the results. Another limitation of our scraper is that it did not access shadow DOMS, which are hidden DOM trees that are attached to the regular DOM. The reason for this is that it slowed our scraper down significantly. This is not likely to impact our results significantly since we only found one website where information we were looking for was located in a shadow DOM.

Chapter 4

The Effect of GPC Banners on User Attitudes & Understanding

The initial draft language of the CPRA mandated that websites display to their users whether they have received an opt-out preference signal like GPC:

> The business should display whether or not it has processed the consumer's opt-out preference signal. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

In a later revision, this language was removed. To understand the impact of removing this clause on Californians, we conducted a multi-stage user study that examined the impact of potential implementations of this language on user attitudes and understanding. We also examined participants' existing understanding of California privacy law and whether they are interested in GPC. We investigated four primary research questions:

(1) How well do GPC-related displays convey information to the participant?

(2) Are participants more distrustful and skeptical of sites where a banner is being displayed that the company is ignoring GPC?

(3) Are participants aware of their opt-out rights?

(4) Are participants aware of GPC and if not, would they be interested in it?

4.1 Methodology

4.1.1 Website

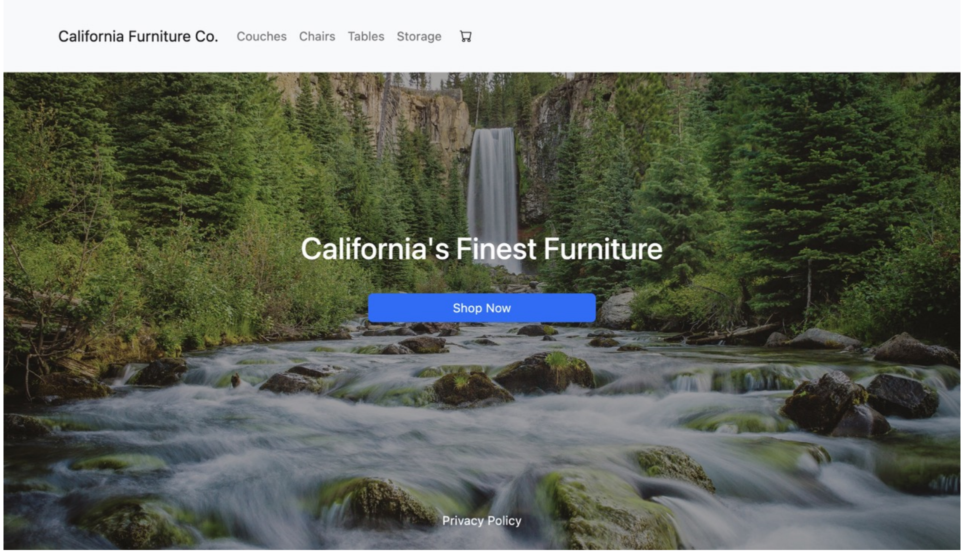
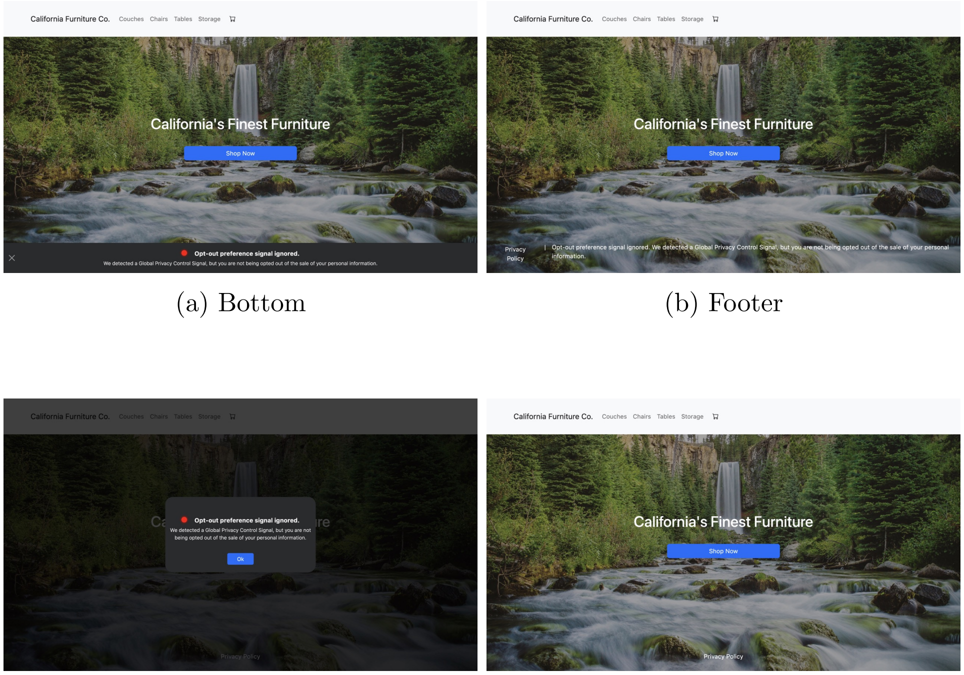


Figure 4.1: Furniture shopping website used in user study.

To conduct our study, we created a fake furniture shopping website called *California Furniture Company*. A shopping website provides a credible privacy threat to a visitor since shopping habits are frequently sold to advertisement companies. A screenshot of our website is shown in Figure 4.1. We chose to deceive our participants and to tell them that they were testing a shopping website so that we did not bias them by telling them by telling them the true purpose of this study beforehand. This deception was approved by the Pomona College IRB and we debriefed the participants at the conclusion of the study about this deception.

4.1.2 Conditions

We created several versions of the homepage to us understand the impact of different ways that a website can display that a GPC signal has been processed:



Opt-out preference signal ignored.
We detected a Global Privacy Control Signal, but you are not being opted out of the sale of your personal information.

(a) Bottom

(b) Footer

(c) Middle

(d) None

Figure 4.2: Example of location conditions on website for ignored verbose subcondition.

- **Bottom:** A bottom banner that still allows participants to interact with the page. The bottom banner includes text next to a glowing red or green circle that indicates whether GPC is on or off. We put the banner at the bottom of the page since this is what websites that have opt out of sale banners most commonly do [ONSB21].

- **Middle:** A middle banner that blocks the rest of the page and requires participants to wait three seconds before they can dismiss the banner. Before the banner can be dismissed, a spinning timer indicates how long the participant still has to wait. While the banner is open, there is a transparent black overlay that visually indicates that the participant is unable to interact with the rest of the site. The middle banner includes text next to a glowing red or green circle that indicates whether GPC is on or off. The goal of this condition was to make it so that it was nearly impossible for the user to miss the GPC information.

- **Footer:** A disclaimer embedded into the footer of the page. The footer only includes text and is visible even on small screens without the participant having to scroll. This condition reflects what we think websites are most likely to do if they are required to display GPC-related information without any specific guidance.
- **None:** A none condition where there was no banner or disclaimer about GPC. This condition was included to reflect a website that is not complying with a requirement to display GPC-related information.

Participants were randomly assigned one of these four conditions. Then, if they received something other than the none condition, they were randomly assigned one of four subconditions that added the following text to the banner/disclaimer:

- **Honored-Verbose:** Opt-out preference signal honored. We detected a Global Privacy Control signal, so you are being opted out of the sale of your personal information.
- **Honored-Concise:** Opt-out preference signal honored.
- **Ignored-Verbose:** Opt-out preference signal ignored. We detected a Global Privacy Control Signal, but you are not being opted out of the sale of your personal information.
- **Ignored-Concise:** Opt-out preference signal ignored.

To summarize, with three possible locations for a banner and four subconditions of varying GPC status and wording, this gave us 12 conditions where the participants received information about GPC. In addition, there was the 13th condition where the participants received no information about GPC. Figure 4.2 has examples of what various conditions on our site looked like.

4.1.3 Recruitment

We recruited participants for our user study through Prolific. As mentioned previously, we chose to deceive our participants by telling them that they were testing the usability of an online shopping website. As such, our study was advertised as “Online Shopping Website [BETA TEST]” with the description “Beta test an online shopping website and then complete a survey about the experience.” We recruited a balanced sample of participants from the United States who met two prescreening criteria: being a resident of California and being comfortable with participating in a deception study. We also recruited only participants who were on a desktop.

4.1.4 Task

Once participants started our study on Prolific, they were brought to a Qualtrics survey that began with them filling out a consent form. From there, participants were provided with a link taking them to our fake shopping website and the following blurb:

> The website linked below is a fake furniture shopping website that we are testing the usability of. Your task is to add a table to your cart and to check out. Once you click on check out, you will receive a completion code. Please paste it below so that we can verify that you attempted the task. After this page, you will be asked various questions regarding your attitudes about this website.

Once the users were done with this task, they returned to the Qualtrics survey and filled in their unique completion code. After that, they filled out the survey that can be found in the appendix. Finally, we debriefed the participants about the deception that occurred in our study and gave them an opportunity to remove their data from the study. In total, the median time it took our participants to complete our study was 4 minutes and 39 seconds. This resulted in an average compensation of $16.13 per hour, which is above California's minimum wage.

4.1.5 Data Collected on Website

We logged interactions for each participant who visited the site. These actions were associated with the user's Prolific ID, a unique identifier they received from the platform we used to recruit participants. We stored no personally-identifiable information such as IP addresses. Logged actions included interactions with the opt-out mechanisms such as clicking a button on a banner or more general interactions with the site such as which pages the participant visited and which links they clicked on. Finally, we logged a heartbeat whenever the webpage was in focus on the participant's device.

Beyond interactions with the site, we also logged other pieces of information. This includes very general information about the user's location such as the city they were in, their zip code, the state they were in and the country they were in. We used a service called ipapi [ipa] to access this information. Additionally, we stored some other general information such as whether the participant sent us a GPC signal, their user agent and the condition that they saw on the homepage.

4.2 Results

4.2.1 Participant Geography

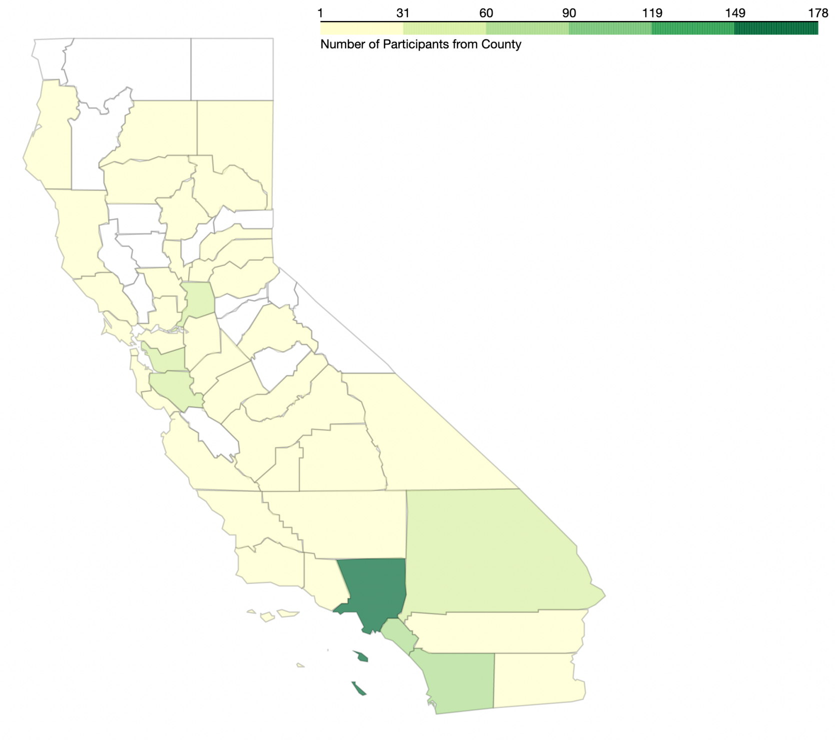


Figure 4.3: Counties where participants were located.

In total, we had 795 participants who participated in our study. Since it is important that participants are residents of California, we began by looking at which state they claimed to be residents of in our survey and which state our location API returned for them. We found that a significant amount used a non-California IP address or self-reported that they were a non-California resident. The exact breakdown the number of participants in each category is found in Table 4.1. The 20 participants who self-reported to be non-California residents were excluded from analysis. We decided to include participants who self-reported to be California residents, but had non-California IP addresses since the CCPA still applies to California residents who are temporarily outside of the state. Thus, the total number of participants became 775. A breakdown of which counties in California the participants who had California IP addresses were located in can be found in Figure 4.3. As would be expected, the county with the most participants is Los Angeles county and many of the more populous counties such as Orange County, San Bernardino County and San Diego County are more strongly represented.

Table 4.1: Breakdown of participant location information.

	CA IP Address	**Non-CA IP Address**
Self-Reported CA Resident	734	41
Self-Reported Non-CA Resident	6	14

4.2.2 Participant Demographics

All of the demographic questions answered by our participants were optional. Demographic information about the age, gender and race of our participants is found in Table 4.2. Our sample is balanced with regards to gender. It skews slightly younger than the actual population of California and mirrors the racial breakdown of California fairly closely. Table 4.3 shows the educational background of our participants. As is to be expected with Prolific, the participants skew slightly more educated than the general population. This is also reflected by the fact that 148 of 772 participants answered that they have formal education in a computer-related field and 163 of 775 participants answered that they work in a computer-related field.

4.2.3 Conditions

As mentioned previously, we had a total of 775 participants in our study. Of these participants 201 saw the bottom banner, 173 saw the middle banner, 208 saw a disclaimer in the footer and 193 saw a site without any GPC-related information. A more detailed breakdown of the conditions of the 775 participants we included in our analysis is shown in Table 4.4.

Table 4.2: Age, gender and race demographics of participants.

Age		**Gender**		**Race**		**Hispanic**	
18-24	153	**Man**	385	**White**	498	**Yes**	156
25-34	294	**Woman**	372	**Black or African Am.**	42	**No**	613
35-44	162	**Did Not Disclose**	8	**Am. Indian or AK Native**	17		
45-59	108	**Self Describe**	7	**Asian**	219		
60-74	51			**Pac. Islander/Native of HI**	9		
75+	7			**Other**	53		

Table 4.3: Educational background of participants.

Highest Level of Education	
Primary school or some secondary school	11
Graduated secondary school	95
Some higher education	210
Bachelor's degree	358
Additional degree beyond Bachelor's	92
Prefer not to respond	6
Other	4

Table 4.4: Breakdown of participants by condition.

	Bottom Banner	**Middle Banner**	**Footer**
Honored Verbose	46	49	43
Honored Concise	53	45	57
Ignored Verbose	48	38	49
Ignored Concise	54	41	59
None		193	

4.2.4 Task Completion

As mentioned previously, users were instructed to place a table in their cart and click on check out. Of our 775 participants, 696 clicked on check out with a table in their cart, 74 clicked on check out with a non-empty cart that contained no tables and 5 users never clicked on check out. Users were also given a code that was a hash of their Prolific ID after they clicked check out and had to enter it into the Qualtrics survey. Of our 775 participants, 769 successfully entered their unique hash. The six participants who entered a wrong value entered either their Prolific ID or the link of the website.

4.2.5 Site interaction

Of our participants, 35 clicked on the site's privacy policy. This amount of interaction with the privacy policy is likely a reflection of users knowing that they are study participants and interacting with the site more than they normally would. Unsurprisingly, of the 173 participants with the middle blocking banner, every participant clicked the button to acknowledge the banner. Of the 201 participants who saw the bottom banner, only four clicked the button to close it.

4.2.6 How well do GPC-related displays convey information to the participant?

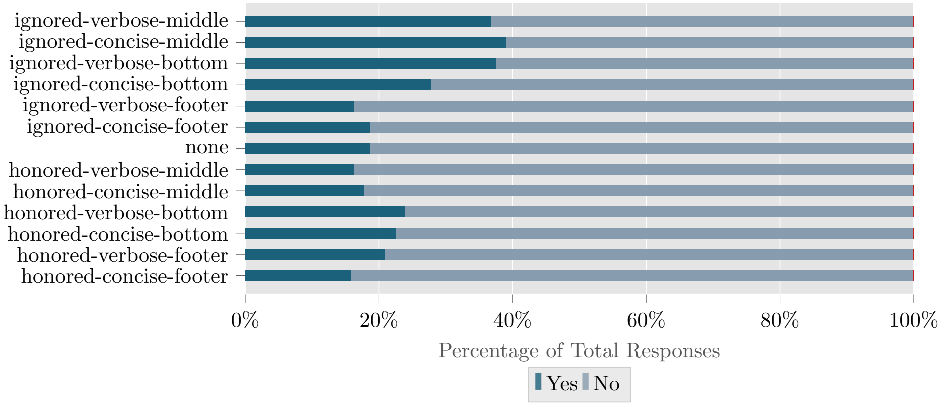


Figure 4.4: From what you observed on this website, does this website sell your personal information?

To investigate how well the GPC-related displays convey information to the user, we asked participants whether the site sells their personal information. The participants should response no for the conditions where GPC is being honored and yes for the conditions where GPC is being ignored. Figure 4.4 shows how the responses to this question varied by condition. The most noteworthy observation is that the yes rate of the middle ignored conditions is the highest at 39.0% for the concise condition and 36.8% for the verbose condition. What also stands out is that the yes rate was similarly high at 37.5% for the verbose bottom condition, but only 27.8% for the concise bottom condition. A one-way ANOVA test that compared the mean values of our conditions, we found a statistically significant p-value of 0.018. This suggests that a middle banner can help people realize that they are not being opted out of sale, regardless of whether the text is verbose. For a bottom banner, on the other hand, the verbose text might be necessary to get the message across.

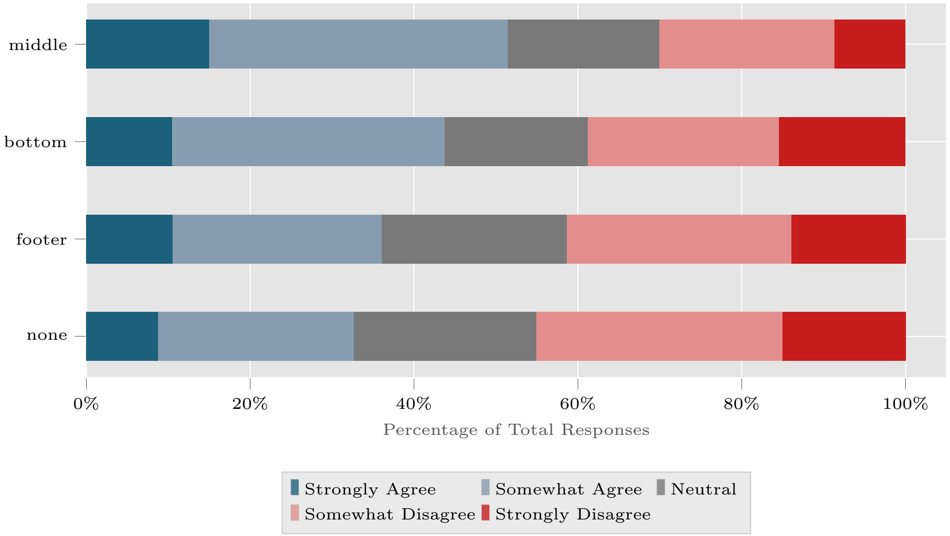


Figure 4.5: I am confident about my answer to the previous question.

After this question, we asked the participants how confident they were about their response to the previous question. Figure 4.5 demonstrates that beyond impacting how well participants understand their privacy rights, the displays also impact how confident participants feel about their knowledge. We find that the middle condition makes users feel most confident, followed by the bottom condition and then the footer condition. This result is intuitive since this order reflects what is most noticeable to users who are casually browsing. This difference between the mean responses to this question is statistically significant with a p-value of 0.0027.

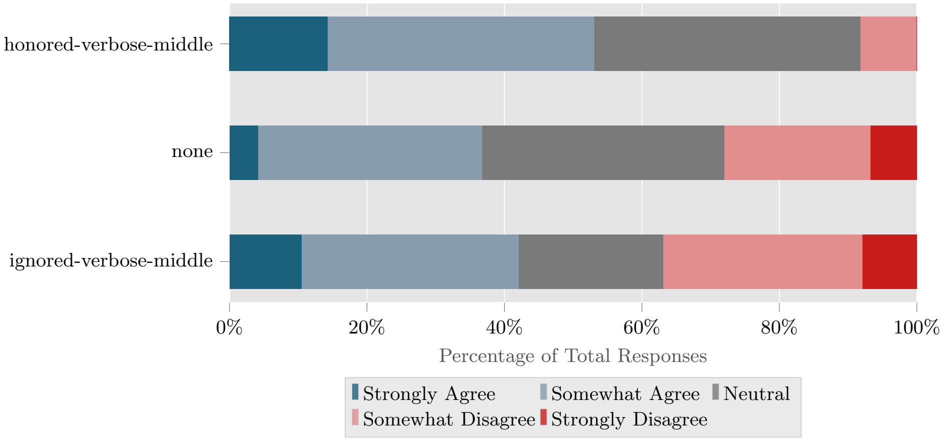


Figure 4.6: I feel like my privacy is protected on this website.

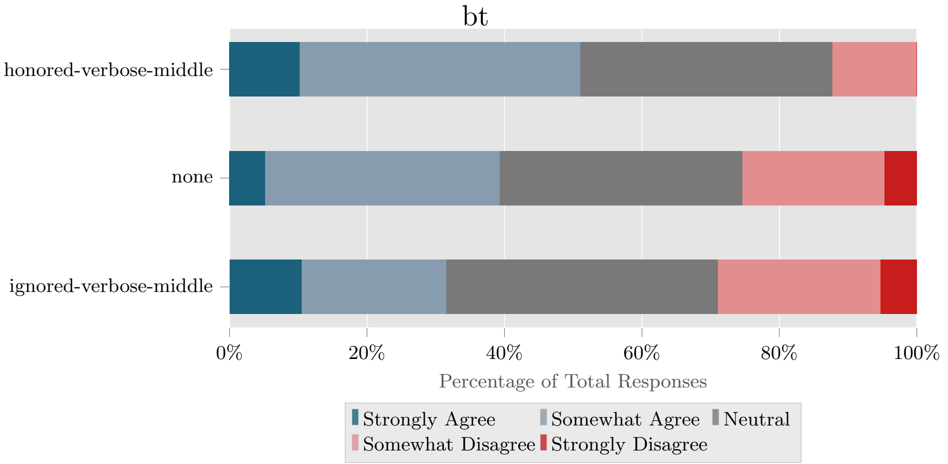


Figure 4.7: I trust this website with my personal information.

4.2.7 Are participants more distrustful and skeptical of sites where a banner is being displayed that the company is ignoring GPC?

We asked participants various questions to gauge their attitudes about the website. One of the questions we asked was whether participants felt that their privacy was protected on the website. We found a statistically significant difference between the verbose middle honored, verbose middle ignored and none groups (p=0.0037). As can be seen in Figure 4.6, participants were less likely to feel like their privacy is not being protected when they

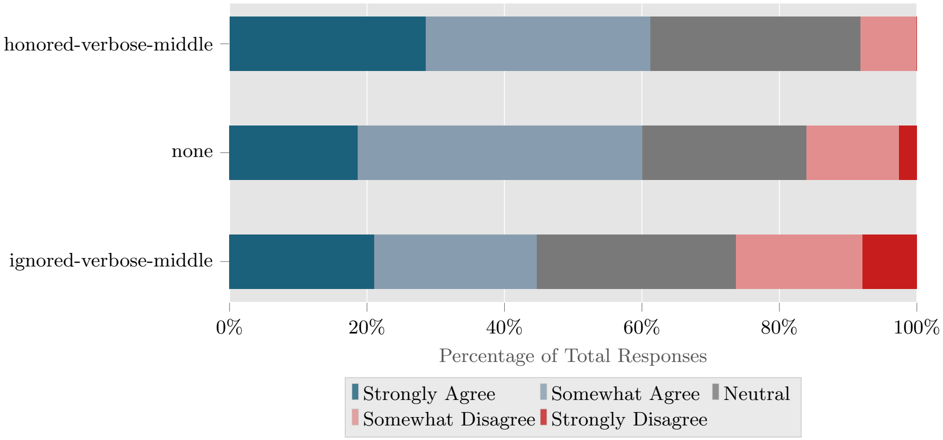


Figure 4.8: I feel at ease while I am on this website.

are very explicitly told that their GPC signal is being honored. There is not a large difference between the ignored group and the none group, suggesting that people are skeptical unless they receive positive affirmation that their privacy is being protected. A similar trend exists with the questions about users trusting the website with their personal information and the users feeling at ease on this website. Although neither of the p-values for these relationships are statistically significant (p=0.058 and p=0.085), they are suggestive. Figures 4.7 and 4.8 show the relevant data. It is again evident that the none condition and ignored condition are quite similar, while the honored condition makes people more at ease and more trusting of the website. An analysis of all 13 conditions for these questions provides no statistically significant relationships—we find p=0.41 for trusting this website with personal information, p=0.19 for feeling like privacy is protected and p=0.31 for feeling at ease.

4.2.8 Are participants aware of their opt-out rights?

To understand whether participants are aware of their opt-out rights, we asked participants whether California privacy law gives users: (1) the right to limit the disclosure of sensitive personal information, (2) the right to opt out of the sale of personal information and (3) the right to opt out of automated decision making. The correct answers to these questions are yes (under the CPRA), yes (under the CCPA) and no (this right is exists under GDPR, but not under California law). Figure 4.9 shows the amount of participants that believed California had each of these rights. The percentage of

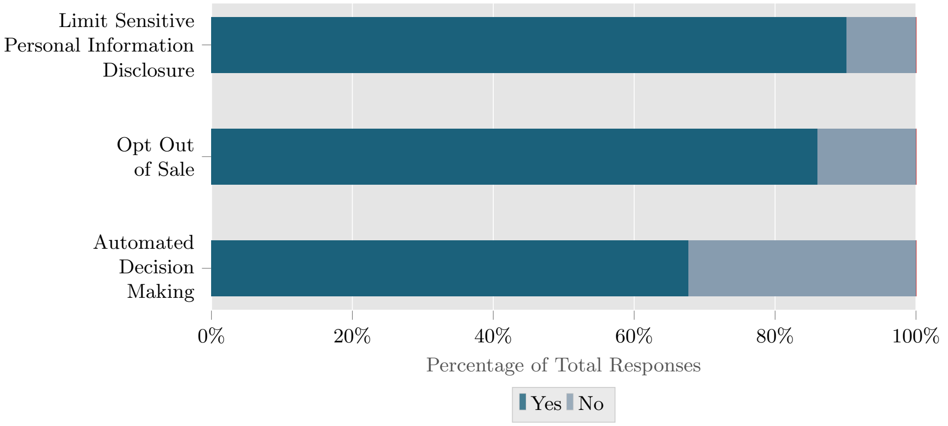


Figure 4.9: Responses to questions about familiarity with California privacy law.

people that said yes was 90.2%, 86.1% and 67.7% respectively. This means that the highest percentages of yes responses are for the two rights that residents of California actually have. This suggests that California residents have some awareness about their privacy rights, but that in general, they may believe that they have more privacy rights than they actually do.

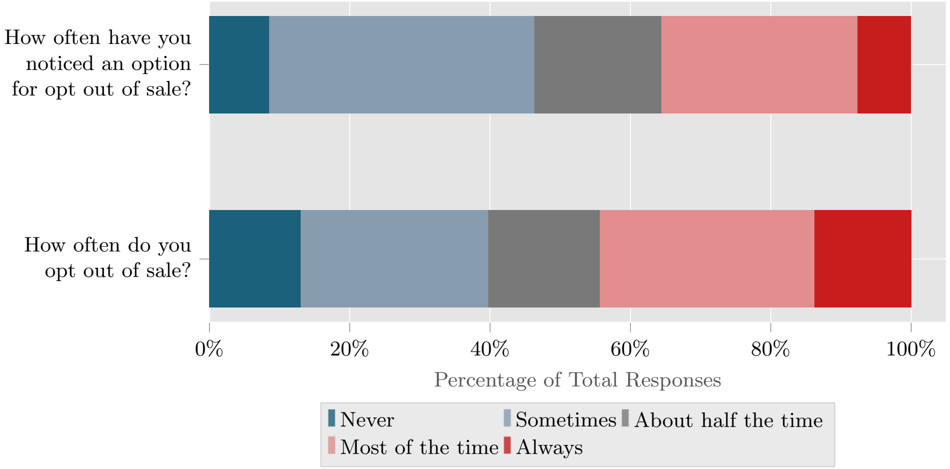


Figure 4.10: Responses to questions about opt out of sale options.

After these questions, we revealed to users that California does require websites to give users the option to opt out of the sale of their personal information. We then asked them how often they have noticed such options and how often they use such options. The data for how users responded to these questions can be found in Figure 4.10. Over 30% of participants claim to notice opt out of sale notices always or most of the time and over 40% claim to opt out of sale always or most of the time. This result may be due to participants wanting to appear more privacy-conscious than they actually are.

4.2.9 Are participants aware of GPC and if not, would they be interested in it?

To understand whether participants are currently aware of GPC, we began by looking at whether people currently have GPC enabled. Of the 775 participants, 75 sent us a GPC signal—this represents 9.7% of participants. Of these participants, 55 were using a Chromium-based browser, 17 were using Firefox and 3 were using Edge. When these users were asked whether they have GPC enabled in our survey, 5 responded yes, 8 responded no and 62 responded that they did not know. This shows that a significant portion of users who currently have GPC enabled may have it enabled without knowing. Beyond this, we also asked users to describe GPC in 20 words or less or to simply type "I don't know." The author of this paper coded these responses and found that 46 of 775 users showed understanding of what GPC is in their response. Many of the responses included misconceptions about GPC. For example, one user mistakenly believes that GPC notifies users when websites are selling their information; they wrote that GPC is "a web browser setting that notifies users if their information is being sold and gives the ability to opt out." Another user understood that GPC helped exercise privacy rights, but believes it to be broader in scope than it actually is; they wrote "Global Privacy Control is a web standard that allows users to exercise their privacy rights and opt-out of online tracking."

The last two questions in our survey asked users to respond how much they agree with the following statements: (1) "If it were available, I would enable an option in my browser that would automatically invoke my right to opt out of sale on all websites I visit." and (2) "If it were available, I would install software (e.g. a browser extension) that would automatically invoke my right to opt out of sale on all websites I visit." These two statements reflect the current ways that users can enable GPC—either by installing a browser extension like OptMeOwt or by enabling a setting within the browser, as can be done in Firefox. Figure 4.11 shows how users responded to the question. Unsurprisingly, users were more interested in the option that would not involve them installing something: 85.5% of participants

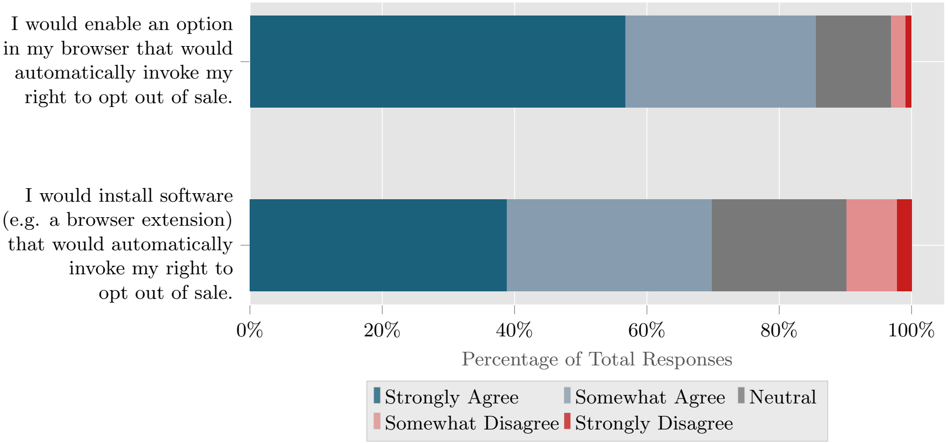


Figure 4.11: Responses to questions about enabling option in browser and installing software to opt out of sale.

strongly or somewhat agreed with the first statement. A slightly lower, but still large percentage of participants also expressed interest in installing software to invoke their right to opt out of sale: 69.8% of participants strongly or somewhat agreed with the second statement. This result suggests two things. Firstly, it suggests that users are interested in GPC and that they would potentially enable the signal if they were aware of it. Second, it underscores the importance of the ongoing efforts to integrate GPC directly into browsers.

Chapter 5

Discussion

Under the CCPA, Californians have the right to opt out of the sale of their personal information. In Chapter 2, we presented the problems associated with existing opt out mechanisms including dark patterns and the time it takes users to opt out using these mechanisms. Privacy advocates have proposed browser based opt out signals as a solution to these problems. A promising development on this front is that the CPRA, which will begin enforcement on July 1, 2023, explicitly mentions that opt out signals are a valid way to opt out of sale. However, to make opt out signals truly effective, they must be respected by websites that sell personal information and be accessible to average Californians.

In this thesis, we conduct a longitudinal measurement study where we examine the top 25,000 websites from the Tranco research list to see whether they respect and mention GPC. In general, we find that while GPC adoption has been increasing, there are still many websites that appear to be non-compliant with the specification. For example, we find that the number of websites with compliant `gpc.json` file has increased from 18 to 44 during the course of our study. While the increase is promising, the absolute number of websites in absolute terms is still extremely small, suggesting that few websites are completely compliant with the specification. Beyond this, we also examined how the US Privacy String changes when we send the GPC signal—in our last measurement, we find that 829 websites are not opting users out of sale before and after the GPC signal is sent. This again suggests that there are problems with GPC compliance.

The second part of this thesis is a user study where we evaluate the effect of GPC-related displays on user attitudes and their understanding of whether they are being opted out. We find that in certain situations, GPC displays can help users understand that websites are selling their personal information. Beyond this, we find that for certain banners, they can make users feel like their privacy is being protected. In our user study, we also find that users would be interested in GPC, especially if it is embedded directly into browsers. We also find that many users have misconceptions with GPC and often don't even know that they are sending the signal.

Based on the findings of this thesis, we have several recommendations for lawmakers, citizens and companies:

Recommendation #1: *Lawmakers Should Put More Emphasis on Enforcement*

Our findings demonstrate that by and large, companies will respect the requirements of laws like the CCPA if they are required to. However, the fact that many companies are still not opting users out of sale when GPC is being sent and that companies are not completely complying with the specification by not having `gpc.json` files demonstrates the need for enforcement by lawmakers. Although the Sephora case mentioned in Chapter 1 is a good start, companies should not be able to get by ignoring California privacy laws. One promising development on this front is that the CPRA created the California Privacy Protection Agency (CPPA), which is tasked with enforcing the CCPA and CPRA.

Recommendation #2: *Lawmakers Should Require Companies to Implement GPC Banners on their Websites*

We recommend that lawmakers reintroduce the requirement for websites to provide information about whether a GPC signal has been processed. We find in this thesis that GPC banners can help user understanding and that they can have a positive impact on user attitudes. It is critical that specific, data-driven requirements for the layout and design of such banners are created. This will ensure that companies are unable to use design practices that seek to place this information in locations where users will not see it.

Recommendation #3: *Lawmakers Should Spread Awareness About GPC & How to Act Upon Privacy Rights*

As we demonstrated in this thesis, many Californians do not know what GPC is or still have significant misunderstandings about what the signal does. As such, it will be critical for the California state government to spread awareness about the signal and how it can be turned on. Given that the European Union has been successful in spreading awareness about their data protection law [SAH20], the California state government can look at their efforts to understand how to best spread awareness about California privacy laws.

Recommendation #4: *Citizens Should Enable and Support GPC*

Given the small amount of time that is required to set up GPC, we recommend that citizens enable the signal in their browser. As this thesis demonstrates, an increasing number of websites are respecting the GPC signal. By enabling the signal one time, users can benefit from the potential privacy protections that the signal offers until they turn the signal off. Additionally, another benefit may be that websites who have received the signal may not send the user an opt out of sale dialogues. This could stop users from having to deal with potentially annoying pop-ups. Beyond enabling GPC, citizens should support the signal by spreading awareness about GPC and by supporting pro-privacy initiatives and lawmakers. Such efforts will help put more pressure on websites to comply with the signal and the government to effectively enforce GPC.

Recommendation #5: *Companies Should Take Initiative to Support GPC on their Websites*

Based on our findings, many companies do not fully comply with GPC. We recommend that companies make an effort to completely comply with the specification, making sure that they have a valid `gpc.json` file and that they give users the ability to easily find information about opt out of sale through the US privacy string and through their privacy policy. We also recommend that websites inform users through a display that their GPC signal has been honored even if lawmakers do not create a requirement for GPC banners. One reason that a site would consider implementing such banners is that they can lead to the user having more positive attitudes about the site.

As mentioned previously, GPC is a promising technology that can make it easier for Californians to opt out of the sale of their personal information. The findings of this thesis simultaneously demonstrate that GPC adoption is increasing and that there is still much work that needs to be done to make GPC more effective. We propose the above recommendations to help make

GPC as strong as it can be and hope that they can serve as a way to allow Californians to act upon their privacy rights in a meaningful way.

Bibliography

[adp] Advanced data protection control. https://www.dataprotectioncontrol.org/.

[Bec21] Attorney General Xavier Becerra, Jan. 28, 2021. https://twitter.com/AGBecerra/status/1354850758236102656.

[BKIN+20] Vinayshekhar Bannihatti Kumar, Roger Iyengar, Namita Nisal, Yuanyuan Feng, Hana Habib, Peter Story, Sushain Cherivirala, Margaret Hagan, Lorrie Cranor, Shomir Wilson, et al. Finding a choice in a haystack: Automatic extraction of opt-out statements from privacy policy text. In *Proceedings of The Web Conference 2020*, pages 1943–1954, 2020.

[CFN+21] Rex Chen, Fei Fang, Thomas Norton, Aleecia M McDonald, and Norman Sadeh. Fighting the fog: Evaluating the clarity of privacy disclosures in the age of ccpa. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, pages 73–102, 2021.

[CHZ+20] 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. *Retrieved September 13th*, 2020.

[gec] Geckodriver. https://github.com/mozilla/geckodriver.

[gpc] Global privacy control. https://globalprivacycontrol.org.

[HJ18] Joanne Hinds and Adam N Joinson. What demographic attributes do our digital footprints reveal? a systematic review. *PloS one*, 13(11):e0207112, 2018.

[HPM+22] Soheil Human, Harshvardhan J Pandit, Victor Morel, Cristiana Santos, Martin Degeling, Arianna Rossi, Wilhelmina Botes, Vitor Jesus, and Irene Kamara. Data protection and consenting communication mechanisms: Current open proposals and challenges. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 231–239. IEEE, 2022.

[HWB21] Maximilian Hils, Daniel W Woods, and Rainer Böhme. Privacy preference signals: Past, present and future. *Proceedings on Privacy Enhancing Technologies*, 2021(4):249–269, 2021.

[HZY+21] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. Toggles, dollar signs, and triangles: How to (in) effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–25, 2021.

[ipa] Ip api. https://ipapi.co/.

[KGHV20] Oksana Kulyk, Nina Gerber, Annika Hilt, and Melanie Volkamer. Has the gdpr hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity*, 6(1):tyaa022, 2020.

[MBS20] 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 (SP)*, pages 791–809. IEEE, 2020.

[MC08] Aleecia M McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *Isjlp*, 4:543, 2008.

[NLV+20] 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.

[oAGRB22] Office of Attorney General Rob Bonta. Attorney general bonta announces settlement with sephora as part of ongoing enforcement of california consumer privacy act, Aug.

24, 2022. https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

[oCLC13] State of California Legislative Counsel. Assembly bill no. 370. california online privacy protection act, 2013.

[oCLC18] State of California Legislative Counsel. Assembly bill no. 375. california consumer privacy act, 2018.

[oCLC20] State of California Legislative Counsel. Proposition 24. california privacy rights act, 2020.

[ONSB21] Sean O'Connor, Ryan Nurwono, Aden Siebel, and Eleanor Birrell. (un) clear and (in) conspicuous: The right to opt-out of sale under ccpa. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, pages 59–72, 2021.

[p3p] Platform for privacy preferences. https://www.w3.org/P3P/.

[SAH20] Joanna Strycharz, Jef Ausloos, and Natali Helberger. Data protection or data frustration? individual perceptions and attitudes towards the gdpr. *Eur. Data Prot. L. Rev.*, 6:407, 2020.

[SB22] Aden Siebel and Eleanor Birrell. The impact of visibility on the right to opt-out of sale under ccpa. *arXiv preprint arXiv:2206.10545*, 2022.

[sel] Selenium. https://www.selenium.dev/.

[tcf] Transparency & consent framework. https://iabeurope.eu/transparency-consent-framework/.

[UDF$^+$19] 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.

[VLPJ] Samaneh Tajalizadehkhoob Maciej Korczyński Victor Le Pochat, Tom Van Goethem and Wouter Joosen. Tranco. https://tranco-list.eu/.

[VNW22] Maggie Van Nortwick and Christo Wilson. Setting the bar low: Are websites complying with the minimum requirements of the ccpa? *Proceedings on Privacy Enhancing Technologies*, 2022(1):608–628, 2022.

[ZA20] Sebastian Zimmeck and Kuba Alicki. Standardizing and implementing do not sell. In *Proceedings of the 19th Workshop on Privacy in the Electronic Society*, pages 15–20, 2020.

[ZWA$^+$23] Sebastian Zimmeck, Oliver Wang, Kuba Alicki, Jocelyn Wang, and Sophie Eng. Usability and enforceability of global privacy control. *Proceedings on Privacy Enhancing Technologies*, 2:1–17, 2023.

Appendix A

Survey Questions

The following questions were asked to our participants after they interacted with the website:

(1) "Please rate how much you agree with the following statement. I trust this website with my personal information." (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(2) "Please rate how much you agree with the following statement. I feel like my privacy is protected on this website." (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(3) "Please rate how much you agree with the following statement. I feel at ease while I am on this website." (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(4) "Please rate how much you agree with the following statement. I would visit this website again." (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(5) "Please rate how much you agree with the following statement. I would be likely to use this website." (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(6) "How much do you agree with the following statement: I am comfortable with websites selling my personal information to third party companies?" (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(7) "From what you observed on this website, does this website sell your personal information?" (Yes / No)

(8) "How much do you agree with the following statement: I am confident about my answer to the previous question." (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(9) "To the best of your knowledge, does California law give users the right to limit the disclosure of sensitive personal information?" (Yes / No)

(10) "How much do you agree with the following statement: I am confident about my answer to the previous question." (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(11) ”To the best of your knowledge, does California law require that websites that sell your data allow you to opt out of the sale of your personal information?” (Yes / No)

(12) ”How much do you agree with the following statement: I am confident about my answer to the previous question.” (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(13) ”To the best of your knowledge, does California law require that websites allow individuals to opt out of automated decision making?” (Yes / No)

(14) ”How much do you agree with the following statement: I am confident about my answer to the previous question.” (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(15) ”Under California law, websites are legally obligated to give you an option to opt out of the sale of your personal information. How often have you noticed websites you visit giving you such an option?” (Never / Sometimes / About half the time / Most of the time / Always)

(16) ”How often do you opt out of the sale of your personal information on websites you visit?” (Never / Sometimes / About half the time / Most of the time / Always)

(17) ”In 20 words or less, what is Global Privacy Control? If you are don’t know, please just say *I don’t know*.” (Free response)

(18) ”Do you currently have Global Privacy Control (GPC) enabled?” (Yes / No / I don’t know)

(19) ”How much do you agree with the following statement: If it were available, I would enable an option in my browser that would automatically invoke my right to opt out of sale on all websites I visit.” (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(20) ”How much do you agree with the following statement: If it were available, I would install software (e.g. a browser extension) that would automatically invoke my right to opt out of sale on all websites I visit.” (Strongly agree / Somewhat agree / Neutral / Somewhat disagree / Strongly disagree)

(21) ”What is your current age?” (18-24 / 25-34 / 35-44 / 45-59 / 60-74 / 75+)

(22) ”What is your gender?” (Man / Woman / Prefer not disclose / Prefer to self describe: ____________)

(23) ”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)

(24) ”Do you consider yourself to be Hispanic?” (Yes / No)

(25) ”In which state do you currently reside?” (50 states / American Samoa / District of Columbia / Guam / Minor Outlying Islands / Northern Mariana Islands / U.S. Virgin Islands / Not in U.S.)