The State of CCPA Compliance Regarding GPC is More Complicated Than You Thought

MICHAEL R. SNEBERGER, KRUTIK MANISH PANDYA, and NITEEQ SHEIK, Arizona State University, Ira A. Fulton School of Engineering, School of Computing and Augmented Intelligence

This project entails a detailed study of California Consumer Privacy Act's (CCPA) requirement that covered businesses provide a "do not sell of share my personal information" (DNS) function to website visitors, specifically evaluating if websites have detected and acted upon the Global Privacy Control (GPC) signal and treated it as a DNS request as required by CCPA. The paper includes, understanding CCPA compliance, Learning about the GPC signal, Identifying websites, developing detection methods, collection of data, analyzing compliance, and document findings.

ACM Reference Format:

Michael R. Sneberger, Krutik Manish Pandya, and Niteeq Sheik. 2023. The State of CCPA Compliance Regarding GPC is More Complicated Than You Thought.

1 INTRODUCTION

Legal requirements mandating measures to protect the privacy and security of personal data/information are now integral components of the digital age. With the introduction of comprehensive data privacy regimes in Europe and California, website operators may be required to adhere to specific regulations related to managing the flow and safeguarding of visitor data. Non-compliance with these regulations can result in severe penalties. Therefore, checking the state of compliance can be highly beneficial to organizations subject to these rules and regulatory bodies enforcing these rules.

While the European Union's General Data Protection Regulation (GDPR) and its companion ePrivacy Directive[1] set up an opt-in regime for websites that avail themselves to the European Union, the California Consumer Privacy Act (CCPA) provides an opt-out regime for residents of California when a website operator is subject to CCPA. What that means is that when visiting GDPR-covered websites, visitors must positively opt in (by way of the "cookie banners" that are seen on many websites) to scripts that automate the exfiltration of their personal data to third parties, whereas residents of California who wish to block automated sharing of their personal information (PI) by websites must positively opt out by way of clicking a DNS button or link on the website or by "allowing consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal."[2]

[1] Soon to be replaced by the Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) or ePrivacy Regulation.

[2] Cal. Code Regs. tit. 11 § 7026(a)(1). While the following states have now enacted privacy laws that require residents be provided with an option to opt out of the sale of their PI, so far only California has made it clear that this includes recognizing the GPC signal sent by web browsers: Colorado; Connecticut; Indiana; Iowa; Montana; Oregon; Tennessee; Texas; Utah; and Virginia. The following states have bills actively moving through the lawmaking process that would require residents to be given a chance to opt out of the sale of their PI: Delaware, Massachusetts, North Carolina, and Pennsylvania.

Authors' address: Michael R. Sneberger, msneberg@asu.edu; Krutik Manish Pandya, kpandya8@asu.edu; Niteeq Sheik, nsheik1@asu.edu

The voters of the State of California[3], the California Legislature, and the agencies enforcing the terms of CCPA - formerly the Office of the Attorney General of the State of California and now the California Privacy Protection Agency (CPPA) - have made it clear through statute,[4] regulations,[5] and enforcement,[6] that when they say websites subject to CCPA must recognize an "opt-out preference signal," they mean the Global Privacy Control (GPC) signal. Therefore, websites whose operators are subject to CCPA must cause their website to recognize the GPC signal and, when the signal is received, effectively invoke the site's DNS function and take actions to stop any sale or share of a visitor's PI to third parties from the website via automated means.

It appears the primary way for a website to memorialize a website visitor's preference regarding the sale or share of their PI with third parties is the OptanonConsent first-party cookie.[7] An alternative method of memorializing a website visitor's wish to opt out of the sale of share of their data is the Interactive Advertising Bureau IAB Tech Lab's US Privacy String.[8] In this paper we survey the state of GPC compliance as commanded by CCPA by either the OptanonConsent cookie or the US Privacy String on the eve of the deprecation of the US Privacy String in 2024.

2 HYPOTHESIS

Current compliance strategies used by websites subject to CCPA are not fully effective: either by:

- not recognizing the GPC signal at all, or
- not successfully taking steps to stop the running of scripts that automatically sell or share visitor PI to third parties

3 REVIEW OF PRIOR WORK

We ran a search for "CCPA GPC" in Google Scholar.[9] Manual review of the search results identified 15 papers that discuss CCPA's requirement that websites recognize the GPC signal and treat and act on that signal as a visitor's DNS request. A deeper review showed that two of these papers undertake work that is the same as the first two stages of our project: they survey websites to see which are subject to CCPA and if those sites recognize and confirm that they have received the GPC signal from the browser of a site visitor. [1. Charatan], [2. Zimmeck, et.al.] How the authors of these two papers undertook their surveys has been helpful in planning our own recreation of these prior surveys with greater depth as a precursor to our added value regarding compliance with the requirement to recognize and act on the GPC signal by websites covered by CCPA. This paper aims to take this prior work one step further and determine if websites that are seemingly compliant actually stop the sale or share of PI of a visitor sending the GPC signal.

4 METHODOLOGY AND RESULTS

There are three steps to the methodology of determining whether websites subject to CCPA are recognizing and acting on the GPC signal appropriately: 1) identify websites that are subject to CCPA; 2) determining whether such websites are recognizing the GPC signal; and finally 3) determining if websites covered by CCPA that recognize the GPC signal actually stop third-party scripts from running thus preventing the sale or share a visitor's data as demanded by CCPA and the GPC signal.[10]

[3] Both CCPA and its amendment the CPRA were public referendums approved by voters in the State of California

[4] Cal. Civ. Code § 1798.115(d)

[5] Cal. Code Regs. tit. 11, § 7025(b)

[6] *See* https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement

[7] This is the mechanism used by the vendor OneTrust.

[8] As discussed below, the US Privacy String is being deprecated and will be replaced in 2024. *See generally*, https://iabtechlab.com/blog/iab-tech-lab-finalizes-us-state-signals/

[9] Running the same search on the global "OneSearch" in the Arizona State University Library online system only found one of the hits found by Google Scholar. Switching to the search "Global Privacy Control" at ASU resulted in an additional article with a copyright notice dated 2024. *See* References at 3.

[10] The code used to perform the research outlined in this paper is available at https://github.com/Sneberger/CCPA-GPC-Checking

4.1 Identifying Websites Subject to CCPA

Websites are subject to the rules set forth in CCPA if the company that operates the website is deemed to be a "business" under CCPA by meeting any one of three criteria:[11]

- Have annual gross revenues in excess of $25,000,000, or
- Have the PI of 100,000 California residents, or
- Derive more than 50% of annual revenue from selling or sharing the PI of Californians

With the exception of the annual revenues of publicly traded companies being available to the public, facts that would indicated a true answer for any of these three criteria are not available to researchers, therefore a surrogate criteria is needed. That criteria is whether the website operator itself believes that it, and thus its site, is subject to CCPA. Similarly to previous work [Charatan [1], at 10; Zimmeck et. al. [2], at 273], we looked for the strings "Do Not Sell," "Do-Not-Sell," "Do Not Share," or "California Privacy" in the HTML code of the website as evidence the website operator believed the site was subject to CCPA.[12]

Aiming to identify 2,000 websites that are subject to CCPA for further review, we first gathered the top 60,000 website URLs using the Tranco library for Python. Once this list was saved in a .csv file offline, with the URLs' extensions parsed into a separate, filterable column, to avoid any global websites that would not need to be CCPA compliant, and to eliminate any websites with .org extensions from the search as non-profits are exempted from complying with CCPA.[13] we filtered the 60,000 URLs to only include those with .com and .net extensions which resulted in 33,843 websites to further scan for CCPA applicability.

After this filtering, we ran the result of websites through a scanning function which consisted of two parts: 1) We imported the URLs for each website into Python using the csv function in Python and 2) We used the BeautifulSoup HTML parser to recursively iterate up to two layers through the HTML code of the website and searched for one of the target strings. This recursive scanning function tried and excepted two kinds of errors: Beautiful Soup-based errors resulting from the inability to access the target website which we called Reguest_Errors, and errors that occurred when a located internal URL returned a NoneType which we called General_Errors.[14] If no errors were excepted, the output of the function was FALSE if none of the strings were found and TRUE if any of the target strings were found. Thus a TRUE result indicated that the website itself contained material indicating the operator of the website was endeavoring to be compliant with CCPA requirements, *i.e.*, the website operator believed the website was subject to CCPA. Ultimately, we identified 1,924 websites that contained the target strings.

It seems that this simple review of websites could result in a number of incorrect FALSE returns as many of the websites that returned an excepted error might have had content that indicates attempted CCPA compliance that was missed by the scanning function, and probably some that returned FALSE did attempt CCPA compliance but their efforts were missed by the scanning function as implemented. To investigate this we took a random sample of 25 websites that had return FALSE and found none of them to include content that clearly indicated their operators believed the

[11] Cal. Civ. Code § 1798.140(d)

[12] This scanning procedure may capture sites that are not be subject to CCPA but rather are discussing CCPA's requirement for a DNS function in an advisory capacity. The authors maintain that this possibility is *de minimus* given the volume of websites scanned.

[13] Cal. Civ. Code § 1798.140(d) which limits the definition of a "business" subject to CCPA as being "organized or operated for the profit or financial benefit of its shareholders."

[14] We also triggered the following warning multiple times: "It looks like you're parsing an XML document using an HTML parser. If this really is an HTML document (maybe it's XHTML?), you can ignore or filter this warning. If it's XML, you should know that using an XML parser will be more reliable. To parse this document as XML, make sure you have the xml package installed, and pass the keyword argument 'features="xml"' into the BeautifulSoup constructor." We ignored and did not log this warning as it merely resulted in a FALSE response. We also saw this notice multiple times: "MarkupResemblesLocatorWarning: The input looks more like a filename than markup. You may want to open this file and pass the filehandle into BeautifulSoup." Again we ignored this as it merely resulted in a FALSE return.

website was subject to CCPA.[15] We sampled 15 of the websites that had returned an excepted Request_Error and found none of them to include content that indicated their operators believed the website was subject to CCPA.[16] Finally we chose a random sample of three URLs that returned TRUE results and found each to indicate they were covered by CCPA. It appears that our identification of websites whose operators *believe* they are subject to CCPA captured approximately 100 percent of the actual number of such websites out of the 33,843 with .com and .net extensions scanned. That said, there are undoubtedly many sites that *are* subject to CCPA but have not made and effort to provide a DNS function to visitors and as a result, were not identified by the scanner.

4.2 Identifying Websites That Recognize the GPC Signal

4.2.1 Websites that Include the gpc.json identifier in .well_kown identifiers

"GPC makes use of .well-known identifiers for sites to signal compliance with the GPC specification."[17] Including gpc.json in a website's list of .well-known identifiers alerts visiting browsers that the website acknowledges the GPC signal. In order to evaluate if the 1,924 websites we identified as being subject to CCPA had the gpc.json to their .well-known identifiers, we ran a scanner on each that searched for the gpc.json identifier.[18] To our surprise, only 32 of the 1,924 websites found to be subject to CCPA had the gpc.json identifier in place.

4.2.2 Websites That Evidence the Recognition of a DNS Request by way of the OptanonConsent Cookie

In order to scan the use of the OptanonConsent first-party cookie in the 1,924 websites we identified as subject to CCPA we created a two-tier, semi-automated python script that utilized the local instance of the Chrome browser on the machine running script. In order to control the sending of the GPC signal by that local Chrome browser we used the GPC enabler browser extension available in the Chrome Extension Manager and noted as "non-official." The scan was accomplished as follows:

(1) Cleared all cookies in the local Chrome browser
(2) Set the GPC enable browser extension to off
(3) Run a script using the csv and web browser library for Python that took in a .csv file containing the 1,924 CCPA website URLs causing each to be visited, load, and store any cookies set in the local browser
(4) Run a separate, Python script utilizing the browser_cookie3 library to identify the OptanonConsent cookies values for each of the 1,924 websites visited, if existent, and parsed the language of the value of those cookies to find the value saved and save it to a .csv file offline
(5) Repeated this process with the GPC signal turned on

The OptanonConsent cookie contains a value that begins with isGpcEnabled=0 if the GPC signal has not been recognized, and contains a value that begins with isGpcEnabled=1 if the GPC signal has been received. We scanned the 1,924 websites we determined to be subject to CCPA and found that 502 websites included the first-party

[15] Of the 25: five appeared to be based in Asia; and 5 appeared to be based in the European Union, provide a cookie banner, and appear to generally follow GDPR protocols; most interestingly, while three of the randomly selected sites proved to not sell or share data by way of third-party scripts on their site, one of the sites clearly states they do not sell or share PI but this statement was proved untrue by using the Blacklight tool (https://themarkup.org/blacklight) which showed multiple cookies and trackers in place. We were unable to reach two by navigating to them manually with a browser. Overall, there were no findings in the randomly selected sites indicating the FALSE return was inappropriate.

[16] Of the 15: one appeared to based in India, one appeared to be based in Germany, and 23 were unable to locate the IP address when manually attempting to browse to the site. Overall, there were no findings in the randomly selected sites indicating any would have been assigned TRUE if the scanner would have been able to reach them.

[17] https://globalprivacycontrol.org/implementation

[18] Thank you to Jan Charatan for providing Python code that used Python's request library and was the basis for this scan.

OptanonConsent cookie with the '0' value indicated, however, only 353 of those switched the value to '1' when revisited with the GPC signal turned on. A further 19 featured the alternative value for the cookie.[19]

4.2.3 Websites That Evidence the Recognition of a DNS Request by way of the US Privacy String

Our next step was to analyze whether websites subject to CCPA properly recognized the GPC signal was to look at the websites' use of the US Privacy String. The US Privacy String is a soft law protocol set forth by the Tech Lab of the International Advertising Bureau (IAB) which is an association of companies in the digital advertising industry.[20] The US Privacy String protocol is outlined in a GitHub page,[21] and according to the IAB Tech Lab "[t]he [US Privacy] String format enables digital properties to store and maintain a consumer's privacy preference and transmit that data to relevant parties. Parties receiving the data are expected to act on it in accordance with any relevant governance."[22] The US Privacy String is - and its successors are - structured to include four text characters that represent the following information:

(1) Version: the version number of the US Privacy String provided
(2) Status of notice given: whether the digital property provided "notice and opportunity to opt-out of sale of data"
(3) **User preference: whether the user has opted out of the sale of their PI**
(4) Whether the digital property is operating under a signed Limited Service Provider Agreement (LSPA) with the IAB

In order to observe the existence and behavior of the US Privacy String on websites we identified to be subject to CCPA we ran a Python script which used the Selenium library and Firefox webdriver[23] to record the coding of the US Privacy String on each website: first when visiting the site without emitting the GPC signal, then second visiting the website while emitting the GPC signal. The results when reviewing the 1.924 website we identified as subject to CCPA get us closer to determining overall compliance. Let us look at our numeric results by String character:

(1) There has only been one version of the US Privacy String so the results here were binary: '0' for no string and '1' for the current US Privacy String.[24]
(2) Regarding the status of notice given without the GPC signal, with the GPC signal turned off we found 260 with and 'Y' value here indicating notice given, 21 with a 'N' value indicating no notice, 370 reporting a '-' value, and 1,273 with no value. When we turned on the GPC signal we found 266 with and 'Y' value here indicating notice given, the same 21 with a 'N' value indicating no notice, 359 reporting a '-' value[25], and 1,278 with no value.
(3) **The third character in the string representing user preference is the heart of our inquiry.** Initially we saw that three of the 1,924 websites subject to CCPA had the user preference character set to Y' meaning the site visitor deemed to have opted out of the sale of share of their PI even before the GPC signal was sent, but to the heart of the matter we identified 306 websites that had this character as 'N' with no GPC signal but only 169 of

[19]Websites that feature the value "isGpcEnabled0/1" at the beginning of the OptanonConset cookie value also have a value such as "groups=C0001%3A1%2CC0002%3A1%2CC0003%3A1% 2CC0004%3A0%2CC0005%3A0" at the end of the value for the cookie. Websites that begin the value of the cookie with "groups" appear to be combining a OneTrust solution for the Data Layer Object with the Google Tag Manager.

[20]http://www.iab.com

[21]https://github.com/InteractiveAdvertisingBureau/USPrivacy/blob/master/CCPA/

[22]The US Privacy String is being deprecated at the end of January 2024, and in its place the IAB Tech Lab has promulgated the Global Privacy Platform (GPP) which in addition to CCPA is meant to address the needs of other, newer state privacy laws. "IAB Tech Lab's Global Privacy Working Group, in partnership with the IAB's Legal Affairs Council have developed the privacy string specifications for five US states (California, Virginia, Colorado, Utah, and Connecticut) that are supported within the GPP." *See* https://iabtechlab.com/blog/iab-tech-lab-finalizes-us-state-signals

[23]Again, thank you to Jan Charatan for providing Python code that was the basis for this scan.

[24]We did find 48 websites that reported a version number of '4' when visited without the GPC signal with 12 of these showing '1' once the GPC signal was sent and 50 websites that reported a version number of '4' when visited with the GPC signal with 14 of those having showed version '1' without receiving the GPC signal. We do not have an explanation for these anomalous values.

[25]IAB Tech maintains that "[i]n situations where the digital property has determined that the consumer does not fall within a US Privacy jurisdiction (such as CCPA), the digital property may signal this with hyphens in the second, third, and fourth character positions in the following manner: '1—'."

these same 306 sites switching the character to 'Y' after the GPC signal was sent. Overall, 188 websites set the character to 'Y' once the GPC signal was sent with the difference being that 19 of these sites either already had the character as 'Y' with no GPC signal (3), had the value '-' with the GPC signal off (7), or had an anomalous result for this character when no GPC signal was sent (9). It should be noted that of the 188 websites that set the US Privacy String third character to 'Y' after receiving the GPC signal, 57 of them also set value for the OptanonConsent cookie to '1,' and three of these websites also featured the gpc.json identifier in .well_kown identifiers section.

(4) As discussed in the Appendix, we do not fully ascribe to the position of IAB Tech that it matters whether a website operator or its third parties are operating under a signed Limited Service Provider Agreement (LSPA),[26] thus it is appropriate to not address these results.

4.3 Identifying if Websites That Trigger a DNS Request After Recognizing the GPC Signal Actually Stop Third-Party Scripts from Exfiltrating Data

Ultimately, after scanning the the **1,924** websites that we identified as being subject to CCPA, we found **510** that have indications that they are compliant with CCPA's requirement that they recognize the GPC signal emitting from visiting browsers: 32 that place the gpc_json; 353 with the OptanonConsent cookie's bearing a value of '1', 188 with the third character of the US Privacy String set to 'Y', minus 63 that feature more than one of these indicators. But do these 26.5 percent of CCPA-covered websites that appear compliant actually stop the sell or share of visitor data to third parties once they receive the GPC signal is our final inquiry.

As a baseline, aggregate look at the effect of the GPC signal on the 510 seemingly compliant sites we wrote a Python script using the webbrowser library and the local version of the Chrome browser on the machine running the script. First with the GPC signal turned off we cleared all cookies in the local Chrome browser then visited each of the 510 sites. Once all sites had been visited we used a Python script using the browser_cookie3 library to count all the cookies the 510 sites placed on the local machine's Chrome browser and noted the results. We then cleared all cookies, turned on the GPC signal, then revisited all 510 sites and again counted all cookies that had been placed in the local Chrome browser. We repeated this ten times and after finding the mean and median of results of the ten runs found that a low of 10 percent, a high of 15 percent, and an average of 11.6 percent *less* cookies where placed on the local Chrome browser when the GPC signal was turned on, showing that in the aggregate, the GPC signal has the effect of minimizing cookies set on a website visitor's machine. But what about the effect of the GPC signal on individual sites?

Without the ability to capture, decrypt, and inspect individual packets flowing from a website visitor the the website's server[27] we cannot accurately detect what PI flows from a website visitor to the website operator or its third parties, but based on what we learned from the aggregate cookie test - that the GPC signal has an overall effect on websites interaction with visitors - we devised a simple plan to inspect the back-and-forth flow of data between specific websites and a visitor. We repurposed the base Python code we used to decode the US Privacy String and added a packet capture function using the pyshark wrapper. With the GPC signal turned off we visited each of the seemingly compliant websites and measured the packet volume for two seconds after visiting the site and stored the volume of packets. We then repeated this process with the GPC signal turned on. After the before-and-after packet counts were gathered our analysis was based on the following assumptions:

[26]Just as the US Privacy String is being deprecated, the LSPA is being replaced with a new Muli-State Privacy Agreement (MSPA). *See* https://www.iab.com/news/multi-state-privacy-agreement-mspa/

[27]We suggest future work might leverage mitmproxy or another tool to more accurately inspect the network traffic directly between a website visitor and third parties: https://mitmproxy.org/

- If the number of packets counted with the GPC signal turned on decreased we determined that it was probable the GPC signal had an effect on the particular website indicating that in addition to evidencing compliance, the website actually reduced data flow from the visitor; and
- If the number of packets counted with the GPC signal turned on increased when the GPC signal was turned on we deemed we cannot make a determination if the GPC signal had an effect on the particular website

Based on these assumptions, of the 510 seemingly compliant websites we found that for 273 websites we found that the GPC signal led to a decrease in traffic immediately after visiting the site, for one website there was no change, and for 236 websites we found that sending them the GPC signal had the effect of increasing the packet traffic immediately after visiting the site. From these results we opine that it is probably that at least 273 of the seemingly compliant sites that actually reduce data traffic to and from a visitor in the two seconds after visiting the site appear to be truly compliant with CCPA's requirement that the GPC signal emitting from a visitor's browser be treated as, and acted upon as a DNS request made by the visitor, *i.e.*, we project effective compliance could be as low 14.2 percent of the 1,924 websites subject to CCPA.

5 DISCUSSION

Using simple scripts written in Python we identified 1,924 websites subject to CCPA, and found that only 510 of those sites appeared to be nominally compliant with CCPA's requirement that subject websites recognize the GPC signal and treat it as a DNS request - or **26.5 percent**. We further found that it is possible that only 273 of these 510 sites actually minimize data flowing from a website visitor once the GPC signal sent - or just **14.2 percent** of all CCPA sites.

6 LIMITATIONS

- The scripts generating the work outlined herein were run in the State of Arizona, USA. It is possible that geofencing techniques employed by websites could have identified visitors resulting from our scripts to not be located in the State of California, and as a result did not serve the visitor with complete GPC-related service. However, we believe this concern is minimized, if not eliminated, by the fact that we were still served with the DNS option which is how we identified websites subject to CCPA at the beginning of our inquiry, *i.e.*, the 1.924 websites we identified as being subject to CCPA provided us with the right to opt out of the sale or share of our PI so it would have been appropriate for the websites to recognized the GPC signal as exercising that right.
- While we have identified three ways for a website to signal compliance with CCPA's requirements that websites recognize the GPC signal, it is almost certainly true that other compliance methodologies are employed by websites to show compliance which were missed by our methodology.
- Our inability to accurately determine if a seemingly compliant websites continue to sell or share visitor PI to third parties precludes us from reaching a concrete conclusion that some websites that appear to be compliant by the review performed here are not actually compliant with a visitor's DNS request by way of GPC.

7 CONCLUSION

While we undoubtedly missed identifying *some* compliant websites - and future work should endeavor to more completely guage compliance - it appears that compliance levels with CCPA's requirement that subject websites recognize the GPC signal and treat it as a DNS request are very low.

8 REFERENCES

(1) A Step Forward and More of the Same: Global Privacy Control and California Privacy Law. Jan Charatan 2023. https://cs.pomona.edu/classes/cs190/thesis_examples/Charatan.23.pdf
(2) Usability and enforceability of global privacy control. Sebastian Zimmeck; Oliver Wang; Kuba Alicki; Jocelyn Wang; and Sophie Eng. 2023. https://www.petsymposium.org/2023/files/papers/issue2/popets-2023-0052.pdf
(3) Generalizable Active Privacy Choice: Designing a Graphical User Interface for Global Privacy Control. Sebastian Zimmeck; Eliza Kuller; Chunyue Ma; Bella Tassone; and Joe Champeau. 2024. https://petsymposium.org/popets/2024/popets-2024-0015.pdf
(4) The Impact of Visibility on the Right to Opt-Out of Sale under CCPA. Adam Siebel; and Eleanor Birrell. 2022. https://arxiv.org/pdf/2206.10545
(5) Bridging the Privacy Gap. Swedish. Masters Thesis of Carl Magnus Bruhner. 2022. https://www.diva-portal.org/smash/get/diva2:1684557/FULLTEXT01.pdf
(6) Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges. Soheil Human; Harshvardhan J. Pandit; Victor Morel; Cristiana Santos; Martin Degeling; Arianna Rossi; Wilhelmina Botes; Vitor Jesus; and Irene Kamara. 2022. https://research.wu.ac.at/files/27510678/2022_IWPE_DPCCM_Human.pdf
(7) Bridging the Privacy Gap: Enhanced User Consent Mechanisms on the Web. Calr Magnus Bruhner; David Hasselquist; and Miklas Carlsson. 2023. https://www.ida.liu.se/~nikca89/papers/madweb23.pdf
(8) A Call for Interdisciplinary Collaboration toward the Realization of Needs-aware AI. S. Human. https://www.sustainablecomputing.eu/blog/category/opinion/
(9) Privacy Preference Signals: Past, Present and Future. European. Maximilian Hils; Daniel W. Woods; and Ranier Bohme. 2021. https://arxiv.org/pdf/2106.02283
(10) Conflicting Privacy Preference Signals in the Wild. Maximilian Hils; Daniel W. Woods; and Ranier Bohme. 2021. https://arxiv.org/pdf/2109.14286
(11) Privacy Preference Signals. PhD Dissertation of Maximilian Hils. European 2022. https://hi.ls/privacy-preference-signals.pdf
(12) Proposal for Resolving Consenting Issues with Signals and User-side Dialogues. Harshvardhan J. Pandit. Ireland. 2021. https://arxiv.org/pdf/2208.05786
(13) Automating privacy decisions – where to draw the line? Victor Morel; Simone Fischer-HübnerSweden. 2023. https://arxiv.org/pdf/2305.08747
(14) The Right to Customization: Conceptualizing the Right to Repair for Informational Privacy. Aurelia Tamo-Larrieux; Zaira Zihlmann; Kimberly Garcia; and Simon Mayer. Switzerland. 2021. https://www.researchgate.net/profile/Zaira-Zihlmann/publication/349119147_Right_to_Customization_Conceptualizing_the_Right_to_Repair_for_Informational_Privacy/links/60c353a3a6fdcc2e6132912d/Right-to-Customization-Conceptualizing-the-Right-to-Repair-for-Informational-Privacy.pdf
(15) COnSeNT 2022: 2nd International Workshop on Consent Management in Online Services, Networks and Things. Paulina J. Pesch; Harshvardhan J. Pandit; Vitor Jesus; and Cristiana Santos. Europe. https://publications.aston.ac.uk/id/eprint/44214/6/Accepted_Manuscript_COnSeNT_2022_paper.pdf

9 APPENDIX

We question IAB Tech's representation that once a website operator and its third party enter into a Limited Service Provider Agreement (LSPA) the website may continue to sell or share PI of a visitor who has opted out of the sale of share of their PI as long as the information is accompanied by a 'Y' value in the third position of the US Privacy String.

This position appears to arise from LSPA Section 4.4(a)(ii)-(iv) which in part attempts to designate the recipient third parties as a service providers by fiat. [28]

A sale or share is defined by CCPA as follows:[29]

> "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, In writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

Note the use of the term "third party" in this definition. The position of the IAB appears to misinterpret CCPA's definition that transferring a website visitor's PI to a Service Provider or a Contractor is *not* a sale or share as the third party is purportedly a Service Provider or Contractor as those designations are set forth in the CCPA.[30] The problem with this position is that both Service Providers[31] and Contractors[32] are formal designations that require the so-designated third party to have a direct contractual relationship with the website operator that burdens the third party with the following prohibitions regarding the PI of the website visitor that have been forwarded to them (paraphrased):

(1) Selling or sharing
(2) Retaining, using, or disclosing for any purpose other than specified in the contract
(3) Retaining, using, or disclosing outside of the direct business relationship
(4) Combining with data received from others

If such a contract is not entered into between the website operator and the third party, then the third party remains a third party as defined by the CCPA,[33] and does not achieve Service Provider or Contractor status. A website operator cannot simply "designate" a third party as a "service provide" as contemplated by LSPA Section 4(a)(ii) and (iv). For example, Google Analytics is not a party to an LSPA, and presumably is not a party to a direct contract with any website operator that formally causes Google Analytics to become a Service Provide or Contractor as defined by the CCPA. Thus Google Analytics remains a third party, and forwarding a website visitor's PI to Google Analytics is a sale or share, as the case may be, pursuant to the CCPA.

Remembering that transferring data to a true Service Provider or Contractor is not a sale, there is no exception set forth in the CCPA allowing PI to be sold or shared with third parties once a website visitor has invoked their right to opt out of the sell or share of their information as long as the third party is party to an agreement that does not cause them to meet the definition of Service Provider or Contractor as those designations are defined by the CCPA and the information is accompanied with notice that the visitor has opted out. Rather Cal. Civ. Code § 1798.120(d) reads as follows:

> A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section

[28] https://www.iabprivacy.com/IAB%20First%20Amended%20and%20Restated%20Multi-State%20Privacy%20Agreement%20(MSPA).pdf
[29] Cal. Civ. Code § 1798.140(ah)
[30] Cal. Civ. Code § 1798.140(ad)
[31] Cal. Civ. Code § 1798.140(ag)
[32] Cal. Civ. Code § 1798.140(j)
[33] Cal. Civ. Code § 1798.140(ai)

> 1798.135, from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent, for the sale or sharing of the consumer's personal information.

In parallel, Cal. Code Regs. Tit. 11, § 7013(a) similarly reads:

> The purpose of the Notice of Right to Opt-out of Sale/Sharing is to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information and to provide them with the opportunity to exercise that right. The purpose of the "Do Not Sell or Share My Personal Information" link is to immediately effectuate the consumer's right to opt-out of sale/sharing, or in the alternative, direct the consumer to the Notice of Right to Opt-out of Sale/Sharing. Accordingly, clicking the business's "Do Not Sell or Share My Personal Information" link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

Cal. Code Regs. Tit. 11, § 7025, which addresses the requirement that the GPC signal be recognized and treated as an exercise of the visitor's right to opt out of the sale or share of their PI, mentions *no exception* for continuing to sell or share the information with a mere indication that the visitor has opted out. Whether a third party providing "analytics" related to advertising can be characterized as a service provide should be a focus of future research.