

Standardizing and Implementing Do Not Sell

Sebastian Zimmeck and Kuba Alicki

Department of Mathematics and Computer Science, Wesleyan University
{szimmeck,kalicki}@wesleyan.edu

Abstract

The California Consumer Privacy Act gives consumers the right to request that businesses do not sell their personal information. “Selling” is defined broadly and covers, among others, making personal information available to ad networks on websites via third party cookies. We began standardizing and implementing Do Not Sell technologies with the goal of integrating Do Not Sell directly into browser settings. Based on OptMeowt, our proof of concept Do Not Sell browser extension, we conduct experiments on the design, implementation, and current state of Do Not Sell. OptMeowt automatically places Do Not Sell cookies on visited sites and sends Do Not Sell headers per our draft standard. We believe that standardizing Do Not Sell provides an important building block for evolving the web towards increased privacy protections.

CCS Concepts: • Security and privacy → Privacy protections; Social aspects of security and privacy; Economics of security and privacy; • Information systems → Online advertising; • General and reference → Computing standards, RFCs and guidelines.

Keywords: Do Not Sell; Do Not Track; DNT; CCPA; CPRA; Privacy Rights; Web Privacy; Ad Tracking; Online Tracking

ACM Reference Format:

Sebastian Zimmeck and Kuba Alicki. 2020. Standardizing and Implementing Do Not Sell. In *19th Workshop on Privacy in the Electronic Society (WPES’20)*, November 9, 2020, Virtual Event, USA. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3411497.3420224>

1 Introduction

Many websites are collecting sensitive data and lawmakers are increasingly responding to the challenge. A crucially important moment was the enactment of the General Data Protection Regulation (GDPR) in 2018. Since then, new privacy laws have been emerging stateside as well. The California

Consumer Privacy Act (CCPA) [5], enforceable since July 1, 2020, introduced new privacy rights to California consumers, most notably the right to direct a business to not sell consumers’ personal information, CCPA §1798.120(a). Some companies have already declared that they will honor Do Not Sell requests for consumers from any state in the US [15]. Similar to the CCPA, Nevada SB 220 §2 also requires the honoring of user requests for opting out of the sale of personal information. Further bills are underway in many other states including Hawaii, Maryland, Massachusetts, and New York. Do Not Sell has gained momentum beyond California. Per CCPA §1798.140(t) “selling” is defined broadly and covers, among others, making users’ personal information available to ad networks on websites via third party cookies.

In a potentially transformative provision, the CCPA Regulations (CCPA Regs) require businesses to treat “user-enabled global privacy controls, such as a browser plugin 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,” CCPA Regs §999.315(c) [4]. Given the ease and frequency with which personal information is collected and sold when a consumer visits a website, consumers should have a similarly easy ability to request to opt out globally [2]. The regulation is intended to spur innovation in privacy services that facilitate the exercise of consumer rights [2]. Against the background of evolving privacy laws we see the opportunity to write a new chapter in the development of the web towards meaningful privacy standards and their implementations.

2 Background and Related Work

Do Not Sell is substantially informed by Do Not Track (DNT).

2.1 Do Not Track: The Road to Do Not Sell

DNT was standardized by the W3C Tracking Protection Working Group [25]. The setting provided a convenient way for users to signal their opt out choice from tracking via a dedicated DNT HTTP header. However, at this point only few browser vendors continue to support DNT. Per §22575(5) of the California Online Privacy Protection Act (CalOPPA), which is the basis for DNT, recipients of a DNT signal only have to say whether they respect it, but they do not need *actually* respect it. The reliance on the industry’s self-regulation proved illusive. Nowadays, most companies simply state in their privacy policy that they will not honor DNT requests. However, the situation is different now for Do Not Sell signals, which must be respected, CCPA Regs §999.315(c).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
WPES’20, November 9, 2020, Virtual Event, USA

© 2020 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 978-1-4503-8086-7/20/11...\$15.00

<https://doi.org/10.1145/3411497.3420224>

2.2 The Current State of Do Not Sell

The currently most used Do Not Sell specification is the Interactive Advertising Bureau's (IAB) US Privacy String; while generally technology-neutral, it is recommended to be implemented in a first party cookie [12]. Another self-regulatory effort is the third party cookie-based solution for ad networks participating in the Digital Advertising Alliance's (DAA) CCPA Opt Out Tool for the Web [7]. While the IAB approach is intended for publishers, the DAA Tool is intended for ad networks. However, cookie-based solutions are not ideal as opt out cookies are easily deleted and major browser vendors will phase out third party cookies [20].

2.3 Privacy Rights Beyond Do Not Sell

Per the CCPA consumers also have rights beyond Do Not Sell: the rights to know (i.e., access to) and delete personal information as well as the right to not be discriminated against for requesting any rights. The rights of the CCPA are similar to those of the GDPR [1]. Designing tools for data access rights is an ongoing effort [23, 24]. The difference between Do Not Sell on one side and access and deletion rights on the other is that the former does not require user verification. Giving a user access to personal information of another user or deleting someone else's personal information can be a problem. Thus, those rights are harder to automate compared to Do Not Sell, which can be based on headers, the DOM, APIs, or cookies that mediate a user's behavior through a browser or other user agent.

2.4 The Emerging Privacy Tech Industry

The CCPA, GDPR, and other new privacy laws have given rise to the privacy tech industry [9, 16, 21] addressing businesses' needs for managing data in compliance with legal requirements [30]. In order to achieve compliance for data transfer requests, major tech companies started the Data Transfer Project (DTP) with the goal of connecting any two participating services for the purpose of transferring data upon a user's request from one service to another [8]. Various academic work on compliance analysis seeks, among others, to identify software implementations that are contradictory to privacy laws, e.g., by identifying discrepancies between privacy practices described (or omitted) in privacy policies and actual code functionality [18, 28, 29, 31, 32].

3 Requirements for a Do Not Sell Standard

We began working towards Do Not Sell standardization in the W3C Privacy Community Group [26, 27]. We intend to establish Do Not Sell as a W3C standard enabling browser vendors, some of which already indicated interest [22], to include Do Not Sell settings directly in their browsers. Currently, we are working with a core group of representatives from browser vendors, publishers, privacy organizations, and other stakeholders to flesh out the details based on the following requirements.

3.1 Do Not Sell Requests via Global Privacy Controls

In order for consumers to make Do Not Sell choices, a business must provide consumers with at least two methods, one of which can be a user-enabled global privacy control, such as a browser plugin or privacy settings, that communicates or signals Do Not Sell requests, CCPA Regs §999.315(a) [3]. Independently of which methods a business adopts, if that business collects personal information from consumers online, it must treat communications or signals from privacy controls as valid requests, CCPA Regs §999.315(c). This obligation is the result of the California Attorney General's experience with DNT signals, which businesses do not need to comply with and which, consequently, are usually not honored [2]. Privacy controls must be designed to clearly communicate or signal that a consumer intends to opt out of the sale of personal information, CCPA Regs §999.315(c)(1) [2]. Affirmatively choosing products or services with privacy-protective features, in particular, opting out by default, is considered a sufficiently clear manifestation of opting out and additional steps are not necessary for the privacy control design [3].

3.2 Do Not Sell Requests via DNT Signals

The CCPA Regs do not prohibit the use of, should a business choose to do so, the DNT signal as a proxy for communicating a consumer's privacy choice to businesses and third parties [3]. Indeed, with regards to website tracking, DNT represents a superset of what is covered by Do Not Sell, which, for example, may not cover collecting personal information for analytics or telemetry purposes. The New York Times is currently taking this approach and interprets DNT signals as Do Not Sell signals [19].

3.3 Do Not Sell Requests via Authorized Agents

Per CCPA Regs §999.315(f) a consumer may authorize an agent via written permission to submit a Do Not Sell request on their behalf. The use of privacy controls is considered a request directly from the consumer. Thus, opting out via an authorized agent supplements privacy control opt outs, in particular, on sites that identify users based on a login and do not exclusively use cookies or other browser technologies to keep track of users' opt out state. Consumer Reports is currently engaged in building tools for opting out via authorized agents.

3.4 Selective Do Not Sell Requests and Exceptions

In responding to a Do Not Sell request, a business may present the consumer with the choice to opt out for certain sales of personal information as long as a global option to opt out is more prominently presented than the other choices, CCPA Regs §999.315(d) [3]. In order to implement such selectivity into global privacy controls it is important to ensure their usability. As privacy controls work across sites, the idea of selective opt outs can be extended to exclude certain sites that

should not receive Do Not Sell signals, for example, because a consumer wants to support those sites.

3.5 Unverified and Fraudulent Do Not Sell Requests

While requests to know and delete must be verified, Do Not Sell requests require no verification, CCPA Regs §999.315(g). In fact, verification would be a barrier and, thus, contradict the CCPA's goal of empowering consumers to exercise their Do Not Sell rights [2, 3]. Businesses may offer a verification-based method as one opt out option, though, it does not absolve them from their obligation to honor global privacy controls [2]. If a business has a good-faith, reasonable, and documented belief that a request is fraudulent, it can reject the request and must inform the requester accordingly, providing an explanation why it believes the request is fraudulent [3]. In particular, "fraudulent" requests cover requests that are not from the consumer or the consumer's agent [3]. Though, such requests will hardly be relevant for global privacy controls.

3.6 Conflicting Consumer Choices

If a global privacy control conflicts with a consumer's existing business-specific privacy setting or participation in a business's financial incentive program, the business shall respect the privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the program, CCPA Regs §999.315(c)(2).

3.7 Responding to Do Not Sell Requests

Principally, upon receiving a Do Not Sell request a business can respond by (1) acknowledging its receipt, (2) confirming the opt out, (3) rejecting it, (4) or responding that the right is not applicable. The right to opt out from sales is only applicable if the business actually sells consumers' personal information [3]. It is also not applicable to a consumer who is not a California resident. Using the IP address of the requesting device to determine the location of the requester may serve as a proxy for residency, however, may miss edge cases, such as California residents temporarily outside of California. If a business believes that a request is fraudulent, it may reject it and must inform the requester with an explanation why it has such belief, CCPA Regs §999.315(g). The explanation can be a high-level summary if not given in bad-faith [3].

3.8 Businesses' Compliance and Third Party Notices

Per CCPA Regs §999.315(e) a business must comply with a Do Not Sell request within 15 business days from the date of receipt. If it sells personal information after having received the request but before complying with it, the business shall notify the recipients that the consumer has opted out and direct them not to sell that consumer's personal information. Businesses have to respect a consumer's opt out for at least 12 months before requesting from the consumer to authorize the sale of personal information again, CCPA §1798.135(a)(5).

3.9 Opting Back In

Requests to opt back in after opting out must use a two-step process whereby consumers (1) clearly request to opt in and (2) separately confirm their choice, CCPA Regs §999.316(a). If consumers who have opted out initiate transactions or attempts to use a product or service that requires the sale of their personal information, a business may inform them that the transaction, product, or service requires the sale of their personal information and provide instructions on how to opt in, CCPA Regs §999.316(b).

4 The CPRA's Potential Impact

The CCPA may possibly be extended by the current lawmaking effort on the California Privacy Rights Act (CPRA) [14]. Most notably, in its current form, the CPRA provides for regulations to define the requirements and technical specifications for an opt out preference signal. It also would introduce additional categories of protected personal information, including sensitive personal information, and consumers could direct businesses to limit the use of such. The CPRA would enable consumers to only limit the use of sensitive personal information instead of prohibiting it completely. It would further allow consumers to make Do Not Share and Do Not Share My Personal Information for Cross-Context Behavioral Advertising requests. These extensions of the CCPA by the CPRA are intended to give consumers more and finer control over their personal information.

5 Implementing Do Not Sell

We are pursuing two types of Do Not Sell implementations: (1) browser extensions and (2) in-browser settings. We started implementing global privacy controls via our open source OptMeowt ("opt me out") browser extension, available for Google Chrome and other Chromium-based desktop browsers [17].

5.1 Sending Do Not Sell Signals

The CCPA is technology-neutral as to how Do Not Sell signals should be sent. OptMeowt is a proof of concept browser extension for experimenting with different methods and informing the design of the Do Not Sell standard for in-browser implementations. OptMeowt is sending Do Not Sell signals using five methods.

1. A new HTTP Do Not Sell header that we are developing in a standardization effort [27]
2. The existing DNT header [25], which is interpreted by some publishers as a Do Not Sell header
3. The IAB's US Privacy String, implemented in a first party cookie [11]
4. Third party cookies of ad networks participating in the DAA's CCPA Opt Out Tool for the Web [7]
5. Custom headers and cookies used by individual websites maintained and updated in a Do Not Sell list

OptMeowt combines all methods in one comprehensive Do Not Sell extension. Figure A.2 in the Appendix shows screenshots. For cookie-based Do Not Sell signals OptMeowt will place or rewrite opt out cookies. For example, `evite.com` implements a first party `usprivacy` cookie whose value will be rewritten to Do Not Sell by OptMeowt upon the user visiting that site. Companies participating in the DAA program are ad networks whose sites users generally do not intentionally visit. Thus, upon installing it, OptMeowt will visit, in the background, all participating sites and place Do Not Sell cookies in the browser storage of the respective domains. OptMeowt will also send a Do Not Sell request via a Do Not Sell header that we are developing towards a standard [27]. All header- and cookie-based opt outs are valid per domain, i.e., users opt out from domains and not sub-domains. We are currently working with a handful of organizations and would like to extend the working group over time to obtain a critical mass to create a standard that all stakeholders can agree to.

5.2 Experimental Results

We tested sending cookie- and header-based Do Not Sell signals with OptMeowt, in particular, to evaluate the placement of Do Not Sell cookies to be recognized by the IAB and DAA.

IAB US Privacy String First Party Cookies. As OptMeowt allows users to opt out of the sale of personal information by setting a site’s IAB US Privacy String value in a `usprivacy` first party cookie to Do Not Sell, we tested this functionality on a set of 50 randomly selected sites that support such implementation. We searched Cookiepedia [6] for sites with `usprivacy` or `us_privacy` cookies.¹ After preliminary experimentation with 20 of the 50 sites, we used the remaining 30 sites for our test of OptMeowt. Using a browser with cleared data and OptMeowt disabled we loaded each site and observed that a `usprivacy` or `us_privacy` cookie was set. Then, we reloaded the site with OptMeowt enabled and observed whether it reset the cookie value to Do Not Sell. We reloaded the site multiple times to ensure that the Do Not Sell value persisted and that the cookie was not replaced by the site. 17 of the 30 sites accepted Do Not Sell requests from outside of California within the US, which is where we are located. For all those 17 sites OptMeowt was able to rewrite the cookie with a Do Not Sell value. The remaining 13 sites did not allow such rewrite as they did not accept Do Not Sell signals from outside California.

DAA Third Party Cookies. The DAA’s Opt Out Tool for the Web [7] is a web-based list of ad networks from which users can select all or individual networks that should not sell their personal information. The DAA Tool works by placing third party cookies in users’ browsers that indicate users’ preferences for not selling their personal information. The cookies

¹We found various sites deviating from the IAB’s recommended naming convention of the `usprivacy` cookie [12]. For example, `ask.com` makes use of the US Privacy String in a `us_privacy` cookie and so does `washingtonpost.com/` in a `wp_usp` cookie.

do not follow a particular format but rather each ad network can use whichever cookie names, values, and parameters they prefer. Upon its first run after installation, OptMeowt will iterate over its list of ad networks and place their respective Do Not Sell third party cookies in the browser (Appendix Table 1). We identified the opt out cookies by using a browser with data cleared and observing for each individual ad network which cookies were placed in the browser upon opting out using the DAA Tool. We assumed that a cookie is an opt out cookie if its name or value is indicative for such behavior. OptMeowt is able to write an opt out cookie just in the same way as it would have been written by the DAA Tool. For 57 out of the 62 ad networks the opt out cookies were placed successfully. For 5 ad networks the DAA Tool did not place the corresponding opt out cookies successfully making it impossible for OptMeowt to do so either. OptMeowt does not place any cookies with user or browser identifiers, which, however, should not preclude the opt out as the CCPA does not require any verification.

We are encouraged by these results as they demonstrate the viability of signaling Do Not Sell requests simply by visiting a website or running a batch opt out process. We see this functionality as an intermediate step in our overarching goal to standardize Do Not Sell as a browser setting.

6 Concluding Remarks and Future Work

New privacy legislation provides an opportunity to standardize Do Not Sell and evolve the web towards increased privacy protection. Privacy protection should be as easy as data collection. We believe that having a standard for Do Not Sell would make the implementation of this right more effective for users and also lead to wider industry adoption. Privacy, just as security, is a secondary goal for most users. Thus, usability plays a crucial role for enabling users to express their privacy choices efficiently and as intended by the law. To that end, we will perform usability studies, e.g., on default browser settings and how complex opt out scenarios can be handled. We are also in the process of generalizing the Do Not Sell paradigm to associate Do Not Sell signals with different legal bindings, for example, depending on where or in which context it was sent or where and by whom it was received. As much of users’ online interactions today happen via mobile apps, we are interested in exploring the potential of Do Not Sell in the mobile ecosystem as well. We envision the CCPA’s Do Not Sell right to be the first of many new privacy rights to be standardized and hope that it may serve as a blueprint for future standardization efforts of those.

Acknowledgments

We thank Ashkan Soltani for a peek into the lawmaking process of the CCPA and CPRA. We are also grateful for the funding from Wesleyan University, its Department of Mathematics and Computer Science, and the Anil Fernando Endowment.

References

- [1] Coline Boniface, Imane Fouad, Nataliia Bielova, Cédric Lauradoux, and Cristiana Santos. 2019. Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data. <https://hal.inria.fr/hal-02072302/document>. In *APF '19*. Springer, Rome, Italy, 1–20. Accessed: September 13, 2020.
- [2] California Department of Justice. 2020. California Consumer Privacy Act Final Statement of Reasons. <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf>. Accessed: September 13, 2020.
- [3] California Department of Justice. 2020. California Consumer Privacy Act Final Statement of Reasons, Appendix A: Summary and Response to Comments Submitted During 45-day Period. <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf>. Accessed: September 13, 2020.
- [4] California Department of Justice. 2020. California Consumer Privacy Act Final Text of Regulations. <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf>. Accessed: September 13, 2020.
- [5] California State Legislature. 2020. California Consumer Privacy Act of 2018. https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Accessed: September 13, 2020.
- [6] Cookiepedia. 2020. Cookiepedia. <https://cookiepedia.co.uk/>. Accessed: September 13, 2020.
- [7] DAA. 2020. DAA CCPA Opt Out Tool for the Web. https://digitaladvertisingalliance.org/DAA_style/ADS/CCPA_Opt_Out_Tool_Technical_Description.pdf. Accessed: September 13, 2020.
- [8] Data Transfer Project. 2020. <https://datatransferproject.dev/>. Accessed: September 13, 2020.
- [9] Didomi. 2020. <https://www.didomi.io/en/>. Accessed: September 13, 2020.
- [10] EasyList filter list project. 2020. EasyList. <https://easylist.to/>. Accessed: September 13, 2020.
- [11] IAB. 2020. IAB CCPA Compliance Framework for Publishers & Technology Companies. <https://www.iab.com/guidelines/ccpa-framework/>. Accessed: September 13, 2020.
- [12] IAB. 2020. US Privacy User Signal Mechanism “USP API”. <https://github.com/InteractiveAdvertisingBureau/USPrivacy/blob/master/CCPA/USP%20API.md>. Accessed: September 13, 2020.
- [13] IETF. 2019. Well-Known Uniform Resource Identifiers (URIs). <https://tools.ietf.org/html/rfc8615>. Accessed: September 13, 2020.
- [14] Alastair Mactaggart. 2019. The California Privacy Rights Act of 2020 Amendments to Version 3. https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf. Accessed: September 13, 2020.
- [15] Microsoft. 2019. Microsoft will honor California’s new privacy rights throughout the United States. <https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/>. Accessed: September 13, 2020.
- [16] OneTrust. 2020. <https://www.onetrust.com/>. Accessed: September 13, 2020.
- [17] privacy-tech-lab. 2020. OptMeowt. <https://github.com/privacy-tech-lab/optmeowt-browser-extension>. Accessed: September 13, 2020.
- [18] R. Slavin, X. Wang, M.B. Hosseini, W. Hester, R. Krishnan, J. Bhatia, T.D. Breaux, and J. Niu. 2016. Toward a Framework for Detecting Privacy Policy Violation in Android Application Code. <https://ieeexplore.ieee.org/document/7886889>. In *ICSE '16*. ACM, Austin, Texas, USA, 25–36. Accessed: September 13, 2020.
- [19] The New York Times Company. 2020. California Notice. <https://www.nytimes.com/privacy/california-notice>. Accessed: September 13, 2020.
- [20] The Verge. 2020. Google to ‘phase out’ third-party cookies in Chrome, but not for two years. <https://www.theverge.com/2020/1/14/21064698/google-third-party-cookies-chrome-two-years-privacy-safari-firefox>. Accessed: September 13, 2020.
- [21] TrustArc. 2020. <https://www.trustarc.com/products/privacy-platform/>. Accessed: September 13, 2020.
- [22] United States Senate Committee on the Judiciary. 2020. Testimony of Alastair Mactaggart, United States Senate Committee on the Judiciary. <https://www.judiciary.senate.gov/imo/media/doc/Mactaggart%20Testimony1.pdf>. Accessed: September 13, 2020.
- [23] Tobias Urban, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. 2019. “Your Hashed IP Address: Ubuntu.”: Perspectives on Transparency Tools for Online Advertising. <https://dl.acm.org/doi/10.1145/3359789.3359798>. In *ACSAC '19*. ACM, New York, NY, USA, 702–717. Accessed: September 13, 2020.
- [24] Sophie Veys, Madison Stamos, Nathan Reiting, Michelle L. Mazurek, and Blase Ur. 2020. Designing Visualization and Exploration Tools for Data Access Under GDPR/CCPA. <https://www.ieee-security.org/TC/SPW2020/ConPro/papers/veys-conpro20-talk.pdf>. In *ConPro '20*. IEEE, Virtual Event, 1–2. Accessed: September 13, 2020.
- [25] W3C. 2020. Do Not Track. <https://www.w3.org/2011/tracking-protection/>. Accessed: September 13, 2020.
- [26] W3C Privacy Community Group. 2020. Standardizing Do Not Sell Email Thread. https://www.w3.org/Search/Mail/Public/search?keywords=CCPA+Do-Not-Sell&hdr-1-name=subject&hdr-1-query=&index-grp=Public_FULL&index-type=t&type-index=public-privacycg. Accessed: September 13, 2020.
- [27] W3C Privacy Community Group. 2020. Standardizing Do Not Sell GitHub Issue. <https://github.com/privacycg/proposals/issues/10>. Accessed: September 13, 2020.
- [28] Xiaoyin Wang, Xue Qin, Mitra Bokaei Hosseini, Rocky Slavin, Travis D. Breaux, and Jianwei Niu. 2017. GUILeak: Identifying Privacy Practices on GUI-Based Data. <https://pdfs.semanticscholar.org/ced1/313acaacd3897b5b231cdccb1383d01d20c4.pdf>. Accessed: September 13, 2020.
- [29] Takuya Watanabe, Mitsuki Akiyama, Tetsuya Sakai, and Tatsuya Mori. 2015. Understanding the Inconsistencies between Text Descriptions and the Use of Privacy-sensitive Resources of Mobile Apps. <https://www.usenix.org/system/files/conference/soups2015/soups15-paper-watanabe.pdf>. In *SOUPS '15*. USENIX Assoc., Ottawa, Canada, 241–255. Accessed: September 13, 2020.
- [30] Sebastian Zimmeck. 2013. The Information Privacy Law of Web Applications and Cloud Computing. <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1564&context=chtlj>. *Santa Clara Computer & High Tech. L.J.* 29, 3 (2013), 451–487. Accessed: September 13, 2020.
- [31] Sebastian Zimmeck, Peter Story, Abhilasha Ravichander, Daniel Smullen, Ziqi Wang, Joel Reidenberg, N. Cameron Russell, and Norman Sadeh. 2019. MAPS: Scaling Privacy Compliance Analysis to a Million Apps. <https://petsymposium.org/2019/files/papers/issue3/popets-2019-0037.pdf>. In *PETS '19*, Vol. 3. Scienc, Stockholm, Sweden, 66–86. Accessed: September 13, 2020.
- [32] Sebastian Zimmeck, Ziqi Wang, Lieyong Zou, Roger Iyengar, Bin Liu, Florian Schaub, Shormir Wilson, Norman Sadeh, Steven M. Bellovin, and Joel Reidenberg. 2017. Automated Analysis of Privacy Requirements for Mobile Apps. https://www.ndss-symposium.org/wp-content/uploads/2017/09/ndss2017_05A-5_Zimmeck_paper.pdf. In *NDSS '17*. Internet Society, San Diego, CA, 1–15. Accessed: September 13, 2020.

A Appendix

A.1 DAA CCPA Opt Out Tool for the Web Cookies

Participating ad networks in the DAA’s Opt Out Tool for the Web [7] make use of custom opt out cookies. The used

cookie values and names, listed in Table 1, do not follow a particular format. Not included in our list are any cookies associated with domains of the DAA Tool itself, in particular, the `optout.privacyrights.info` cookies as well as the `integrate.privacyrightscookietest.com` cookies. In our experiments with the DAA Tool (§ 5.2) we observed that some cookies placed during the opt out process contained automatically generated tokens or IDs that could potentially track a particular user or browser. We did not include such cookies in our list. Do Not Sell requests do not require verification, CCPA Regs §999.315(g), and as such it should be sufficient under the law to place a cookie with a Do Not Sell value to opt out from the sale of personal information. There is no need for a user or browser identifier. Some ad networks place cookies under multiple domains possibly to ensure a complete opt out from all their different ad servers. Maintenance of the list in OptMeowt is done manually. The list can be updated similar to ad blocking lists such as EasyList [10]. Ultimately cookie-based Do Not Sell opt outs — whether based on first or third party cookies — are disadvantageous from a user’s perspective as they only work for browsers and on a per-browser basis. Also, if a user accidentally deletes an opt out cookie, e.g., by clearing browser data, they have to opt out again. Thus, we see cookie-based opt outs only as a temporary measure that we hope to replace with more stable and usable measures that are header-, DOM-, or API-based.

Ad Network	Do Not Sell Cookie Name(s)
33Across	33x_nc, tyntOptOut
4Info	optout
AddThis	N/A*
Adelphic	cu
Amobee	optOut, 00, opt-out
Apollo Program	aid
Audiencerate	OPT-OUT
AuDigent	au_adgt_optout
Beeswax	bto
Catalina BuyerVision	aa
Choozle	N/A*
Clicksco	ccoptout
Cognitiv	daa_opt_out
Connexity	oo, ad_retarget_opt_out
Criteo	optout, oo
Cross Pixel	uid, uuid, OPTOUT
Datonics	optout
Dstillery	orbptout
EMX	opt-out*



Ad Network	Do Not Sell Cookie Name(s)
Eyeota	mako_uid
Flashtalking	flashtalkingad1
Havas Edge	ccpa_optout
IHS Markit Digital	u, ub
Index Exchange	CMO
iPromote	optout
IQM.com	iqm.priba.optout
LiveIntent	tuuid
Lotame	_cc_cc
Merkle	opt-out, opt-out-type
mPlatform	optouts
Nativo	opt_out
Neustar/Aggregate Knowledge	aa
Oath Inc	optout, OptOut, JEB2, ACID, atdses
OpenX	OX_dnt
Oracle Data Cloud	N/A*
Outbrain	opout, zoptout
OwnerIQ	optout
Parrable	_ccpa_optout
PebblePost	ppid
Pulpo	_PM_OPTOUT
PulsePoint	CWOptOutCookie
Qualia	daa-opt-out
Resonate	R00C
Retargetly	_rlopt, out
Rubicon Project	trp_optout
Samba.TV	samba_dnt
ScorecardResearch	NO_COOKIE
Semasio	N/A*
ShareThis	st_optout
Simplifi	opted_out, opted_out_legacy
Skimlinks	OPTOUT
Sovrn	tracking_optout
SteelHouse	opt_out
Swoop	swoop-nai-optout
Tapad	ID, TapAd_DID, TapAd_TS
TaskRabbit	ads_opt_out
The Trade Desk	TTDOptOutOfDataSale
Throtle	optout
Unruly Group	ccpa_optout
VDX.tv	ANON_ID, ANON_ID_old
Weborama	optout
Yieldmo	OPTOUT

* The DAA Tool failed to place Do Not Sell cookies.

Table 1. The set of ad networks participating in the DAA’s Opt Out Tool for the Web [7] as of August 4, 2020 and the names of their Do Not Sell cookies. Our OptMeowt browser extension places these cookies automatically and opts out users from the sale of personal information.

A.2 OptMeowt Screenshots

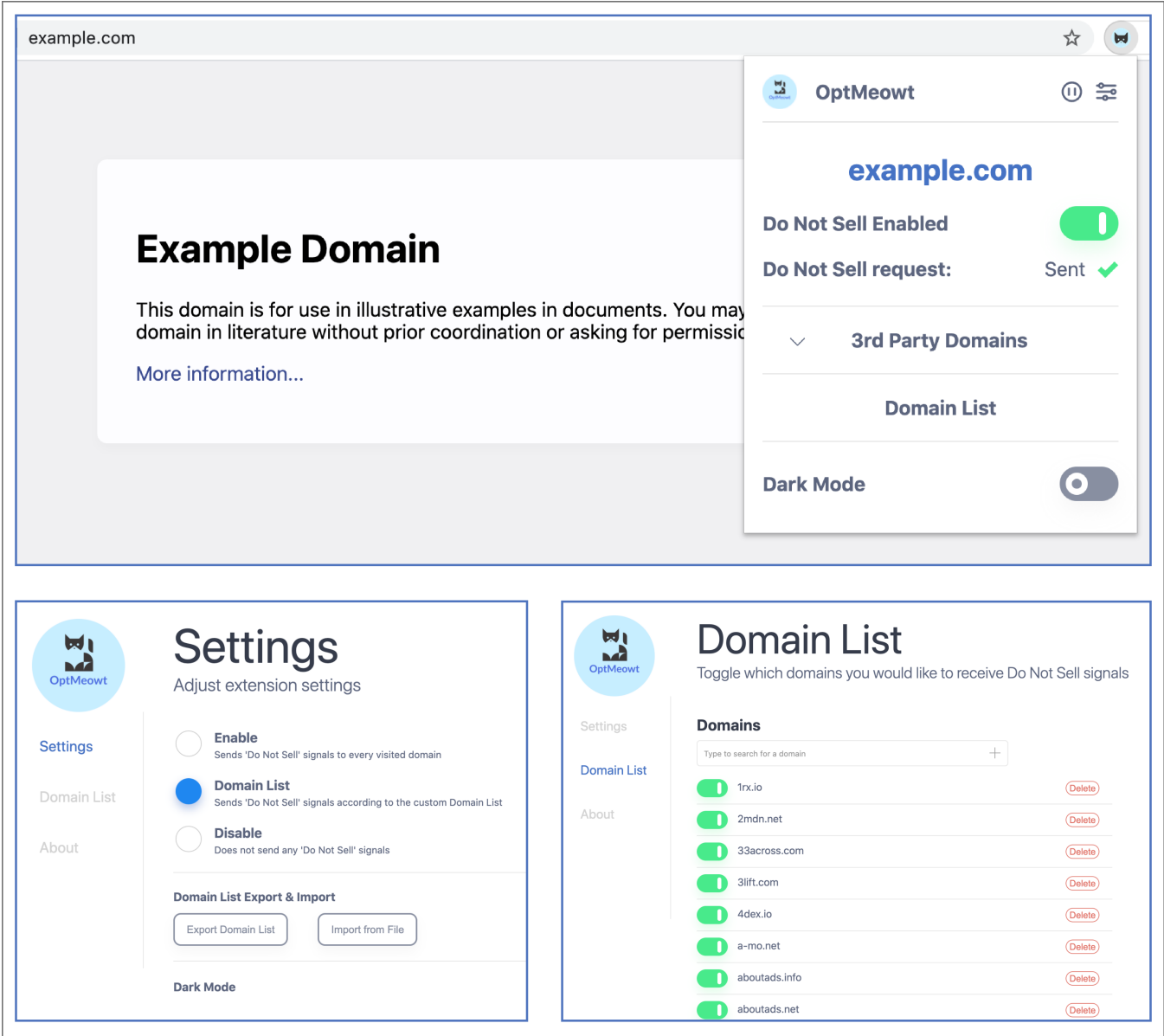


Figure 1. Screenshots of our OptMeowt browser extension for sending Do Not Sell signals to websites. OptMeowt’s code is publicly available under an open source license [17]. The response functionality for sending responses from the sites back to the users is currently in development. One option is to send responses via headers. Another option is the use of .well-known URIs [13]. Such URIs allow sites to store information, such as how they respond to Do Not Sell requests, in predefined locations that can be retrieved by browser extensions or browsers. Responses can be complex to handle as they need to cover various edge cases, for example, conflicting consumer choices (§ 3.6).