Stanford Law School

Center for Internet and Society

Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel 650 723-5205
Fax 650 725-4086
cyberlaw.stanford.edu

October 28, 2020

To Whom It May Concern:

We are pleased to submit comments to the California Attorney General's office regarding the Third Set of Proposed Modifications to CCPA Regulations released on October 12, 2020. We make these comments on behalf of ourselves individually and provide our institutional affiliation for identification purposes only.

In sum, we are heartened by the OAG's decision to further clarify §999.315 - Requests to Opt-Out. From our own experience conducting empirical research on the implementation of "Do Not Sell My Personal Information" links across a variety of websites, we observed a wide discrepancy in how individual companies have implemented this process. We found evidence of so-called "dark patterns"—as defined in Proposition 24, "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice." Whether intentionally designed to thwart Californians' exercise of their Do Not Sell right, or as a result of poor design choices, the end result is the same: unfair barriers to completing these requests. While these design choices may negatively impact all California consumers, they may have disproportionate impacts on vulnerable individuals, such as the elderly, non-English speakers, and individuals with lower written literacy and technology experience.

Our research group reviewed the Do Not Sell (DNS) processes of dozens of websites across a variety of different business types, including: brick and mortar retail stores, car dealerships, theme parks, grocery stores, pharmacies, banks, and newspapers. We observed the following problems, of which we include examples in the attached appendix:

- Do Not Sell flows (the steps by which a consumer initiates a Do Not Sell request up to completion) that included unnecessary steps for making a DNS request, such as:
    - Sending consumers from the DNS link on a company's homepage to the company's privacy policy page (or other indirect routes), rather than directly to a DNS form, thus requiring consumers to hunt through the policy to find the link to the DNS form (see Appendix 1 for an example);
    - Requiring consumers to select a button or toggle embedded within a page to make a request, often without instructions or clear labels, such that is it unclear which option initiates the DNS state (see Appendix 2 for examples);
- DNS forms that asked consumers to provide personal information that appeared extraneous to the DNS request;

- Forms offered only in English by companies that likely have large non-English speaking customer bases (see Appendix 3 for an example);
- DNS landing pages and/or forms that used confusing (e.g., double negatives) or manipulative language (e.g. emotionally charged or guilt-inducing) that attempts to persuade consumers not to exercise their rights (see Appendix 4 for an example);
- DNS landing pages that included copious amounts of text preceding the form that was not directly salient to making a request. Forcing consumers to spend additional time or energy to read extraneous information may decrease the likelihood of completing a DNS request (see Appendix 5 for an example);
- For companies that honor DNS requests only via email, many of these companies provided little or no instruction to consumers about how to complete the request (e.g., what information to include in an email), did not offer automated shortcuts for composing emails (e.g., mailto functionality that can prepopulate an email with the address and subject link when clicked), and provided email addresses that appeared to be non-specific to DNS requests, which may increase the burden on the consumer to engage in continual back-and-forth with the company to make the DNS request.

Consumer Reports, which released a report on October 1st, 2020 entitled "California Consumer Protection Act: Are Consumers' Digital Rights Protected," also found many of the same issues we report here, as well as additional concerns.[1]

We are pleased to see the OAG address some of the issues above with additional clarifications to the statute in order to improve what should be a simple and straightforward process for consumers. These clarifications make it less onerous for both consumers to exercise their rights and for companies to comply with the CCPA. By reducing the gray area that forces companies to rely heavily on interpretation, the updated regulations diminish the potential for DNS processes to be designed in ways that are confusing, deceptive, or manipulative to consumers, whether deliberately or by accident.

At the same time, while the clarifications reduce company discretion in designing DNS processes, the current OAG guidelines still leave room for companies to implement DNS processes in ways that subvert consumers' ability to exercise their rights under the statute.

We would like to see companies and/or policymakers also address the following:

1. Provide forms, rather than email addresses, for consumers to make DNS requests

DNS requests that require consumers to send an email, without outlining the information consumers must provide for the request to be fulfilled, are particularly burdensome on consumers.

2. Offer DNS forms in languages other than English, and also use simple, easy to understand language

Non-English speakers are particularly vulnerable to confusing or misleading language in DNS requests. For businesses that provide essential services and/or have a substantial non-English speaking clientele, company DNS forms should accommodate different languages (see Appendix 3 for examples of English-only privacy policies for companies with large non-English speaking customer populations).

[1] Available at: https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

3. Avoid crowding DNS forms with extraneous information

DNS forms are not the place for companies to produce treatises on why they think they do not sell information. And while providing references to useful background information on the CCPA may be helpful to consumers (including links to official guidance from the OAG's CCPA website), reproducing hundreds of words of text that is not required reading for exercising one's DNS rights is not helpful and discourages consumers from completing their requests.

4. Provide consumers a streamlined form that does not require them to take extraneous steps to complete a DNS request. For multiple-purpose forms (e.g. forms allowing consumers to also exercise their deletion and access rights), make the selection choices simple and clear.

5. Absent a mandate to respect Global Privacy Control signals, provide a standardized interface for consumers to exercise their DNS rights.

The CCPA presently requires companies to provide "two or more designated methods for submitting requests to opt-out."[2] The vast majority of companies have elected not to adopt mechanisms such as the Global Privacy Control[3], which would provide a simple and straightforward means for consumers to communicate DNS preferences with all websites they visit using a browser plug-in or setting. Unfortunately, the original requirement of the statute to develop "a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information" (§1798.185(4)(C)) was dropped during the review period. While we filed comments in February 2020 urging that the Attorney General (OAG) not adopt the version of the button proposed at that time, we did support the OAG following the advice of the CMU report to create a standardized control.[4] Unfortunately, our research demonstrates that absent a standardized control mechanism, companies are using inconsistent and in some cases, unclear and misleading methods to allow consumers to exercise their DNS rights. Further, executing DNS requests for even a single website requires consumers to repeat these steps using every browser on every device (including mobile devices) they have used to access the website in order to fully ensure that a single company honors their DNS preference. This is, on a practical level, unworkable for consumers, and illustrates the unreasonable burden consumers must shoulder to exercise their CCPA rights.

Accordingly, we urge California policymakers to mandate the adoption of the Global Privacy Control standard. In the CCPA, §999.315(c) mandates that businesses treat "user-enabled global privacy controls, such as browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request." The current "process" for making DNS requests on websites where cookies, rather than a user account, are the basis by which consumers are tracked is, as we note above, is highly complicated and likely deeply confusing for most consumers (Please see Appendix 6 for examples.) As the attached examples demonstrate, consumers are expected to either submit opt-out requests on each browser and device they use to visit a company's website, or are asked to allow the site to place a cookie in order to provide a DNS signal (which becomes obsolete if a consumer elects to clear her browser cookies).

The Global Privacy Control could provide consumers with a delegated means of seamlessly providing DNS requests to companies without having to engage in the burden of making independent DNS requests for each

[2] §999.315(a)
[3] https://globalprivacycontrol.org/
[4] Cranor, et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* (February 4, 2020).

website they visit and on each browser and device they use. However, as we note above, businesses can refuse to honor a consumer's privacy-specific preferences if the preferences were set in the software, such as the legacy "Do Not Track" option in web browsers. As of right now, California law dictates that companies must disclose whether they respond to "Do Not Track" requests, ultimately giving them the discretion as to whether or not to honor these requests from consumers.

In closing, while we believe the §999.315 clarifications are a positive development for consumers hoping to exercise their rights under the CCPA, there are still several measures companies should take to ensure that they are not actively undermining DNS processes, particularly for vulnerable populations.

Sincerely,

Jennifer King, Ph.D
Director of Consumer Privacy
Center for Internet and Society, Stanford Law School

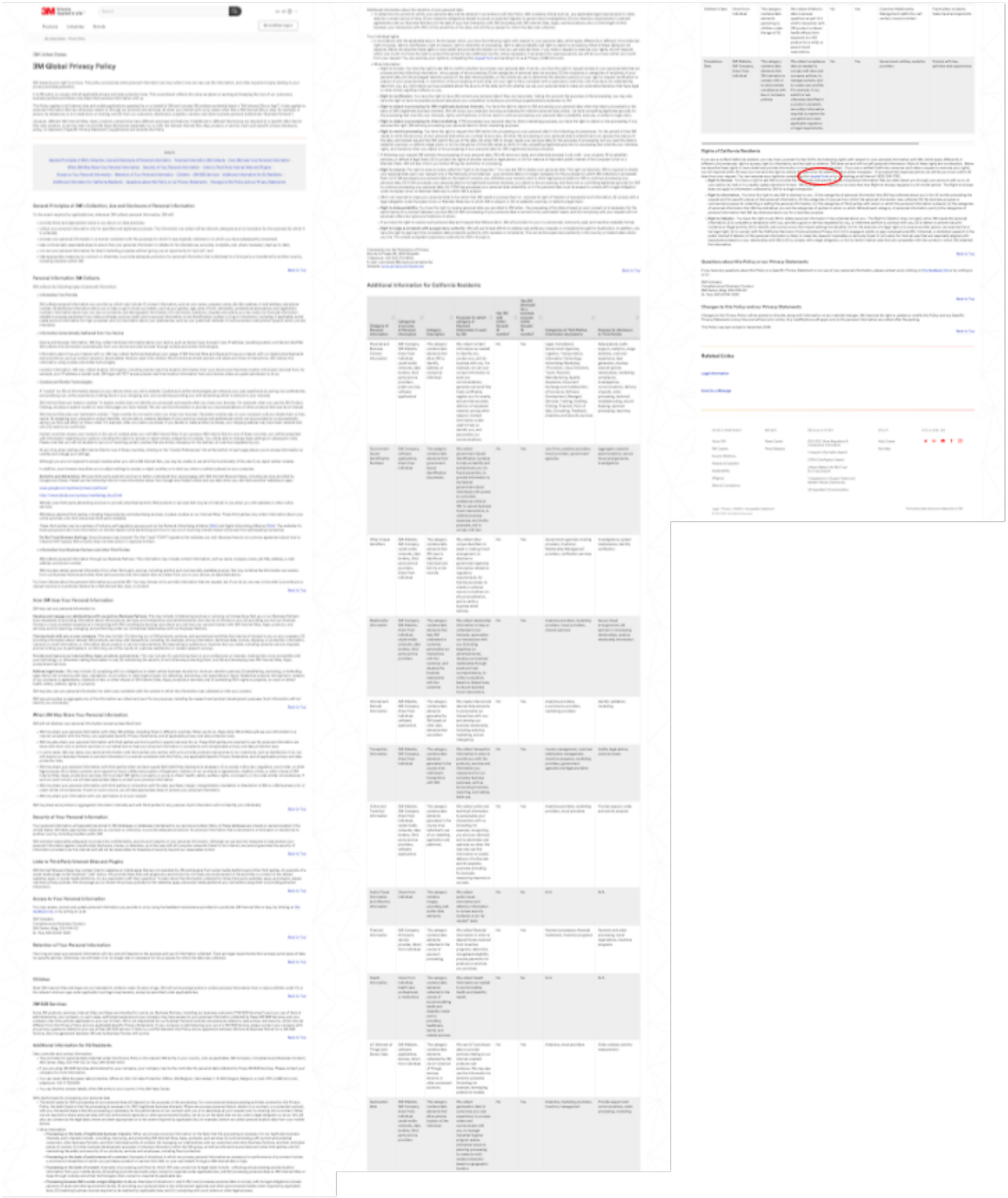
Adriana Stephan
M.A. Student
Cyber Policy, Stanford University

Emilia Porubcin and Claudia Bobadilla
Undergraduate Students, Stanford University

Morgan Livingston
Undergraduate Student, University of California, Berkeley

**Appendix 1: 3M Company (https://www.3m.com/3M/en_US/company-us/privacy-policy/), visited 10/26/20**

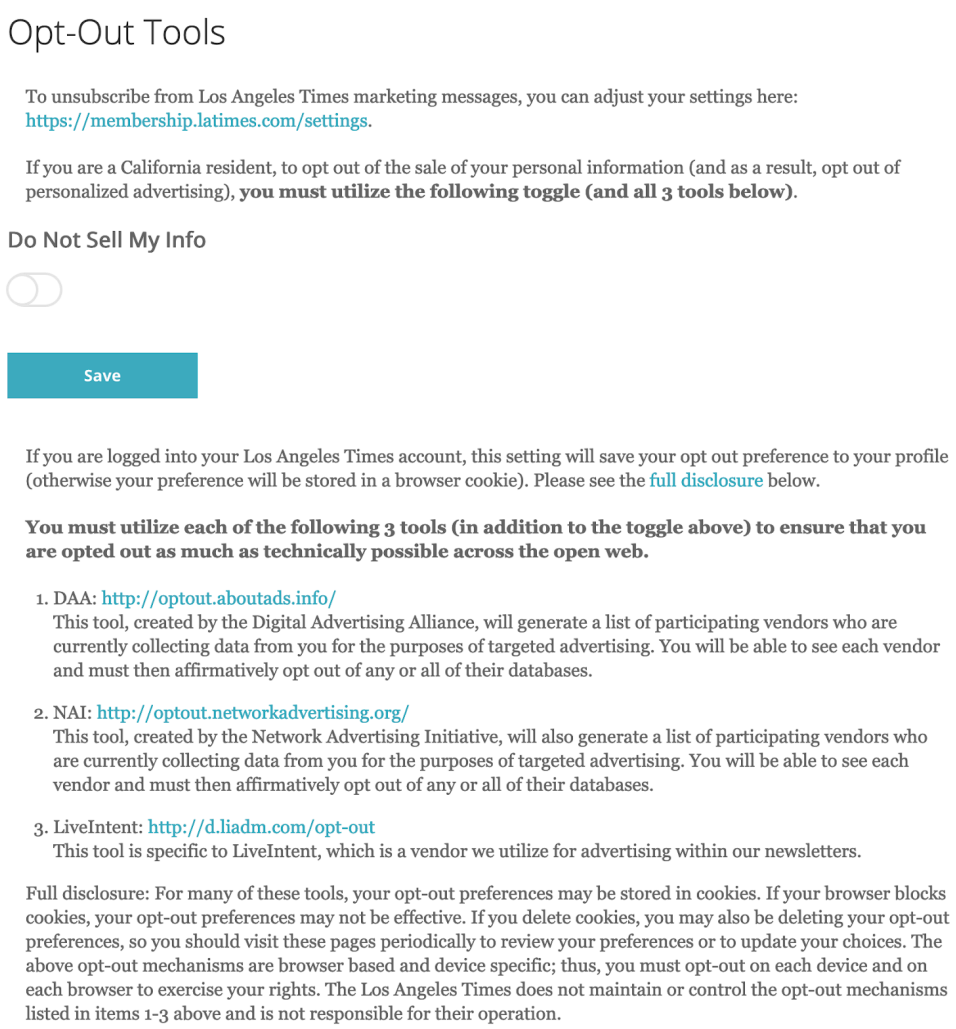
Please note that there is no “Do Not Sell” link from the homepage; this page is accessed via the privacy policy link in the footer. Due to the length of this page we have cut it into smaller sections in order to fit it all one printed page. The link in the red circle is the link to the DNS form.



## Appendix 2: Examples of unclear or confusing DNS toggles or buttons

These examples illustrate how companies are using a specific form of interaction design (toggle switches) that neither clearly communicates to consumers what toggling the switch will accomplish, nor whether they have successfully opted out or not. The LA Times (Example 1) is slightly clearer than Examples 2 and 3 given that the switch is grey when arriving at the page (indicating "off"), and when clicked turns green (indicating "on"), as well as providing a "Save" button to confirm the selection. Even so, there are no instructions to follow nor text indicating the switch state. Example 2 offers consumers the choice to "agree" or "disagree", but with what exactly is unclear (are you agreeing to opt-out? Or not?). Example 3 provides no instruction of what will occur when the toggle is switched; the consumer must deduce that the existing state (blue, presumably "on") means that one's data is being sold to third parties, and that toggling it to grey ("off") will stop the sale.

### Example 1: Los Angeles Times (visited 10/26/20)



Opt-Out Tools

To unsubscribe from Los Angeles Times marketing messages, you can adjust your settings here: https://membership.latimes.com/settings.

If you are a California resident, to opt out of the sale of your personal information (and as a result, opt out of personalized advertising), **you must utilize the following toggle (and all 3 tools below)**.

Do Not Sell My Info

Save

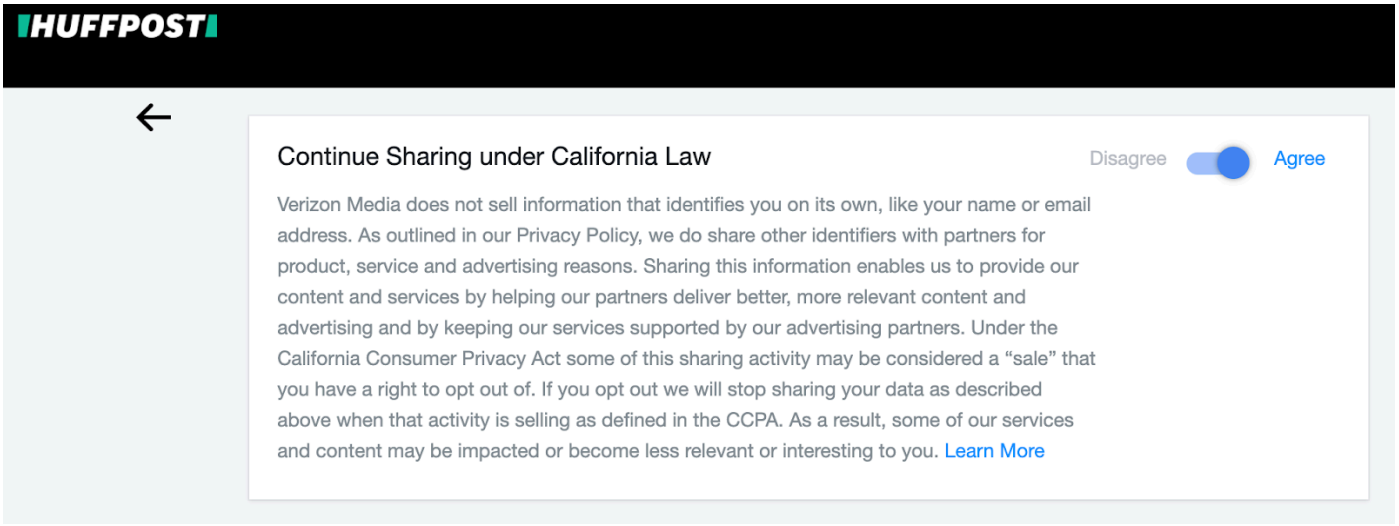
If you are logged into your Los Angeles Times account, this setting will save your opt out preference to your profile (otherwise your preference will be stored in a browser cookie). Please see the full disclosure below.

**You must utilize each of the following 3 tools (in addition to the toggle above) to ensure that you are opted out as much as technically possible across the open web.**

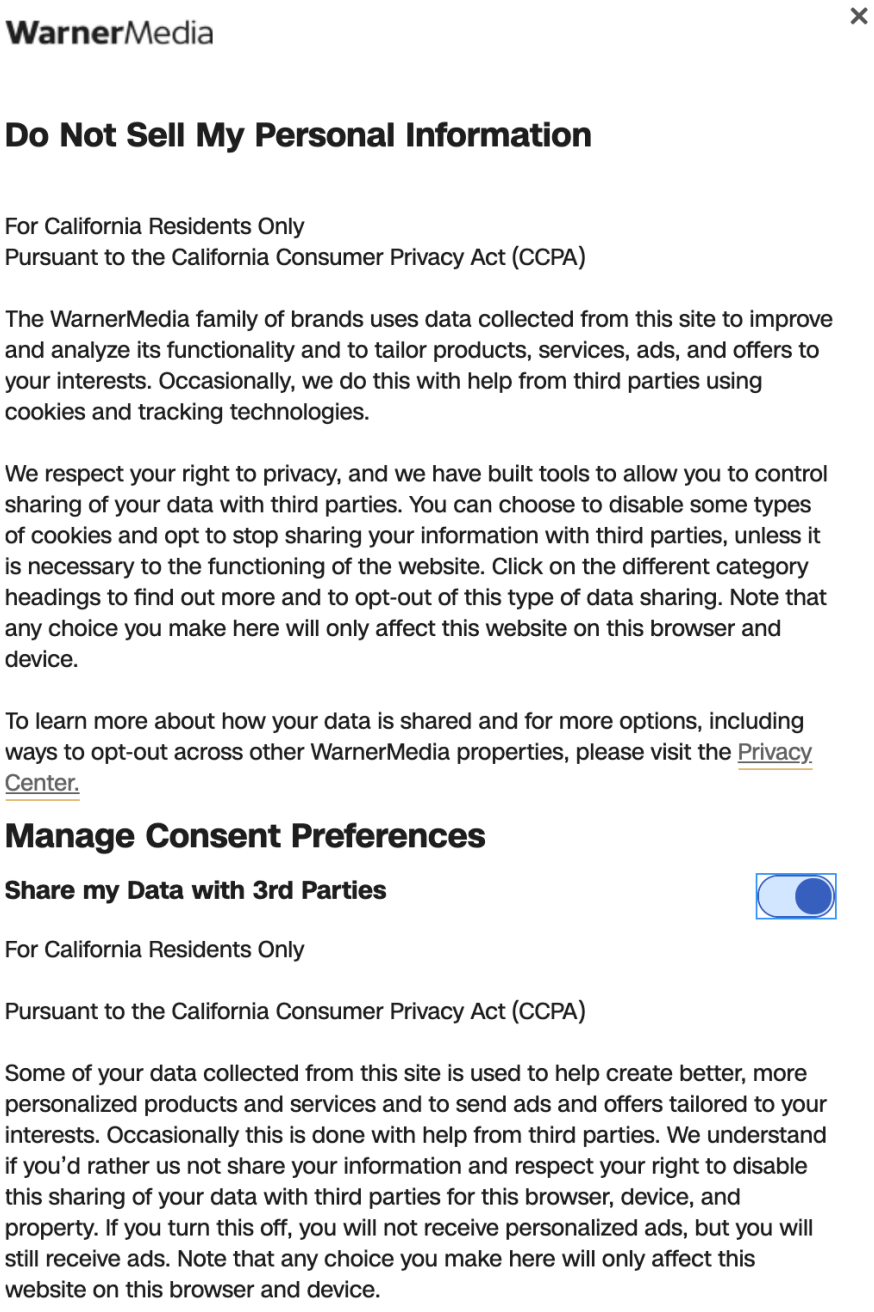
1. DAA: http://optout.aboutads.info/
   This tool, created by the Digital Advertising Alliance, will generate a list of participating vendors who are currently collecting data from you for the purposes of targeted advertising. You will be able to see each vendor and must then affirmatively opt out of any or all of their databases.
2. NAI: http://optout.networkadvertising.org/
   This tool, created by the Network Advertising Initiative, will also generate a list of participating vendors who are currently collecting data from you for the purposes of targeted advertising. You will be able to see each vendor and must then affirmatively opt out of any or all of their databases.
3. LiveIntent: http://d.liadm.com/opt-out
   This tool is specific to LiveIntent, which is a vendor we utilize for advertising within our newsletters.

Full disclosure: For many of these tools, your opt-out preferences may be stored in cookies. If your browser blocks cookies, your opt-out preferences may not be effective. If you delete cookies, you may also be deleting your opt-out preferences, so you should visit these pages periodically to review your preferences or to update your choices. The above opt-out mechanisms are browser based and device specific; thus, you must opt-out on each device and on each browser to exercise your rights. The Los Angeles Times does not maintain or control the opt-out mechanisms listed in items 1-3 above and is not responsible for their operation.

**Example 2: Huffington Post/Verizon Media (visited 10/27/20)**



**Example 3: CNN.Com/Warner Media (visited 10/27/20)**



WarnerMedia

## Do Not Sell My Personal Information

For California Residents Only
Pursuant to the California Consumer Privacy Act (CCPA)

The WarnerMedia family of brands uses data collected from this site to improve and analyze its functionality and to tailor products, services, ads, and offers to your interests. Occasionally, we do this with help from third parties using cookies and tracking technologies.

We respect your right to privacy, and we have built tools to allow you to control sharing of your data with third parties. You can choose to disable some types of cookies and opt to stop sharing your information with third parties, unless it is necessary to the functioning of the website. Click on the different category headings to find out more and to opt-out of this type of data sharing. Note that any choice you make here will only affect this website on this browser and device.

To learn more about how your data is shared and for more options, including ways to opt-out across other WarnerMedia properties, please visit the Privacy Center.

## Manage Consent Preferences

**Share my Data with 3rd Parties**

For California Residents Only

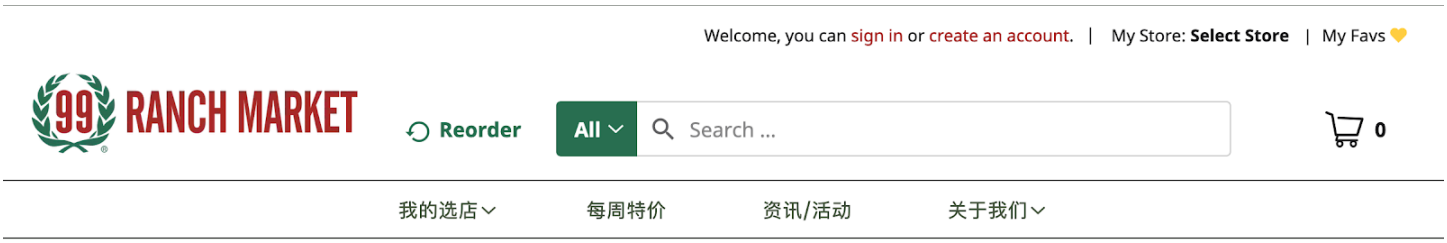
Pursuant to the California Consumer Privacy Act (CCPA)

Some of your data collected from this site is used to help create better, more personalized products and services and to send ads and offers tailored to your interests. Occasionally this is done with help from third parties. We understand if you'd rather us not share your information and respect your right to disable this sharing of your data with third parties for this browser, device, and property. If you turn this off, you will not receive personalized ads, but you will still receive ads. Note that any choice you make here will only affect this website on this browser and device.

## Appendix 3: Examples of English-only privacy policies for companies with large non-English speaking customer populations

### 99 Ranch Market (https://www.99ranch.com/zh-hans/privacy-policy), visited 10/26/20

Please note this site does not have a Do Not Sell link on the homepage; this page is accessed via the Privacy Policy link (also only in English), though the site offers an option to set the language to Chinese (simplified or traditional). In this example, the language was set to Chinese (simplified). Please note: this screenshot includes only the top portion of the webpage




## Privacy Policy

Tawa Supermarket, Inc. and our affiliates are committed to protecting your privacy. We recognize that privacy is an important issues for our customers and employees and we want to be transparent about how we collect, use, and disclose your personal information—this Privacy Notice provides you with notice of our processing activities and your rights under the law. Personal Information generally means any information that identifies you as an individual person, along with other information we associate with it. This includes information that is maintained by us in a manner that identifies you or your household. Personal information does not include publicly available information or information that is de-identified or aggregate consumer information.

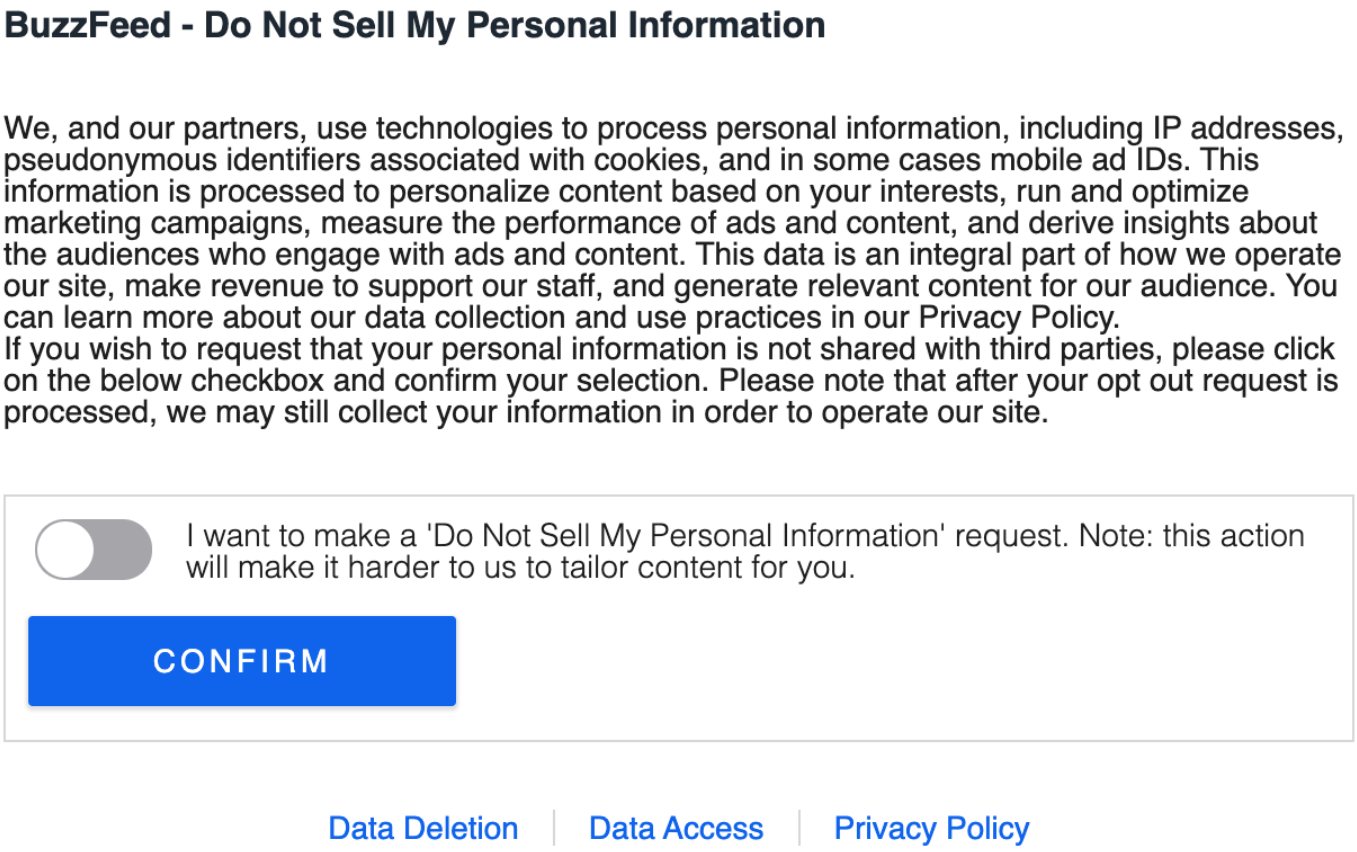
By using any of our websites and mobile applications in the United States (collectively, "Sites") or otherwise providing Personal Information to us, you agree to this Privacy Policy. This Privacy Notice is intended for individuals in the United States who are over the age of 16. If you live outside of the United States and choose to use the Sites connected with this Privacy Notice, you do so at your own risk and understand that your information will be sent to and stored in the United States.

**Application**

This Privacy Notice applies to Tawa Supermarket, Inc., Tawa Inc. (Retail), Tawa Services, Inc., Welcome Market, Inc., Welcome California Market, Inc., and Welcome Services, Inc.

**Appendix 4: Examples of websites using "guilt-shaming" or other coercive language in their DNS requests.**

**Example 1: Buzzfeed.com (visited 10.27/20)**
Please note the text on the opt-out button: "this action will make it harder to us [sic] to tailor content for you."



**Example 2: Forever 21 (https://www.forever21.com/us/shop/info/optout), visited 10/27/20**

Please note the language in this notice that attempts to minimize the effects of cookie tracking ("data contained in these Cookies does not typically identify you," warns the consumer that avoiding tailored ads "may not be what you want," and informs consumers that even after they exercise their rights, "we will still continue to share data with our service providers." Finally, the company uses this notice to argue with the definition of the term "sale" in the CCPA, attempting to delegitimize the regulation.


## Do Not Sell My Info

The CCPA gives California consumers the right to opt-out of the sale of their personal information ("PI").

The only way you can exercise this right as it relates to the use of cookies and other tracking technologies, is to click on the Do Not Sell My Information Toggle below from each browser and device you use.

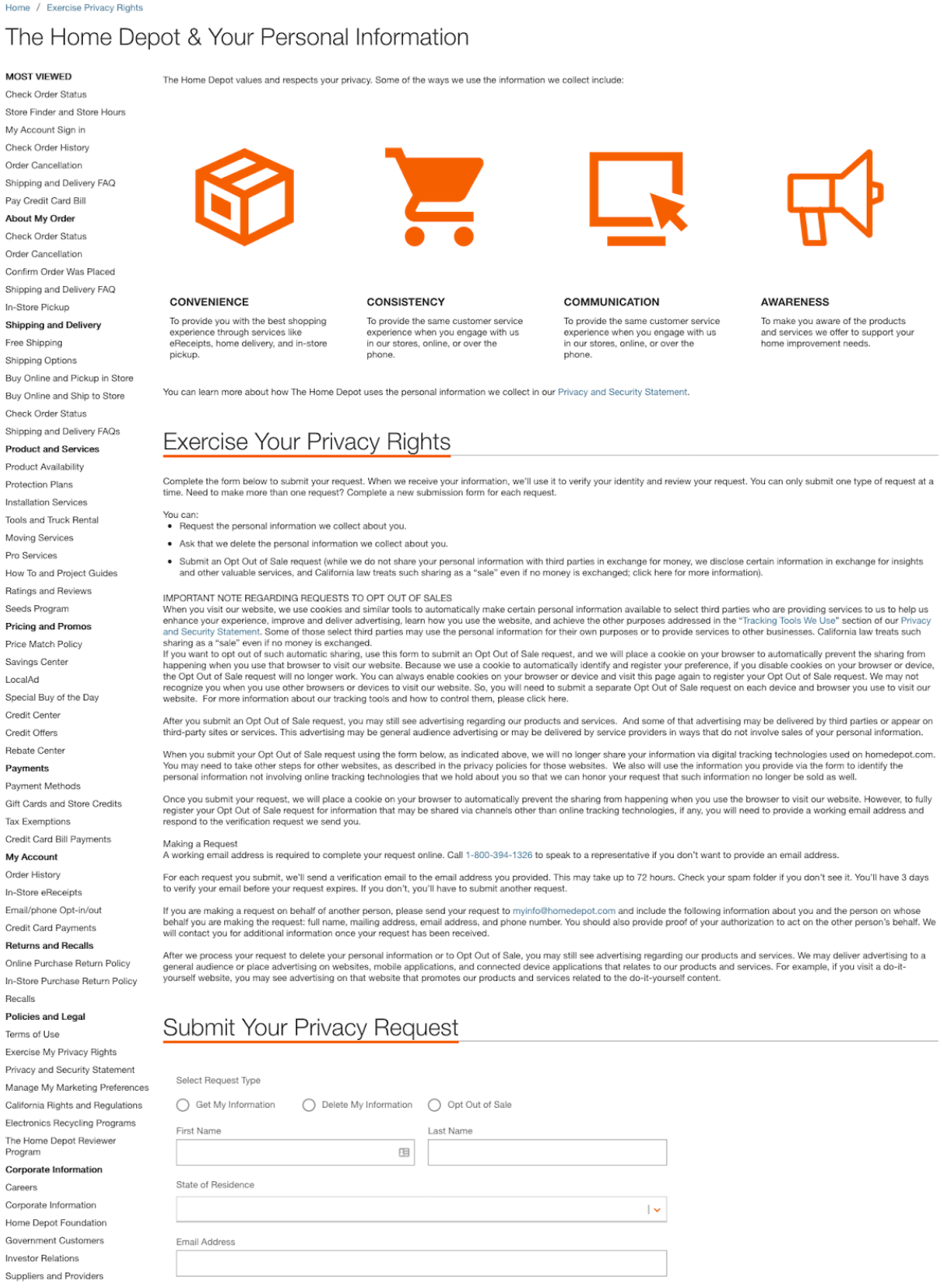
However, before you click on the Do Not Sell My Information Toggle below, we hope that you will consider a few more things:

- First, remember that the data contained in these Cookies does not typically identify you by name or other directly identifiable means.
- Second, opting-out of sales of your PI in the digital advertising context (i.e, by means of Cookies) will not stop you from getting ads, but these ads will not be tailored to your interests. This may not be what you want.
- Third, if you opt-out, your experience on our Sites and when you otherwise engage with us will be much less personalized.
- Fourth, even after you opt-out, we will still continue to share data with our service providers who use the data on our behalf.

The CCPA defines "sale" in an unusual way, and with no guidance yet from the State of California as to how broadly the term should be interpreted, a number of differing reasonable interpretations are possible.

Some may argue that when certain third parties place Cookies on the consumer's device when the consumer engages with our site or app, the PI collected by such Cookies constitutes a "sale" under the CCPA. We do not agree with this interpretation. However, pending a consensus as to what "sale" actually means under the CCPA, we are providing a way for California consumers to opt-out of future Cookie-based "sales" of their PI, by (i) enabling the Google Restricted Processing solution into our use of certain Google products, (ii) using the IAB Tech Lab "do not sell" signal with third parties that we work with and that are participating in the IAB CCPA Compliance Framework, and (iii) disabling other third parties' Cookies that are not covered by either (i) or (ii) above. The solutions referenced in (i) and (ii) each conveys to the recipient that PI can only be used for restricted purposes, such as providing us services, and cannot be sold by the recipient downstream. We make no guaranty as to how third parties will treat our Do Not Sell signals.

**Appendix 5: Example of opt-out form nested beneath excessive text**
**Home Depot (https://www.homedepot.com/privacy/Exercise_My_Rights), visited 10/27/20**
Please note: this screenshot includes only the top portion of the webpage



Home / Exercise Privacy Rights

# The Home Depot & Your Personal Information

**MOST VIEWED**
Check Order Status
Store Finder and Store Hours
My Account Sign in
Check Order History
Order Cancellation
Shipping and Delivery FAQ
Pay Credit Card Bill
**About My Order**
Check Order Status
Order Cancellation
Confirm Order Was Placed
Shipping and Delivery FAQ
In-Store Pickup
**Shipping and Delivery**
Free Shipping
Shipping Options
Buy Online and Pickup in Store
Buy Online and Ship to Store
Check Order Status
Shipping and Delivery FAQs
**Product and Services**
Product Availability
Protection Plans
Installation Services
Tools and Truck Rental
Moving Services
Pro Services
How To and Project Guides
Ratings and Reviews
Seeds Program
**Pricing and Promos**
Price Match Policy
Savings Center
LocalAd
Special Buy of the Day
Credit Center
Credit Offers
Rebate Center
**Payments**
Payment Methods
Gift Cards and Store Credits
Tax Exemptions
Credit Card Bill Payments
**My Account**
Order History
In-Store eReceipts
Email/phone Opt-in/out
Credit Card Payments
**Returns and Recalls**
Online Purchase Return Policy
In-Store Purchase Return Policy
Recalls
**Policies and Legal**
Terms of Use
Exercise My Privacy Rights
Privacy and Security Statement
Manage My Marketing Preferences
California Rights and Regulations
Electronics Recycling Programs
The Home Depot Reviewer Program
**Corporate Information**
Careers
Corporate Information
Home Depot Foundation
Government Customers
Investor Relations
Suppliers and Providers

The Home Depot values and respects your privacy. Some of the ways we use the information we collect include:

**CONVENIENCE**
To provide you with the best shopping experience through services like eReceipts, home delivery, and in-store pickup.

**CONSISTENCY**
To provide the same customer service experience when you engage with us in our stores, online, or over the phone.

**COMMUNICATION**
To provide the same customer service experience when you engage with us in our stores, online, or over the phone.

**AWARENESS**
To make you aware of the products and services we offer to support your home improvement needs.

You can learn more about how The Home Depot uses the personal information we collect in our Privacy and Security Statement.

## Exercise Your Privacy Rights

Complete the form below to submit your request. When we receive your information, we'll use it to verify your identity and review your request. You can only submit one type of request at a time. Need to make more than one request? Complete a new submission form for each request.

You can:
- Request the personal information we collect about you.
- Ask that we delete the personal information we collect about you.
- Submit an Opt Out of Sale request (while we do not share your personal information with third parties in exchange for money, we disclose certain information in exchange for insights and other valuable services, and California law treats such sharing as a "sale" even if no money is exchanged; click here for more information).

IMPORTANT NOTE REGARDING REQUESTS TO OPT OUT OF SALES
When you visit our website, we use cookies and similar tools to automatically make certain personal information available to select third parties who are providing services to us to help us enhance your experience, improve and deliver advertising, learn how you use the website, and achieve the other purposes addressed in the "Tracking Tools We Use" section of our Privacy and Security Statement. Some of those select third parties may use the personal information for their own purposes or to provide services to other businesses. California law treats such sharing as a "sale" even if no money is exchanged.
If you want to opt out of such automatic sharing, use this form to submit an Opt Out of Sale request, and we will place a cookie on your browser to automatically prevent the sharing from happening when you use that browser to visit our website. Because we use a cookie to automatically identify and register your preference, if you disable cookies on your browser or device, the Opt Out of Sale request will no longer work. You can always enable cookies on your browser or device and visit this page again to register your Opt Out of Sale request. We may not recognize you when you use other browsers or devices to visit our website. So, you will need to submit a separate Opt Out of Sale request on each device and browser you use to visit our website. For more information about our tracking tools and how to control them, please click here.

After you submit an Opt Out of Sale request, you may still see advertising regarding our products and services. And some of that advertising may be delivered by third parties or appear on third-party sites or services. This advertising may be general audience advertising or may be delivered by service providers in ways that do not involve sales of your personal information.

When you submit your Opt Out of Sale request using the form below, as indicated above, we will no longer share your information via digital tracking technologies used on homedepot.com. You may need to take other steps for other websites, as described in the privacy policies for those websites. We also will use the information you provide via the form to identify the personal information not involving online tracking technologies that we hold about you so that we can honor your request that such information no longer be sold as well.

Once you submit your request, we will place a cookie on your browser to automatically prevent the sharing from happening when you use the browser to visit our website. However, to fully register your Opt Out of Sale request for information that may be shared via channels other than online tracking technologies, if any, you will need to provide a working email address and respond to the verification request we send you.

Making a Request
A working email address is required to complete your request online. Call 1-800-394-1326 to speak to a representative if you don't want to provide an email address.

For each request you submit, we'll send a verification email to the email address you provided. This may take up to 72 hours. Check your spam folder if you don't see it. You'll have 3 days to verify your email before your request expires. If you don't, you'll have to submit another request.

If you are making a request on behalf of another person, please send your request to myinfo@homedepot.com and include the following information about you and the person on whose behalf you are making the request: full name, mailing address, email address, and phone number. You should also provide proof of your authorization to act on the other person's behalf. We will contact you for additional information once your request has been received.

After we process your request to delete your personal information or to Opt Out of Sale, you may still see advertising regarding our products and services. We may deliver advertising to a general audience or place advertising on websites, mobile applications, and connected device applications that relates to our products and services. For example, if you visit a do-it-yourself website, you may see advertising on that website that promotes our products and services related to the do-it-yourself content.

## Submit Your Privacy Request

Select Request Type
Get My Information  Delete My Information  Opt Out of Sale
First Name  Last Name
State of Residence
Email Address

## Appendix 6: Examples of instructions for opt-outs based on cookie tracking

Please note: the Buzzfeed, Los Angeles Times, Verizon Media, and Warner Media examples used in the earlier appendices are also examples of the confusing and multi-step processes consumers must follow to ensure that their DNS requests are respected by companies relying on third party tracking mechanisms. In the examples below, consumers are instructed that they will have to replicate the process for making their requests using every browser on every device they have used to access these websites.

### Example 1: Office Depot cookie example (visited 10/22/20)

IMPORTANT NOTE REGARDING REQUESTS TO OPT OUT OF SALES
When you visit our website, we use cookies and similar tools to automatically make certain personal information available to select third parties who are providing services to us to help us enhance your experience, improve and deliver advertising, learn how you use the website, and achieve the other purposes addressed in the "Tracking Tools We Use" section of our Privacy and Security Statement. Some of those select third parties may use the personal information for their own purposes or to provide services to other businesses. California law treats such sharing as a "sale" even if no money is exchanged.
If you want to opt out of such automatic sharing, use this form to submit an Opt Out of Sale request, and we will place a cookie on your browser to automatically prevent the sharing from happening when you use that browser to visit our website. Because we use a cookie to automatically identify and register your preference, if you disable cookies on your browser or device, the Opt Out of Sale request will no longer work. You can always enable cookies on your browser or device and visit this page again to register your Opt Out of Sale request. We may not recognize you when you use other browsers or devices to visit our website. So, you will need to submit a separate Opt Out of Sale request on each device and browser you use to visit our website. For more information about our tracking tools and how to control them, please click here.

### Example 2: Walmart cookie example (visited 10/22/20)

We respect the privacy of your personal information. The information you provide here will only be used to process your opt out of sale request. To assure the implementation of your request across all devices associated with your account, you should login to your account with each of your devices. If you are not logged in or do not provide accurate account details, you should complete an opt out of sale request on each browser or device that you use to access our websites and mobile services. In addition, if you are not logged into your account while making your request, and you later clear your Walmart cookies, your opt out of sale request will need to be resubmitted. Please note that your request will apply to future sales of your personal information and will not impact sales made prior to your request.