

---

**From:** Irene Ly [REDACTED]  
**Sent:** 11/8/2021 7:29:28 AM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Ariel Fox Johnson [REDACTED]  
**Subject:** PRO 01-21: Common Sense Comments  
**Attachments:** Common Sense Comments to the California Privacy Protection Agency - Nov 2021.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Hello Ms. Castanon,

Attached is Common Sense's response to CPPA's invitation for comments in the PRO 01-21 proceeding. Thank you for the opportunity to weigh in.

Best,  
**Irene Ly**  
Policy Counsel | Common Sense  
[REDACTED]



## Comments to the California Privacy Protection Agency

### Introduction

Common Sense Media (Common Sense) and Privacy Rights Clearinghouse are pleased to submit these comments in response to the California Privacy Protection Agency (CPPA)'s invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA). Common Sense is an independent, nonpartisan voice for children that champions policy solutions that puts children--all those under 18--first and works to ensure that they can thrive in the 21<sup>st</sup> century. Privacy Rights Clearinghouse is a nonprofit organization dedicated to improving privacy for all by empowering individuals and advocating for positive change.

### ***Question 1: Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses***

- 1. Processing Children's Personal Information Presents a Significant Risk to Consumers' Privacy and Security That Should Require Businesses to Regularly Submit Risk Assessments*

Processing personal information of children and teenagers poses a significant risk to consumers' privacy and security, and businesses that process such information must be subject to the CPRA's requirement to conduct risk assessments. Children and teens spend increasing amounts of time online and are especially susceptible to privacy harms because their brains are still developing and they do not fully comprehend the consequences of sharing or the nature of advertising. Privacy policies and terms of service are insufficient to protect children, who can be easily exploited and manipulated and suffer behavioral, social, emotional, and physical harms. Risk assessments are therefore critical.

Children across all age groups are spending more time on devices and online than ever before. According to Common Sense research, even before the pandemic, children from birth to age 8 in the United States were using about two and a half hours of screen media per day, while 8- to 12-year-olds used just under five hours' worth, and teens used just under seven and a half hours.<sup>1</sup> These numbers do not include the time spent using screens for school or homework. Children in lower-income households also spend an average of nearly two hours a day more with screen media than those in higher-income homes. Similar patterns were found in Latino and Black children in comparison to white children. With education largely shifting online in 2020, kids also experienced a sizable 69 percent increase in the amount of time they spent

---

<sup>1</sup> The Common Sense Census: Media use by kids age zero to eight, 2020. San Francisco, CA: Common Sense Media.



using a screen for education, particularly 5- to 10-year old's.<sup>2</sup> While many children have returned to the classroom, reliance on technological tools is expected to continue.

The increasing presence of kids and teens online raises concerns for many reasons.<sup>3</sup> Young children and teens are prone to oversharing,<sup>4</sup> and because their brains are still developing, they have also been shown to not understand the consequences of their sharing.<sup>5</sup> They believe that the information they share remains on their device, or within an app or game, and that deleting the app or information within an app will delete it from the internet. They also do not understand that an app may gather information about them from sources outside the app.<sup>6</sup>

Children also have difficulty identifying advertising. More than half of thousands of free children's apps may serve kids ads that violate the Children's Online Privacy Protection Act (COPPA).<sup>7</sup> Yet research shows that children under the age of eight cannot comprehend the persuasive intent of advertising and are prone to accepting advertiser messages as truthful, accurate, and unbiased.<sup>8</sup> Over 75 percent of kids aged 8 to 11 cannot distinguish advertising from other content.<sup>9</sup> Even older children still lack the digital skills and critical ability to assess the safety of content they encounter online.<sup>10</sup> Privacy also exacerbates equity issues, as shown through findings that children with low socioeconomic status were more likely to play games collecting and sharing information for advertisements.<sup>11</sup>

Companies can exert influence over children through exploiting their susceptibility to coerce them into making choices they would not otherwise make, such as through behavioral targeted advertising. Misuse and the inadvertent disclosure of a child's personal information can lead to a wide range of behavioral, social, emotional, and physical risks, which are detailed extensively

---

<sup>2</sup> Ryan Tuchow, [Kid device usage changing as a result of the pandemic](#), Kidscreen, (Feb. 19, 2021).

<sup>3</sup> Testimony of Ariel Fox Johnson Before the United States House of Representatives Committee on Energy and Commerce, Common Sense (March 11, 2021).

<sup>4</sup> [Who Knows What About Me?](#), Children's Commissioner, (Nov. 8, 2018). The UK Children's Commissioner found that, pre-pandemic, children posted an average of 26 times a day to social media. By age 18, they average a total of 70,000 posts.

<sup>5</sup> Children may not understand what is going on, whereas teens may have a slightly better sense but be more likely to partake in risky behavior.; see Adriana Galvan et al., *Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents*, 26 Journal of Neuroscience 25 (2006) (teens' brain development can bias them towards risky behaviors).

<sup>6</sup> Anonymous Author(s). 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": How Children Conceptualize Data Processing and Digital Privacy Risks. In CHI '21: ACM CHI Conference on Human Factors in Computing Systems, May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, US.

<sup>7</sup> Reyes et. al, "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. Proceedings on Privacy Enhancing Technologies, (2018).

<sup>8</sup> American Psychological Association. *Advertising leads to unhealthy habits in children; says APA task force*. [Press release] (Feb. 23, 2004).

<sup>9</sup> Common Sense Media, *Privacy Matters: Protecting Digital Privacy for Parents and Kids*, (2018).

<sup>10</sup> Nyst, Carly. (2017). *Privacy, protection of personal information and reputation*. Retrieved from UNICEF website: [https://www.unicef.org/csr/css/UNICEF\\_CRB\\_Digital\\_World\\_Series\\_PRIVACY.pdf](https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf).

<sup>11</sup> Zhao F, Egelman S, Weeks HM, Kaciroti N, Miller AL, Radesky JS. Data collection practices of mobile applications played by preschool-aged children. *JAMA Pediatrics*, accepted for publication.



in Common Sense's report *Privacy Risks & Harms*.<sup>12</sup> Children can experience cyberbullying, radicalization, substance abuse, limited educational opportunities, self-harm, contact from strangers, identity theft and increased parent-child conflict. These risks can be magnified for children who are already in more vulnerable groups.<sup>13</sup>

Privacy policies and terms of services alone cannot be relied upon to notify children and their parents of the implications of sharing information online and to obtain consent to collect and share their information. Even older and literate children struggle to understand privacy policies, which are often long and full of legal jargon. Only 17 percent of teens and 36 percent of parents say they read the terms of service "almost all the time."<sup>14</sup> Although parents are talking to their children more than ever about privacy,<sup>15</sup> the onus should not only be on parents to keep their children safe online. Even with consumers' perfect understanding of privacy policies, businesses can still misuse and exploit personal information collected about children.

Defining all children's personal information and data as information that presents a "significant risk to consumers' privacy or security," which would require businesses to submit regular risk assessments to the Agency regarding their processing activities, would be a step in the right direction to addressing the above discussed harms.

*2. Because Children's Personal Information Poses a Significant Processing Risk, Businesses Must Perform Risk Assessments that Consider the Purposes, Necessity, and Potential Harms of Such Processing in Early Stages of Product Development*

In conducting risk assessments, businesses should build them in at the start of their design processes and regularly thereafter. Businesses must consider the purpose and necessity of their processing--specifically whether it is needed for the product to work; the potential harms to children of such processing; and what mitigation measures are available.

Businesses should conduct risk assessments both early in the product or platform development stage and regularly after deployment. Platforms often engage in adult-centric design practices instead of taking into account the developmental needs of children when designing their products and features. Research has shown that platforms are often engaged in manipulative design practices that exploit children's developmental vulnerabilities.<sup>16</sup> By requiring risk assessments during the early product development stages, products targeted at children or often used by children can be designed with their safety and privacy in mind. This would also

---

<sup>12</sup> Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). *Privacy risks and harms*. San Francisco, CA: Common Sense Media.

<sup>13</sup> This includes children from poor households, children in communities with a limited understanding of different forms of sexual abuse and child exploitation, children who are out of school, children with disabilities, children who suffer from depression or other mental health problems, and children from marginalized groups. Nyst at 81.

<sup>14</sup> Common Sense Media, *Privacy Matters: Protecting Digital Privacy for Parents and Kids*, (2018).

<sup>15</sup> *Ibid*

<sup>16</sup> [Letter from Common Sense and Dr. Jenny Radesky on Article 26 of the Digital Services Act](#) (June 7, 2021).



save business resources, preventing a business from needing to make major overhauls after it has already developed, tested, or launched its product for public use and avoid preventable harms from the start.

Regular risk assessments after product deployment are also necessary to ensure businesses are continually operating with children in mind and assessing their data collection practices so that they do not begin collecting more information than is strictly necessary. Risk assessments should be conducted whenever a business adopts new technology or features, or wants to collect additional information, or on an annual or bi-annual basis.

Given the unique developmental stages and vulnerabilities of children, the risks of any data collection of children that is not necessary for the functioning of a product should be treated as outweighing the benefits. Common Sense supports the prohibition of behavioral targeted advertising to children altogether.<sup>17</sup> Businesses should perform risk assessments under the assumption that all information collected about children is sensitive personal information, and carefully scrutinize the implications of any data collection and processing.

The UK Age Appropriate Design Code, which went into enforcement effect in September 2021, also requires businesses conduct data protection impact assessments,<sup>18</sup> and we propose the law should be used as a model for what businesses should cover in these risk assessments submitted to the Agency. The assessments should have a detailed description of the nature, scope, context, and purposes of the processing. This includes information about whether the product or service is designed for children or whether children are likely to access the service, the age range of those children, any plans for establishing the age of those children or any parental controls, the intended benefits to children, the commercial interests of the business for the processing, and whether any profiling or automated decision making is involved. Also, in line with the Code, the assessment should assess the necessity of the processing, the proportionality of the benefits with its risks to children, and whether it complies with the CPRA, COPPA, and any other applicable laws.

With that information, the assessment must carefully consider any harm or damage the data processing may inflict on a child's physical, emotional, developmental, or social health. In particular, businesses should assess whether the processing may cause or lead to an increased risk of physical harm, sexual exploitation, social anxiety, self-esteem issues, depression, bullying, peer pressure, or compulsive use.

Finally, the assessment should identify measures to mitigate those risks and its plans for adopting them. Mitigation measures can include imposing new safeguards or eliminating a

---

<sup>17</sup> Testimony of Ariel Fox Johnson Before the United States House of Representatives Committee on Energy and Commerce, Common Sense (March 11, 2021).

<sup>18</sup> Alyona Eidinger, [What is the Age Appropriate Design Code?](#), Common Sense Media, (Jan. 20, 2021); Information Commissioner's Office, [Age Appropriate Design: A Code of Practice for Online Services](#), (Sept. 2, 2020).

specific feature or collection of specific data altogether. If the assessment finds that the risks posed by processing cannot be mitigated, businesses should cease processing the data.

By requiring risk assessments that detail data processing activities, assess the necessity and potential harms of processing, and propose any mitigation measures that can be implemented, businesses will be more transparent and can be held accountable for its data processing of children.

The CPPA should require that these risk assessments be disclosed to them, the Attorney General's office, and any other applicable regulatory or enforcement agencies for the particular business. To the extent doing so would further privacy interests, the agency may choose to disclose information from the reports at its own discretion, while keeping any trade secrets confidential and redacted. This will help further promote accountability and transparency among businesses.

***Question 5: Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information***

***1. The Use of Sensitive Information Should Be Limited Only to What is "Necessary to Perform the Service"***

All data about children under 18 is sensitive information, and thus businesses should only use this sensitive information when it is strictly necessary to perform the service it is offering to consumers. This is in line with already existing requirements under the Children's Online Privacy Protection Act for children under 13, along with international best practices such as the UK's Age Appropriate Design Code. This would be stricter than the current right consumers have under the CPRA, but is necessary to best protect children and make their best interests the priority instead of a business' commercial interests. Businesses should also change their assumptions about the reasonable expectations of consumers to better reflect reality and research that has found consumers are concerned about targeted advertising and the privacy concerns it poses.

The CPRA states that "a consumer shall have the right, at any time, to direct a business that collects sensitive information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services to perform the services." Under prohibitions dating back to the CCPA, the rules protecting children under 16 are default protected (no sale unless opt-in), and the most privacy protective way to read the CPRA is if that framework was extended to children under 16's for sensitive information as well. This is consistent with the CPRA's preamble which notes that "Children are particularly vulnerable from a negotiating perspective with respect to their privacy rights." The default should be that businesses can only use children's sensitive information for purposes that are strictly necessary to operate its service. This would best protect young people because it would mandate a default framework that puts children's privacy and security above minor commercial benefits a business may get.



The CPPA should also reconsider what an average consumer who requests a business to provide a good or service reasonably expects when evaluating whether a business is using sensitive information for necessary purposes. Businesses should not reasonably expect that consumers expect targeted advertising. Instead, businesses should expect that consumers would prefer other non-intrusive types of advertising that do not rely on collecting data about consumers to generate it such as contextual advertising, in which ads are displayed based on a website's content.

There are studies that would support this reasonable expectation. A study found that college students perceived the risk of targeted advertising to be higher than the benefits, which drives them to perceive more privacy concerns and avoid the advertising.<sup>19</sup> A cybersecurity survey found that just 17 percent of respondents across the United States, France, Germany, and the United Kingdom viewed tailored advertisements as ethical.<sup>20</sup> Most relevant, a survey has shown that 82 percent of parents and 68 percent of teens are concerned about how social networking sites are using their data to allow advertisers to target them with ads.<sup>21</sup> With children, teens, and their parents voicing so much concern about the use of their data for targeted advertising in conjunction with their discussed developmental vulnerabilities, there is a compelling reason to revise what businesses consider these groups' reasonable expectations.

#### ***Question 6: Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information***

- 1. All Children's Data Should be Treated as Sensitive Personal Information Subject to the Right to Have Limited Use and Disclosure*

The term "sensitive personal information" should be interpreted as broadly as possible, particularly when it comes to children's data. Even data that may not be considered sensitive because it is deemed "collected or processed without the purpose of inferring characteristics about a consumer" can be used to make sensitive inferences. For example, cell tower location data indicating where a phone stays overnight could be used to infer a couple is getting a divorce,<sup>22</sup> and a business could use a person's shopping history to infer she is pregnant.<sup>23</sup> As a result, consumers must have the right to limit the use and disclosure of broadly defined sensitive personal information. There is no circumstance in which it is logical for a business to stop a consumer from exercising this right when it involves information that has already been categorized as sensitive.

---

<sup>19</sup> Business News Daily Editor, *Invasion of Privacy: What Consumers Think of Personalized Online Ads*, Business News Daily (Feb. 21, 2020), <https://www.businessnewsdaily.com/4632-online-shoppers-personal-ads.html>.

<sup>20</sup> RSA, *The Dark Side of Customer Data* (Feb. 6, 2019), <https://www.rsa.com/en-us/company/news/the-dark-side-of-customer-data>.

<sup>21</sup> Common Sense Media, *Privacy Matters: Protecting Digital Privacy for Parents and Kids*, (2018).

<sup>22</sup> Diane L. Danois, [\*Cohabitation, the Termination of Alimony, and Cell Phones\*](#), The Huffington Post (June 11, 2013).

<sup>23</sup> Kashmir Hill, [\*How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did\*](#), Forbes (Feb. 16, 2012).



## *2. No Use or Disclosure of Sensitive Personal Information Should be Permissible*

No use or disclosure of a consumer's sensitive personal information by businesses should be permissible in spite of a consumer's direction to limit the use or disclosure of it. This is contrary to the purpose and intent of the CPRA, which a majority of Californians voted for in order to expand privacy rights. The consumers' rights under the CPRA should always take priority, and businesses should not be permitted to override a consumer's decision to exercise her right to limit the use or disclosure of her data in any circumstance. Businesses should not ever aim to use or disclose any more sensitive personal information than is strictly necessary.

### ***Question 8j: "Dark Patterns" Should be Defined to Include Manipulative Design Features That Encourage Children to Give Up Personal Information***

Dark patterns can cover a wide range of design choices that benefit an online service by pushing users to make potentially harmful choices that they would not otherwise make. The definition of "dark patterns," which would be better referred to as "manipulative design," should be drafted as broadly as possible and include at least design features that encourage children to give up personal information.

In a notable paper in the area, dark patterns were defined as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions."<sup>24</sup> However, dark patterns include many types of practices and features. Researchers have found at least one dark pattern in 95 percent of apps in a study of 240 popular apps.<sup>25</sup> The definition the CPPA adopts should be as broad as possible to include the many ways dark patterns can take form.

Firstly, the term "manipulative design" should be adopted in place of "dark patterns" in CPPA regulations (recognizing the text of the CPRA refers to "dark patterns"). Evolving scholarship highlights how the term "dark patterns" perpetuates implicit racial biases because it is part of a dualism that sees darkness as inherently bad and light as good and thus should be updated.<sup>26</sup> The term "manipulative design" is also more informative and better acknowledges how businesses are essentially tricking consumers into making certain choices they would not make in the absence of the feature – whether they mean to or not. Common Sense has shifted to using the term "manipulative design" recently, and will officially adopt the term in future content and filings in place of "dark patterns."

---

<sup>24</sup> Mathur et. al, "Dark Patterns at Scale: Findings From a Crawl of 11K Shopping Websites," Proceedings of the ACM on Human-Computer Interaction (2019).

<sup>25</sup> Linda Di Geronimo et. al, "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception," Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (2020).

<sup>26</sup> Kat Zhou, [FTC Dark Patterns Workshop Transcript](#), Federal Trade Commission (April 29, 2021) at 15; Kate Conger, ["Master," "Slave" and the Fight Over Offensive Terms in Computing](#), N.Y. Times (Apr. 13, 2021).



In particular, the definition of manipulative design should include design features that encourage children to give up more personal information than necessary or than they may freely wish to.

Apps often encourage children to disclose personal information to play a game or participate in certain parts of it, interfering with promises companies set out in privacy policies.<sup>27</sup> A third of 135 Android apps reviewed in a 2018 study that were marketed to or played by children prompted players to rate the app on the Google Play store, and 14 percent prompted players to share information on social media.<sup>28</sup> The information shared often results in children unknowingly agreeing to provide the company with wide permissions to extract information about social media contacts, enabling companies to collect even more data. Additionally, a study found that almost half of 153 apps in Google Play's "Designed for Families" category transmitted advertising identifiers.<sup>29</sup> Multiplayer games also tend to use default settings that reveal the most personal information, which is particularly harmful for children who are unlikely to change or know how to change the settings.<sup>30</sup> The employment of manipulative design features trap users into data collection, making people lose the ability to make truly informed decisions.<sup>31</sup>

A broad definition of "dark patterns" or "manipulative design" like the one proposed here would put businesses on alert to deter them from engaging in dark patterns and allow parents to better understand what can be considered a "dark pattern" that they should watch out for.

## Conclusion

Common Sense appreciates the CPPA's work on this rulemaking and urges the Agency to take the steps recommended in these comments to ensure that children and teens' privacy rights are protected.

Respectfully submitted,  
Ariel Fox Johnson, Senior Counsel, Global Policy  
Irene Ly, Policy Counsel  
Common Sense

---

<sup>27</sup> Johanna Gunawan, "[Right at the Source: Privacy Manipulative Design in User Interfaces](#)," Common Sense Media (Oct. 13, 2021).

<sup>28</sup> Meyer M, Adkins V, Yuan N, Weeks HM, Chang YJ, Radesky J, *Advertising in Young Children's Apps: A Content Analysis*, J. Dev. Behav. Pediatr. (2019).

<sup>29</sup> Fangwei Zhao, et al, Data Collection Practices of Mobile Applications Played by Preschool-Aged Children, JAMA Pediatrics (Sept. 8, 2020), <https://jamanetwork.com/journals/jamapediatrics/articleabstract/2769689>.

<sup>30</sup> Eric J. Johnson, Steven Bellman, Gerald L. Lohse, Defaults, Framing, and Privacy: Why Opting In-Opting Out, Marketing Letters 13 (2002), Pages 5-15, <https://link.springer.com/article/10.1023/A:1015044207315>.

<sup>31</sup> Gunawan *supra* at note 27.

---

**From:** Jamie Court [REDACTED]  
**Sent:** 11/8/2021 1:42:46 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** PRO 01-21 Comments  
**Attachments:** CommentsCCPA11-8-21FINALL.docx

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Please accept the attached comments on your rulemaking.

Thanks

Jamie Court

Jamie Court  
President | Consumer Watchdog

[REDACTED]  
6330 San Vicente Blvd Ste 250  
Los Angeles, CA 90048  
<http://ConsumerWatchdog.org>

Expose. Confront. Change.

**The information contained in this e-mail message may be privileged, confidential and protected from disclosure. It is intended only for the named addressee(s). If you are not the intended recipient, any dissemination, distribution or copying is strictly prohibited. Unless you are the addressee of this message, you may not use, copy or disclose the contents of this message to anyone. If you think that you have received this e-mail message in error, please delete the message and advise the sender by reply e-mail or by calling [REDACTED]**





November 8, 2021

California Privacy Protection Agency  
915 Capitol Mall 350 A  
Sacramento, CA 95814

Re: Invitation For Preliminary Comments On Rulemaking

Dear Commissioners,

You have asked for comments related to additional rights over a new category of information: “sensitive personal information,” specifically,

- a. What constitutes “sensitive personal information” that should be deemed “collected or processed without the purpose of inferring characteristics about a consumer” and therefore not subject to the right to limit use and disclosure.
- b. What use or disclosure of a consumer’s sensitive personal information by businesses should be permissible notwithstanding the consumer’s direction to limit the use or disclosure of the consumer’s sensitive personal information.

We are writing with concerns about one specific area: protection of consumers from the commodification of their driving data.

Personal data collected by our cars is the new gold rush of the auto industry. Cars collect more data than our phones. As Bill Hanvey writes in the *New York Times*: “You may or may not choose to share your data with these services. But while you can turn off location data on your cellphone, there’s no opt-out feature for your car.” (Bill Hanvey, “Your Car Knows When You Gain Weight,” *New York Times*, May 20, 2019)

The California Privacy Rights Act was intended to limit the use of data about driving habits with regard to “precise geolocation” and allow consumers to opt out of its sharing and sale.

**First, tracking of a driver’s precise geolocation infers characteristics about drivers and must be subject to the right to limit use and disclosure.** Car companies’ tracking of our precise geolocation allows for inference of consumer behaviors—everything from what they eat or drink to who they communicate with—and is currently used for marketing products, government and corporate surveillance, and insurance purposes.

In 2019, the president of the Auto Care Association wrote in the *New York Times*, “They know how fast we drive, where we live, how many children we have — even financial information. Connect a phone to a car, and it knows who we call and who we text.”

Cars record geolocation every few minutes, some every few seconds, according to the *Washington Post*, which had to hack its way into a Chevy to find out what kind of data was

**EXPOSE. CONFRONT. CHANGE.**

4530 San Vicente Blvd, Suite 130 Los Angeles, CA 90048

tel: 310-392-0522 • Fax: 310-392-8874

[www.ConsumerWatchdog.org](http://www.ConsumerWatchdog.org)

collected. Inside, the travels of a total stranger were reconstructed, including trips to certain gas stations and restaurants. (Geoffrey A. Fowler, “What does your car know about you? We hacked a Chevy to find out,” *Washington Post*, December 17, 2019.)

Consumer data gets into the hands of third-parties. The *Washington Post* report found that info from Chevy’s OnStar Service is directly fed to apps for Dominos, IHOP, and Shell, among others. Geolocation data buyers include energy companies and retailers like Starbucks and McDonalds, so they can better know when a person is likely to buy a cup of coffee or meal, according to Forbes. These companies know that our car data is the key to unlocking our consuming behavior. (Sarwant Singh, “Are car companies going to profit from your driving data?,” *Forbes*, Nov 6, 2017).

Data miner Wejo touts its mobility data of over 10 million connected cars, which it says it can access in real time. It can even see the speed in which cars are traveling on 95 percent of roads in the U.S.

The Ulysses Group, a location-based intelligence company, said in its own documents: “Ulysses can provide our clients with the ability to remotely geolocate vehicles in nearly every country except for North Korea and Cuba on a near real time basis,” according to a company document. “Currently, we can access over 15 billion vehicle locations around the world every month,” the document adds.

About 500 companies now have our personal car data, according to Privacy4Cars, a company that seeks to delete personal car data, and that number has gone up in just a few months, from about 200.

Auto insurance companies in California are prevented by law from using telematics to determine auto insurance rates, though the companies seek such data and use it elsewhere.

California consumers need a strong opt out mechanism for the use of precise geolocation to prevent insurance companies from illegally discriminating against them in underwriting and marketing based on the neighborhoods where they travel and live. For these consumers, it is a civil rights issue. California insurance companies are precluded from basing rates on ZIP-code, but if they know precise geolocation they can “redline” neighborhoods by not marketing to certain customers online.

**Second, car manufacturers will argue that there are “legitimate operational uses” for this data that should exempt them from the requirements of the Act. The fact is there no legitimate operational use for sale or sharing of this data, or for the use of precise geolocation to the core functioning of the vehicle.**

“Legitimate operational use” of precise geolocation data should be limited to any service a consumer has purchased or agreed to that requires precise geolocation data. For example, GPS has to track your precise location, but the sale or sharing of that data should be subject to the “opt out” requirement because the sale and sharing of that data is not necessary for its operational use.

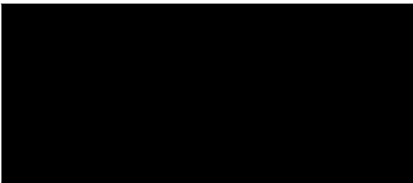


In the course of the rulemaking process we intend to offer expert testimony showing that use of precise geolocation is not necessary for the functioning of any vehicle on the road today. To the degree that “add on” services require the use of precise geolocation, the opt-out requirement for the sale and sharing of that data must still apply.

Car companies use and exploit precise geolocation data not for operations of the product they have sold, but for future business opportunities – be it selling or sharing the data for profit, or future product development. The law requires that consumers have the opportunity to opt out of its use.

Congratulations on your appointments. We look forward to working with you on creating regulations that protect consumers’ privacy.

Sincerely,



Jamie Court  
President



Justin Kloczko  
Privacy and Technology Advocate

---

**From:** Steve McCarthy [REDACTED]  
**Sent:** 11/8/2021 4:41:43 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** CRA preliminary comments  
**Attachments:** CPRA Pre-Rulemaking CRA Comments Pro 01-21 11.8.21.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Please find attached our preliminary comments on the CPRA.

Thank you.

Steve McCarthy  
Vice President, Public Policy  
California Retailers Association  
[REDACTED]







November 8, 2021

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

Dear Ms. Castanon:

On behalf of the California Retailers Association, I am pleased to submit the following preliminary comments in response to your Agency's questions related to the California Privacy Rights Act of 2020.

Our specific responses to Agency questions are listed below; however, I would like to highlight three key issues for retailers at the outset of this proceeding:

- **Automated Decision-Making:** The right to opt out from profiling and automated decision-making should be limited to processing that results in decisions regarding access to healthcare, education, employment, and other essential services and resources. A right for consumers to opt out from all profiling and automated decision-making will disadvantage small to mid-size retailers that do not possess large databases of first-party data, without any corresponding benefit to consumers, and will be a departure from emerging US norms.

In addition, many retailers will have substantial problems complying with rules on automated decision-making because as a matter of practice, vendors of AI systems do not provide information to retailer clients regarding their algorithms nor does California law obligate processors to do so. As such, all but the largest California-based retailers have no way to force vendors to provide information necessary to a consumer making the request. While large retailers may be able to require their AI or ADM vendors to provide this information contractually, small to mid-sized retailers signing standard form contracts may not have the counsel or leverage to require vendor transparency regarding algorithms or require the vendor to assist the retailer in responding to consumer inquiries. The responsibility for responding to these requests appropriately should fall to the service provider with the information and expertise respond to respond to the requesting consumer appropriately.

- **Dark Patterns:** Consumer trust is paramount for success in the retail world and "dark pattern" practices undermine trust. CRA is supportive of restrictions on behavior that seeks to defraud customers into purchasing items they did not intend or other similar dark pattern tactics. However, those regulations should be narrowly tailored to address truly fraudulent behavior and avoid unintended consequences that would impact traditional retail practices or services that consumers want and expect, such as the highlighting of promotions

and discounts consumers can avail themselves of when shopping. Such practices do not limit consumer "choice".

- **Global Opt-Out:** Though the global opt-out remains optional in nature, retailers wish to highlight concerns with the lack of universal standards for global opt-out mechanisms and the substantial implementation challenges. Global opt-out would override any granular opt-in/opt-out decisions made by the same consumer. Retailers will need to know what capabilities they need to turn on and off after receiving such an identifier.

Please see our responses to specific questions below in **BOLD**. If you have any further questions please feel free to contact Steve McCarthy at [REDACTED] or [REDACTED].

Sincerely,

[REDACTED]

Steve McCarthy  
Vice President, Public Policy

#### Responses to Questions

1. *Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses*

The CPRA directs the Agency to issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to 1) perform annual cybersecurity audits; and 2) submit to the Agency regular risk assessments regarding their processing of personal information.

Comments on the following topics will assist the Agency in creating these regulations:

- a. When a business's processing of personal information presents a "significant risk to consumers' privacy or security."

**For many retailers, a risk to consumer information occurs when large amounts of customer data are processed by third-party vendors whose primary purpose is to act as a data processor for the client, as opposed to storing the data or where data processing activities are ancillary to the greater vendor relationship. These data processors should be required to perform assessments and provide audits.**

- b. What businesses that perform annual cybersecurity audits should be required to do, including what they should cover in their audits and what processes are needed to ensure that audits are "thorough and independent."

**No comment.**

- c. What businesses that submit risk assessments to the Agency should be required to do, including what they should cover in their risk assessments, how often they should submit risk assessments, and how they should weigh the risks and benefits of processing consumers' personal information and sensitive personal information.

**Risk assessments should evaluate whether consumer data is used for the business purpose, retained for a finite period of time, and access is limited to those who require it. Where possible, the agency should eliminate unnecessary duplication of risk assessments and accept those assessments performed pursuant to comparable federal or international privacy requirements, or those that may cover multiple processing**

**1121 I Street, Suite 607 • Sacramento, CA 95814 • P: 916/443-1975 • [www.calretailers.com](http://www.calretailers.com)**



operations.

- d. When “the risks to the privacy of the consumer [would] outweigh the benefits” of businesses’ processing consumer information, and when processing that presents a significant risk to consumers’ privacy or security should be restricted or prohibited.

No comment.

## 2. Automated Decisionmaking

The CPRA provides for regulations governing consumers’ “access and opt-out rights with respect to businesses’ use of automated decisionmaking technology.”

Comments on the following topics will assist the Agency in creating these regulations:

- a. What activities should be deemed to constitute “automated decisionmaking technology” and/or “profiling”?
- b. When consumers should be able to access information about businesses’ use of automated decisionmaking technology and what processes consumers and businesses should follow to facilitate access.

**Please see initial comments on “automated decisionmaking”.**

- c. What information businesses must provide to consumers in response to access requests, including what businesses must do in order to provide “meaningful information about the logic” involved in the automated decisionmaking process.

**At most, retailers who use third-party data processors could provide categories of data used with AI algorithms and purpose for use. A retailer cannot provide meaningful information about the logic involved because the retailer does not develop the AI logic.**

- d. The scope of consumers’ opt-out rights with regard to automated decisionmaking, and what processes consumers and businesses should follow to facilitate opt outs.

**Some automated decisionmaking is tied directly to business processes and service offerings. In these situations, an opt-out is akin to a refusal to do business. Businesses should not be required to create separate products for those who opt-out. Consumers retain the effective ability to opt-out by deleting their information and declining to do business with the company.**

## 3. Audits Performed by the Agency

The CPRA gives the Agency the authority to audit businesses’ compliance with the law.

Comments on the following topics will assist the Agency in creating regulations to define its audit authority:

- a. What the scope of the Agency’s audit authority should be.

No comment.

- b. The processes the Agency should follow when exercising its audit authority, and the criteria it should use to select businesses to audit.

**Agency audits should prioritize those entities that are high-risk processors, such as companies whose core business is to process data on behalf of other companies and companies involved in large-scale processing of sensitive personal information.**

- c. The safeguards the Agency should adopt to protect consumers’ personal information from disclosure to an auditor.

**The regulations should include standards for the secure handling of consumer information, including limitations on access within the Agency, use of encryption, and ensuring data is deleted when it is no**



longer needed. The Agency should make tools available to companies selected for audit to allow for the anonymization or de-identification of records before they are delivered to the Agency. Where possible, the Agency should allow entities to fulfill audit information requests rather than sifting through company information.

4. *Consumers' Right to Delete, Right to Correct, and Right to Know*

- a. The new rules and procedures, or changes to existing rules and procedures, needed for consumers to make requests to correct inaccurate personal information.

**Retailers should be allowed to offer both online and offline customer service options to make corrections. Not all retailers may be able to offer electronic service. In addition, there should be a reasonable amount of time for retailers to make corrections or request extensions as necessary.**

**Consumer correction requests should be accompanied with evidence that proves the consumer's factual information is false. Businesses should not be required to undertake their own research or reviews, nor should "correction" requests include subjective inferences or conclusions about matters such as customer behavior.**

- b. How often, and under what circumstances, a consumer may request a correction to their personal information.

**Requests should be limited to no more than once per day, to protect against hackers using automated systems to burden businesses with requests.**

- c. How a business must respond to a request for correction, including the steps a business may take to prevent fraud.

**The request should be accompanied by identity verification with at least two data points chosen at the retailer's discretion before the retailer may proceed with changes. The Agency may consider including a list of acceptable data points retailers and other businesses may choose. Requests should be limited to consumers themselves or herself or another party with power of attorney.**

- d. When a business should be exempted from the obligation to take action on a request because responding to the request would be "impossible, or involve a disproportionate effort" or because the information that is the object of the request is accurate.

**Retailers have multiple different places where data are kept or stored, but there are primary data stores that constitute a live "master record" from which consumer information is transmitted. Corrections should be required only to that master record. Data that is difficult to access and rarely used, including archived data stores, previous backups, and disconnected systems should be exempt from correction requirements.**

- e. A consumer's right to provide a written addendum to their record with the business, if the business rejects a request to correct their personal information.

**No Comment.**

5. *Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information*

The CCPA gives consumers the right to opt out of the sale of their personal information by covered businesses.<sup>28</sup> In 2020, the Attorney General adopted regulations to implement consumers' right to opt out of the selling of their personal data under the CCPA. The CPRA now provides for additional rulemaking to update the CCPA rules on the right to opt-out of the sale of personal information, and to create rules to limit the use of sensitive personal information, and to account for other amendments.

Comments on the following topics will assist the Agency in creating these regulations:

**1121 I Street, Suite 607 • Sacramento, CA 95814 • P: 916/443-1975 • [www.calretailers.com](http://www.calretailers.com)**



- a. What rules and procedures should be established to allow consumers to limit businesses' use of their sensitive personal information.

**Retailers should have an exception for the use of precise geolocation that is directly related to the retailer fulfilling its obligations to deliver purchases or information about purchases customers have made (e.g., curbside or store pickup), or for other operational purposes (e.g., resource planning within stores based on in-store traffic patterns).**

- b. What requirements and technical specifications should define an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information.

**Please see comments above regarding "global opt-out".**

- c. What technical specifications should be established for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age?

**Any age signal should be universally accepted, identifiable, and should not indicate precise age but perhaps an age range.**

- d. How businesses should process consumer rights that are expressed through opt-out preference signals?

**No comment.**

- e. What businesses should do to provide consumers who have previously expressed an opt-out preference via an opt-out preference signal with the opportunity to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information.

**The selection of more granular preferences with an entity should override the general signal. Otherwise, retailers and others will face a constant challenge of tracking and responding to general preferences and the consumer's own granular preferences.**

#### *6. Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information*

The CCPA gives businesses certain responsibilities, and consumers certain rights, related to consumers' personal information. The CPRA amends the CCPA to give consumers additional rights over a new category of information: "sensitive personal information," and directs the Agency to amend existing regulations and/or issue new regulations to implement these rights. These rights include the new right to limit the use and disclosure of sensitive personal information discussed above.

Comments on the following topics will assist the Agency in creating regulations on this topic:

- a. What constitutes "sensitive personal information" that should be deemed "collected or processed without the purpose of inferring characteristics about a consumer" and therefore not subject to the right to limit use and disclosure.

**Data used solely for the purposes of establishing identity, and data that is reasonably necessary to provide the service requested by the consumer.**

- b. What use or disclosure of a consumer's sensitive personal information by businesses should be permissible notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information.



**Retailers should be able to use geolocation for the purpose of providing services, and anything required to provide those services, to a customer pursuant to a contract or other purchasing arrangement.**

*7. Information to Be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)*

When businesses are required to disclose specific pieces of information to a consumer, the CPRA generally requires the disclosure to cover the 12 months prior to a consumer's request. However, for all information processed on, or after January 1, 2022, consumers may request, and businesses must disclose, information beyond the 12-month window subject to the exception described in a. below.

Comments on the following topic will assist the Agency in creating regulations on this topic:

What standard should govern a business's determination that providing information beyond the 12-month window is "impossible" or "would involve a disproportionate effort."

**Retrieval and production of such information may be impossible and would certainly require a disproportionate amount of effort if it is located in a non-active or downstream location. This includes information in Service Provider locations/data stores and information that has been de-identified and commingled with other information for analytics purposes.**

**Relevance of specific information to the purpose of the request should also be a factor in determining whether it should be produced.**

*8. Definitions and Categories*

The CCPA and CPRA provide for various regulations to create or update definitions of important terms and categories of information or activities covered by the statute.

Comment on the following topics will assist the Agency in deciding whether and how to update or create these definitions and categories:

- a. Updates or additions, if any, that should be made to the categories of "personal information" given in the law.

**No comment.**

- b. Updates or additions, if any, that should be made to the categories of "sensitive personal information" given in the law.

**No comment.**

- c. Updates, if any, to the law's definitions of "deidentified" and/or "unique identifier." Changes, if any, that should be made to the definition of "designated methods for submitting requests" to obtain information from a business.

**Do not require more than two designated methods (one online; one with a customer service rep)**

- d. Further defining the business purposes for which businesses, service providers, and contractors may combine consumers' personal information that was obtained from different sources.

**Retailers and their vendors should be allowed to combine such information where it is necessary to fulfill contractual obligations to a customer (e.g., purchase fulfillment), and for product and service improvement purposes. This will be important to avoid disadvantaging small- to mid-sized retailers that lack the large databases of first party data held by large entities.**

- e. The changes, if any, that should be made to further define when a consumer



“intentionally interacts” with a person.

- f. The changes, if any, that should be made to further define “precise geolocation.”

**No comment.**

- g. What definition of “specific pieces of information obtained from the consumer” the Agency should adopt.

**No comment.**

- h. The regulations, if any, that should be adopted to further define “law enforcement agency-approved investigation.”

**No comment.**

- i. The regulations, if any, that should be adopted to further define “dark patterns.”

**Please see comments at the top on “dark patterns”.**

#### *9. Additional Comments*

Please provide any additional comments you may have in relation to the Agency’s initial rulemaking.

**No Comment.**





---

**From:** Ridhi Shetty [REDACTED]  
**Sent:** 11/8/2021 2:00:28 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Cody Venzke [REDACTED]  
**Subject:** PRO 01-21: Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020  
**Attachments:** CDT Comments to Cal. Privacy Protection Agency.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Dear Debra Castanon,

The Center for Democracy & Technology respectfully submits the attached comments in response to PRO 01-21, the Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Protection Act of 2020.

Best regards,  
Cody Venzke and Ridhi Shetty

**Ridhi Shetty** | Policy Counsel, Privacy & Data Project  
Center for Democracy & Technology [cdt.org](https://cdt.org)  
E: [REDACTED] P: [REDACTED] [she/her/hers]

Check out **CDT's podcast, Tech Talks**, where we discuss current tech and internet policy topics and explain how they affect our daily lives. Listen and subscribe using [SoundCloud](#), [iTunes](#), and [Google Play](#), as well as [Stitcher](#) and [TuneIn](#).



***Via email.***

*November 8, 2021*

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

Re: Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (PRO 01-21)

## **I. Introduction**

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the invitation of the California Privacy Protection Agency (“Agency”) for preliminary comments on proposed rulemaking under the California Privacy Rights Act (CPRA). CDT is a nonpartisan, nonprofit 501(c)(3) organization that is dedicated to advancing civil liberties and civil rights in the digital age and challenging exploitative and discriminatory uses of technology. CDT’s focus includes privacy and the responsible use of data and algorithmic decision-making by commercial enterprises and in the administration of government-funded programs and services.

These comments will focus on areas where commercial data practices implicate fundamental rights, including private, for-profit entities that contract with and provide services for governmental entities. Specifically, these comments call on the Agency to help:

- equip consumers to hold automated decision-making systems accountable for bias and denying access to fundamental rights;
- establish sufficient standards for deidentification of data and restrictions on its use;
- ensure appropriate training for staff that use algorithmic systems;
- ensure that businesses’ collection and use of sensitive personal information are subject not only to an opt-out right, but also to additional safeguards that restrict the collection and processing of such information; and
- avoid unintended consequences for businesses that provide services to governmental entities, by ensuring that CPRA regulations appropriately distinguish what rights and duties apply with respect to data collected and processed by such service provider.



**II. The Agency should ensure that consumers have access to information about automated and algorithmic decision-making to guard against algorithmic bias and protect their fundamental rights.**

The CPRA requires the Agency to promulgate regulations that govern “access and opt-out rights with respect to businesses’ use of automated decision-making technology, including profiling” and that require businesses to respond to consumers’ access requests with “meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.”<sup>1</sup> The CPRA also elaborates on what “meaningful information” should entail. The regulations must require businesses to provide notices and information “in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer.”<sup>2</sup>

The right to access information about automated decision-making (ADM) should include information necessary for consumers to understand the decision that was made and how it was made. At minimum, the right to access should include the principal reasons for adverse actions, specific data used in the decision, and how the system arrived at its output.<sup>3</sup> Moreover, explanations of data and decisions should be “psychologically coherent,” meaning that the information provided to consumers should be more than a list of variables, but a humanly intelligible explanation of what factors distinguished one decision from another.<sup>4</sup> Further, the explanation should be “faithful” to the system, reflecting how the system actually generated its particular decision.<sup>5</sup>

The CPRA does not define “automated decision-making,” though it does define “profiling” as the “automated processing of personal information ... to analyze or predict aspects concerning [a] natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.”<sup>6</sup> Regulations governing access to the “use of automated decision-making technology” must encompass *both* the algorithm and other technical information and the overall decision-making context in which the technology is used. That is, the regulations should encompass two components: (a) information about the design, training data and methods, logic, input, and output of the algorithm involved in the decision-making process, and (b) the overall decision-

<sup>1</sup> Cal. Civ. Code §1798.185(16).

<sup>2</sup> Cal. Civ. Code §1798.185(6).

<sup>3</sup> Ctr. for Democracy & Tech., Comments on Financial Institutions’ Use of Artificial Intelligence, Including Machine Learning 2-4 (Jul. 1, 2021), <https://cdt.org/wp-content/uploads/2021/07/2021-07-01-CDT-Request-for-Information-and-Comment-on-Financial-Institutions-Use-of-Artificial-Intelligence-including-Machine-Learning.pdf> [hereinafter “Comments on Financial Institutions’ AI Use”].

<sup>4</sup> Michael Yang, *Explaining “Explainability”*, CTR. FOR DEMOCRACY & TECH. (Aug. 9, 2021), <https://cdt.org/insights/explaining-explainability>.

<sup>5</sup> *Id.*

<sup>6</sup> Cal. Civ. Code §1798.140(z).



making system in which the algorithm is embedded, including the role of humans in deploying the algorithm and the interpretation and use of the algorithm's output.<sup>7</sup>

Moreover, the CPRA regulations should encompass automated decision-making systems whenever they play a role in the decision-making process, even where an algorithm's decision is not final and is subject to human review. Human involvement alone does not ensure that ADM systems are being properly used or reviewed for disparate impact.<sup>8</sup> In fact, people may default to the recommendations or outcomes of automated processes rather than as an initial input to inform next steps to achieve fairer and more beneficial outcomes.

In developing regulations, the Agency should ensure that consumers will have access to the information needed to detect the most concerning practices and harms of automated decision-making (ADM) and algorithmic systems,<sup>9</sup> including in particular "where the use of biased AI could raise human rights concerns or violate anti-discrimination laws."<sup>10</sup> Specifically, the regulation should enable access to information that will reveal disparate impact, as ADM systems often execute decision-making policies in a facially neutral manner that makes it harder to detect discriminatory effects.<sup>11</sup> Three areas in which ADM is increasingly being deployed -- housing, employment, and education -- demonstrate the importance of ensuring the Agency's regulations provide access to the information needed to determine the existence of discrimination:

---

<sup>7</sup> HANNAH QUAY-DE LA VALLEE AND NATASHA DUARTE, CTR. FOR DEMOCRACY & TECH., ALGORITHMIC SYSTEMS IN EDUCATION: INCORPORATING EQUITY AND FAIRNESS WHEN USING STUDENT DATA 6-8 (2019), <https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf> [hereinafter "ALGORITHMIC SYSTEMS IN EDUCATION"].

<sup>8</sup> *Id.* at 9, 13 (describing how dropout early warning systems have been misused or caused necessary resources to be misdirected).

<sup>9</sup> As described below, the CPRA does not define "automated decision-making" and it does not refer to algorithmic decision-making or algorithmic systems. However, an "algorithm" is a "process performed by a computer to answer a question or carry out a task, such as sorting students into schools or classifying social media posts," and "algorithmic decision-making" is "a decision system that involves algorithms, human decision-makers, legal and social structures, and other forces." *Id.* at 6-8. Although "automated decision-making" and "algorithmic decision-making" are not identical, there is substantial overlap between the terms. See European Parliamentary Research Service, Understanding Algorithmic Decision-Making 3-4 (2019), [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS\\_STU\(2019\)624261\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf); MARK MACCARTHY, BROOKINGS, FAIRNESS IN ALGORITHMIC DECISION-MAKING (2019), <https://www.brookings.edu/research/fairness-in-algorithmic-decision-making>. We encourage the Agency to include algorithmic decision-making within the scope of its rulemaking.

<sup>10</sup> Ctr. for Democracy & Tech., Comments on the National Institute for Standards and Technology's Proposal for Identifying and Managing Bias in Artificial Intelligence 1 (Sept. 10, 2021), <https://cdt.org/wp-content/uploads/2021/09/Comments-NIST-AI-Special-Publication-1270-CLEAN-Google-Docs.pdf> [hereinafter "Comments on NIST Proposal"].

<sup>11</sup> Ctr. for Democracy & Tech., Comments to the U.S. Department of Housing and Urban Development on Reconsideration of HUD's Implementation of the Fair Housing Act's Disparate Impact Standard 6 (Oct. 18, 2019), <https://cdt.org/wp-content/uploads/2019/10/Comments-opposing-HUD-NPRM-algorithmic-defenses.pdf> [hereinafter "Comments to HUD"].



- **Housing:** Housing providers use ADM systems that evaluate similar types of data as are used in consumer finance decisions.<sup>12</sup> This data can include credit, education, employment, and criminal history; income; public records; and banking, purchase, and web activity.<sup>13</sup> Yet some of this data may be proxies for racism or ableism or lead to disparate impact and inequity in housing for marginalized communities. For example, the ostensible purpose of looking at criminal history is to avoid exposing current residents to new residents who may pose a threat. But the U.S. Department of Housing and Urban Development has advised that blanket prohibitions based on criminal records can be discriminatory.<sup>14</sup>

Challenging the outcomes of ADM systems used in housing decisions requires access to information about how the applicant's data was processed through ADM and the extent to which ADM influences the ultimate decision.<sup>15</sup> Without access to this information, applicants cannot show they were denied housing based on proxies for protected traits, flag risks of disparate impact, or offer additional information that shows why they would in fact be able to meet their obligations should they be approved.<sup>16</sup> Thus, to address algorithmic bias in housing, it is crucial that consumers are provided access to information about what data is used for decision-making and how ADM processes this data, with a meaningful chance to respond.

- **Hiring:** ADM is also increasingly common in hiring processes and has had disparate impacts on job applicants in many ways.<sup>17</sup> For example, CDT testified before the California Department of Fair Employment and Housing this year about how various algorithm-driven hiring decisions can worsen hiring disparities for job applicants with disabilities.<sup>18</sup> Resume parsing tools have rejected applicants whose resumes lack language that the tools were designed to or learned to look for, or that had employment gaps that may be due to disability or extended illness,

<sup>12</sup> Comments on Financial Institutions' AI Use, *supra* note 3, at 2; Lydia X.Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, CTR. FOR DEMOCRACY & TECH. (Jul. 7, 2021),

<https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/>.

<sup>13</sup> Comments on Financial Institutions' AI Use, *supra* note 3, at 2.

<sup>14</sup> U.S. Dep't of Hous. and Urban Dev., Office of General Counsel Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions, Apr. 4, 2016, [https://www.hud.gov/sites/documents/HUD\\_OGCGUIDAPPFHASTANDCR.PDF](https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF).

<sup>15</sup> Comments to HUD, *supra* note 11.

<sup>16</sup> *Id.*

<sup>17</sup> *Hearing on Algorithms and Bias Before the Cal. Dep't of Fair Employment and Hous.*, (Apr. 30, 2021) (testimony of Lydia X.Z. Brown), <https://cdt.org/wp-content/uploads/2021/04/California-Fair-Employment-Housing-Council-Public-Hearing-Lydia-X-Z-Brown-statement-30-Apr-2021.pdf> [hereinafter "Testimony of Lydia X.Z. Brown"]; CTR. FOR DEMOCRACY & TECH., ALGORITHM-DRIVEN HIRING TOOLS: INNOVATIVE RECRUITMENT OR EXPEDITED DISABILITY DISCRIMINATION? 10 (2020), <https://cdt.org/wp-content/uploads/2020/12/Full-Text-Algorithm-driven-Hiring-Tools-Innovative-Recruitment-or-Expedited-Disability-Discrimination.pdf> [hereinafter "ALGORITHM-DRIVEN HIRING TOOLS"].

<sup>18</sup> Testimony of Lydia X.Z. Brown, *supra* note 17.



pregnancy, or caregiving needs.<sup>19</sup> Gamified aptitude tests, video interview analysis, and personality tests have assessed characteristics or behaviors that often are not relevant to how applicants would be required to perform on the job or would perform if they received accommodations in the workplace.<sup>20</sup> Thus, applicants have been denied job opportunities not because they cannot perform, but because data related to their traits, behaviors, or other factors affected by protected characteristics do not mirror data about “high-performing” employees.

When employers use these types of hiring technologies to assess applicants, they tend not to give applicants advance notice about the manner in which their application materials or they personally will be evaluated, or the criteria based on which the applicants may be disqualified.<sup>21</sup> The introduction of ADM to the hiring process has also made it less likely for applicants to access information about why they have received an adverse decision. Similar to the housing context, without being provided with such information, they will not be able to challenge discriminatory hiring decisions under laws such as Title VII,<sup>22</sup> the Americans with Disabilities Act,<sup>23</sup> or state employment discrimination law.<sup>24</sup>

- **Education:** K-12 educational agencies and institutions are navigating a growing market of ADM tools designed to transform a wide range of district and school functions such as assigning students to schools, preventing dropout, and keeping students safe.<sup>25</sup> ADM is also used to scan students’ documents and messages for sexual material and signs of self-harm, bullying, or drug or alcohol use<sup>26</sup> and initiate intervention by administrators or even law enforcement.<sup>27</sup> These decisions can significantly affect students’ experiences, relationships, and future opportunities, whether by determining which school a student attends or by deciding whether or not that student is a threat to school safety.

---

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

<sup>21</sup> ALGORITHM-DRIVEN HIRING TOOLS, *supra* note 17, at 10; MIRANDA BOGEN & AARON RIEKE, UPTURN, HELP WANTED: AN EXAMINATION OF HIRING ALGORITHMS, EQUITY, AND BIAS (2018), <https://www.upturn.org/reports/2018/hiring-algorithms/>.

<sup>22</sup> 42 U.S.C. §2000e et seq.

<sup>23</sup> 42 U.S.C. §12111 et seq.

<sup>24</sup> Cal. Gov’t Code §12940.

<sup>25</sup> ALGORITHMIC SYSTEMS IN EDUCATION, *supra* note 7, at 6-8.

<sup>26</sup> Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning — and Now Won’t Leave*, THE 74 (Sept. 14, 2021), <https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/>.

<sup>27</sup> Liz Bowie, *Baltimore City Student Laptops are Monitored for Mentions of Suicide. Sometimes, The Police are Called.*, BALT. SUN (Oct. 12, 2021), <https://www.baltimoresun.com/education/bs-md-laptops-monitoring-20211012-a2j3vstyijhhij36n57ri5zdhi-story.html>.



Again, however, the use of ADM can lead to discrimination. For example, schools are increasingly using facial recognition technology, which relies on ADM, for proctoring exams, protecting student safety, monitoring unusual behavior, or even enforcing health and safety measures such as social distancing.<sup>28</sup> Facial recognition technology, however, disproportionately misidentifies students of color, especially Black students,<sup>29</sup> and may further marginalize them by subjecting them to increased interactions with police and school disciplinary systems.<sup>30</sup> Proctoring software struggles to recognize students of color, especially Black students,<sup>31</sup> and disproportionately flags the behavior of students with disabilities, whose movements or accommodations may be flagged by the algorithm as suspicious.<sup>32</sup> The Agency's regulations should ensure that students and their parents have access to sufficient information about the use of these types of technologies, how they work, how the algorithms were trained, how the ADM tool is used in the overall decision-making process, and other information necessary to determine whether use of the ADM is resulting in bias or discrimination.

**III. The regulations should articulate a high bar for truly deidentifying data and recognize that data harms extend beyond individuals by placing restrictions on the use of deidentified data.**  
***Responsive to Question 8(c).***

The CPRA and its predecessor, the California Consumer Privacy Act (CCPA), apply only to information that "could reasonably be linked, directly or indirectly, with a particular consumer or household,"

---

<sup>28</sup> Rebecca Heilweil, *The Dystopian Tech That Companies Are Selling to Help Schools Reopen Sooner*, RECODE (Aug. 14, 2020), <https://www.vox.com/recode/2020/8/14/21365300/artificial-intelligence-ai-school-reopening-technology-covid-19>; Alfred Ng, *Facial Recognition in Schools: Even Supporters Say It Won't Stop Shootings*, CNET (Jan. 24, 2020), <https://www.cnet.com/features/facial-recognition-in-schools-even-supporters-say-it-wont-stop-shootings>; Emily Tate, *Safety in Mind, Schools Turn to Facial Recognition Technology. But at What Cost?*, EdSURGE (Jan. 31, 2019), <https://www.edsurge.com/news/2019-01-31-with-safety-in-mind-schools-turn-to-facial-recognition-technology-but-at-what-cost>.

<sup>29</sup> SHOBITA PARTHASARATHY ET AL., UNIVERSITY OF MICHIGAN, *CAMERAS IN THE CLASSROOM* 31 (2021), [https://stpp.fordschool.umich.edu/sites/stpp/files/uploads/file-assets/cameras\\_in\\_the\\_classroom\\_full\\_report.pdf](https://stpp.fordschool.umich.edu/sites/stpp/files/uploads/file-assets/cameras_in_the_classroom_full_report.pdf).

<sup>30</sup> *Id.* at 32, 44.

<sup>31</sup> Shea Swauger, *Software That Monitors Students During Tests Perpetuates Inequality And Violates Their Privacy*, MIT TECH. REV. (Aug. 7, 2020), <https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics>; Shea Swauger, *Our Bodies Encoded*, Hybrid Pedagogy (Apr. 2, 2020), <https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education>.

<sup>32</sup> NAT'L DISABLED LAW STUDENTS ASSOCIATION, *REPORT ON CONCERNS REGARDING ONLINE ADMINISTRATION OF BAR EXAMS 3-4*, 14-22 (2020), [https://ndlsa.org/wp-content/uploads/2020/08/NDLSA\\_Online-Exam-Concerns-Report1.pdf](https://ndlsa.org/wp-content/uploads/2020/08/NDLSA_Online-Exam-Concerns-Report1.pdf) ("I am definitely very concerned that the AI will include a racial and/or disability bias."); Mary Retta, *Exam Surveillance Tools Monitor, Record Students During Tests*, TEEN VOGUE (Oct. 26, 2020), <https://www.teenvogue.com/story/exam-surveillance-tools-remote-learning> ("Neuro-divergent students such as myself, who exhibit behavior related to our condition like high rates of eye movement, are consistently punished. This software serves to disproportionately penalize those whose behaviors deviate in any way from what is considered the 'norm.'").



which both laws label “personal information.”<sup>33</sup> Neither act provides protections for “deidentified” information — or information that cannot be linked to a particular person.<sup>34</sup> Without those protections, supposedly deidentified data can pose risks for both individuals and groups. The Agency should promulgate regulations that take three steps to help ensure that “deidentified” data remains deidentified and to limit secondary uses of even deidentified data.

First, the Agency should ensure that deidentified data stays that way. Reidentification of data has become increasingly feasible as the amount of publicly available data has increased, creating privacy risks for individuals. For example, just four points of “anonymous” location data are enough to uniquely identify individuals 95 percent of the time,<sup>35</sup> and research has demonstrated that health records may be reidentified by cross-referencing publicly available records.<sup>36</sup> Complex datasets with increasing numbers of data points can pose significant obstacles to truly deidentifying data.<sup>37</sup>

The CPRA requires a business to take “reasonable measures” to avoid reidentification, “publicly commit[ting] . . . not to attempt to reidentify the information,” and contractually ensuring that recipients of the deidentified data are bound by the same obligations.<sup>38</sup> Regulations under the CPRA should make explicit that “reasonable measures” include technical safeguards to prevent reidentification of individuals and procedural safeguards, including internal policies that prohibit reidentification.

Second, businesses should be required to describe their methods for deidentifying data in their risk assessments under the CPRA, accompanied by an assessment of the risk of reidentification and the measures taken to mitigate that risk.<sup>39</sup> As the National Institute of Standards and Technology has recognized, “[b]ecause an important goal of de-identification is to prevent unauthorized re-identification, such attempts [at re-identification] are sometimes called re-identification attacks,” and

---

<sup>33</sup> Cal. Civ. Code § 1798.140(o) (effective Jan. 1, 2020); *id.* § 1798.140(v) (operative Jan. 1, 2023); *accord* 15 U.S.C. § 6501(8) (defining “personal information” under the Children’s Internet Privacy Protection Act); 34 C.F.R. § 99.3 (defining “personally identifiable information from education records” under the Family Educational Rights and Privacy Act); 45 C.F.R. § 160.103 (defining “individually identifiable health information” under the Health Insurance Portability and Accountability Act)

<sup>34</sup> Cal. Civ. Code § 1798.140(h) (effective Jan. 1, 2020); *id.* § 1798.140(m) (operative Jan. 1, 2023).

<sup>35</sup> Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REP. (2013), <https://www.nature.com/articles/srep01376>.

<sup>36</sup> CHRIS CULNANE ET AL., HEALTH DATA IN AN OPEN WORLD, ARXIV (2017), <https://arxiv.org/abs/1712.05627>.

<sup>37</sup> Joseph Jerome, *De-Identification Should Be Relevant to a Privacy Law, But Not an Automatic Get-Out-of-Jail-Free Card*, CTR. FOR DEMOCRACY & TECH. (Apr. 1, 2019), <https://cdt.org/insights/de-identification-should-be-relevant-to-a-privacy-law-but-not-an-automatic-get-out-of-jail-free-card/>.

<sup>38</sup> Cal. Civ. Code § 1798.140(m) (operative Jan. 1, 2023).

<sup>39</sup> See Joseph Jerome, *The Washington Privacy Act Raises Important Considerations for Comprehensive Privacy Proposals*, CTR. FOR DEMOCRACY & TECH. (Feb. 7, 2019), <https://cdt.org/insights/the-washington-privacy-act-raises-important-considerations-for-comprehensive-privacy-proposals>.



are akin to cybersecurity risks.<sup>40</sup> To help mitigate those risks, “it is important to understand the techniques and business rules that are being applied when taking steps to remove personally identifiable information” because “depending on the approach, data may still be recoverable.”<sup>41</sup>

Finally, the regulations should require deidentified data to be accompanied by use and redisclosure limitations. Even data that cannot be reidentified may still pose harms for groups and the people that compose them. Deidentified data may be used to train algorithmic or automated decision-making, which may then perpetuate harms on populations due to biases embedded in the training data.<sup>42</sup> Deidentified data has been used broadly for ADM in critical fields such as housing,<sup>43</sup> credit,<sup>44</sup> and education.<sup>45</sup> For example, in education, dropout early warning systems may involve machine learning trained on data that encompasses a broad range of factors like attendance, behavioral information, home and family stability, demographics, and how the student is faring relative to similarly situated students.<sup>46</sup> The use of deidentified or aggregate datasets may result in “large disparities in how the software treats students of different races,” which may directly impact students’ educational opportunities.<sup>47</sup>

Secondary uses of deidentified data may also pose challenges to maintaining public trust in the stewards of the data or ensuring that an individual’s consent is meaningfully respected. Limiting sharing and reuse helps protect against reidentification, harmful secondary uses, and violations of individuals’ original consent.<sup>48</sup> Secondary uses may include data that is repurposed and aggregated for research. Algorithmic or automated decision-making systems often rely on repurposed data from disparate, integrated data sets to identify unanticipated patterns, which incentivizes data holders to integrate and repurpose data sets without knowing in advance how the data will be used.<sup>49</sup> While repurposing data may be useful for gaining insights and improving systems, it complicates other data

<sup>40</sup> SIMSON GARFINKEL, NAT’L INSTITUTE OF STANDARDS & TECH., DE-IDENTIFICATION OF PERSONAL INFORMATION 9-10 (2015), <https://csrc.nist.gov/publications/detail/nistir/8053/final>.

<sup>41</sup> ELIZABETH LAIRD AND HANNAH QUAY-DE LA VALLEE, CTR. FOR DEMOCRACY & TECH., BALANCING THE SCALE OF STUDENT DATA DELETION AND RETENTION IN EDUCATION 14 (2019), <https://cdt.org/wp-content/uploads/2019/03/Student-Privacy-Deletion-Report.pdf>.

<sup>42</sup> Comments on NIST Proposal, *supra* note 10, at 2.

<sup>43</sup> Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, CTR. FOR DEMOCRACY & TECH. July 7, 2021), <https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice>.

<sup>44</sup> Comments on Financial Institutions’ AI Use, *supra* note 3, at 5-6.

<sup>45</sup> RELMAN COLFAX, FAIR LENDING MONITORSHIP OF UPSTART NETWORK’S LENDING MODEL 18-22 (2021), [https://www.reلمانlaw.com/media/news/1089\\_Upstart\\_Initial\\_Report\\_-\\_Final.pdf](https://www.reلمانlaw.com/media/news/1089_Upstart_Initial_Report_-_Final.pdf).

<sup>46</sup> ALGORITHMIC SYSTEMS IN EDUCATION, *supra* note 7, at 9.

<sup>47</sup> Todd Feathers, *Major Universities Are Using Race as a “High Impact Predictor” of Student Success*, THE MARKUP (Mar. 2, 2021), <https://themarkup.org/news/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success>.

<sup>48</sup> BALANCING THE SCALE OF STUDENT DATA DELETION AND RETENTION IN EDUCATION, *supra* note 41, at 16.

<sup>49</sup> *Id.* at 15.



ethics issues like transparency, community engagement, and consent.<sup>50</sup> Similarly, deidentifying and repurposing education data for commercial purposes may jeopardize public trust.<sup>51</sup>

**IV. The CPRA addresses training to handle consumer inquiries about how consumers may exercise their data rights, but businesses should train employees to also ensure that data is used responsibly. *Responsive to Question 9.***

The CCPA regulations and the CPRA require businesses to “establish, document, and comply with a training policy” that informs “all individuals responsible for handling consumer inquiries” about businesses’ practices and compliance with the CPRA and about “how to direct consumers to exercise their rights” under the CPRA.<sup>52</sup> While employees should be able to respond to inquiries about how businesses are complying with the CPRA and how consumers may exercise agency of their own data, this is not enough. Employees must be equipped to hold businesses accountable for the data practices in which employees may also be engaging.

The CPRA regulations should expand training requirements to educate employees about the ethical use of data.<sup>53</sup> Training should inform employees about restrictions on their access to consumer data and on secondary uses of consumer data.<sup>54</sup> It should ensure that employees understand the purposes for which data may be disclosed, the necessity of limits on redisclosure, and ramifications for failing to adhere to those limits.<sup>55</sup> Deidentification must be carried out only by specific employees with relevant expertise and training in how reidentification of deidentified data can occur, how to ensure sufficient deidentification to reduce the risk of reidentification, how to recognize when data should be thoroughly destroyed, and how to effectively carry out data destruction techniques.<sup>56</sup> Finally, changes to data practices may necessitate new or modified training, so these programs should be reviewed frequently and revised to ensure that employees continue to effectively protect consumer data.<sup>57</sup>

---

<sup>50</sup> *Id.*

<sup>51</sup> Benjamin Herold, *Schools Collect Tons of Student Information. Deleting It All Is a Major Challenge*, EDUCATIONWEEK (Mar. 15, 2019), <https://www.edweek.org/technology/schools-collect-tons-of-student-information-deleting-it-all-is-a-major-challenge/2019/03?cmp=SOC-SHR-FB> (“Most vendors don’t really care about data deletion, because they only want to monetize de-identified data, which most policies allow for unlimited use.”).

<sup>52</sup> Cal. Code Regs. tit. 11, §999.317(a), (g)(3); Cal. Civ. Code §1798.130(a)(6).

<sup>53</sup> See generally ELIZABETH LAIRD AND HANNAH QUAY-DE LA VALLEE, CTR. FOR DEMOCRACY & TECH., DATA ETHICS IN EDUCATION AND THE SOCIAL SECTOR: WHAT DOES IT MEAN AND WHY DOES IT MATTER? (2021), <https://cdt.org/wp-content/uploads/2021/02/2021-02-19-Data-Ethics-and-Ed-and-Social-Sector-FINAL.pdf>.

<sup>54</sup> *Id.* at 14-16.

<sup>55</sup> ELIZABETH LAIRD AND HANNAH QUAY-DE LA VALLEE, CTR. FOR DEMOCRACY & TECH., DATA SHARING AND PRIVACY DEMANDS IN EDUCATION: HOW TO PROTECT STUDENTS WHILE SATISFYING POLICY AND LEGAL REQUIREMENTS 5-9 (2019), <https://cdt.org/wp-content/uploads/2019/11/2019-11-13-CDT-Data-Integration-Issue-Brief-Final.pdf>.

<sup>56</sup> BALANCING THE SCALE OF STUDENT DATA DELETION AND RETENTION IN EDUCATION, *supra* note 41, at 12-14.

<sup>57</sup> DATA SHARING AND PRIVACY DEMANDS IN EDUCATION, *supra* note 55, at 5-6.



**V. The right to opt out of or limit use of sensitive personal information should be accompanied by additional, necessary safeguards.**

The CCPA regulation and the CPRA require businesses to provide consumers the choice to opt out of sale and sharing of PI and limit the use and disclosure of sensitive personal information (SPI). Businesses can do so by either providing a link or method on their homepages for consumers to opt out of sharing of PI and use of SPI, or by providing the means to opt out via an opt-out preference signal.<sup>58</sup> The CPRA requires regulations to make sure that these options are easy for consumers to use, do not interfere with their online experience, and do not obstruct competition.<sup>59</sup> The CPRA regulations must also limit the use of SPI to enable consumers to “exercise their choices without undue burden” and “to prevent business from engaging in deceptive or harassing conduct,” but the CPRA also requires regulations to allow businesses “to inform consumers of the consequences” of opting out of the sale or sharing of PI or of limiting the use of SPI.<sup>60</sup>

In addition to providing an opt-out right, the CPRA also requires the Agency to issue regulations, with the goal of strengthening consumer privacy while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer’s sensitive personal information, including “[d]etermining any additional purposes for which a business may use or disclose a consumer’s sensitive personal information.”<sup>61</sup>

While the right to opt out can help consumers exercise some control over how their data is used and shared, opt-out options put the onus on consumers to protect themselves, which is less effective to protect their rights.<sup>62</sup> This burden should belong to businesses. Accordingly, the Agency should impose basic rules that limit a business’s ability to use and disclose particularly sensitive personal information. In particular, regulations must require businesses to put in place ethical use, purpose, and disclosure guardrails to protect consumers’ rights regarding the use of SPI. These protections should include:

- Prohibiting data use that harms individuals or groups;<sup>63</sup>
- Require an entity to minimize the data it collects and processes based on the purpose for which the entity needs data (e.g., to provide a product or service requested by a consumer)

<sup>58</sup> Cal. Civ. Code §1798.135(a)-(b); Cal. Code Regs. tit. 11, §999.315(a),(c),(f).

<sup>59</sup> Cal. Civ. Code §1798.185(19)(A), (20).

<sup>60</sup> Cal. Civ. Code §1798.185(a)(4)(A).

<sup>61</sup> Cal. Civ. Code §1798.185(a)(19)(B).

<sup>62</sup> Ctr. for Democracy & Tech., Comments to the Federal Trade Commission on Implementation of the Children’s Online Privacy Protection Rule, at 5, Dec. 11, 2019, <https://cdt.org/wp-content/uploads/2019/12/CDT-COPPA-2019-Rule-Review-Comments.pdf>.

<sup>63</sup> DATA ETHICS IN EDUCATION AND THE SOCIAL SECTOR, *supra* note 53, at 5.



- Prohibit unfair data practices, particularly the repurposing or secondary use or sharing of sensitive data without the express, opt-in consent of the consumer;<sup>64</sup>
- Requiring procedures for determining when data is no longer needed and for completing data destruction;<sup>65</sup>
- Prescribing procedures for accountability, redress, and mitigation of algorithm-driven disparate impact;<sup>66</sup> and
- Requiring that the process for developing an opt-out preference signal engages a wide base of stakeholders, including consumer groups, governmental entities that contract with businesses, and technology vendors, who among other considerations can collectively evaluate the merits of selective consent or global opt-out.<sup>67</sup>

The CPRA also calls for the regulatory process to solicit public participation in “[u]pdating or adding categories of personal information [and] categories of sensitive personal information to those enumerated... in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.”<sup>68</sup> Regulations must be proactive in this area, with additional safeguards to protect a wider range of SPI categories. Under the CPRA, “sensitive personal information” is PI that reveals, among other types of data, social security numbers; financial account and account log-in details; precise geolocation information; information about race, ethnicity, sexual orientation, religious or philosophical beliefs; and genetic data.<sup>69</sup> Some protected classes are included among these types of information, but CPRA regulations must recognize other protected classes as SPI, including gender identity, disability, and immigration status. In addition, some of the currently enumerated types of SPI, such as social security numbers and financial account details, reflect increased risk of financial harm to all consumers, while others reflect data about protected classes that can cause biased decision-making. The regulations should ensure that safeguards for SPI overall are tailored to the different risks involved for each type of SPI.

<sup>64</sup> DATA SHARING AND PRIVACY DEMANDS IN EDUCATION, *supra* note 55, at 14-16; ANDREW CRAWFORD AND ALICE LEITER, CTR. FOR DEMOCRACY & TECH. AND EHEALTH INITIATIVE, PROPOSED CONSUMER PRIVACY FRAMEWORK FOR HEALTH DATA 9, 11 (2021), <https://cdt.org/wp-content/uploads/2021/02/2021-02-09-CDT-and-eHI-Proposed-Consumer-Privacy-Framework-for-Health-Data-d-FINAL.pdf>.

<sup>65</sup> DATA ETHICS IN EDUCATION AND THE SOCIAL SECTOR, *supra* note 53, at 12-14.

<sup>66</sup> Comments to the U.S. Department of Education, Office of Civil Rights, Protecting Privacy Rights and Ensuring Equitable Algorithmic Systems for Transgender and Gender Non-Conforming Students, at 5, Jun. 11, 2021, <https://cdt.org/wp-content/uploads/2021/06/CDT-Title-IX-Comments-Protecting-Privacy-Rights-and-Ensuring-Equitable-Algorithmic-Systems.pdf> [hereinafter “Comments on Algorithms and Title IX”]; Comments to the U.S. Department of Education, Office of Civil Rights, on Protecting Privacy Rights and Ensuring Equitable Algorithmic Systems for Students of Color and Students with Disabilities, at 5, Jul. 23, 2021, <https://cdt.org/wp-content/uploads/2021/07/2021-07-23-CDT-Title-VI-Comments.pdf> [hereinafter “Comments on Algorithmics and Title VI”]; ALGORITHMIC SYSTEMS IN EDUCATION, *supra* note 7, at 24; Comments on Financial Institutions’ AI Use, *supra* note 3, at 2-5, 7-9; Testimony of Lydia X.Z. Brown, *supra* note 17, at 7-8; ALGORITHM-DRIVEN HIRING TOOLS, *supra* note 17, at 19-20.

<sup>67</sup> Cal. Civ. Code §1798.185(19)(A).

<sup>68</sup> Cal. Civ. Code §1798.185(a)(1).

<sup>69</sup> Cal. Civ. Code §1798.140(ae).



The CPRA regulations should also revisit how the CPRA covers inferences. In its definition of PI, the CPRA includes “[i]nferences drawn from [other types of PI] to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.” These elements can be proxies for other protected traits, so the resulting “inferences” should be recognized as SPI, not just PI.<sup>70</sup> Therefore, opt-out and other protections that the CPRA provides for SPI should extend to inferences of sensitive data and other proxies for sensitive data, subject to a disparate impact analysis.

The CPRA regulations must limit any exceptions to rights regarding SPI. The CPRA itself already creates an exception allowing the use and sharing of SPI that “is collected or processed without the purpose of inferring characteristics about a consumer,” subject to regulation, so this exception should not be expanded.<sup>71</sup> Even when a data practice is not done with the intention of inferring characteristics about a consumer, the collection, use, or disclosure of sensitive data can still harm individual consumers<sup>72</sup> and protected groups at large.<sup>73</sup> Therefore, exceptions to opt-out rights should only be considered when the business identifies a clear purpose, intended use, and demonstrable need for the data. The business must provide assurances that the data will be subject to the safeguards described above and destroyed when no longer needed, with explicit procedures for redress if these requirements are not met.

**VI. Regulations under the CPRA should avoid unintended consequences that would result from requiring service providers for governmental entities to respond to consumer requests under the CPRA.**

For-profit and not-for-profit entities provide data processing to support critical governmental services, such as through cloud infrastructure, videoconferencing, web hosting, and supporting remote learning. It is critical that the Agency’s regulations continue to recognize and accommodate the role of service providers for governmental entities and not inadvertently subject the governmental data they hold to rules directed toward private, for-profit entities.

---

<sup>70</sup> See e.g., Allie Reed, *Medicare AI Will Infer Race to Close Health Equity Gap*, BLOOMBERG (Aug. 5, 2021, 5:30 AM), <https://news.bloomberglaw.com/health-law-and-business/medicare-ai-will-infer-race-to-close-health-equity-gap>.

<sup>71</sup> Cal. Civ. Code §§1798.121(d) and 1798.185(a)(19)(C)(iv).

<sup>72</sup> Elizabeth Laird, *Endangering Student Privacy in the Name of School Safety*, CTR. FOR DEMOCRACY & TECH. (Sept. 10, 2018), <https://cdt.org/insights/endangering-student-privacy-in-the-name-of-school-safety/>.

<sup>73</sup> Comments on Algorithms and Title IX, *supra* note 66; Comments on Algorithms and Title VI, *supra* note 66.



The distinction between a “service provider” and a “business” is well established in privacy law.<sup>74</sup> The distinction is critical to ensuring that there are clear duties among the entities that are ultimately responsible for personal information—a “business” under the CCPA and CPRA—and the entities that they contract with to process the information—a “service provider.”<sup>75</sup>

That distinction is particularly important for service providers for governmental entities. Governmental entities such as schools contract with private businesses to provide services such as cloud storage, student information systems, educational applications, or access to online services. Data held on behalf of governmental entities may be necessary to support governmental services, be particularly sensitive, or be subject to specific laws regarding public access and privacy;<sup>76</sup> consequently, it is important that the responsible governmental entity retains ultimate control over the governmental data held by its contractors.

Recognizing the unique role of service providers for governmental entities, the regulations under the CCPA clarified that a service provider for a nonprofit or governmental entity is not subject to the “full panoply of CCPA obligations,”<sup>77</sup> but rather must collect, use, and destroy data only as directed by the controlling nonprofit or governmental entity.<sup>78</sup> The California Attorney General explained the importance of the rule:

[A] public school district may use a service provider to secure student information, including each student’s grades and disciplinary record. Without this regulation, service providers used by public and nonprofit entities may be required to disclose or delete records in response to consumer requests because they may constitute businesses that maintain consumers’ personal information. Service providers for public and nonprofit entities could also be asked to disclose personal information maintained by a government agency, despite the fact that such files may be expressly exempt from disclosure under the Public Records Act.<sup>79</sup>

---

<sup>74</sup> See, e.g., 45 C.F.R. § 160.310 (Health Insurance Portability and Accountability Act rules for “business associates”); Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, General Data Protection Regulation, 2016 OJ (L 119) 1.

<sup>75</sup> Cal. Civ. Code § 1798.140(o), (v) (effective Jan. 1, 2020); see Ctr. Democracy & Tech., *Comparison of CDT’s Proposed Privacy Bill with GDPR and CCPA* (Dec. 13, 2018), <https://cdt.org/insights/comparison-of-cdts-proposed-privacy-bill-with-gdpr-and-ccpa/>.

<sup>76</sup> Cal. Attorney Gen., Final Statement of Reasons 30 (2020), <https://oag.ca.gov/privacy/ccpa/regs>.

<sup>77</sup> Cal. Attorney Gen., Summary and Response to Comments Submitted during 45-Day Period, resp. 53 (2020), <https://oag.ca.gov/privacy/ccpa/regs>.

<sup>78</sup> Cal. Code Regs. tit. 11, § 999.314(a) (business that provides services to a non-business must adhere to the “service provider” provisions of the CCPA).

<sup>79</sup> Cal. Attorney Gen., Final Statement of Reasons 30 (2020), <https://oag.ca.gov/privacy/ccpa/regs>.



The existing rule mitigates the “unintended result” under the CCPA that governmental data held by a for-profit business might be subject to the CPRA’s rights to access, correct, and delete individual information, despite existing laws governing the disclosure of public records and the privacy of governmental data.

New regulations under the CPRA should maintain the current treatment of service providers for governmental entities. The CPRA reiterated the CCPA’s definition of service providers as acting “on behalf of a business” without addressing the issue of service providers for governmental entities; consequently, it is important that the Agency maintain these vital protections in its regulations. Doing so avoids situations where sensitive data such as a student’s academic performance or accommodations for disabilities would be deleted or altered and helps ensure that governmental entities such as schools can provide services efficiently and effectively. It maintains the balance of the public’s rights to access public records and to privacy in governmental data that has long been established in existing law.

## **VII. Conclusion**

CDT appreciates the Agency’s focus on addressing the impact that businesses’ data practices have on consumers. In advancing the regulatory process, we urge the Agency to prioritize the impact that private entities’ data and ADM practices have for those seeking to exercise fundamental rights. Nondiscrimination and appropriate scoping of obligations, safeguards, and exceptions are vital to ensuring that for-profit data practices avoid data exploitation and serve consumer interests.

Respectfully submitted,

Cody Venzke  
*Policy Counsel, Equity in Civic Tech Project*  
*Center for Democracy & Technology*  
[REDACTED]

Ridhi Shetty  
*Policy Counsel, Privacy & Data Project*  
*Center for Democracy & Technology*  
[REDACTED]

---

**From:** Maureen Mahoney [REDACTED]  
**Sent:** 11/8/2021 1:52:00 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** Consumer Reports Comments on Proposed CPRA Rulemaking, PRO 01-21  
**Attachments:** Consumer Reports CPRA Comments No. 01-21 11.08.21.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Attached, please see Consumer Reports' comments in response to the California Privacy Protection Agency's Invitation for Preliminary Comments on the Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21).

Thank you for your consideration.

Sincerely,  
Maureen Mahoney

--

Maureen Mahoney, Ph.D.  
Senior Policy Analyst  
[REDACTED]

Pronouns: she/her/hers

[CR.org](https://www.consumerreports.org)



\*\*\*

This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.

\*\*\*



Comments of Consumer Reports  
In Response to the  
California Privacy Protection Agency  
Proposed Rulemaking under the California Privacy Rights Act of 2020  
(Proceeding No. 01-21)

By

Justin Brookman, Director of Technology Policy  
Maureen Mahoney, Senior Policy Analyst  
Nandita Sampath, Policy Analyst

November 8, 2021



## Table of Contents

<b>I.</b>	<b>Introduction.....</b>	<b>3</b>
<b>II.</b>	<b>Consumers’ Rights to Opt-Out of the Selling or Sharing of Their Personal Information.....</b>	<b>4</b>
	a. The CPPA should clarify that compliance with global privacy controls is mandatory under the CPRA.....	4
	b. The CPPA should provide and regularly update a list of global privacy signals that must be interpreted by companies as an opt-out signal.....	6
	c. Clarify that consent to share information despite a general opt-out signal must be specific, informed, and easily withdrawn.....	7
	d. Clarify that the sharing opt out applies to retargeting.....	9
	e. Prohibit service providers from combining data.....	10
	f. Clarify that consumers who have already opted out under CCPA need not resubmit opt-out requests in order to be opted out of data sharing.....	11
<b>III.</b>	<b>Consumers’ Rights to Limit the Use and Disclosure of Sensitive Personal Information.....</b>	<b>11</b>
	a. Clarify that when a consumer limits the use and disclosure of their sensitive information, it is unlawful to process sensitive data for most secondary uses, including monetization, personalization of advertising, and customization of content based on such data.....	12
	b. Businesses must honor limit use requests submitted through authorized agents.....	12
<b>IV.</b>	<b>Defining dark patterns.....</b>	<b>13</b>
	a. Maintain the existing prohibition on the use of dark patterns.....	13
	1. The existing rules appropriately rein in the number of allowable steps to opt out.....	14
	2. The existing rules correctly prohibit companies from asking for unnecessary information to opt out.....	14
	3. The existing rules correctly stop businesses from making consumers search through a privacy policy to opt out.....	15
	b. Clarify that companies that sell personal information must post the opt out logo to their homepages, along with the “Do Not Sell My Personal Information” link...15	
	c. Develop a standardized opt-in interface to help prevent dark patterns in obtaining consent.....	16



<b>V.</b>	<b>Automated decision-making.....</b>	<b>17</b>
	a. Require increased transparency measures from companies designing algorithms with significant legal effects.....	17
	b. Identify and ban pseudoscience in AI and other egregious algorithmic harms...	19
	c. Design an accreditation system for private auditing companies to perform audits on algorithms with significant legal effects.....	19
<b>VI.</b>	<b>Consumers' Right to Correct.....</b>	<b>21</b>
	a. Businesses should be required to delete disputed information if it cannot provide documentation to back it up.....	22
	b. Businesses should delete challenged information that they cannot link to a single identifiable consumer.....	24
	c. Businesses should be required to review correction requests in which the consumer submits new information that is relevant to the complaint, unless the request appears to be vexatious or in bad faith.....	25
<b>VII.</b>	<b>Consumers' Right to Know.....</b>	<b>26</b>
	a. In response to a verifiable request, businesses should be required to provide all information that belongs to that identifiable consumer, even if it is beyond the twelve month window.....	26
<b>VIII.</b>	<b>Financial incentives.....</b>	<b>27</b>
	a. Clarify that financial incentives in markets that lack competition is an unfair and usurious practice.....	27
	b. Direct businesses to calculate the value of the data to the business and make it available per access requests before being permitted to share data with third parties pursuant to loyalty programs.....	28
<b>IX.</b>	<b>Conclusion.....</b>	<b>28</b>

## I. Introduction

Consumer Reports<sup>1</sup> appreciates the opportunity to provide preliminary comments on the proposed rulemaking under the California Privacy Rights Act (CPRA).<sup>2</sup> We thank the California Privacy Protection Agency (CPPA) for soliciting input to make the California Consumer Privacy Act (CCPA), as amended by Proposition 24, work for consumers.

Privacy laws should protect consumer privacy by default, through strong data minimization that limits data use, collection, sharing, and retention to what is reasonably necessary to provide the service requested by the consumer.<sup>3</sup> But at the very least, opt outs should be workable for consumers. It's essential that the regulations clarify that businesses are required to honor browser privacy signals, including the Global Privacy Control specifically, as an opt out of sharing and sale.<sup>4</sup> Even with such a requirement in the current CCPA regulations,<sup>5</sup> and guidance from the AG that businesses must honor Global Privacy Control signals as an opt out of sale,<sup>6</sup> many companies have simply disregarded this right.<sup>7</sup> Second, when a consumer opts out, the CPPA must not permit companies to make their personal information available to third parties for a commercial purpose. Otherwise, key rights will not be accessible in practice for consumers.

The rulemaking also provides a prime opportunity to set baseline protections with respect to automated decision-making. Though automated decision-making can have discriminatory effects, it is largely unregulated. We urge the CPPA to adopt key protections with respect to transparency and auditing of the algorithms used in important decisions that affect consumers, and to prohibit uses that lead to egregious harms.

---

<sup>1</sup> Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

<sup>2</sup> *Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020*, CALIFORNIA PRIVACY PROTECTION AGENCY (Proceeding No. 01-21) (Sept 22, 2021), [hereinafter "Invitation for Comments"] [https://cppa.ca.gov/regulations/pdf/invitation\\_for\\_comments.pdf](https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf).

<sup>3</sup> *Model State Privacy Act*, CONSUMER REPORTS (February 2021), [https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR\\_Model-State-Privacy-Act\\_022321\\_vf.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf).

<sup>4</sup> Global Privacy Control, <https://globalprivacycontrol.org/> (last visited Nov. 6, 2021).

<sup>5</sup> Cal. Code Regs tit. 11 § 999.315(c).

<sup>6</sup> State of California Department of Justice, California Consumer Privacy Act, Frequently Asked Questions (FAQs), at B(7), (last visited Nov. 7, 2021), <https://oag.ca.gov/privacy/ccpa>.

<sup>7</sup> Russell Brandom, *Global Privacy Control Wants to Succeed Where Do Not Track Failed*, THE VERGE (Jan. 28, 2021), <https://www.theverge.com/2021/1/28/22252935/global-privacy-control-personal-data-tracking-ccpa-cpra-gdpr-duckduckgo>.



Below, we outline key recommendations to uphold consumer privacy and advance civil rights, consistent with the CPRA.

## **II. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information**

Too many companies have failed to adhere to the letter and spirit of the California Consumer Privacy Act, and Consumer Reports has found that some consumers have run into difficulties when attempting to opt out of the sale of their information under the CCPA.<sup>8</sup> Without clarifying regulations specifying that companies adhere to browser privacy signals as a global opt out of sale, consumers will have few options but to opt out at every company one by one, even though there are hundreds, if not thousands, of companies that sell consumer data.<sup>9</sup> In addition, Consumer Reports has found that some companies have ignored the opt out with respect to behavioral advertising, and instead send consumers to ineffective third-party industry sites.<sup>10</sup> And finally, it can be particularly time-consuming to opt out at certain companies — some even require consumers to download separate, third party apps to stop the sale of their data.<sup>11</sup>

- a. The CCPA should clarify that compliance with global privacy controls is mandatory under the CPRA.

The CCPA should issue clarifying regulations specifying that compliance with global privacy signals is not optional, but mandatory under the CPRA. Due to the complexity of the CPRA's language, there has been some ambiguity as to whether companies must always comply with such signals. Section 135 — which details how companies must respond to requests to opt out of the sale of data — provides two different possible paths to compliance in Section 135(a) and Section 135(b). Only Section 135(b) specifically mentions complying with global opt-out signals; as a result, several reporters<sup>12</sup> and law firms<sup>13</sup> have stated that companies may choose to ignore global opt-out signals if they opt to comply with Section 135(a) instead of Section 135(b).

---

<sup>8</sup> Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, CONSUMER REPORTS (Oct. 1, 2020), [https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR\\_CCPA-Are-Consumers-Digital-Rights-Protected\\_092020\\_vf.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf).

<sup>9</sup> See, for example, State of California Department of Justice, Data Broker Registry (last visited Nov. 7, 2021), <https://oag.ca.gov/data-brokers> (includes approximately 500 data brokers).

<sup>10</sup> Maureen Mahoney et al., *The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act*, CONSUMER REPORTS at 16 (Feb. 2021), [https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR\\_AuthorizedAgentCCPA\\_022021\\_VF\\_.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf).

<sup>11</sup> *Are Consumers' Digital Rights Protected?*, *supra* note 8, at 24.

<sup>12</sup> Wendy Davis, *Ad Industry Protests California AG's Proposed Privacy Rules*, MEDIAPOST (June 9, 2020), <https://www.mediapost.com/publications/article/352362/ad-industry-protests-california-ags-proposed-priv.html>.

<sup>13</sup> Kate T. Spelman, David P. Saunders and Effiong K. Dampha, *New Draft of California Privacy Ballot Initiative Released*, JENNER & BLOCK (last visited Nov. 6, 2021), [https://jenner.com/system/assets/publications/19414/original/2019%20Data%20Privacy%20and%20Cybersecurity%](https://jenner.com/system/assets/publications/19414/original/2019%20Data%20Privacy%20and%20Cybersecurity%20Initiative.pdf)

Such a reading of the statute is inconsistent with the purpose of CPRA as well as the plain language of Section 135(e) which plainly states that companies must honor global privacy control opt-out requests *regardless* of whether a company complies with Section 135(a) or Section 135(b). Section 135(e) provides:

A consumer may authorize another person to opt-out of the sale of sharing or the consumer’s personal information, and to limit the use of the consumer’s sensitive personal information, on the consumer’s behalf, including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b) of this Section, indicating the consumer’s intent to opt-out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act of the consumer’s behalf, pursuant to regulations adopted by the Attorney General, regardless of whether the business has elected to comply with subdivision (a) or (b) of this Section. For purposes of clarity, a business that elects to comply with subdivision (a) of this Section may respond to the consumer’s opt-out consistent with Section 1798.125.

This language clearly states that a consumer may designate another person to exercise their privacy rights on their behalf — including through a global opt-out preference signal — and such a request must be honored regardless of whether the company has chosen to comply with Section 135(a) or Section 135(b).

Such a reading is also consistent with the bifurcated compliance structure of Section 135. Under Section 135(a), companies must include clear and conspicuous links on their internet homepage labeled “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information.” However, if a consumer endeavors to exercise either of these rights, they may bargain with the consumer, asking for permission to disregard the opt-out request (whether a signal or an individual request) pursuant to rules laid out in Section 125 of the statute.

Section 135(b), on the other hand, allows a company to not place prominent “Do Not Sell” or “Limit the Use” links on their site so long as they do not bombard users with consent dialogs or enticements seeking to disregard an opt-out request. Instead, the company can only provide a link through which consumers can later change their preferences. This section was designed to encourage companies to not deluge consumers with permission requests as has been the experience with websites under the GDPR and the ePrivacy Directive in Europe.<sup>14</sup>

---

20\_20New20Draft20of20California20Privacy20Ballot20Initiative20Released20-20ATTORNEY20ADVERTISING.pdf.

<sup>14</sup> *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent*, PRIVACY INTERNATIONAL (May 21, 2019), <https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent>.



To interpret Section 135(a) as letting companies ignore global preference signals would on the other hand strongly encourage companies to comply with Section 135(a) instead; the ability to disregard easily expressed global preferences would strongly outweigh any marginal benefits from not having to include opt-out links of a company’s website. Such a reading would be inconsistent with the purpose of providing Section 135(b) at all. Fortunately, Section 135(e) is explicit that under both paths, companies must honor global preference signals.

Moreover, companies are already required to honor global privacy controls under the CCPA today.<sup>15</sup> There is no rationale for interpreting CPRA — which has the stated intent of strengthening the CCPA<sup>16</sup> — as weakening one of CCPA’s core protections. Indeed, without global privacy controls and comparable scalable options, California’s opt-out rights are not meaningfully usable by consumers. A Consumer Reports study of CCPA opt-out rights in October 2020 found that it could be very difficult for consumers to stop the sale of their information. About 14% of the time, broken or inaccessible opt-out processes prevented consumers from opting out of the sale of their information.<sup>17</sup>

Consumers deserve an easy and practically usable way of globally expressing certain privacy preferences. The CPPA should put an end to any uncertainty around the CPRA’s language and issue clarifying language that covered companies must always honor global preference signals that comply with the statute’s requirements.

- b. The CPPA should provide and regularly update a list of global privacy signals that must be interpreted by companies as an opt-out signal.

Currently, there is no definitive list of what “user-enabled global privacy controls” companies must treat as legally valid opt-out requests under the CCPA.<sup>18</sup> In January 2021, then Attorney General Becerra tweeted that CCPA mandates that companies honor the Global Privacy Control, at the very least.<sup>19</sup> Since then, the Attorney General’s office has updated the CCPA FAQs to formalize that GPC opt outs are legally binding,<sup>20</sup> and the office has stated that it has

---

<sup>15</sup> Cal Code Regs tit. 11 § 999.315(c).

<sup>16</sup> California Privacy Rights Act of 2020 §§ 3, 3(C)(1); see also *Crafting Better Privacy Laws, Based on the California Model: A Conversation with Alastair Mactaggart*, WIREWHEEL (Jul. 20, 2021), <https://wirewheel.io/ccpa-state-privacy-laws/> (Mactaggart is quoted, “One of the great benefits of California’s law is that it allows for my device, my global setting, my phone, my computer to do it for me.”)

<sup>17</sup> *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?*, *supra* note 8.

<sup>18</sup> Cal. Code Regs. tit. 11 § 999.315.

<sup>19</sup> @AGBecerra, Twitter (Jan. 28, 2021), <https://twitter.com/AGBecerra/status/1354850321692934144>.

<sup>20</sup> State of California Department of Justice, California Consumer Privacy Act, Frequently Asked Questions (FAQs), *supra* note 6, at B(7).

begun sending warning letters to companies who do not comply with the signal.<sup>21</sup> However, there is no clear guidance on the legal status of any other global controls or browser settings.

The CPPA should create and regularly update a list of signals and settings that should be treated as legally binding requests under the CPRA. The Global Privacy Control, with over 50 million unique users each month, should be designated as conveying a legally binding request to opt out of the sharing or selling of a user's personal information under Section 13. The CPPA should consider giving similar status to other comparable settings, including the "Do Not Track" signal still embedded in browsers such as Chrome that have yet to enable GPC. Mobile operating systems such as "Limit Ad Tracking" on iOS as well as other IoT platform settings could also be reasonably interpreted as a request not to have data shared or sold under the CPRA. CPRA does not mandate that a request to opt out specifically invoke the CPRA, so any signal from a California resident conveying a request that is roughly equivalent to the right afforded by the statute should be interpreted as legally binding.

- c. Clarify that consent to share information despite a general opt-out signal must be specific, informed, and easily withdrawn

Any consent to track notwithstanding a general global privacy control signal has to be clear, specific, and in response to a dedicated prompt. The regulations should also specify that it has to be at least as easy to decline permission as it is to say yes. Moreover, consistent with the CPRA's prohibition on dark patterns<sup>22</sup> and prohibition on retaliation,<sup>23</sup> any such interface must not be coercive or abusive.

For example, the use of vague and unspecific cookie consent notices, originally offered in response to GDPR and the ePrivacy Directive, should not be sufficient to confer consent to sell or share personal information despite a global opt-out signal. Many cookie consent notices conflate consent for both functional and secondary processing, by using design choices that nudge them to accept all processing. For example, we looked at the websites of the 25 top publishers, according to Washington and Lee University, using data from Pew and Comscore,<sup>24</sup> from Los Angeles, California, as simulated by a VPN. The majority of the sites studied have their own separate cookie management interface. California visitors to the *Time* news site, for example, encounter a pop-up:

---

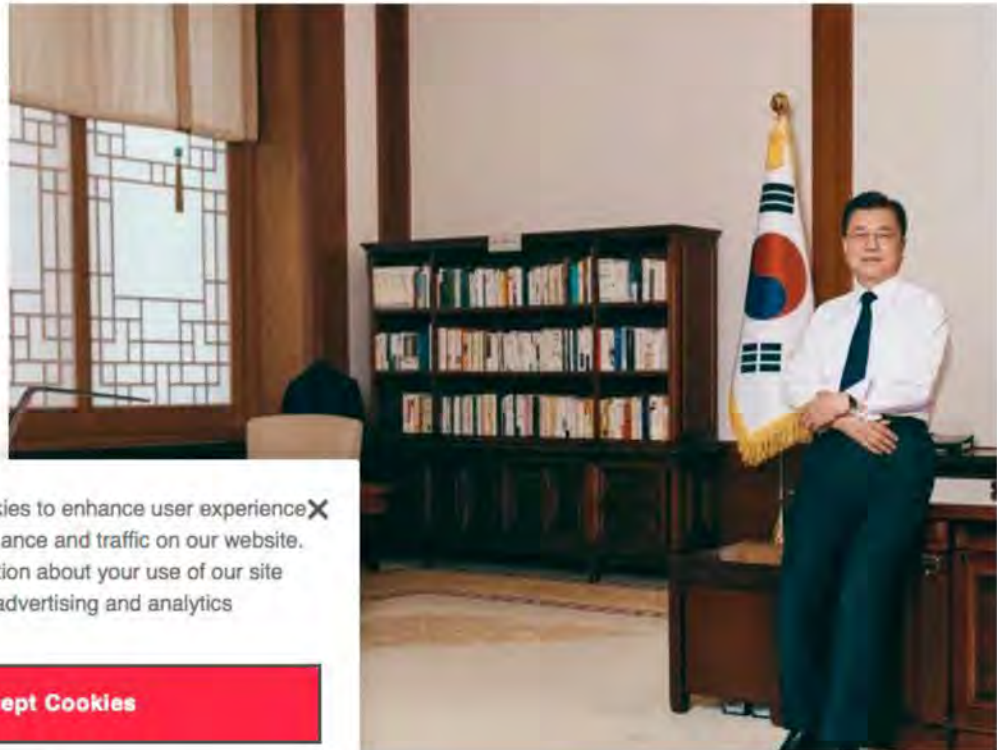
<sup>21</sup> State of California Department of Justice, CCPA Enforcement Case Examples, "Manufacturer and Retailer Stopped Selling Personal Information," (last visited Nov. 7, 2021), <https://oag.ca.gov/privacy/ccpa/enforcement>.

<sup>22</sup> Cal. Civ. Code § 1798.140(h).

<sup>23</sup> *Id.* at § 1798.125(a).

<sup>24</sup> Washington and Lee University Library, Top Online News Sites (Summer 2015), <https://libguides.wlu.edu/c.php?g=357505&p=2412837>.





This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners.

**Accept Cookies**

[Cookie Settings](#)

/// SOUTH KOREA ///

Clearly, with the red highlighting, the user is encouraged to click on “Accept Cookies[,]” in order to consent to the disclosure of information about their activities on the site with social media, advertising, and analytics companies. The consumer has to click on “Cookie Settings,” to ensure that targeting cookies are not permitted. This can hardly be interpreted as an intentional direction to share data. Companies should be encouraged to make it easier for consumers to exercise their preferences, not more difficult.

Even if a company does obtain clear and informed consent to track users notwithstanding a global signal, they must provide opt out links and other easy methods for a user to subsequently

retract such consent. Some have argued that if a consumer agrees to let a business share their personal information, then the business does not have to provide an opt out link for the consumer to stop the sharing or sale of their personal data.<sup>25</sup> The regulations should provide for clear and consistent means for users both to find out whether they have been deemed to provide such consent and how they can easily retract it.

d. Clarify that the sharing opt out applies to retargeting

Many companies have exploited ambiguities in the CCPA’s definition of sale and the rules surrounding service providers to ignore consumers’ requests to opt out of behavioral advertising.<sup>26</sup> Companies such as Amazon claim that they are not “selling” data and that consumers can’t opt out of these data transfers under the CCPA — even though they share it with their advertising partners.<sup>27</sup> Some companies claim that because data is not necessarily transferred for money, it does not constitute a sale.<sup>28</sup> But addressing targeted advertising is one of the main goals of the CCPA.<sup>29</sup> We appreciate that the CPRA clarifies that consumers have the right to opt out of data sharing for the purpose of cross-context targeted advertising,<sup>30</sup> and removes the delivery of cross-context targeted advertising as a business purpose for which businesses could claim an exemption from the opt out.<sup>31</sup> However, more needs to be done to ensure that consumers have adequate protections over this data.

While cross-site behavioral targeting is clearly encompassed by the CPRA’s definitions, there remains a hypothetical loophole when it comes to *retargeting*, which is based on a user’s activity on just one other site (say, browsing a pair of shoes). While excluding retargeting from the definition of cross-context targeted advertising would be a tendentious stretch — and most

---

<sup>25</sup> David A. Zetony, Greenberg Traurig LLC, *Under The CPRA will companies be required to offer consumers the ability to opt-out of behavioral advertising if they have already received opt-in consent?*, NAT’L LAW REVIEW, Volume XI, Number 301 (Oct. 28, 2021), <https://www.natlawreview.com/article/under-cpra-will-companies-be-required-to-offer-consumers-ability-to-opt-out>.

<sup>26</sup> Maureen Mahoney, *Many companies are not taking the California Consumer Privacy Act seriously—the attorney general needs to act* (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>.

<sup>27</sup> “Amazon.com Privacy Notice,” (Feb. 12, 2021), [https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref\\_=footer\\_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40\\_\\_SECTION\\_FE2374D302994717AB1A8CE585E7E8BE](https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_FE2374D302994717AB1A8CE585E7E8BE); “Amazon Advertising Preferences” <https://www.amazon.com/adprefs>.

<sup>28</sup> Tim Peterson, *‘We’re Not Going to Play Around’: Ad Industry Grapples with California’s Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), <https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/>; Tim Peterson, *WTF is California’s New, and Potentially Stronger Privacy Law?*, DIGIDAY (July 6, 2020), <https://digiday.com/marketing/california-privacy-rights-act/>.

<sup>29</sup> Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>; Cal. Civ. Code § 1798.140(o); Cal. Civ. Code § 1798.140(t).

<sup>30</sup> Cal. Civ. Code § 1798.120(a).

<sup>31</sup> *Id.* at § 1798.140(e)(6).



observers have not read the CPRA in this way<sup>32</sup> — others have raised doubts as to whether retargeting is covered under the sharing opt out.<sup>33</sup>

We urge the CPPA to issue clarifying regulations that cross-context targeting based on behavior on just one other site is included within the definition of cross-context targeted advertising. This language will provide much-needed clarity, given the widespread non-compliance and bad faith interpretations of the CCPA with respect to targeted advertising. As AARP points out, “No one likes being followed by an ad, even if we know it’s anonymous. It gets even more worrisome when companies that we’ve given identifiable information to, such as Facebook, Amazon and Google, get involved.”<sup>34</sup>

e. Prohibit service providers from combining data

Additionally, the CPPA should clarify that service providers may not combine data across clients. Service providers should be working on behalf of one company at a time. Allowing companies to claim that they are service providers for everyone swallows the rules and lets third parties amass huge, cross-site data sets, allowing them to glean even deeper insights into consumers’ most personal characteristics. The CPRA’s definition of “service provider” clearly states that a service provider is prohibited from “sharing or selling the personal information” whilst acting as a service provider.<sup>35</sup> Allowing service providers to merge data sets across different clients would run afoul of that provision, as the service provider would effectively be sharing one client’s data with another, with itself acting on behalf of both parties.<sup>36</sup>

The CPPA should issue regulations to clarify the intent and purpose of the CPRA’s service provider definition. We suggest the following language:

---

<sup>32</sup> See, for example, *Changes to CCPA Put Retargeting in the Regulatory Bullseye*, AD LIGHTNING (Dec. 8, 2020), <https://blog.adlightning.com/changes-to-ccpa-put-retargeting-in-the-regulatory-bullseye>.

<sup>33</sup> Arsen Kourinian, *How Expansion of Privacy Laws, Ad Tech Standards Limit Third-Party Data Use for Retargeting*, IAPP (Apr. 27, 2021), <https://iapp.org/news/a/how-the-expansion-of-data-privacy-laws-and-adtech-standards-limits-companies-ability-to-use-third-party-data-for-retargeting/>. (“Major companies are well-positioned to adapt to these developments, as they likely still have a treasure trove of first-party data that they can rely on for retargeting and measuring marketing performance on their owned and operated properties.”) See also *Consumer Retargeting: What’s the Problem?* WIREWHEEL (Jan. 28, 2021), [https://wirewheel.io/consumer-retargeting/?utm\\_medium=Organic-Social&utm\\_source=Facebook&utm\\_campaign=2021-02-17-Mark-retargeting-video](https://wirewheel.io/consumer-retargeting/?utm_medium=Organic-Social&utm_source=Facebook&utm_campaign=2021-02-17-Mark-retargeting-video) (Quoting Marc Zwillinger: “I think we are going to get into a much more interesting question when we talk about whether the CPRA prevents retargeting. We may have some different views on that and certainly Alistair McTaggart will probably have a different view.”)

<sup>34</sup> Erin Griffith, *Why Is That Ad Following You Across the Web?* AARP, <https://www.aarp.org/home-family/personal-technology/info-01-2014/how-to-stop-retargeting-ads.html>.

<sup>35</sup> Cal. Civ. Code § 1798.140(ag)(1)(a).

<sup>36</sup> Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), [https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle\\_facebook\\_google\\_data\\_brokers.pdf](https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf).

A service provider may not combine the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers.

There is precedent for such a prohibition, such as in California’s newly adopted SB 41 (Genetic Information Privacy Act), which precludes service providers from combining genetic information received from other clients.<sup>37</sup>

- f. Clarify that consumers who have already opted out under CCPA need not resubmit opt-out requests in order to be opted out of data sharing.

Left unaddressed by the statute is whether businesses that have honored consumers’ opt out requests under the CCPA are required to automatically opt consumers out of sharing when the CPRA goes into effect in 2023. We urge the CPPA to clarify that businesses must automatically opt such consumers of the sharing of their information when the CPRA goes into effect. Otherwise, consumers would have to identify the companies from which they have already opted out and resubmit, which they are unlikely to be able to do. Moreover, since, as indicated by the recent AG enforcement notice, the existing definition of sale in the CCPA already covers data shared for cross-context targeted advertising,<sup>38</sup> consumers would reasonably expect that they had opted out of such sharing already.

### **III. Consumers’ Rights to Limit the Use and Disclosure of Sensitive Personal Information**

The CPRA provides the right for consumers to limit the use and disclosure of their sensitive personal information, including their financial account information, email, and geolocation data, to what is necessary to provide the service.<sup>39</sup> Particularly since the responsibility falls upon the consumer to ask the business to limit the use and sharing, the protections should be comprehensive and as easy as possible to initiate.

---

<sup>37</sup> SB 41 at 56.18 (b)(10)(B), (2021), [https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill\\_id=202120220SB41](https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB41).

<sup>38</sup> State of California Department of Justice, CCPA Enforcement Case Examples, “Media Conglomerate Updated Opt-Out Process and Notices,” (last visited Nov. 6, 2021), <https://oag.ca.gov/privacy/ccpa/enforcement>.

<sup>39</sup> Cal. Civ. Code § 1798.121(a).



- a. Clarify that when a consumer limits the use and disclosure of their sensitive information, it is unlawful to process sensitive data for most secondary uses, including monetization, personalization of advertising, and customization of content based on such data.

Especially since the “limit use” right only takes effect upon the consumer’s specific request, and since it involves sensitive data, businesses should be very limited indeed in how they are allowed to use such data when “limit use” is enabled. Most secondary uses, including monetization, personalization of advertising, and customization of content should be prohibited when the consumer or their agent has authorized the additional protections.

The ways that ads are targeted — including first-party targeting — can perpetuate historic patterns of discrimination and unequal outcomes among protected classes. For example, the Department of Housing and Urban Development has charged Facebook for targeting housing advertisements based on protected categories like race and religion.<sup>40</sup> Such sensitive information should not be used in determining the advertising and content that consumers view, particularly under “limit use”.

Companies should still be allowed to use information to fix errors and engage in fraud prevention, even when “limit use” is enabled, if such use is necessary and proportionate to the purpose.

- b. Businesses must honor limit use requests submitted through authorized agents.

The limit use function will only be useful if consumers are able to easily activate it. It only takes effect if the consumer actively requests the use of their sensitive data to be limited, which means that hundreds, if not thousands, of different companies may be using that data without permission. Thus, as outlined in 1798.135(e), businesses must be required to honor requests submitted by authorized agents — consistent with the manner in which opt out requests from authorized agents are processed. Otherwise, it is unlikely that consumers will reap the benefits of this new right.

Authorized agents may be more effective than global controls for these sorts of opt-outs, as first-party uses and relationships vary by context, and individuals may want to be able to exercise nuanced choices as to which parties’ uses should be limited. On the other hand, sale and sharing of data generally breaks contextual integrity and consumers who object to such practices (as most do) will likely want to prohibit all parties from engaging in such behavior.

---

<sup>40</sup> *United States Department of Housing and Urban Development, on behalf of Complainant Assistant Secretary for Fair Housing and Equal Opportunity v. Facebook, Inc.* HUD ALJ No. FHEO No. 01-18-0323-8 [https://www.hud.gov/sites/dfiles/Main/documents/HUD\\_v\\_Facebook.pdf](https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf); Tracy Jan and Elizabeth Dwoskin, *HUD Is Reviewing Twitter’s and Google’s Ad Practices as Part of Housing Discrimination Probe*, WASH. POST (Mar. 28, 2019), <https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination>.

#### IV. Defining dark patterns

Subverting consumer intent online has become a real problem, and it's important to address. In response to Europe's recent GDPR privacy law, many websites forced users through confusing consent dialogs to ostensibly obtain consent to share and collect data for any number of undisclosed purposes.<sup>41</sup> And researchers increasingly have been paying attention to manipulative dark patterns as well. A 2019 Princeton University study of 11,000 shopping sites found more than 1,800 examples of dark patterns, many of which clearly crossed the line into illegal deception.<sup>42</sup> Consumer Reports research has also identified numerous dark patterns, including in smart TV's, food delivery apps, and social media.<sup>43</sup> For example, CR testers found that for all of the smart TVs examined, a consumer moving quickly through the television set-up process will end up providing consent to the tracking of everything they watch through automatic content recognition.<sup>44</sup> And, Consumer Reports is helping to collect dark patterns through the Dark Patterns Tipline, a project to crowdsource examples of these deceptive interfaces to help advocate for reform.<sup>45</sup>

- a. The existing prohibition on the use of dark patterns in opt-out processes should be maintained.

We appreciate that the existing CCPA regulations “require minimal steps to allow the consumer to opt-out” and to prohibit dark patterns, “a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer’s choice to opt-out.”<sup>46</sup> These regulations are essential given the difficulties that consumers have experienced in attempting to stop the sale of their information.

---

<sup>41</sup> *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

<sup>42</sup> Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM Hum.-Comput. Interact. (2019), <https://webtransparency.cs.princeton.edu/dark-patterns/>.

<sup>43</sup> *Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds*, CONSUMER REPORTS (Feb. 7, 2018), <https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-find>; *Collecting #Receipts: Food Delivery Apps and Fee Transparency*, CONSUMER REPORTS (Sept. 29, 2020), [https://digital-lab-wp.consumerreports.org/wp-content/uploads/2020/09/Food-delivery\\_-Report.pdf](https://digital-lab-wp.consumerreports.org/wp-content/uploads/2020/09/Food-delivery_-Report.pdf); Consumers Union Letter to Fed. Trade Comm'n (Jun. 27, 2018), <https://advocacy.consumerreports.org/wp-content/uploads/2018/06/CU-to-the-FTC-Facebook-Dark-Patterns-6.27.18-1-1.pdf>; *Consumer Reports Calls On FTC to Take Tougher Action to Stop Hidden Resort Fees*, CONSUMER REPORTS (Aug. 6, 2019), [https://advocacy.consumerreports.org/press\\_release/consumer-reports-calls-on-ftc-to-take-tougher-action-to-stop-hidden-resort-fees/](https://advocacy.consumerreports.org/press_release/consumer-reports-calls-on-ftc-to-take-tougher-action-to-stop-hidden-resort-fees/).

<sup>44</sup> *Samsung and Roku Smart TVs Vulnerable to Hacking*, *supra* note 46.

<sup>45</sup> Dark Patterns Tipline, <https://darkpatternstipline.org/>.

<sup>46</sup> Cal. Code Regs. tit. 11 § 999.315(h).



1. The existing rules appropriately rein in the number of allowable steps to opt out.

We appreciate that the existing rules limit the number of allowable steps in the opt-out process.<sup>47</sup> As we noted in our recent study, some “Do Not Sell” processes involved multiple, complicated steps to opt out, raising serious questions about the workability of the CCPA for consumers. For example, at the time of our study, the data broker Outbrain did not have a “Do Not Sell My Personal Information” link on its homepage (this has since been corrected). The consumer could click on the “Privacy Policy” link at the bottom of the page, which sent the consumer through at least six different steps in order to opt out of the sale of their information on that device. (The consumer could cut out several steps by clicking on “Interest-Based Ads” on the homepage.) As one consumer told us, “It was not simple and required reading the ‘fine print.’”<sup>48</sup> Moving forward, the newly-adopted CCPA regulations should help address this problem.

2. The existing rules correctly prohibit companies from asking for unnecessary information to opt out.

We also appreciate the guidance that opt-out processes “shall not require the consumer to provide personal information that is not necessary to implement the request.”<sup>49</sup> In our study, the overwhelming reason for a consumer to refrain from part of a DNS request process, or give up altogether, was not feeling comfortable providing information requested. Out of the 68 reports that the tester chose not to provide information they were asked for as part of the process, 59 said it was because they were not comfortable doing so. For example, nearly all consumers declined to provide a photo in order to process their opt-out requests. Out of 7 instances in which consumers reported that they were asked to provide a photo selfie, in 6 the consumer declined.<sup>50</sup>

Consumers told us that they were just as averse to providing government IDs. One tester of Searchbug reported: “I hated having to send an image of my Driver License. I thoroughly regret having done so. It feels like an invasion of privacy to have to do that, just so I can take steps to PROTECT my privacy. Feels wrong and dirty.”<sup>51</sup> Even consumers that ended up providing the drivers’ license ended up confused by the company’s follow-up response. One tester of Hexasoft Development Sdn. Bhd. responded: “After sending them a copy of my California driver license to satisfy their residency verification, I got an email back which simply stated that ‘[w]e will update the ranges in the future release.’ I have no idea what that means.”<sup>52</sup> Out of 17 reports of being asked for an image of a government ID, in 10 the consumer chose not

---

<sup>47</sup> *Id.* at § 999.315(h)(1).

<sup>48</sup> *Are Consumers’ Digital Rights Protected?*, *supra* note 8, at 18-21.

<sup>49</sup> Cal. Code Regs tit. 11 § 999.315(h)(4).

<sup>50</sup> *Are Consumers’ Digital Rights Protected?*, *supra* note 8, at 34.

<sup>51</sup> *Id.*

<sup>52</sup> *Id.*

to. Out of 40 reports of being asked to provide a government ID number, in 13 the consumer refrained from providing it.<sup>53</sup>

This information is clearly not necessary, as most data brokers simply requested name, address, and email to process opt outs (where authentication is not required). Unnecessary collection of sensitive data has significantly interfered with consumers' ability to exercise their rights under the CCPA, and we appreciate that the newly-adopted CCPA rules explicitly prohibit this.

3. The existing rules correctly stop businesses from making consumers search through a privacy policy to opt out.

We are also pleased that the existing rules preclude businesses from requiring consumers to dig through privacy policies to opt out.<sup>54</sup> In our study, in some cases, consumers proactively reported finding language surrounding the DNS request link and process excessively verbose and hard to understand. For example, one tester reported of the data broker US Data Corporation, "There is a long, legalistic and technical explanation of how and why tracking occurs, not for the faint of heart." Another said of Oracle America, "The directions for opting out were in the middle of a wordy document written in small, tight font." Another found the legal language used by Adrea Rubin Marketing intimidating: "they seemed to want to make the process longer and unnecessarily legalese-y, even a bit scary--under threat of perjury."<sup>55</sup>

b. Clarify that companies that sell personal information must post the opt out button to their homepages, along with the "Do not Sell My Personal Information" link.

We appreciate that the existing rules include a logo, or button, for companies that sell personal information to post alongside the "Do Not Sell My Personal Information" link on the homepage.<sup>56</sup> However, unless use of the button is required, it is unlikely that companies will adopt it. While we think it is clear that the language in § 999.306(f)(1)-(3) requires companies selling personal information to post the button on their homepages, some observers have a different interpretation, that posting of the button is optional.<sup>57</sup> And in fact, the authors have yet to encounter a website in which this graphic is used. An optional interface counters the direct instructions in the CCPA, to issue rules "For the development and use of a recognizable and

---

<sup>53</sup> *Id.*

<sup>54</sup> Cal. Code Regs tit. 11 § 999.315(h)(5).

<sup>55</sup> *Are Consumers' Digital Rights Protected?*, *supra* note 8, at 32.

<sup>56</sup> Cal. Code Regs tit. 11 §999.306(f)(1)-(3).

<sup>57</sup> See, eg, @JulesPolonetsky, Twitter (Dec. 10, 2020), <https://twitter.com/JulesPolonetsky/status/1337116699548667907>.



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.”<sup>58</sup> [emphasis added]

To help eliminate any uncertainty that the opt out button is required, we propose the following tweak to the language:

Opt-Out Button. (1) The following opt-out button ~~may~~ **shall** be used in addition to posting the notice of right to opt-out, ~~but~~ **and** not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations. (2) Where a business posts the “Do Not Sell My Personal Information” link, the opt-out button shall be added to the left of the text as demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link. (3) The button shall be approximately the same size as any other buttons used by the business on its webpage.

Without more clearly establishing that use of the opt-out button is required on the homepage, it is likely that companies continue to disregard it. Standardized notice is essential to making CCPA disclosures meaningful and understandable for consumers and to limiting company’s discretion to craft less clear or useful interfaces. And widespread adoption of the button should better ensure that consumers can more easily opt out of the sale of their personal information.

- c. Develop a standardized opt-in interface to help prevent dark patterns in obtaining consent.

The CPPA should also develop standardized disclosures, so that companies have more clarity about appropriate interfaces and design choices. As discussed above, we appreciate that the CCPA requires rulemaking entities to create a uniform Do Not Sell logo<sup>59</sup> — this standardization can help companies avoid dark patterns (if, as we recommend, the CPPA makes clear that use of the button is required).<sup>60</sup>

Given the persistent problems with dark patterns in cookie consent interfaces, which purport to obtain consumers’ consent for any number of inappropriate data uses, the CPPA should develop a model interface — or at least language — for obtaining consent to opt back into the sharing of information, and for obtaining consent for the sharing or sale of children’s

---

<sup>58</sup> Cal. Civ. Code § 1798.185(a)(4)(C).

<sup>59</sup> *Id.*

<sup>60</sup> See, for example, 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* (Feb. 4, 2020), <https://cups.cs.cmu.edu/pubs/CCPA2020Feb04.pdf>.

information. Overall, the CPPA should err strongly on the side of clear, simple, bright-line rules instead of vague, debatable standards that could afford bad faith actors too much wiggle room to justify deceptive behavior.

## **V. Automated decision-making**

As automated decision-making that uses artificial intelligence is on the rise for commercial applications like determining housing and employment eligibility, facial recognition, and even software for self-driving cars, the potential to perpetuate existing societal inequalities is worrying. AI models are trained on data that tends to represent historical outcomes (for example, hiring algorithms compare applicants to those who currently hold positions at a given company which can tend to exclude minorities and women). Many of these algorithms (intentionally or unintentionally) could be used to discriminate against groups of people that have historically been excluded from services or opportunities in the past.<sup>61</sup> Also, some companies claim that correlations between unrelated data can predict behavior or other outcomes, with little evidence, often leading to discriminatory results.<sup>62</sup>

Further, some of these algorithms are black boxes to both the end-users as well as the engineers that design them. Establishing appeals processes or other pathways to provide opportunities for individuals to correct data about themselves becomes less meaningful when there are thousands of data points and opaque models and results.

It will be close to impossible to entirely rid algorithms of bias,<sup>63</sup> but pursuant to the CPRA, which directs the Agency to develop rules providing opt out and access rights with respect to automated decision-making,<sup>64</sup> the CPPA can put guardrails in place to mitigate or prevent harmful effects of discrimination.

### **a. Require increased transparency measures from companies designing algorithms with significant legal effects**

While there are laws that prohibit discrimination based on certain characteristics for various sectors, due to the opacity of more complicated algorithms, it is difficult to tell whether algorithmic discrimination is occurring at all. There are virtually no laws, other than CPRA, that require companies to disclose how their algorithms work, the types of data they use to make decisions, or mandate providing ways for consumers to contest decisions made about them. For

---

<sup>61</sup> Nandita Sampath, *Racial Discrimination in Algorithms and Potential Policy Solutions* (Feb. 26, 2021), <https://medium.com/cr-digital-lab/racial-discrimination-in-algorithms-and-potential-policy-solutions-75c5911ed29>.

<sup>62</sup> Arvind Narayanan, Princeton University, *How To Recognize AI Snake Oil*, <https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf>.

<sup>63</sup> Chris Caruso, *Why AI Will Never be Perfect* (Sept 28, 2016), <https://medium.com/@chriscaruso/why-ai-will-never-be-perfect-c34aec481048>.

<sup>64</sup> Cal. Civ. Code § 1798.185(a)(16).

decision-making involving significant legal effects, consumers deserve transparency. We advise that for algorithms with significant legal effects (including housing, credit/lending, insurance, employment), meaningful transparency measures need to be created in order to identify and mitigate discrimination. Section 21(a)(16) allows the Agency to issue regulations governing access and opt-out rights. To facilitate this, at the very least, companies should be required to provide notice in its privacy policy that algorithms are being used to make significant decisions about them to provide some degree of transparency and accountability.<sup>65</sup>

Companies often use multiple data points that are fed into the algorithm to make a decision about how a consumer behaves, and companies should be required to provide all of that data access requests. Companies should be required to disclose the types of data collected, the specific data that it has on the consumer in order to profile them, and how each data point is factored into the final algorithmic decision (to the extent possible), pursuant to access requests.<sup>66</sup> For example, if a particular data point holds more weight in a decision, the consumer should be informed and given a quantitative value if possible. In order to give consumers this information in a meaningful way, companies should use more transparent and interpretable algorithms and avoid using algorithms that tend to be more complicated to understand like neural networks.

For housing and employment-related targeted advertising, discrimination based on protected classes including race, gender, religion, etc. is prohibited.<sup>67</sup> Consumers deserve transparency as to why certain ads are shown to them which should include providing consumers with meaningful information when the consumer requests it. For example, some companies like Facebook provide users with the option to learn more about why they see certain ads. However, the information is often overly broad and generalized, with explanations like "interests" or "offline activity."<sup>68</sup> For targeted ads with the potential of significant legal effects, consumers should be shown how ads are targeted to them with improved specificity.

For other sensitive algorithms like determining insurance premiums, companies should also disclose *why* data points that are factored into the algorithms were chosen, provide explanations for ways consumers can improve their algorithmic "risk score," and also make sure consumers have the ability to contest inaccurate data about themselves. This requires that consumers have easy access to real-time information about themselves that can be accessed without hurting their score and also requires a straightforward process to contest inaccurate

---

<sup>65</sup> *Invitation for Comments*, *supra* note 2, at 2(b) and 2(d).

<sup>66</sup> Under Cal. Civ. Code § 1798.185(21)(a)(16), the Agency has the authority to require businesses to provide meaningful information about the algorithm's logic and the outcome of the process.

<sup>67</sup> Ava Kofman & Ariana Tobin, *Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement*, PRO PUBLICA (Dec. 13, 2019), <https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement>.

<sup>68</sup> *Why Am I Seeing Ads From An Advertiser at Facebook?*, Facebook.com Help Center (last visited Nov. 1 2021), <https://www.facebook.com/help/794535777607370>.



information that must be corrected in a timely manner (or be provided a clear explanation as to why the data is not inaccurate).

b. Identify and ban pseudoscience in AI and other egregious algorithmic harms

There are certain harmful applications of AI where improved transparency and better consumer control of data are not enough, and should be prohibited. Some AI companies claim that their technology is capable of doing certain things that are not substantiated by science or claim certain accuracy rates of their technology without third-party validation.<sup>69</sup> Under Section 21(a)(15), the Agency has the authority to require businesses to submit risk assessments weighing consumer harm with the processing of their personal information, “with the goal of restricting or prohibiting such processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.”<sup>70</sup> And some of these pseudoscientific algorithms can cause real harm.

In the employment space, companies like HireVue have been criticized for building video interviewing software that claims to rank job applicants based on the tone of their voice and facial expressions. There is little evidence that these factors are related to job performance; more importantly, these kinds of algorithms have the potential to discriminate against those with certain skin colors, accents, or disabilities.<sup>71</sup> Generally, using AI to predict subjective processes like job success, recidivism, etc. will result in discriminatory outcomes; trying to quantify subjective processes where the goals might be different depending on who designs the AI system tends to hurt those historically marginalized. While unfair and deceptive practices are outlawed at the state and federal levels, the CPPA needs to make more clear what kinds of AI applications fall under this category.

c. Design an accreditation system for private auditing companies to perform audits on algorithms with significant legal effects

Third-party auditing can be an effective way to mitigate disparate impacts and other algorithmic harm. Pursuant to Section 21(a)(18), which directs the Agency to establish regulations with respect to auditing companies, including identifying criteria for selection of entities to audit, the Agency should design an accreditation system for companies that use AI that ensures accountability.<sup>72</sup> It is important to ensure that audits performed on different companies' AI are done in a standardized and stringent manner. There are virtually no industry-wide or legal

---

<sup>69</sup> Narayanan, *supra* note 65.

<sup>70</sup> Enforcement against unsubstantiated claims in AI can also be pursued by the Attorney General under California's Unfair Competition Law.

<sup>71</sup> Drew Harwell, *Rights Group Files Federal Complaint Against AI-Hiring Firm HireVue, Citing 'Unfair and Deceptive' Practices*, WASH. POST (Nov. 6, 2019), <https://www.washingtonpost.com/technology/2019/11/06/prominent-rights-group-files-federal-complaint-against-ai-hiring-firm-hirevue-citing-unfair-deceptive-practices/>.

<sup>72</sup> Cal. Civ. Code § 1798.185(a)(18).

standards for what kinds of information companies should be providing to auditors about their technology in order for an audit to take place, and even what the audit should be addressing. Considering AI applications are diverse and varied, these standards need to be nuanced based on the technology's impact.

Certain private auditing companies market their auditing services to AI companies in the hopes of mitigating some potential harm. However, since there are no legal requirements for a third-party audit in most cases, the incentive structure here is skewed in a way that may not be optimal for unbiased and robust testing. Companies that voluntarily undergo auditing may be doing it as a PR stunt, either to push back against criticism of their product or to attempt to show some kind of transparency.<sup>73</sup> Furthermore, due to the lack of requirements in making the results of audits public, companies can cherry-pick and publish the positive attributes of their audit results while withholding the auditors' acknowledgement and assessment of any potential harms.

Since there are generally no real requirements for companies to have to undergo an audit at all, AI companies likely have a decent amount of leverage in terms of what types of audits they want to undergo, what specific algorithms they want to be audited, and how much of their information they want to give to auditors (even under an NDA). The incentive structure here is clearly skewed towards AI companies that in most cases do not legally need the services of these auditors. Furthermore, as the number of auditing companies increase, they will likely be competing on a basis of audits that are most comfortable and convenient for AI companies, reducing some of the potential benefits that a stringent and standardized audit can provide. It is also likely that different auditing companies have wildly different techniques in terms of which biases/issues they search for and how they go about identifying them — Auditor A might obtain a significantly different impact assessment of a company's algorithm than Auditor B. Finally, the results of these audits are not usually something companies legally need to address if there is indeed a problem.

Overall, there is a lack of industry and legal standards for what an audit should be composed of, what issues of bias and other harm need to be addressed, and what kinds of information about the technology companies need to provide to auditors to carry out the audit. There is also a lack of transparency requirements regarding how the results of these audits should be released to the public (if at all) and, most importantly, how companies need to address the results of the audit.

We recommend that the CPPA design an accreditation system for private auditing companies, require companies that deploy algorithms with significant legal effects (including but not limited to housing, employment, insurance, credit/lending) undergo audits, and establish

---

<sup>73</sup> Alfred Ng, *Can Auditing Eliminate Bias from Algorithms?* THE MARKUP (Feb. 23, 2021), <https://themarkup.org/ask-the-markup/2021/02/23/can-auditing-eliminate-bias-from-algorithms>.

what audits for particular applications should consist of and what information companies must disclose to auditors about their technology. The Agency should also require that auditors disclose the results of a company's audit if discrimination based on a protected class is identified and the company has not been able to mitigate the issue within a specified period of time.

## VI. Consumers' Right to Correct

Studies of the credit reporting error reinvestigation process under the Fair Credit Reporting Act (FCRA) can be instructive with respect to error correction under CPRA.<sup>74</sup> Credit reporting errors are pervasive — in a recent Consumer Reports study, 34% of participants found at least one error on one of their credit reports.<sup>75</sup> Under the FCRA, when a consumer reports an error, consumer reporting agencies (CRAs) have a legal responsibility to investigate the issue fully.<sup>76</sup> But the automated system developed by the CRAs to resolve disputes does not always adequately address consumer complaints. The dispute investigation system places much of the power to adjudicate the dispute into the hands of the data furnisher, which often performs just a cursory investigation.<sup>77</sup> With respect to the CPRA's requirement to "use commercially reasonable efforts to correct the inaccurate personal information" about a consumer,<sup>78</sup> and pursuant to the Agency's authority to develop regulations with respect to businesses' responses to correction requests,<sup>79</sup> we recommend adopting regulations that help address these potential issues under CPRA.

---

<sup>74</sup> Syed Ejaz, *A Broken System: How the Credit Reporting System Fails Consumers and What to Do About It*, CONSUMER REPORTS (Jun. 10, 2021), <https://advocacy.consumerreports.org/wp-content/uploads/2021/06/A-Broken-System-How-the-Credit-Reporting-System-Fails-Consumers-and-What-to-Do-About-It.pdf>; Chi Chi Wu et al., *Automated Injustice Redux: Ten Years After a Key Report, Consumers Are Still Frustrated Trying to Fix Credit Reporting Errors*, NAT'L CONSUMER LAW CTR. (Feb. 2019), [https://www.nclc.org/images/pdf/credit\\_reports/automated-injustice-redux.pdf](https://www.nclc.org/images/pdf/credit_reports/automated-injustice-redux.pdf). NCLC has found that despite significant credit reporting reforms over the course of the last decade, serious problems with the credit reporting dispute process remain; *Key Dimensions and Processes in the U.S. Credit Reporting System: A review of how the nation's largest credit bureaus manage consumer data*, CONSUMER FIN. PROTECTION BUREAU (Dec. 2012), [https://files.consumerfinance.gov/f/201212\\_cfpb\\_credit-reporting-white-paper.pdf](https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf); Chi Chi Wu, *Automated Injustice: How a Mechanized Dispute System Frustrates Consumers Seeking to Fix Errors in their Credit Reports*, NAT'L CONSUMER LAW CTR. (Jan. 2009), [https://www.nclc.org/images/pdf/pr-reports/report-automated\\_injustice.pdf](https://www.nclc.org/images/pdf/pr-reports/report-automated_injustice.pdf); Maureen Mahoney, *Errors and Gotchas: How Credit Report Errors and Unreliable Credit Scores Hurt Consumers*, CONSUMERS UNION (2014), <https://advocacy.consumerreports.org/research/errors-and-gotchas-how-credit-report-errors-and-unreliable-credit-scores-hurt-consumers/>.

<sup>75</sup> *A Broken System*, *supra* note 77, at 4.

<sup>76</sup> 15 U.S.C. § 1681(a)(1)(A).

<sup>77</sup> See, e.g., Chi Chi Wu, *Automated Injustice*, *supra* note 77, at 21-25; *Key Dimensions*, *supra* note 77, at 35.

<sup>78</sup> Cal. Civ. Code § 1798.106(a).

<sup>79</sup> *Id.* at § 1798.185(a)(8)(A).



- a. Businesses should be required to delete disputed information if it cannot provide documentation to back it up.

In ensuring that consumers are able to correct inaccurate information pursuant to CPRA,<sup>80</sup> and in developing rules on businesses' responses to correction requests,<sup>81</sup> the CPPA should direct companies to delete disputed information that cannot be backed up with documentation. With respect to credit reporting, the CRAs and furnishers primarily rely on an automated online system known as e-OSCAR to transmit information about disputes to one another, and to resolve them.<sup>82</sup> However, it does not always serve the best interests of consumers. First, CRA call center agents have often not been equipped to provide consumers with the help they need. In 2013, Experian call center agents in Santiago, Chile revealed that they had no power to actually investigate error complaints, but merely to code the disputes, and accept the account of the furnisher.<sup>83</sup>

The CRAs allow the furnishers a great deal of power in conducting the investigations and determining whether or not an error has occurred. The CRAs often take the word of the furnisher in handling these complaints. This is problematic for consumers for two reasons. First, this unfairly places the responsibility on the consumer to show that the furnisher has made a mistake.<sup>84</sup> FCRA requires CRAs to remove any information from a report that "cannot be verified," thus furnishers have the responsibility to prove the consumer wrong.<sup>85</sup> Second, furnishers often fail to conduct a thorough investigation into the problem, which raises questions about the veracity of their claims in some cases.<sup>86</sup>

Furnisher investigations are inadequate to correct many types of errors. According to an industry source, attorney Anne P. Fortney, a typical furnisher investigation had the employee "at a minimum, verify the consumer information by matching the name, Social Security number and other pertinent data; and review the account history, including payment history and any historical notes related to the account."<sup>87</sup> These investigations can be lacking, especially when the errors

---

<sup>80</sup> *Id.* at § 1798.106(a).

<sup>81</sup> *Id.* at § 1798.185(a)(8)(A).

<sup>82</sup> Report to Congress on the Fair Credit Reporting Act Dispute Process, FED. TRADE COMM'N at 15 (2006), <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-and-board-governors-federal-reserve-system-report-congress-faircredit/p044808fcradisputeprocessreporttocongress.pdf>; e-OSCAR, [www.e-oscar.org](http://www.e-oscar.org).

<sup>83</sup> *Steve Kroft, 40 Million Mistakes: Is Your Credit Report Accurate?*, CBS NEWS (Aug. 25, 2013), <http://www.cbsnews.com/news/40-million-mistakes-is-your-credit-report-accurate-25-08-2013/> (60 Minutes broadcast originally aired on Feb. 10, 2013) (see 2 of transcript).

<sup>84</sup> *Automated Injustice*, *supra* note 77, at 28.

<sup>85</sup> 15 U.S.C. § 1681i(a)(5)(A).

<sup>86</sup> *Automated Injustice Redux*, *supra* note 77, at 14-15.

<sup>87</sup> Credit Reports: Consumers' Ability to Dispute and Change Inaccurate Information: Hearing Before the H. Comm. on Fin. Servs., 110th Cong. (2007) (statement of Anne P. Fortney), <http://archives.financialservices.house.gov/hearing110/osfortney061907.pdf> (see 9 of PDF).

were already caused by or reflected in the furnisher's computer records. In other cases, it is clear that the employees in charge of the reinvestigation fail to uphold even these minimum standards.

Many courts have found that the existing procedures CRAs and furnishers use fall short of what constitutes a "reasonable" investigation as required by FCRA. For example, In *Dickman v. Verizon Communications, Inc.* (2012), the court refused to dismiss the case against Verizon and found that there were questions about the adequacy of their investigation process in part because, as the plaintiff argued, Verizon informed the CRAs "that he had become delinquent on the [n]ew [a]ccount three months before he actually opened it."<sup>88</sup> This error revealed that Verizon had not fully investigated the error complaint, since it supplied information that was clearly false. Verizon claimed that it followed a similar procedure as described by Fortney to investigate errors—checking the account, verifying the name and other identifiers, and looking at the record of past payments.<sup>89</sup>

In *Boggio v. USAA Federal Savings Bank* (2012), USAA employees responded to an error complaint by simply reconfirming the plaintiff's identity, and did not review any underlying documentation in his file.<sup>90</sup> The court denied USAA's motion for summary judgment in their favor because it could not conclude that USAA's investigation was "reasonable" as a matter of law.<sup>91</sup> The plaintiff sued because he believed he was incorrectly listed as a "co-obligor" on his ex-wife's loan—information that had been forwarded to the CRAs.<sup>92</sup> Deposition testimony revealed that USAA employees are "not permitted to make any phone calls to anyone" or review any documents submitted by paper.<sup>93</sup>

*Dixon-Rollins v. Experian Information Solutions, Inc.* (2010) revealed that TransUnion and furnishers did not conduct a reasonable investigation of the plaintiff's dispute as required by law.<sup>94</sup> The court upheld the judgment and award for the plaintiff, finding that TransUnion had not fulfilled its duty to investigate in part because it did not forward any of the documentation that plaintiff Dixon-Rollins provided to the debt collector during the reinvestigation, and simply accepted the debt collector's word.<sup>95</sup> Although Dixon-Rollins had paid off the debt, her four attempts to have the incorrect information altered on her credit report were in vain.<sup>96</sup> The debt

---

<sup>88</sup> 876 F.Supp.2d 166, 174 (E.D.N.Y. 2012).

<sup>89</sup> *Id.* at 173.

<sup>90</sup> 696 F.3d 611, 619 (6th Cir. 2012).

<sup>91</sup> *Id.* at 619-20.

<sup>92</sup> *Id.* at 613.

<sup>93</sup> Brief for Appellant, *Boggio v. USAA Fed. Sav. Bank*, 696 F.3d 611, 2012 WL 2481111, at \*8 (6th Cir. 2012) (No. 11-4040.)

<sup>94</sup> *Dixon-Rollins v. Experian Info. Solutions, Inc.*, 753 F. Supp. 2d 452, 465 (E.D. Pa. 2010) (defendant "repeatedly failed to carry out its statutory duty" under FCRA). The plaintiff sued both Experian and TransUnion, but reached a settlement with Experian. *Id.* at 456.

<sup>95</sup> *Id.* at 456-7, 459. The award was reduced, however. *Id.* at 456.

<sup>96</sup> *Id.* at 457.

collector simply checked its records and reconfirmed to the CRA—incorrectly—that the debt had not been paid.<sup>97</sup>

These examples help to demonstrate how minimal steps taken by CRAs and furnishers do not always properly address or even clarify the underlying dispute. In many cases, CRAs have accepted the word of the furnisher, even when they don't have evidence to back up their case. This is true even for disputes from furnishers who are debt collectors. CRAs have accepted a furnisher's response to the dispute, even if the consumer is actually correct, has documentation that she is correct, and the furnisher has sent nothing to back up its response. The National Consumer Law Center notes that this not only places the burden of proof on the consumer, it unfairly gives the furnisher the role of being the judge in the dispute against it.<sup>98</sup>

Therefore, to ensure that consumers are able to correct inaccurate information pursuant to CPRA, the agency should direct companies to delete disputed information that cannot be backed up with documentation. Businesses should not simply accept the word of the data provider in a dispute without any evidence. Disputed information should be removed from a consumer's record if the provider is unable to provide documented proof of its claims following a consumer dispute.

b. Businesses should delete challenged information that they cannot link to a single identifiable consumer.

In developing rules on businesses' responses to correction requests,<sup>99</sup> the agency should direct companies to delete disputed information when it cannot be linked to a single identifiable consumer. So-called "mixed files" — in which information from multiple people, often family members with similar names and the same address, is pulled into a single credit report — are a common source of credit reporting mistakes.<sup>100</sup> The case of *Miller v. Equifax Information Services LLC* (2013)<sup>101</sup> highlighted some of these lapses in the CRA investigation system, especially when trying to correct a mixed file. In this case, the court upheld the judgment and granted Julie Miller \$1.8 million in both punitive and compensatory damages after Equifax ignored her efforts to remove errors from her credit report.<sup>102</sup> Over the course of two years, Miller challenged a number of collections entries on her credit report that did not belong to her,

---

<sup>97</sup> *Id.*

<sup>98</sup> Making Sense of Consumer Credit Reports: Hearing Before the Subcomm. on Fin. Inst. and Consumer Protection of the Sen. Comm. On Banking, Housing and Urban Affairs, 112th Cong. (2012) (statement of Chi Chi Wu, NCLC), available at [http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore\\_id=1b5d9716-9a48-4757-90d8-7a69d33af0ca](http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=1b5d9716-9a48-4757-90d8-7a69d33af0ca) (see 22-24 of PDF).

<sup>99</sup> *Id.* at § 1798.185(a)(8)(A)

<sup>100</sup> *Automated Injustice Redux*, *supra* note 77, at 13-14.

<sup>101</sup> No. 11-1231 (D. Or. Jan. 29, 2014).

<sup>102</sup> *Miller*, No. 11-1231, slip. op. at 2. At trial, the jury had granted \$18 million. *Id.*



but Equifax failed to remove them.<sup>103</sup> Equifax’s representative testified that while she couldn’t conclusively explain the reason for this lapse, Equifax employees may have let the marks remain because they couldn’t verify the plaintiff as the owner of the credit file.<sup>104</sup> Although Equifax maintained that it established special procedures to deal with a mixed file, in this case, standard procedures were not followed.<sup>105</sup>

These mixed files are likely to be even more common with respect to information held by data brokers, since information, such as about browsing history, could likely be linked to all consumers that use a particular device. Thus, businesses should delete challenged information that they cannot link to a single identifiable consumer.

- c. Businesses should be required to review correction requests in which the consumer submits new information that is relevant to the complaint, unless the request appears to be vexatious or in bad faith.

Given the challenges that consumers have experienced in correcting credit reporting errors, it is likely that they will encounter similar problems in correcting errors under the CCPA. With respect to the new correction rights under the CPRA, the CPPA has authority to establish “[H]ow often, and under what circumstances, a consumer may request a correction” of their personal information.<sup>106</sup> Consumers should be permitted to submit additional documents or evidence in support of their dispute, without having to worry that the dispute will be marked “frivolous” and dismissed. Such dismissals occur all too often in credit reporting disputes.<sup>107</sup> Thus, companies should be required to consider new information and documentation provided to them by consumers even in an ongoing dispute, as long as it is relevant to the complaint.

Of course, if a bad actor were attempting to interfere with the functioning of the service by sending hundreds of requests per day, it would be reasonable just to ignore these bad-faith requests and not look up the consumer's file each time.

---

<sup>103</sup> Complaint at 6, *Miller v. Equifax Info. Servs.*, No. 11-1231 (D. Or. Jan. 29, 2014); see also Laura Gunderson, *Equifax Must Pay \$18.6 Million After Failing to Fix Oregon Woman's Credit Report*, THE OREGONIAN (July 26, 2013), [http://www.oregonlive.com/business/index.ssf/2013/07/equifax\\_must\\_pay\\_186\\_million\\_a.html](http://www.oregonlive.com/business/index.ssf/2013/07/equifax_must_pay_186_million_a.html) (noting that the Miller judgment would be the largest award ever obtained in a case against a major CRA).

<sup>104</sup> Transcript of Record at 278-84, *Miller v. Equifax Info. Servs.*, No. 11-1231 (D. Or. Jan. 29, 2014).

<sup>105</sup> *Id.* at 442-47.

<sup>106</sup> Cal. Civ. Code § 1798.185(a)(8).

<sup>107</sup> *Automated Injustice Redux*, *supra* note 77, at 21-22.

## VII. Consumers' Right to Know

- a. In response to a verifiable request, businesses should be required to provide all information that belongs to that identifiable consumer, even if it is beyond the 12-month window.

Businesses should not reidentify information in order to respond to an access request. But if the company has identifiable data, it should provide that data to the consumer or their authorized agent pursuant to an access request, even if the data is older than 12 months.<sup>108</sup> Since this access requirement applies only to data collected on or after January 1, 2022,<sup>109</sup> and businesses have been required to comply with access requests since 2020, they will have had ample time to prepare to respond to such requests.

If a company collects and retains a consumers' personal information, at the very least, they should give the consumer the ability to access that information. These access rights are necessary for consumers seeking to take additional action to exercise their portability and correction rights. Further, the information consumers receive through such access requests may cause them sufficient concern that they then decide to delete or stop the sale of this information.

And businesses should be incentivized to get rid of old data. Retaining old and unnecessary data is a serious security risk; a recent data breach at Capital One involved data that was more than ten years old.<sup>110</sup> Exempting old data from access requests doesn't help businesses or consumers when there is such a threat of inadvertent disclosure. The CCPA changed the incentive structure for maintaining data: companies that previously had no reason to map data finally had to do so in order to be prepared to respond to requests — leading some of them to delete old data that was no longer needed.<sup>111</sup> But unless companies are held to the requirement to honor access requests with respect to data that is more than a year old, companies will have fewer incentives to do so.

Finally, the CPRA requires companies to delete data that is no longer necessary for disclosed purposes,<sup>112</sup> so it should not be too burdensome for companies to respond to access requests for the remaining data.

---

<sup>108</sup> Cal. Civ. Code § 1798.185(9).

<sup>109</sup> *Id.* at § 1798.130(a)(2)(B).

<sup>110</sup> Emily Flitter and Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, N.Y. TIMES (Jul. 29, 2019), <https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html>.

<sup>111</sup> Kaveh Waddell, *California Privacy Law Prompts Companies to Shed Consumer Data*, CONSUMER REPORTS (Feb. 11, 2020), <https://www.consumerreports.org/privacy/california-privacy-law-ccpa-prompts-companies-to-shed-consumer-data-a8999779184/>.

<sup>112</sup> Cal. Civ. Code § 1798.100(3).

## VIII. Non-Discrimination

Californians have a right to privacy under the California Constitution, and consumers should not be charged for exercising those rights.<sup>113</sup> Unfortunately, there is contradictory language in the CCPA, including as amended by CPRA, that could give companies the ability to charge consumers more for opting out of the sale of their data or otherwise exercising their privacy rights.<sup>114</sup> We offer several recommendations to help ensure that these loopholes are not inappropriately exploited.

- a. The CPPA should clarify that financial incentives in markets that lack competition is an unfair and usurious practice.

To prevent some of the worst abuses associated with financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The CCPA prohibits financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.<sup>115</sup> And, the CPPA currently has the authority under CPRA to issue rules with respect to financial incentives.<sup>116</sup> Thus, we urge the CPPA to exercise its authority to prohibit the use of financial incentives in market sectors that lack competition. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates — about \$30 per month — for not leveraging U-Verse data for ad targeting.<sup>117</sup> Where consumers have few choices, market forces don't impose sufficient constraints on companies from penalizing exercising privacy rights. And, there is rising concentration across many industries in the United States,<sup>118</sup> further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.<sup>119</sup> The CPPA should exercise its authority to put reasonable limits on these programs in consolidated markets.

---

<sup>113</sup> Cal. Cons. § 1, [https://leginfo.legislature.ca.gov/faces/codes\\_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I](https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I).

<sup>114</sup> Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).

<sup>115</sup> *Id.* at § 1798.125(b)(4).

<sup>116</sup> *Id.* at § 1798.185(a)(6).

<sup>117</sup> Jon Brodtkin, *AT&T To End Targeted Ads Program, Give All Users Lowest Available Price*, ARS TECHNICA (Sept. 30, 2016), <https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/>.

<sup>118</sup> *Too Much of a Good Thing*, THE ECONOMIST (March 26, 2016), <https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing>.

<sup>119</sup> *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets*, FED. TRADE COMM'N (Feb. 26, 2019), <https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology>.



- b. Businesses must calculate the value of the data to the business and make it available per access requests before being permitted to share data with third parties pursuant to loyalty programs.

Under the existing CCPA regulations, companies that provide financial incentives to consumers that could implicate their CCPA rights are required to give notice, including “A good-faith estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference[.]”<sup>120</sup> However, a check of two top loyalty programs suggests that too many companies aren’t taking this requirement seriously, offering only vague explanations in their disclosures with respect to the value of consumers’ data.<sup>121</sup>

The CPPA should carry over the prohibition on discrimination if a company cannot meet the affirmative burden of offering a good faith estimate and demonstrating that a financial incentive is reasonably related to the value of the data. It should specifically extend that idea to loyalty programs, to prohibit secondary sharing unless a company can meet those two evidentiary burdens.

## **IX. Conclusion**

We thank the CCPA for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Maureen Mahoney ([REDACTED]) for more information.

---

<sup>120</sup> Cal. Code Regs tit. 11 § 999.307(b)(5)(a).

<sup>121</sup> See, for example, Sephora, Privacy Policy, Notice of Financial Incentive, “The value of your personal information to us is related to the value of the free or discounted products or services, or other benefits that you obtain or that are provided as part of the applicable Program, less the expense related to offering those products, services, and benefits to Program participants[.]” (Nov. 1, 2021), <https://www.sephora.com/beauty/privacy-policy#USNoticeIncentive>; CVS, Privacy Policy, Financial Incentives, Member Special Information, “The value we place on the personal information in connection with these incentives is calculated by determining the approximate additional spending per customer, per year compared to individuals who are not enrolled in ExtraCare[.]” (Sept. 16, 2021), [https://www.cvs.com/help/privacy\\_policy.jsp#noticefi](https://www.cvs.com/help/privacy_policy.jsp#noticefi).

---

**From:** Edwin Portugal [REDACTED]  
**Sent:** 11/8/2021 2:03:51 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Castanon, Debra@CPPA [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b9766af8eba04290bfa5ae3e150c60e7-Castanon, D]; Matt Kownacki [REDACTED]; Danielle Arlowe [REDACTED]  
**Subject:** AFSA Comment Letter re: CPRA rules PRO 01-21  
**Attachments:** AFSA comment letter - PRO 01-21 CA CPPA privacy rulemaking.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Dear Ms. Castanon,

Attached is a comment letter from the American Financial Services regarding the California Privacy Protection Agency's proposed rules PRO 01-21. Thank you in advance for consideration of our comments.

Please do not hesitate to reach out to us if you have any questions.

Thanks,  
Edwin



**Edwin Portugal**  
*State Government Affairs Analyst*



[@AFSA\\_DC](#) | [LinkedIn](#) | [@AFSA\\_SGA](#)

November 8, 2021

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

**Re: PRO 01-21 — Preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020**

Dear Ms. Castanon:

On behalf of the American Financial Services Association (“AFSA”),<sup>1</sup> thank you for the opportunity to provide comments on the California Privacy Protection Agency’s (“Agency”) invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (PRO 01-21). AFSA members share the state’s goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access.

**Extension of Employee and B2B Exemption**

The California Privacy Rights (CPRA) extends the CCPA’s partial exemption of employee and business contact data until January 1, 2023. The partial employee exemption specifically exempts personal information that is collected by a business about a person in the course of the person acting as a “job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of” the business to the extent that the personal information is collected and used solely within the employment context. The exemption also applies to personal information used for emergency contact purposes, as well information that is necessary to administer employment benefits. Under the exemption, employers are still required to inform employees and applicants, at or before the time of collection, of the categories of personal information to be collected and the purposes for which the information will be used (i.e., a “notice at collection”). Further, employers are not exempt from the “duty to implement and maintain reasonable security procedures and practices,” and employees and applicants retain the private right of action in the event that certain of their personal information is subject to a data breach.

Under the business-to-business exemption, businesses are not required to provide certain notices or extend certain consumer rights to their business contacts. Specifically, the exemption applies to information “reflecting a written or verbal communication or a transaction” between the business and an employee or contractor of another organization (i.e., a business, non-profit or government agency), where the communication or transaction occurs in the context of (1) the business conducting due diligence on that other organization, or (2) the business providing or receiving a product or service to or from such organization.

---

<sup>1</sup> Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.



The expiration of the exemptions will leave employees, job applicants, employers and individuals serving other businesses in a service provider context confused regarding the interplay between the CPRA and employment laws because most of the rights under the CPRA either are already addressed or do not make sense in the employment or B2B context.

We request that the regulations make the exemptions permanent or extend them to allow for additional time to comply. This would be in line with the approach of other states such as Colorado and Virginia who chose to exclude human resources data from the scope of their privacy laws, along with proposed legislation (e.g., New York and North Carolina) not including employee or B2B data within their purview. It is no surprise these states chose not to include employee or B2B data within their scope because most privacy rights are either already addressed under other existing laws or do not apply in the employment or B2B context. For example, in California, employees already have the right to access their payroll records, their employment agreements and broadly their personnel file. Additionally, under California law, an employer may not “discriminate, retaliate, or take any adverse action against an employee” if the employee decides to correct his or her data by updating or changing “name, Social Security number, or federal employment authorization document.” Job applicants may also challenge an employer’s decision to deny employment that was erroneously based on a conviction history report. And as a general matter, it is an unlawful practice under California employment laws to discriminate against an employee for opposing any unpermitted practices or exercising his or her rights under the law.

Furthermore, other rights under the CPRA (e.g. right to opt out of the sale or sharing of data and the right to limit the use of sensitive personal information) do not apply in the employment or B2B context. Businesses do not sell employee or service provider data and do not track employees or service providers for targeted advertisements, so there is no need to opt out of selling or sharing. Also, there is no need to limit the use of sensitive personal information because it is collected solely for human resources functions or tax compliance purposes.

If the exemptions are not permanently extend the regulations should align employment and privacy rights in the CPRA regulations by: (1) defining “professional or employment-related information” to mean an employee’s personnel file or in a case of a B2B interaction the individuals personal contact information (business information such as work email address, business location, title, etc. should be excluded); (2) clarifying that the right to correct is limited to rectifying objective personal information that can be verified through official documentation, such as correcting a name, an address or other data generally maintained under official government records; and (3) ensuring the CPRA’s deletion right does not contradict legal retention obligations under employment or other laws (e.g. California Labor Code § 1198.5 Equal Employment Opportunity Commission regulations, Age Discrimination in Employment Act and Fair Labor Standards Act) requires employers to maintain a copy of each employee’s personnel records for a period of no less than three years after termination of employment .

**Processing that presents a significant risk to consumers’ privacy or security, including cybersecurity audits and risk assessments performed by businesses.**

Section 1798.185(a)(15) of the California Privacy Rights Act (CPRA) involves issuing regulations requiring businesses to conduct annual cybersecurity audits and “regular” risk assessments if the business’s “processing of consumers’ personal information presents significant risk to consumers’



privacy or security.” In determining whether the processing “may result in significant risk to the security of personal information,” the CPRA identifies two factors to be considered: (1) the size and complexity of the business; and (2) the nature and scope of processing activities.

The CPRA's risk assessment requirement is similar to the EU General Data Protection Regulation. Article 35 mandates a data protection impact assessment be carried out in consultation with the data protection officer for processing “likely to result in a high risk,” but unlike the CPRA, it does not require DPIAs to be filed with a regulatory authority. While Article 35 identifies particular circumstances where DPIAs are necessary, it also calls for guidance regarding what kind of processing is subject to the DPIA requirement. Both the European Data Protection Board and individual countries, like the U.K. Information Commissioner's Office, have issued such guidance. Such guidance can be instructive to the CPPA as they develop regulations. However, as discussed below, financial institutions are already subject to sufficient regulatory requirements for the protection of consumer data.

The Gramm-Leach-Bliley Act Safeguards Rule (16 CFR 313.1 *et seq*) already sets forth standards for covered financial institutions for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. Additionally, the Safeguards Rule already requires that covered financial institutions routinely audit, test and monitor the risks in order to evaluate and adjust their information security program. Such safeguards ensure that data that presents a heightened risk to the privacy of consumers is appropriately protected. Requiring covered financial institutions to comply with the audit and risk assessment provisions of the CPRA is over-burdensome and unnecessary. Duplicative regulatory burdens resulting in increased costs to consumers without a tangible benefit.

### **Consumers’ right to delete and right to correct.**

*Right to Delete.* Under the CPRA, the “right to delete” seems to remain largely the same except for one notable change—in addition to directing service providers to delete consumer’s personal information from their records upon receiving a verifiable consumer request, businesses will also be required to notify “contractors” to do the same, “and notify all third parties to whom the business has sold or shared such personal information, to delete the consumer’s personal information, unless this proves impossible or involves disproportionate effort.”

What qualifies as “disproportionate effort” is not defined. We request that the regulations provide clarification and guidance regarding what is needed to establish whether deletion is impossible or involves disproportionate effort. At the very least, data that is not stored in a structured database (unstructured data) be explicitly excluded from the requirement to delete.

*Right to Correct.* Under the CPRA, consumers have a new right to request a business that maintains inaccurate personal information about the consumer correct such inaccurate personal information, taking into the account the nature of the personal information and the purposes of the processing of the personal information. Financial institutions are subject to laws and regulations such as GLBA and the Fair Credit Reporting Act (FCRA), which would exempt much of the information that financial institutions hold from the right to correct. However, we would suggest that the CPRA regulations further clarify and define that the right to correct non-exempt data be limited to data that is not subjective (e.g.



name, address, SSN, etc.). Any type of data that is subjective or cannot be independently verified as true and correct should not be subject to the right to correct.

### **Consumers' rights to opt out of sharing of their personal information**

*Sharing.* "Sharing" is a new defined term under the CPRA and 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. The CPRA imposes several additional responsibilities on business that "share" personal information. They must disclose the "sharing" to consumers in their privacy policy, give consumers a way to opt out, and post a "Do Not Share My Personal Information" link on their homepage.

The addition of "sharing" seems directly targeted at online advertising but it is unclear on how it will impact the activities of businesses that use cookies on their websites to track consumers. When consumers use or direct a business to "intentionally interact" with third parties, it is not considered a "sale" or the "sharing" of personal information. Deliberate interactions such as visiting an entity's website or purchasing goods or products from a party may constitute "intentional interactions" as defined in the CPRA. We request that the regulations further clarify and define what the types of intentional interactions that would not be considered "sharing." For example, if a consumer visits a lender's website to view their rates and terms is that an intentional interaction. If that information is shared with Google to display loan ads to the customer, would that be considered "sharing"?

### **Look-Back Period for Consumer Requests**

Although the CPRA does not come into effect until January 1, 2023, consumer requests to access data can "look back" at data collected by a business on or after January 1, 2022. Moreover, for any personal information collected starting January 1, 2022, the CPRA gives consumers the right to make a request to know beyond the CCPA's standard one-year look back. The exception to this expanded right is if such a look-back request would be "impossible" or require "disproportionate" effort. We request that the CPRA regulations define a specific look-back period (e.g. 12 to 24 months) or at the least clarify that business that have purged or cannot otherwise retrieve data using reasonable effort be exempt from a longer look-back period. The Section 1798.145(j)(2) of the CPRA does state that nothing in the CPRA requires businesses to keep personal information for any specified length of time or to retain personal information about a consumer if it otherwise would not in its "ordinary course of business," so the regulations should clarify that businesses are not required to provide information that has been purged or is otherwise not retrievable without unreasonable effort (e.g. data stored in back-up servers).

### **Sensitive Personal Information**

Pursuant to the CPRA, consumers have the right to restrict a business's use of sensitive personal information to, among other things, that use which is necessary to perform the services or provide the goods or services requested; to certain "business purposes" identified in the CPRA; and as otherwise authorized by CPRA regulations. Examples of such business purposes include verifying consumer



information, fulfilling transactions, providing financing and payment processing, providing advertising and marketing, except for cross-context behavioral advertising. Businesses that use sensitive personal information for purposes other than those specified in the CPRA are also required to provide consumers notice of such use and inform them of their right to limit the use or disclosure of their sensitive information. As with the right to opt out of the sale of personal information under the CCPA, businesses may opt to providing such right through a new, separate link titled "Limit the Use of My Sensitive Information" posted on the business's internet homepage, or, at the business's discretion, utilizing a single, clearly-labeled link that allows a consumer to both opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

We ask that the regulations clarify that the requirements to allow customers to limit the use of sensitive information and provide customers with an opt-out link be limited to consumer data that is not subject to the GLBA. Furthermore, the rights regarding sensitive information should not be extended to employees or information provided in the B2B context.

Additionally, we request that the regulations exclude employee, job applicant and B2B information from the rights relating to sensitive personal information. Those rights do not apply in the employment or B2B context. Businesses do not sell employee, job applicant or service provider data and do not track those individuals for targeted advertisements, so there is no need to opt out of selling or sharing. Likewise, sensitive personal information is collected solely for human resources functions or tax compliance and not for any other purpose, so there is no need to "limit" the use of such data.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact me at [REDACTED] or [REDACTED].

Sincerely,

[REDACTED]  
Matthew Kownacki  
Director, State Research and Policy  
American Financial Services Association

---

**From:** MacGregor, Melissa [REDACTED]  
**Sent:** 11/8/2021 2:09:23 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Chamberlain, Kim [REDACTED]  
**Subject:** PO 01-21  
**Attachments:** California CPPA Regulatory Response November 8 2021 FINAL.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Please see the attached response to the **Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)**. Please let me know if you have any questions.

**Melissa MacGregor**  
Managing Director and Associate General Counsel  
SIFMA  
1099 New York Avenue, NW, Washington, DC 20001

[REDACTED]  
[www.sifma.org](http://www.sifma.org)  
@SIFMA





November 8, 2021

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

**Re: Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)**

Dear Ms. Castanon:

The Securities Industry and Financial Markets Association ("SIFMA")<sup>1</sup> welcomes the opportunity to respond to the California Privacy Protection Agency ("CPPA") Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 ("CPRA").<sup>2</sup> SIFMA previously provided comments on the Attorney General's rulemaking under the California Consumer Privacy Act of 2018 ("CCPA").<sup>3</sup> SIFMA and its members are strongly committed to the protection of consumer data, privacy, and security, and its members have operated for years under the well-established protections of the Gramm-Leach-Bliley Act. SIFMA is responding to several of your specific requests but is also providing some additional thoughts on what other areas may be ripe for additional guidance from the CPPA.

**1. Audits and Risk Assessments**

SIFMA members perform audits and risk assessments for many purposes – including privacy and data protection – under various federal and state mandates. SIFMA believes that any additional rulemaking or guidance provided on when a covered business meets the "significant risk to consumers' privacy or security" standard for initiating a risk assessment should focus on factors that should be considered in making this determination, which may align with triggers for other audits or risk assessments. Further, internal audits should satisfy the requirements so long as they meet the audit industry standards, thus balancing the need to provide or obtain relevant information without placing an undue burden on businesses, especially small businesses. In further developing any guidance on audits and assessments, the CPPA should consider implementing requirements similar to the requirements adopted by the New

---

<sup>1</sup> SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

<sup>2</sup> Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) (September 22, 2021), [https://cppa.ca.gov/regulations/pdf/invitation\\_for\\_comments.pdf](https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf)

<sup>3</sup> Letter from Melissa MacGregor, SIFMA to The Honorable Xavier Becerra (December 6, 2019), <https://www.sifma.org/resources/submissions/proposed-california-consumer-privacy-act-regulations-ccpa-rules/>.



York State Department of Financial Services (“NYDFS”) under 23 NYCRR Part 500 or Europe’s General Data Protection Act (“GDPR”) audit requirements. Many SIFMA members are currently complying with such audit and reporting requirements thus making compliance with a similar requirement in California more seamless and efficient in both jurisdictions. Further the NYDFS rules provide sufficient flexibility based on a company’s industry, size, locations, activities, etc.

SIFMA does not believe that additional rulemaking is necessary for assessing risks to consumer privacy versus benefits of businesses processing data, but additional guidance may be beneficial for further clarifying how the CPPA expects firms to make those assessments.

## **2. Automated Decisionmaking**

### **a. Activities deemed to constitute “automated decisionmaking technology” and/or “profiling”**

Automated decisionmaking technology has evolved and grown to become an important part of how some companies do business. In regulating the use of that technology, the CPPA should ensure that the CPRA is no more onerous than, and does not conflict with, equivalent requirements under GDPR as these are well-established requirements. The CPPA should limit the scope of the definition to cover only the processing of personal information solely by automated means, without human intervention, that may negatively impact a consumer’s legal rights. The definition should not include automated processes that do not impact a consumer’s legal rights such as the use of algorithms to flag suspicious transaction activity.

The existing definition of “profiling” under the CPRA does not require additional rulemaking as it is sufficiently clear, but additional guidance on the term may be helpful for covered businesses in interpreting the requirements.

### **b. Consumer access to information about businesses’ use of automated decisionmaking technology and processes consumers and businesses to facilitate access**

The CPPA should consider, for ease of consumer use and efficiency, using the same online method for making requests regarding automated decision-making, that the CCPA and CCPA regulations currently provide for regarding access and deletion requests for consumer information.

### **c. Responding to consumer access requests**

When responding to consumer access requests, the CPPA should consider allowing firms to use a consumer-friendly brief description of the logic involved including, for example, the categories of personal information or factors considered and relative consideration given to such categories or factors. The CPPA should also consider allowing covered businesses to use the same categories of personal information as provided for in the CCPA and CCPA regulations, if the covered business determines that it would be helpful for consistency and the consumer’s general understanding.



**d. Scope of consumer opt-out rights for automated decisionmaking and processes to facilitate opt-outs**

In drafting regulations to govern consumers' "access and opt-out rights with respect to businesses' use of automated decision-making technology," care should be taken to narrowly capture the activities within scope of definition of automated decision-making technology. Automated decision-making that is based upon the consumer's consent or is necessary to perform a contract between the business and the consumer should be excluded from the opt-out requirement. This approach is consistent with Article 22 of the GDPR where similar exceptions to the right of a data subject to opt out of automated processing are included. One example of how this exception would operate is where an individual gives their express consent for a loan application which results in a decision that uses automated decision-making technology. Additional areas that should be outside the scope of the consumer's right to opt-out with respect to automated decision-making are fraud and network security concerns, as businesses should be enabled to prevent system attacks and harm to individuals. This exception is also recognized in the GDPR under Recital 71 which permits automated decision-making for fraud purposes as permitted by law.

**3. Audits Performed by the CPPA**

Audits performed under the CPRA should be reasonably designed to assess a covered business' compliance with the CPRA and should be risk-based. The CPPA should take a principles-based approach including sampling the covered businesses policies, standards and procedures with associated evidence. The CPPA should give ample advance notice to covered businesses including all information requests. Audits should not be performed more frequently than once every three years unless the CPPA has reason to believe the subject company is not complying with the law. The CPPA's information requests should be narrowly tailored such that they are not unnecessarily burdensome to comply with but still provide adequate information to assess the company's compliance with the law, and the CPPA should remain open to a constructive dialog with the business about refining the scope of such requests where appropriate. Such audits should not include reviews of underlying personal information or reviews of any privileged communications or conversations. Further, covered businesses should not be required to give CPPA auditors unfettered access to company systems or data collection applications. Audits should be done in coordination with other regulators whenever possible to avoid duplication. Finally, any findings by the CPPA should be kept confidential and not subject to public information requests as they may contain sensitive information that may put consumers or the covered business at risk.

**4. Consumers' Right to Delete, Right to Correct, and Right to Know**

The CPRA amended the CCPA to allow consumers to request correction of inaccurate personal information held by covered businesses. Although SIFMA agrees that consumers should have the right to request material corrections of inaccurate information, covered businesses must have the ability to request sufficient information to authenticate the identity of the requesting party to prevent fraud or accidental or unnecessary changes to information. Further, consumers should only be able to request a correction of their information up to two times per year.

Covered businesses should also be permitted to take any steps necessary to prevent fraud including the misuse or misappropriation of personal information. The CPPA should not set a threshold time period for



a covered business to respond as not all businesses or types of information are the same or as easily accessible. Covered businesses should be granted a reasonable amount of time to respond which would afford businesses the necessary flexibility to triage requests that require immediate attention without sacrificing responsiveness to consumer needs. A business should be permitted to treat a request for correction as a request to delete personal information, particularly where the information is not maintained for critical business operations or the information has been provided via a third-party source.

Additionally, the CPPA might consider limiting the right to correct to only that personal information which the business has collected directly from the consumer or generated through its interactions with the consumer. Finally, covered businesses should have the right to object to or reject a request because the request is impossible, is without basis, or requires a disproportionate effort. Any additional guidance should include examples or circumstances for when covered businesses can lawfully reject those requests or require consumers to provide additional information before complying with those requests. A business that lawfully and appropriately rejects a request for correction should not be required to accept from the consumer a written addendum to the consumer's record. There is simply no reason to require a business to flag a record that the business has determined in good faith (and in compliance with the CCPA) need not be amended.

#### **5. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information**

The CPPA should take into consideration the efforts and investments that covered businesses have made to comply with the existing rules and regulations adopted under the CCPA. Any requirements and technical specifications must be reasonably supported by the platforms through which a business collects personal information to avoid covered businesses having to entirely redevelop their existing system. Businesses should not be required to embrace particular technological solutions that introduce unknown reputation, compliance or security risks without (a) safe harbor protections from the CPPA and (b) being afforded ample time to study these solutions and their potential implications for the business.

#### **6. Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information**

The CPRA includes the right to limit the use and disclosure of sensitive personal information by covered businesses if the sensitive personal information is collected or processed to infer characteristics about a consumer.<sup>4</sup> The scope of "inferences" and the processing of sensitive personal information that can be limited by consumers should be narrowly drawn toward discriminatory, harmful, and unexpected uses of sensitive personal information. Using and disclosing sensitive personal information for purposes that are reasonably foreseeable, or necessary to ensure that a product or service being offered to consumers is operating as intended, is secure, and complies with law, is not inferring information about a consumer and should not be interpreted as such. Moreover, the CPPA should consider refining the otherwise broad scope of "sensitive personal information" to encompass only those elements that are susceptible to inferences and exclude elements that are used for purposes such as identification and verification. For example, the processing of passport numbers, financial account numbers and account credentials is

---

<sup>4</sup> See 1798.121(d)(noting that "[s]ensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is *not* subject to this section.")(emphasis added).



unlikely to give rise to any inferences that cause material harm to consumers. This provision is intended to be narrow in scope, but if the scope is deemed to be broader, then there are various exemptions that may be necessary for covered businesses to be run effectively including responding to court orders or information that be necessary for the security of the covered business.

#### **7. Information to Be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)**

In considering regulations implementing how covered businesses must respond to consumer requests for information, the CPPA should take several things into account. First, businesses should not be required to disclose information not accessed by a business during its normal operations (e.g., information recorded on a storage device not readily accessible by the business during its regular operations or encrypted information to which the encryption key is not accessible by the business in its regular course of business). Businesses should also not be required to disclose information that is unreasonably voluminous or requires extraordinary cost.

#### **8. Definitions and Categories**

SIFMA and its members believe that “defining the business purposes for which businesses, service providers, and contractors may combine consumers’ personal information” is best left to the discretion of businesses and their service providers. In any event, it is important that any definition or guidance put forth by the agency emphasize that the mere act of combining personal information in the same database is not prohibited if the proper access controls are in place. By way of example, the FACTA Affiliate Marketing rule<sup>5</sup> (which prohibits the “use” of eligibility information received from affiliate for marketing purposes) establishes a framework whereby there is no violation of the rule if the affiliate receives the information through a common database but does not use it to make the solicitation. In short, putting personal information in the same place is not (and should not be) a problem. Rather, problems may arise when the holder of the information starts treating the entire data set as one consolidated mass for the holder to do with as it pleases.

\* \* \*

SIFMA appreciates the opportunity to provide these comments to the CPPA. If you would like to discuss this further, I can be reached at [REDACTED].

Sincerely,

[REDACTED]

Melissa MacGregor  
Managing Director and Associate General Counsel

cc: Kim Chamberlain, Managing Director & Associate General Counsel, State Government Affairs, SIFMA

---

<sup>5</sup> 12 C.F.R. § 41.20 *et seq.*

---

**From:** Adonne Washington [REDACTED]  
**Sent:** 11/8/2021 9:13:38 AM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** David Brody [REDACTED]  
**Subject:** Lawyers' Committee for Civil Rights Under Law Response to PRO 01-21  
**Attachments:** LCCRUL CA Comments.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Good afternoon,

On behalf of the Lawyers' Committee for Civil Rights Under Law, we are providing these comments in response to the California Privacy Protection Agency's Request for Comments, PRO 01-21. Please let us know if there is any additional information needed.

Best,

Adonne Washington (She/Her)  
Digital Justice Associate Counsel  
Lawyers' Committee for Civil Rights Under Law  
<https://lawyerscommittee.org/>



November 8, 2021

California Privacy Protection Agency  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

**Comments of the Lawyers' Committee for Civil Rights Under Law on the Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)**

The California Privacy Rights Act of 2020 ("CPRA") amends and extends the California Consumer Privacy Act of 2018 ("CCPA"), an act established to give consumers more control over the personal information that businesses collect.<sup>1</sup> To implement the law, the CPRA established a new agency, the California Privacy Protection Agency ("Agency") and vested it with the "full administrative power, authority and jurisdiction to implement and enforce the CCPA."<sup>2</sup> The Agency's responsibilities include updating existing regulations and adopting new regulations to enforce the CCPA and CPRA.<sup>3</sup> The Agency seeks input from stakeholders through a request for comment on the initiation of a consumer privacy rulemaking.<sup>4</sup> The Lawyers' Committee for Civil Rights Under Law ("Lawyers' Committee") provides this comment in response to the Agency's request.

The Lawyers' Committee is a national, nonprofit racial justice organization founded in 1963 at the request of President John F. Kennedy to mobilize the private bar to combat discrimination against Black Americans and other people of color. The Lawyers' Committee's Digital Justice Initiative focuses on issues at the intersection of technology, data, privacy, and civil rights to ensure that everyone can equally access and enjoy the Internet and the many opportunities it provides.<sup>5</sup>

Enacting strong privacy laws and regulations is essential to combatting discrimination on the basis of race, gender, religion, sexual orientation, disability, and other protected characteristics. Individuals' personal information is the raw material used by bad actors to discriminate in economic opportunities like housing and employment, to engage in election disinformation and voter intimidation, to exploit children and the elderly, and to target Black Americans and other groups for racist threats and harassment campaigns. This data also fuels advertisement targeting and content recommendation algorithms that reproduce and amplify historical and systemic discrimination.

---

<sup>1</sup> CA Civil Code, § 1798.100

<sup>2</sup> CA Civil Code, § 1798.199.10(a)

<sup>3</sup> *Id.*

<sup>4</sup> California Privacy Protection Agency, *Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020*, California Government: California Privacy Protection Agency (Sep. 22, 2021) [https://cppa.ca.gov/regulations/pdf/invitation\\_for\\_comments.pdf](https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf)

<sup>5</sup> Lawyers' Committee Digital Justice Home Page, <https://www.lawyerscommittee.org/digitaljustice/> (last visited October 27, 2021).



Privacy rights are civil rights. “Protected association furthers ‘a wide variety of political, social, economic, educational, religious, and cultural ends’ and ‘is especially important in preserving political and cultural diversity and in shielding dissident expression from suppression by the majority.” *Am. for Prosperity Found. v. Bonta*, 141 S.Ct. 2373, 2382 (2021) (quoting *Roberts v. United States Jaycees*, 468 U.S. 609, 622 (1984)); see also *NAACP v. Alabama*, 357 U.S. 449, 462 (1958) (noting the “vital relationship between freedom to associate and privacy in one’s associations”). Private companies’ collection, use, and sharing of personal information can be just as harmful and cause chilling effects equivalent to compelled disclosure by a state actor. California, on behalf of the public welfare, has a compelling interest in protecting the civil rights of its people.

Digital redlining depends on data. Commercial data practices are inextricably intertwined with equal opportunity. When demographic information is used to restrict access to commercial opportunities, it affects “resource distribution and public well-being.” *Leaders of a Beautiful Struggle v. Baltimore Police Dept.*, 2 F.4th 330, 348-49 (4th Cir. 2021) (en banc) (Gregory, C.J., concurring) (historic redlining in Baltimore continues to affect “investment in construction; urban blight; real estate sales; household loans; small business lending; public school quality; access to transportation; access to banking; access to fresh food; life expectancy; asthma rates; lead paint exposure rates; diabetes rates; heart disease rates; and the list goes on.”). Like the sprawling consequences of historic redlining, other harms arise as negative externalities (including downstream effects) from data-exploitative business models and the market incentives they create.

We urge the Agency, as it begins rulemaking, to prohibit discriminatory use of consumer data by implementing data minimization requirements and use limitations, conducting robust supervision of data use by companies, and holding accountable companies who misuse individuals’ data. By regulating how companies can collect, use, and share personal data, the Agency can prevent harms before they occur and reduce discrimination. If there was less data in the ecosystem, and rules restricting risky and harmful practices, there would be fewer downstream harms of all types.

In a recent letter submitted to the FTC, the Lawyers’ Committee, along with other civil society organizations, highlights areas where privacy rights are most important for consumer protection, such as data minimization, use limitations, and transparency.<sup>6</sup> In conjunction with these comments, the letter to the FTC highlights the harms that can be caused by unfair and deceptive commercial data practices. We ask the Agency to take into consideration the recommendations and asks made to the FTC, as they are applicable here as well.

---

<sup>6</sup> Lawyers’ Committee for Civil Rights Under Law, (Aug. 4, 2021) <https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf>

Data minimization is the principle that a company should only collect, use, retain, and share as much personal data as is necessary to achieve a specified and legitimate purpose.<sup>7</sup> Requiring data minimization in the upcoming rules will reduce the potential for information collected from Black and Brown communities to be used for deceptive or harmful purposes. The rules should also contain use limitations that prohibit the use of personal information to discriminate or cause unfair disparate impacts on marginalized communities. Many automated decision-making systems used in online commerce, if not carefully designed and tested, can reinforce structural racism and systemic inequities, especially as it relates to housing, employment, and finance. The rules should also establish a robust system of transparency to help identify and study discriminatory data practices. Knowing in detail what information companies are collecting, how they are using it, and with whom they are sharing it will assist in ending online discrimination, exploitation of personal data, and abusive practices.

We thank the Agency for taking the time to receive and review comments and look forward to working with you to protect privacy and civil rights as the Agency goes through the rulemaking process.

---

<sup>7</sup> FTC, *Internet of Things: Privacy & Security in a Connected World*, Future of Privacy 1, iv (2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

Chair Lina Khan  
Commissioner Rohit Chopra  
Commissioner Rebecca Slaughter  
Commissioner Noah Phillips  
Commissioner Christine Wilson

Federal Trade Commission  
600 Pennsylvania Ave., N.W.  
Washington, D.C. 20580

Chair Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson:

We, the undersigned civil rights, civil liberties, and consumer protection organizations, write to bring your attention to the urgent need for the Federal Trade Commission to protect civil rights and privacy in data-driven commerce. The Internet is an irreplaceable venue for free expression, trade, employment and housing opportunities, banking, education, entertainment, and, of course, civic engagement. As courts have recognized for decades and recently reaffirmed, privacy rights are civil rights<sup>1</sup> and commercial data practices are inextricably intertwined with equal opportunity.<sup>2</sup>

We ask the FTC to (1) initiate rulemaking and take other appropriate actions to regulate unfair and deceptive commercial data practices such as those discussed below; (2) create an Office of Civil Rights; and (3) commit greater resources to aggressively enforce against unfair and deceptive practices. We urge the FTC to use all tools at its disposal.

### **Unfair and Deceptive Commercial Data Practices Cause Substantial Harm**

As has been extensively documented by independent researchers, journalists, courts, companies, and this Commission, unfettered data practices employed single-mindedly for private gain cause significant harm to the public. Tech companies directly cause or contribute to many of these harms. Like the sprawling consequences of historic redlining, other harms arise as negative externalities (including downstream effects) from data-exploitative business models and the market incentives they create. Addressing direct harms and changing incentives will have positive effects for the Internet ecosystem as a whole.

---

<sup>1</sup> See *Am. for Prosperity Found. v. Bonta*, \_\_ S.Ct. \_\_, 2021 WL 2690268, \*6 (July 1, 2021) (discussing *NAACP v. Alabama*, 357 U.S. 449 (1958)).

<sup>2</sup> See *Leaders of a Beautiful Struggle v. Baltimore Police Dept.*, \_\_ F.4th \_\_, 2021 WL 2584408, \*14 (4th Cir. June 24, 2021) (en banc) (Gregory, C.J., concurring) (discussing how past redlining of Baltimore continues to affect resource distribution and public well-being, including “investment in construction; urban blight; real estate sales; household loans; small business lending; public school quality; access to transportation; access to banking; access to fresh food; life expectancy; asthma rates; lead paint exposure rates; diabetes rates; heart disease rates” and more.).



## Harms to Civil Rights and Equal Opportunity

- 1) Automated decision-making systems produce and [reproduce](#) new and longstanding patterns of discrimination in [recruiting](#), [employment](#), [finance](#), [credit](#), [housing](#), [K-12](#) and [higher education](#), [policing](#), [probation](#), [healthcare](#), as well as the promotion of key services through digital advertising.
  - a. Ex.: Facebook has been sued by [advocates](#) and the [U.S. government](#) for enabling discrimination by allowing advertisers to restrict ad viewership by race, religion, national origin, and other protected characteristics. Google and Twitter have similarly [been investigated by HUD](#) for housing discrimination.
- 2) Unscrupulous [political operatives](#) and [foreign adversaries](#) have used [conventional advertising and targeting tools](#) on social media platforms to interfere with U.S. elections and engage in voter suppression. Social media [plays a key role in disinformation campaigns](#) that spread conspiracy theories, threaten election integrity, and lead to violence such as the [January 6 attack on the U.S. Capitol](#).
- 3) [Disinformation campaigns in non-English languages](#) are particularly rampant due to disregard by major platforms such as Facebook. The ability to target these types of campaigns depends on the privacy-invasive architecture of social media platforms.
- 4) Platform design choices routinely enable discrimination within important consumer services and workplaces.
  - a. Ex: Airbnb enabled landlords to reject prospective guests with what were perceived to be distinctly Black names at [higher rates](#) than guests with what were perceived to be distinctly white names.
  - b. Ex: Uber enabled drivers to [discriminate](#) against passengers with what were perceived to be distinctly Black names and provide more [expensive services](#) to women passengers. Uber likewise used [biased consumer-reviews](#) to make workplace decisions that may violate civil rights.
- 5) Social media firms' algorithmic design choices create pathways to white supremacy, which can lead to violence and deprivation of civil rights.
  - a. Ex: An internal Facebook study [obtained by the Wall Street Journal](#) noted that "64% of extremist group joins are due to our recommendation tools...our recommendation systems grow the problem."
  - b. Ex: YouTube video recommendations systemically recommend [harmful](#) and [progressively more extreme](#) content to viewers, creating pathways to [radicalization](#).
- 6) Firms reify and advance existing social prejudices, particularly racism, throughout technology and online services, including through [search engine](#) and other [predictive](#)



[text results](#), [voice technologies](#), [facial analysis](#), and other biometric and [visual processing techniques](#).

- 7) Workers are increasingly monitored through digital surveillance programs [in and beyond the place of employment](#), raising novel questions as to whether and how these applications enable exploitation and discrimination. Tech firms [dehumanize](#) workers through intrusive [surveillance](#) and intermediating working relationships with opaque, [sometimes degrading](#) workplace management software.
- 8) [Delivery service drivers](#) protested a nearly-invisible method of pay calculation that put customers' tips toward guaranteed minimum wages.
- 9) Platform companies use "[psychological tricks](#)" on workers, not dissimilar to the dark patterns used on consumers, to maximize company growth.
- 10) Facial recognition and other biometric surveillance technologies erode civil liberties, [particularly for Black and Brown communities](#). The [biases in these technologies](#) and their [use by law enforcement](#) have led to traumatic violations of civil liberties, including a [number of recent wrongful arrests](#) of innocent Americans misidentified by faulty facial recognition software.
- 11) Ambient state and private surveillance in public spaces has a [chilling effect](#) on basic freedoms and [disproportionately affects Black and Brown communities](#).

### **Harms to Consumer Protection and Invasions of Privacy**

- 1) Digital [firms employ](#) "[dark pattern](#)" [techniques](#) to [confuse and exploit consumers](#), including intentionally complicating the process of [opting-out of data collections](#).
- 2) Digital firms use similar designs to [trick consumers](#) into sharing personal data or [buying services](#) they may [not want](#).
- 3) Digital firms use similar designs to obscure [pricing](#) and [fee structures](#) for services up front.
- 4) Digital firms use similar designs and practices to make it difficult for consumers to change [privacy settings](#), [delete accounts](#), or [cancel services](#).
- 5) Amazon has labeled as "Amazon's Choice" or sold from its warehouses products that are [deceptively labeled, or have been declared unsafe or banned by federal regulators](#).
- 6) E-commerce sites like Amazon and Google have continued to sell items they promised to ban, such as [pill presses that have been used to manufacture counterfeit prescription drugs](#) or [firearm accessories](#).
- 7) Millions of businesses listings on mapping sites are fraudulent [with analysts cited by the WSJ estimating up to 11 million listings on Google maps may be false listings](#).



- 8) Negligence and lax safety standards enable bad actors to commit elaborate frauds on digital platforms.
  - a. Ex: Various [Airbnb scams](#).
  - b. Ex: Applications on smartphone app stores with billions of downloads have been found to be [committing ad fraud](#).
- 9) Research conducted by Consumer Reports found that nearly [half of consumers struggle to distinguish between a paid ad and an objective search result](#).
- 10) Large online advertising platforms are combining data with [real-world purchasing](#) and [customer information](#) to track them across the web and in the physical world.
- 11) Navigation applications [optimize routes for speed](#) regardless of the negative impact on public safety and traffic. Multiple people [have been killed](#) by so-called “self-driving” or auto-pilot enabled cars on public roads. Some [evidence](#) suggests the entry of a ride-sharing application into a city increases the number of fatal accidents by 3%.
- 12) Platform transportation companies erode the [hard-won public safety protections](#) put in place over decades around seatbelts, child safety seats, distracted driving, helmet-wearing, and more.
- 13) E-commerce and [platform](#) companies whose delivery drivers kill or maim pedestrians refuse to take responsibility for those injuries, despite incentivizing dangerous driving behavior.
  - a. Ex: Amazon [incentivized drivers](#) to rush through holiday delivery. Upon being sued by the family of a pedestrian who was killed, [they claimed](#): “The damages, if any, were caused, in whole or in part, by third parties not under the direction or control of Amazon.com.”
- 14) Firms’ amplification and enabling of [public health misinformation at scale](#) has eroded public trust in vaccines and public health officials. [Too many American families and their loved ones](#) have been [severely harmed](#) by their belief in misinformation, particularly during the COVID-19 pandemic, and [vaccine hesitancy](#) remains an issue.
- 15) Large online advertising platforms like [Google have placed ads on sites promoting COVID-19 conspiracy theories](#) in [contrast to the commitments they made to combat COVID-19 misinformation](#).
- 16) [Platform design choices that algorithmically amplify](#) false information and propaganda in order to [increase engagement on social media](#) can [grossly warp](#) public discourse and [understanding](#) around public events, complicating the media landscape for consumers.



- 17) Firms [track](#) Americans in gross detail, relying on contrived interpretations of consumer consent or without explicit consent.
  - a. Ex. Mobile phone trackers collect precise location [over 14,000 times per day](#).
- 18) Firms collect consumer data [that they do not need without consent](#).
- 19) Firms accept and [purchase user data](#) collected by other firms without their consent.
  - a. Ex: Facebook received [ovulation data](#) from a third party without user consent.
- 20) Firms collect consumer data under the [pretense](#) of consent, perpetuating the fallacy that consumers are in a position to read, understand, or [give informed consent](#) (often consumers *must* use services and lack other options or the ability not to consent).
- 21) Firms use deceptive disclosures and settings to [trick consumers](#) into allowing data sharing with third parties.
- 22) Firms use personal consumer data—including private [emails](#), [conversations](#), and [photographs](#)—to develop algorithmic products without full consumer knowledge, consent, or reciprocity.
- 23) Firms fail to secure or delete obsolete user data, resulting in significant individual and collective costs. While firms may prefer to paint themselves as victims, a [more apt metaphor](#) might be oil companies who fail to prevent oil spills.
  - a. Ex: Experian's API weakness likely exposed "[most Americans](#)" [credit scores](#), creating a feeding frenzy for identity thieves.
  - b. Ex: [Popular genetic testing services](#) have [insufficient security](#) leading to [significant potential](#) for exploitation of genomic and health information.
- 24) Poor data protection can result in both [exploitative and exclusionary](#) conduct.
- 25) Privacy harms are especially acute in combination with competitive harms: [experts have shown](#) that firms that achieve market dominance and successfully suppress competitive threats are able to lower privacy protections to pursue and extract greater data gains from consumers.
  - a. Ex: [Facebook pivoted away](#) from privacy-protection toward privacy exploitation upon achieving significant market power.
- 26) Digital firms use unprecedented data collection and targeting tools to [exploit behavioral shortcomings](#) and [biases](#) amongst consumers in real-time.
- 27) Digital firms employ a bevy of dynamic pricing strategies, which nearly [three-quarters of Americans](#) think is a [problem](#).

## **FTC Should Regulate and Stop Unfair and Deceptive Commercial Data Practices**

The following practices relating to the use of consumers' personal data are unfair or deceptive. They cause many of the harms discussed above, either directly or by causing downstream negative externalities. The FTC should take immediate action to address them using all tools at its disposal, including but not limited to rulemaking.

### **Civil Rights and Equal Opportunity**

- 1) Using criteria that have the purpose or effect of resulting in adverse eligibility determinations or to target or deliver advertisements for housing, employment, credit, insurance, or educational opportunities on the basis of protected characteristics. This does not include using protected characteristics (a) for legitimate self-testing for the purpose of preventing unlawful discrimination, complying with legal requirements, or assessing diversity, equity, and inclusion programs; or (b) for the bona fide and primary purpose of expanding an applicant, candidate, participant, or customer pool by increasing diversity and inclusion.
- 2) Using personal data to violate rights protected by federal law, where such rights are capable of being violated by a private actor. This includes using personal data to deprive or defraud someone of the right to vote in violation of federal law.
- 3) Disclosing non-public information related to an individual's sexual life without specific opt-in consent, such as their sexual activity, relationships, orientation, gender identity or expression, preferences, communications, or behavior. This does not include automated linking to, republishing of, or indexing such information if it was already disclosed by others—such as routine search engine operations.
- 4) Offering online services that are not accessible to persons with disabilities.
- 5) Failing to provide disclosures and policies in all languages in which the company routinely provides service.
- 6) Using machine learning or artificial intelligence technology to process personal data or aggregate data about a population without ensuring, prior to deployment and through regular assessment, that such processing does not directly or indirectly result in adverse eligibility decisions or exclusion from commercial opportunities on the basis of protected characteristics.
- 7) Using machine learning or artificial intelligence technology in a manner that does not comport with what the technology is marketed or represented to do, if such use causes harm to consumers.
- 8) Claiming that a product using machine learning or artificial intelligence technology can predict future outcomes with a degree of certainty or accuracy, or predict human behavior at all, if the claimant does not possess reliable evidence that such technology has any such capability greater than a simple linear regression analysis or random chance.

- 9) Representing that a product using machine learning or artificial intelligence technology has a source, sponsorship, approval, certification, accessories, characteristics, components, uses, or benefits that it does not have, or that such product is of a certain standard, quality, grade, style, or model when it is not.
- 10) Designing, modifying, or manipulating a user interface of a service, directed at children under the age of 13, with the purpose or substantial effect of cultivating compulsive usage.
- 11) Using personal data to target or deliver personalized advertisements to children under the age of 13. This does not include contextual advertising.
- 12) Using personal data to conduct psychological experiments on users without opt-in consent and compliance with best practices for such research, if it is reasonably foreseeable that such experiments may result in harm physical or mental health.

## **Data Protection**

- 1) Failing to minimize data collection and retention. Collected data should be limited to what is necessary to provide the service requested by the consumer; should not be used for secondary purposes; and should not be retained for longer than is necessary to satisfy the purpose for which it was collected. Secondary uses should not be allowed without additional and specific opt-in consent.
- 2) Using facial recognition technology on persons in traditional public forums or places of public accommodation without opt-in consent.
- 3) Collecting, sharing, or otherwise using an individual's biometric data, including but not limited to facial recognition technology, without specific opt-in consent and without a valid business necessity.
- 4) Disclosing, without authorization or in excess of authorization, the content of a communication to anyone who is not a party to the communication or who does not have authorization to access it, including both state actors and private parties.
- 5) Collecting sensor recordings of environmental data from a consumer device, in conjunction with personal data, without opt-in consent. This includes data collected by a microphone, camera, or other sensors capable of measuring chemicals, light, radiation, air pressure, speed, weight or mass, positional or physical orientation, magnetic fields, temperature, or sound. This does not include processing by an entity that did not directly collect the data.
- 6) Collecting personal data as a third party about users of an online service, where such data is not publicly available, without opt-in consent from affected individuals. This includes, for example, cursor movements and clicks, heat maps, in-app activity, location information, third party tracking beacons and cookies, and other third-party methods of tracking user activity.



## **Due Process**

- 1) Requiring consumers to consent to pre-dispute binding arbitration clauses or class action waivers.
- 2) Requiring consumers to waive privacy or other rights to obtain service or requiring that consumers who do not waive their rights pay a higher fee. This does not include customer loyalty programs, such as grocery store discount cards.
- 3) Denying consumers the ability to access, correct, delete, or port their personal data in response to a reasonable request.
- 4) Failing to provide an effective and prompt appeal when requests to access, correct, delete, or port data are denied.
- 5) Using dark patterns and other misleading user interfaces to unfairly or deceptively induce consent or other adverse actions from a consumer.

## **Transparency**

- 1) Failing to affirmatively disclose, in a clear and conspicuous manner, how a data processor collects, uses, shares, and retains personal data, including failing to explain a consumer's ability to control the use of their data.
- 2) Failing to affirmatively disclose when and how a company uses machine learning or other artificial intelligence technology to process personal data, when such processing affects commercial goods, services, or opportunities that a consumer may receive. This includes failure to disclose non-sensitive information from risk assessments.
- 3) Failing to conspicuously provide all relevant privacy policies and controls in one place, such as scattering privacy policies, updates, or controls across multiple parts of a website or app. This practice is particularly deceptive when a consumer's intent to change a privacy control in one area can be undermined by failure to change other controls in other areas, and such discrepancy is not conspicuous.
- 4) Refusing to tell a consumer to whom the company disclosed their personal data, or with whom the company contracts to share such data, in response to a reasonable request.
- 5) Failing to notify a consumer when the company discloses their personal data to a state actor unless the company is legally required not to disclose.
- 6) Misstating or mischaracterizing the subject matter, methods, frequency, or results of any of one's own internal or external assessments.

## **Security**

- 1) Failing to secure personal data, to protect the integrity of personal data, or to prevent unauthorized access or processing of personal data.

- 2) Failing to promptly notify affected parties following a data breach.
- 3) Failing to comply with state data breach laws and regulations when such failure affects interstate commerce and is not inconsistent with federal law.
- 4) Disclosing non-public personal data to a service provider or third party without contractually requiring the service provider or third party to meet the same privacy standards as the company, or without engaging in reasonable oversight to ensure compliance with such requirements.

### **Accountability**

- 1) Retaliating against whistleblowers who attempt to report unfair or deceptive practices.
- 2) Knowingly aiding and abetting another person engaging in an unfair or deceptive practice.
- 3) Failing to report to the Commission if a company has knowledge that a service provider, affiliate, or customer has engaged in an unfair or deceptive practice involving the company's goods or services. This does not include content immunized by 47 U.S.C. 230.
- 4) Failing to provide an annual sworn certification from a C-suite officer or equivalent senior officer that a company (other than a small business) is fully compliant with the FTC's data privacy rules.

### **Office of Civil Rights**

The FTC should create an Office of Civil Rights. There are [more than 30 civil rights offices](#) within federal agencies. The harms and unfair or deceptive practices discussed in this letter are part of a large, interconnected data ecosystem. Expanding the Commission's expertise on discrimination and equal opportunity will help it holistically assess the equities of modern digital trade. Such an Office will create a focal point for Agency expertise and stakeholder engagement on these important issues. The Office could also advise on actions the Commission may take, and coordinate with other agencies, to help respond to commercial data practices that may result in unjust disparate treatment or impact on the basis of race, ethnicity, religion, national origin, immigration status, disability, sex, gender identity or expression, sexual orientation, age, or familial status.

As the FTC looks to chart a new course for oversight of unfair and deceptive practices arising from commercial data practices and big tech, we look forward to working with you to protect civil rights, promote algorithmic fairness, advance equal opportunity, and preserve privacy and free expression.

For more information, please contact [David Brody](#) and [Sara Collins](#).

Sincerely,

Access Now

Accountable Tech

Asian Americans Advancing Justice | AAJC American  
Association for Justice

ADL

Center for American Progress

Center for Digital Democracy

Center for Democracy and Technology

Center on Privacy & Technology at Georgetown Law

Common Cause

Common Sense Media

Consumer Action

Consumer Federation of America

Electronic Privacy Information Center

HTTP

Lawyers' Committee for Civil Rights Under the Law

Media Alliance

National Council of Asian Pacific Americans National  
Fair Housing Alliance

National LGBT Task Force

OCA – Asian Pacific American Advocates

Public Citizen

Public Knowledge

Ranking Digital Rights

The Greenlining Institute



---

**From:** Tracy Rosenberg [REDACTED]  
**Sent:** 11/8/2021 2:09:39 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** PRO 01-21: Preliminary Comments from Media Alliance and Oakland Privacy  
**Attachments:** Preliminary Comments CPPA - Media Alliance and Oakland Privacy.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Greetings,

Please find enclosed some preliminary comments in response to your request.

Thank you for your time and attention.

Sincerely,

Tracy Rosenberg

--

Tracy Rosenberg  
Executive Director  
Media Alliance  
2830 20th Street Suite 201  
San Francisco, CA 94110  
[www.media-alliance.org](http://www.media-alliance.org)

[REDACTED]  
Encrypted email at [REDACTED]  
Text via Signal  
Pronouns: She/Her/Hers

-



Virus-free. [www.avg.com](http://www.avg.com)



California Privacy Protection Agency  
915 Capital Mall, Suite 350-A  
Sacramento CA 95814  
Web: [www.cppa.ca.gov](http://www.cppa.ca.gov)

**Preliminary Comments on Proposed Rule-making  
from Media Alliance and Oakland Privacy**

**November 8, 2021**

Thank you for the opportunity to make preliminary comments to the Agency as you embark on your rule-making and enforcement duties granted under the California Privacy Rights Act of 2020.

Oakland Privacy is a citizen's coalition that works regionally to defend the right to privacy, enhance public transparency, and increase oversight, particularly regarding the use of surveillance techniques and equipment. We were instrumental in the creation of the first standing municipal citizens' privacy advisory commission in the City of Oakland, and we have engaged in privacy enhancing legislative efforts with several Northern California cities and regional entities. As experts on municipal privacy reform, we have written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections and community control.

Media Alliance is a Bay Area democratic communications advocate. Our members include professional and citizen journalists and community-based media and communications professionals who work with the media. Our members are concerned with communications rights, especially at the intersections of class, race and marginalized communities.

### **Question 1 a-d Cyberscurity Audits and Risk Assessments**

Question 1(a) asks when a business use of personal information poses a significant risk to privacy or security. The question of what "privacy harm" consists of is a challenging one. We would suggest two criteria for the agency to consider. The first relates to the stakes for the affected consumer. Does the business' use of personal information contribute to whether a consumer can access something of significance to them. Will the personal information a business collects be a part of a process that determines if they can rent an apartment, buy a house, acquire a line of credit, get into a college, get a job, or access medical care or insurance services? Does the consumer, in other words, face a significant risk of not being able to get something of significance to them based on how a business collects or processes their personal information. The second criteria we would recommend is whether a business sells, shares or distributes a consumer's personal information beyond the ecosystem of one business and their direct service providers. When a consumer's information is, to describe it colloquially, sent out into the wild, then the definition of significant risk is met due to the possible distortion of the putative reason the information was collected and the relative lack of control of the original data collection entity or middleman.

The question goes on to ask what should be included in an annual cybersecurity audit and how to ensure that it is thorough and independent. An annual cybersecurity audit should focus on a few things including a) what information is collected, both directly and indirectly b) the nature of the automated and human processing of the data, including which parts are done by algorithm and which parts by human beings c) retention protocols including security measures d) sharing/selling protocols e) impact, including volume, quantity, percentages, and demographic markers. An audit is independent if it is performed by a third party with no direct or indirect financial interest in the outcome and this included linked business practices, board member presence or investments.



The third section addresses risk assessments including what they consist of, how often they should be performed, and how to weigh risks and benefits. A risk assessment asks a company to consider the dark side of their products and services and measure the extent to which that dark side is present in their current operations. In other words, if things go wrong, how do they go wrong and is that happening and if so, how much? A risk assessment should consist of a description of the automated processes involved including their quantity and scope, a statement of potential threats, risks and harms that can be conceptualized and then a measurement of the extent to which each of these potential threats, risks and harms is or may be actualized, with an emphasis on those that are present in whatever quantity as opposed to theoretical harms, although potential harm should always be addressed. Such an assessment should occur with business data processes that meet criteria for significant privacy risk or privacy harms as soon as possible. We suggested some possible criteria for that determination above. Whatever criteria the Agency decides upon, the goal should be for initial risk assessments to be performed for high risk business data processes within the next three years or by the end of 2024. We would then recommend that the process be renewed biannually. The Agency may wish to set up tiers of risk with lower risk business data processes renewing their risk assessments every four years. When it comes to balancing risks and benefits, it is probably inevitable that businesses will conclude that the benefits exceed the risks in their own risk assessment statements, so the goal should be tabulating both the benefits and the risks so those measurements can be available to both the Agency, legislators and the public to determine if and when actions are needed to contain risks. That said, companies should be encouraged to proactively address the risks they uncover to the extent they are willing and able to do so.

## **Question 2 (a-d) Automated Decision Making**

Question 2 focuses on automated decision making processes. The first question asks what activities constitute automated decision making and profiling. As we mentioned above, automated decisionmaking involves data processes that allow or grant access to a consumer to services and products that the, which can include housing, jobs, benefits, insurance and medical services, banking and lines of credits, financial aid, educational admissions or in the case of pretrial and probation, the level of their personal freedom. These decisions can be fully automated, partially automated or marginally automated. While fully automated decision making is particularly high in risk factors, studies have shown that human-adjudicated decision making that relies on data processing shows similar risk factors as humans are notoriously reluctant to override the formulas, so both fully automated and human-assisted processes constitute automated decision making.

The second question asks about when consumers should be able to access information about automated decision making processes. That's easy. When they are subjected to them! Any human being whose application is being submitted to an algorithmic for a result should have access to the parameters of the decision making process including what factors are being weighed and the approximate contribution of each of them to the final result. When students take a class in a university, it is the usual practice to provide them with a grading syllabus so they understand what their final grade will consist of and the relative factoring of their term papers, quizzes and exams, attendance and class participation. It isn't clear why we would expect or provide anything less for

algorithmic decision making that affects important life opportunities. Black box algorithms that are “too difficult to explain” are a red flag that the data processing lacks appropriate controls and is probably subject to unintended consequences including disparate impacts and hidden bias.

The last question addresses the scope of customer's opt-out rights. CPRA allows consumer opt-out with very limited exceptions. When it comes to automated decision making, those opt-out decisions may have an impact on the algorithmic formula which may reject consumer profiles that lack plentiful information. So it should always be an option for consumers to request and receive a fully human review and/or appeal of any data-aided decision making process.

### **Question 3 (a-c) Audits Performed by the Agency**

Question 3 asks about the scope of the Agency's audit authority. The Agency's audit authority should be focused on the primary rights provided for in CPRA/CCPA including the right to opt-out, the right to correct, and the right to delete. So the initial focus of the Agency's audit work should be directed at basic business compliance with the fundamental privacy rights as defined. This could include complaint-based auditing follow-up as well as possibly some random audits that seek to get a bead on general business compliance. However, the Agency should not overly limit the scope of its auditing program as changes in technology will inevitably present new privacy challenges down the line that may require new parameters or pose privacy harms that were not obvious in 2021 and 2022. So we would advocate for a broad statement of authority to audit California businesses whenever their activities present significant risks to Californian's privacy.

The second section addresses the process and criteria to select businesses for audit. The Agency, which has limited resources, will have to choose between a largely complaint-based process that would consist of waiting for consumer, advocates and journalists to identify potential non-compliance and problematic processes and a randomized auditing process that would engage with a representative sampling. While we do think it will be important for the agency to be responsive to complaints, we encourage some level of randomized auditing as it is will be important for the Agency to have a sense of the general rate of compliance in order to inform future rule-making.

The last question addresses safeguarding consumer information from auditors. We don't want to tie the hands of CPPA auditors too extensively, so we would recommend strong prohibitions on any unauthorized distribution (as in immediate termination) and strong encryption protocols for the transfer of PII between companies and the auditing staff and between members of the auditing team.

### **Question 4 a-e Consumer Right to Know, Right to Correct and Right to Delete**

Question 4 asks about a customer's right to know, right to correct and right to delete. The first question asks how often a consumer may ask to correct inaccurate information. There is no doubt that inaccurate information increasingly presents troubling issues for consumers. As computer-driven decision making processes grow more ever-present, inaccurate PII, whether caused by sloppy data collection processes or identity theft, can cause consumers to be punished in a variety of ways. So

while we are sensitive to the fact that businesses can face a burdensome obligation, we are reluctant to constrain the ability to have incorrect information removed too extensively. The Agency may want to consider the different kinds of inaccurate information that may be present and impose a more liberal protocol for certain kinds of essential information relating to finances, health information and criminal/civil legal information that can have significant impacts on consumers, as opposed to less cogent information in order to best bridge the tension between businesses desire for streamlines processes and the unimpeachable right of consumers not to be denied significant life opportunities due to incorrect data about them.

The second question asks for the procedures businesses should follow to prevent fraud in the correction of online information. To the extent that businesses are able, they should use established two factor authentication processes to confirm identity and have backup processes like secret questions for consumers who don't have smartphones. These processes are preferable to biometric identification, which creates enhanced privacy risks under the slogan of verifying identity.

The next question asks when businesses should be exempt from requirements to provide consumers with a right to know, right to delete and right to correct under the disproportionate effort or accuracy claims. For consumers asking to correct information that is in fact, correct, consumers should be offered the opportunity to simply delete the information if they believe it is incorrect. No one should be forced to keep information on their online profile if they don't want it there. While it may be beyond businesses ability to correct already-correct information, they may not and should not hamper a customer's absolute right to delete the information and simply offer the consumer the alternative: no they may not change/correct this piece of information, but they may permanently delete it. When it comes to disproportionate effort, while we are open to the ability of businesses to request extensions for particularly expansive information requests, inalienable rights granted to consumers under state law should not be lightly subject to dismissal based on it being a pain to accommodate them. The fundamental rights contained in this section: the right to know, the right to correct and the right to delete are not ipso facto a disproportionate burden to businesses, or if they are, it is a disproportionate burden the government has decided that they must bear. We can accept that right to know requests to the same company can be limited to prevent duplicative requests from disgruntled customers, but other than that, we cannot think of a justifiable rationale for denying these basic rights to California consumers.

### **Question 5 a-e Consumer Opt Out Rights**

These questions address opt-out protocols. Please see joint comments submitted on this question by a coalition of state privacy groups to which we belong.

### **Question 6 a-b Limits on Use and Disclosure of Sensitive Information**

This section addresses the CPRA's grant of limitations on the use and disclosure of sensitive personal information including. The questions are basically asking when these rights should be



constrained, and we are not sure that we really have an answer for that. Basically, they shouldn't be. The right to limit the use and disclosure of sensitive personal information limits use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services. This is exactly correct. Such information is provided to a company for a specific use, that of performing services or providing goods, and there is no inherent right to use or disclose the information, whose use and disclosure can be very harmful to consumers, for any other reason beyond the purpose for which it was provided. We do not believe that it should be permissible for a business to "notwithstanding" a customer's direction to limit the use and disclosure of a customer's sensitive information. There are perhaps highly limited exceptions for matters of a potential crime or a cogent threat to the life of another, but even in those cases, we would be wary of an over-broad exception that goes beyond the existing duty to warn regulations that already exist.

#### **Question 7 a    Information Provided in Response to a Right to Know Request**

Question 7 asks what criteria should accompany a business determination that it is not possible to provide information about what information a business collected about a customer and where it was shared or sold beyond a 12 month look back period. The criteria should be that the business is not possession of the information because it does not have access to the records of collection or the actual information due to retention periods and has purged or deleted the information or because the saved businesses records of shares or sales of customer information do not go back as far as the customer has requested. We're not sure what other criteria would be appropriate. If the business has the records, then there is no statute or legislation that would justify refusing to provide that information to the affected consumer if they ask for it. It is possible that a look-back period could have a rule-making insertion of a basement limitation, but we're not sure what purpose that would serve. Either the records exist or they do not. Public records law, a similar kind of transparency regulation, uses the standard of existence and we're not sure why private sector use of personal information would not be subject to the same standards. If it is a disproportionate burden on businesses, then that would incentivize limited data retention policies that are more restricted than "forever", which we think serves privacy interests and the intentions of CCPA/CPRA.

#### **Question 8 a-j    Definitions**

Question 8 asks for proposed modifications to various definition language within CPRA/CCPA. We shall address a few of these. In the definition of sensitive information, the CPRA changed the definition of biometric information from that information that "can be used" to establish individual identity to information that is "used or intended to be used" to establish individual identity. We find that distinction unhelpful, at best, and suggest that it be addressed in rule-making. Biometric information is information that can be used to establish individual identity is exactly as sensitive regardless of whether that is the intention of the collection or not. It does not lose its capacity for privacy harm if collected for another intention, nor does the intent necessarily determine all the eventual uses.

Similarly, the change in CPRA of the definition of de-identified information from: “information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer. . . .” to “information that cannot reasonably be used to infer information about or otherwise be linked to, a particular consumer” is also unhelpful and substitutes a clear definition for one that is significantly less clear. Reasonable inferring is a cloudy term and lacks the definitional clarity of information that cannot be linked to a particular individual. If information can be linked to an individual, then the information by definition is not de-identified and arguments about what can and cannot be reasonably inferred about an individual are likely to never end. At a minimum, the agency should strive to define “reasonably inferred” and the day light that exists between the inability to connect personal information to a specific individual and the ability to do so that prevents reasonable inferences about that individuals.

We have on-going concerns about the “law enforcement agency approved investigation” clause, as we have observed in extensive work with law enforcement that the word “investigation” can and often is stretched extremely broadly. An investigation should be demarcated with a specific case number, and to the extent the information is highly sensitive, a warrant, court order or subpoena should be encouraged, if not required. (We realize that may be beyond the jurisdiction of the CPPA, but even if procedures cannot be mandated, they can be encouraged).

The definition of dark patterns in CPRA is broad and probably requires further clarification by the Agency, but it is such a large topic that it somewhat exceeds the range of these comments. We suggest that the Agency go through a full rule-making on the phenomenon of dark patterns to more clearly gauge exactly what processes have the substantial effect of subverting or impairing user autonomy and choice. We will add that the universal adoption of global privacy controls would play a significant role in reining in the use of dark patterns by reducing the amount of case-by-case and site-by-site opt-outs which greatly enable the use of dark patterns.

## **Question 9 Additional Comments**

Question 9 asks for additional comments. We have two.

Firstly, we hope that the Agency will address problems or ambiguities in the exemption of publicly available information contained in CPRA. We are concerned with the nature of a business' “reasonable belief” that information is lawfully available, especially as this relates to the data broker industry and other aggregators of consumer data. We believe this can and will be interpreted to mean any lack of discrete information that information **was** obtained illegally and encourage a negligent disregard for hacked, leaked or information that is casually sold or shared without permission. What constitutes a business' reasonable belief that information is lawfully available? In other words, is that proactive knowledge that in fact the information is lawfully available or simply a lack of information that it is not? We believe it is contingent on the agency to more clearly define the parameters of what a reasonable belief constitutes within the data aggregation landscape. We also have concerns regarding the third bullet point which permits the spread of information beyond the disclosure point if the consumer has not restricted the information to a particular audience. This can place an undue

burden on consumers if they are not aware whether or how to execute on such a restriction and is a place where confusing or exploitative dark patterns can be used to undermine the consumer's ability to place such restrictions on the spread of their information to audiences that it was not intended for. In other words, while we understand that consumers place much information into the public sphere, if the protection offered to them is that they can restrict the information to particular audiences, then it must be clear to them that they can do so and how to do it, or the protection offered is insufficient.

Secondly, we continue to have concerns about financial incentives for surrendering privacy rights contained in the CPRA. Section 1798.125, the non-discrimination clauses in CPRA, continues to leave the door wide open for a two-tiered system that will inevitably over time focus data market places on low-income consumers who will forego the economic damages of “opting out”. The lukewarm protections provided by CPRA against this nightmare scenario i.e. that the price and service quality differentiation be “reasonably related to the value of the customer's data” remain without definition. And the stark reality is for low-income consumers, it is wildly unrealistic to expect them to be able to absorb the “value of their data” to every single business they encounter in the course of their lives. It seems inevitable to us that although that market has not yet become widespread, largely due to rule-making associated with CCPA and CPRA and the looming prospect of federal data privacy legislation, that businesses will eventually realize the necessity of financially incentivizing consumers to opt-in if they wish to maintain troves of data, and that those financial incentives will divide the opt-ins and opt-outs in accordance with the financial divides in society. It is not clear to us what, if anything, the CPRA/CCPA protocol will do to prevent this development, which will create constitutional rights that only some can afford to utilize. We already see this, in a micro example, with the use of grocery and gas cards, which provide such substantial benefits to consumers, especially those with lower incomes and less shopping choices, that they are virtually mandatory if you don't want to be bankrupted by the cost of food. When financial incentives move from the fairly innocuous arenas of gas and grocery cards and frequent flyer plans to the far more serious areas of insurance, health-adjacent data banks, and economic indicators, then we face a significant problem. At a minimum, the Agency should take assertive action to define the term “reasonably related to the value of the data of the business”. At a maximum, the Agency should strongly consider further limits on the ability of businesses to bribe consumers not to opt out by exerting financial consequences if they choose to do so. The ability of all consumers, regardless of their financial position, to make an uncoerced choice based on their concerns about their personal privacy, depends on it.



Thank you for the opportunity to submit comments to the California Privacy Protection Agency.

Respectfully,

A black rectangular redaction box covering the signature of Tracy Rosenberg.

Tracy Rosenberg  
Executive Director  
Media Alliance  
2830 20<sup>th</sup> Street  
San Francisco, CA 94110

Email:   
Web: <https://media-alliance.org>

and on behalf of  
Oakland Privacy  
4799 Shattuck Avenue  
Oakland CA 94609  
Email: [contact@oaklandprivacy.org](mailto:contact@oaklandprivacy.org)  
Web: <https://oaklandprivacy.org>

---

**From:** John Davisson [REDACTED]  
**Sent:** 11/8/2021 2:20:16 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Alan Butler [REDACTED]; Susan Grant [REDACTED]; Ruth Susswein [REDACTED]  
[REDACTED]; Linda Sherry [REDACTED]; Christine Bannan [REDACTED]  
**Subject:** PRO 01-21 - Comments of EPIC, CA, CFA, & OTI  
**Attachments:** PRO-01-21-Comments-EPIC-CA-CFA-OTI.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Dear Ms. Castanon,

On behalf of the Electronic Privacy Information Center, Consumer Action, the Consumer Federation of America, and New America's Open Technology Institute, please find attached comments in response to the agency's September 2021 invitation for public input concerning regulations under the California Privacy Rights Act and the California Consumer Protection Act.

Best,  
John

—  
John Davisson  
Senior Counsel  
Electronic Privacy Information Center  
1519 New Hampshire Ave NW  
Washington, DC 20036  
[REDACTED]

<https://www.epic.org/>

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, CONSUMER  
ACTION, THE CONSUMER FEDERATION OF AMERICA, AND NEW AMERICA'S OPEN  
TECHNOLOGY INSTITUTE

to the

CALIFORNIA PRIVACY PROTECTION AGENCY

On Proposed Rulemaking Under the California Privacy Rights Act of 2020

(Proceeding No. 01-21)

November 8, 2021

---

The Electronic Privacy Information Center, Consumer Action, the Consumer Federation of America, and New America's Open Technology Institute submit these comments in response to the California Privacy Protection Agency (CPPA)'s September 2021 invitation for public input concerning the agency's development of regulations under the California Privacy Rights Act of 2020 (CPRA) and the California Consumer Protection Act of 2018 (CCPA). We support the efforts of the CPPA to establish robust data privacy protections for Californians. As the agency formulates regulations under the CPRA and CCPA, we urge you to continue "protect[ing] consumers' rights" and "strengthening consumer privacy" at every opportunity, consistent with the expressed will of California voters.<sup>1</sup> In particular, we urge you to impose rigorous risk assessment obligations on businesses whose data processing activities could reasonably harm individuals' privacy or security; to maximize the transparency of automated decisionmaking systems and minimize the burdens on individuals who wish to opt out of such systems; and to prevent any exceptions to user-directed limits on the use and disclosure of sensitive personal information from swallowing the rule.

---

<sup>1</sup> California Privacy Rights Act of 2020 §§ 3, 3(C)(1).



## **I. Our organizations**

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has long supported the establishment of a comprehensive federal privacy law while arguing that federal law should not preempt stronger state laws. EPIC has previously provided comments on the CCPA<sup>2</sup> and published a detailed analysis of the CPRA before its approval by California voters.<sup>3</sup>

Consumer Action<sup>4</sup> has been a champion of underrepresented consumers since 1971. A national, nonprofit 501(c)(3) organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers and regulators to advance consumer rights and promote industry-wide change particularly in the fields of consumer protection, credit, banking, housing, privacy, insurance and utilities.

The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

The Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators. OTI sits within New America, a think tank based in Washington, DC.

---

<sup>2</sup> Comments of EPIC to Cal. Office of the Att’y Gen. (Feb. 25, 2020), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf>; Comments of EPIC to Cal. Office of the Att’y Gen. (Dec. 6, 2019), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf>.

<sup>3</sup> EPIC, *California’s Proposition 24* (2020), <https://epic.org/californias-proposition-24/>.

<sup>4</sup> <https://www.consumer-action.org/>.

## **II. The agency should adopt an expansive definition of ‘significant risk’ and impose robust risk assessment obligations on covered businesses.**

We urge the CPPA to adopt regulations that will (1) ensure a wide range of hazardous data practices meet the CPRA’s “significant risk” standard; and (2) require businesses engaged in those hazardous data practices to conduct and publish meaningful and timely privacy risk assessments.

### ***a. The meaning of ‘significant risk’***

Establishing a strong and effective definition of the term “significant risk” in the CPRA is vital.<sup>5</sup> Under section 1798.185(a)(15), the agency must issue regulations requiring “businesses whose processing of consumers’ personal information presents *significant risk* to consumers’ privacy or security” to conduct regular cybersecurity audits and risk assessments.<sup>6</sup> The CPRA does not define “significant risk,”<sup>7</sup> but the agency should interpret this term broadly to maximize the privacy protection afforded to California residents and to ensure that businesses routinely evaluate the hazards of processing and storing personal information. A “significant risk” must be understood to mean a *material* or *nontrivial* risk rather than an exceptional or unusual one. Establishing too high a threshold for audits and risk assessments would unduly limit the businesses from which a careful analysis of privacy and cybersecurity risks is required and undermine the express data protection purposes of the CPRA.

Not only is a broad reading of “significant risk” consistent with the aims of the CPRA; it also aligns with the meaning of the term in a related provision of the Civil Code concerning personal data. Section 1798.81.6 imposes various obligations on credit reporting agencies whose computer systems are “subject to a security vulnerability that poses a *significant risk* . . . to the security of

---

<sup>5</sup> Civ. Code § 1798.185(a)(15).

<sup>6</sup> *Id.* (emphasis added).

<sup>7</sup> However, it identifies “the size and complexity of the business and the nature and scope of processing activities” as factors to consider in the context of cybersecurity audits. Civ. Code § 1798.185(a)(15)(A).

computerized data that contains personal information[.]”<sup>8</sup> The term “significant risk” is defined in the same section as a risk that “*could reasonably result* in a breach of the security of the system . . . of personal information[.]”<sup>9</sup> Carrying this definition forward to the CPRA, the agency should construe the phrase “presents significant risk to consumers’ privacy or security” as referring to data processing that *could reasonably result* in harm to consumers’ privacy or security, not merely processing that is likely or certain to cause such harm. This also follows from the categories of information that the CPRA requires businesses to include in a risk assessment. Such assessments must specify “*whether* [their] processing involves sensitive personal information,”<sup>10</sup> which indicates that risk assessments are required even when a business does not process special categories of personal data that qualify as “sensitive.”<sup>11</sup>

Although it is impossible to develop an exhaustive compilation of data processing activities that “present[] significant risk to consumers’ privacy or security”—and therefore trigger a business’s cybersecurity and risk assessment obligations—there are some forms of processing that definitively fit this description.<sup>12</sup> Senator Kirsten Gillibrand’s Data Protection Act<sup>13</sup> offers a particularly useful compilation of hazardous data processing activities (defined there as “high-risk data practice[s]”),<sup>14</sup> many of which align with the CPRA’s enumerated categories of sensitive personal information:

- a. [T]he use of an automated decision system;
- b. the processing of data in a manner that involves an individual’s protected class, familial status, lawful source of income, financial status such as the individual’s income or assets), veteran status, criminal convictions or arrests, citizenship, past, present, or future physical or mental health or condition, psychological states, or any other factor used as a proxy for identifying any of these characteristics;
- c. a systematic processing of publicly accessible data on a large scale;

---

<sup>8</sup> Civ. Code § 1798.81.6(a) (emphasis added).

<sup>9</sup> Civ. Code § 1798.81.6(c) (emphasis added).

<sup>10</sup> Civ. Code § 1798.185(a)(15)(A) (emphasis added).

<sup>11</sup> Civ. Code § 1798.140(ae).

<sup>12</sup> Civ. Code § 1798.185(a)(15).

<sup>13</sup> S. 2134, 117th Cong. (2021), <https://www.congress.gov/bill/117th-congress/senate-bill/2134/text>.

<sup>14</sup> Civ. Code § 1798.140(ae).



- d. processing involving the use of new technologies, or combinations of technologies, that causes or materially contributes to privacy harm;
- e. decisions about an individual's access to a product, service, opportunity, or benefit which is based to any extent on automated decision system processing;
- f. any profiling of individuals on a large scale;
- g. any processing of biometric information for the purpose of uniquely identifying an individual, with the exception of one-to-one biometric authentication;
- h. combining, comparing, or matching personal data obtained from multiple sources;
- i. processing which involves an individual's precise geolocation;
- j. the processing of personal data of children and teens under 17 or other vulnerable individuals such as the elderly, people with disabilities, and other groups known to be susceptible for exploitation for marketing purposes, profiling, or automated processing; or
- k. consumer scoring or other business practices that pertain to the eligibility of an individual, and related terms, rights, benefits, and privileges, for employment (including hiring, firing, promotion, demotion, and compensation), credit, insurance, housing, education, professional certification, or the provision of health care and related services.<sup>15</sup>

As the agency develops regulations construing section 1798.185(a)(15), we urge you to include these forms of data processing in a non-exhaustive list of activities that “present[] significant risk to consumers’ privacy or security[.]”<sup>16</sup>

***b. The scope of risk assessments***

As Professor Gary T. Marx writes, the object of a privacy risk assessment is to “anticipate[] problems, seeking to prevent, rather than to put out fires.”<sup>17</sup> We urge the agency to implement the risk assessment provisions of the CPRA with this purpose in mind.

Under section 1798.185(a)(15)(A), when a business is engaged in “activities that “present[] significant risk to consumers’ privacy or security,” it must submit “on a regular basis a risk assessment with respect to [its] processing of personal information[.]” The CPRA specifies two categories of information that the assessment must contain: (1) “whether the processing involves sensitive personal information,” and (2) an analysis “identifying and weighing the benefits resulting

---

<sup>15</sup> *Id.*

<sup>16</sup> Civ. Code § 1798.185(a)(15).

<sup>17</sup> *Privacy Impact Assessment at v* (David Wright & Paul de Hert, eds., 2012).

from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing[.]”<sup>18</sup> The goal of a risk assessment is to “restrict[] or prohibit[] the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.”<sup>19</sup>

First, although the categories of information set out by section 1798.185(a)(15)(A) are both essential, a risk assessment (also known as a privacy impact assessment or data protection impact assessment) must go further.<sup>20</sup> The E-Government Act of 2002 offers a useful starting point for setting the parameters of a risk assessment. Before initiating a new collection of personal information or procuring information technology that will process personal information, a federal agency must conduct, review, and publish a privacy impact assessment that explains:

- (I) what information is to be collected;
- (II) why the information is being collected;
- (III) the intended use of the agency of the information;
- (IV) with whom the information will be shared;
- (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and]
- (VI) how the information will be secured[.]”<sup>21</sup>

The Office of Management and Budget (OMB) adds that privacy impact assessments under the E-Government Act:

1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
2. should address the impact the system will have on an individual’s privacy, specifically identifying and evaluating potential threats relating to each of the

---

<sup>18</sup> Civ. Code § 1798.185(a)(15)(A) (emphasis added).

<sup>19</sup> Civ. Code § 1798.185(a)(15)(A).

<sup>20</sup> See EPIC, *Privacy Impact Assessments* (2021), <https://epic.org/issues/open-government/privacy-impact-assessments/>.

<sup>21</sup> E-Government Act, Pub. L. No. 107-347, § 208(b)(2)(B)(ii), 116 Stat. 2899, 2901 (Dec. 17, 2002).

- elements identified in section II.C.1.a.(i)-(vii) [of the OMB Guidance], to the extent these elements are known at the initial stages of development;
3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.<sup>22</sup>

The OMB also requires privacy impact assessments concerning “major information systems” to “reflect more extensive analyses of”:

1. the consequences of collection and flow of information,
2. the alternatives to collection and handling as designed,
3. the appropriate measures to mitigate risks identified for each alternative and,
4. the rationale for the final design choice or business process.<sup>23</sup>

And Article 35 of the European Union’s General Data Protection Regulation (GDPR), which requires data protection impact assessments for all high-risk data processing activities, specifies that an assessment must include:

- a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- c. an assessment of the risks to the rights and freedoms of data subjects . . . ; and
- d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.<sup>24</sup>

At a minimum, we recommend that the risk assessments required of businesses under the CPRA include the categories of information set out in the E-Government Act and the GDPR.

Second, in assessing the “risks to the rights of the consumer associated with . . . processing,” businesses should be required to evaluate the full range of privacy harms and civil rights violations

---

<sup>22</sup> OMB, *OMB Circular A-130: Managing Information as a Strategic Resource* (2016), app. II at 10 [hereinafter *OMB Circular*].

<sup>23</sup> *Id.* at 34.

<sup>24</sup> Commission Regulation (EU) 2016/679, art. 35, 2016 O.J. (L 119).



that may result from processing and disclosure of personal data.<sup>25</sup> Too often, risk assessments focus on the narrow question of whether personal data collected by the institution is secure from breaches. Although this is an essential element of data protection—one built into the CPRA’s requirement for annual cybersecurity audits—it is only the beginning of a more fulsome analysis that institutions must undertake when processing personal data. Businesses must consider not only the harms of unintended or unauthorized uses of data, but also the harms of *intended* uses of the data, including screening, scoring, and other forms of algorithmic decisionmaking.<sup>26</sup> Businesses must also account for the full range of harms that can result from the processing and misuse of personal information. Professors Danielle Keats Citron and Daniel Solove have recently mapped out this spectrum, which includes numerous physical, economic, reputational, psychological, autonomy, discrimination, and relationship harms.<sup>27</sup> And businesses must take special account of the uneven impact of data processing, which disproportionately harms people of color, low-income individuals, and other marginalized populations.<sup>28</sup>

Third, ensuring the right timing and frequency of risk assessments is critical. As the CPRA’s requirement of “regular” privacy risk assessments reflects,<sup>29</sup> an assessment cannot be treated as a static, one-off undertaking. Rather, “it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should

---

<sup>25</sup> Civ. Code § 1798.185(a)(15)(A).

<sup>26</sup> See EPIC, *Screening and Scoring* (2021), <https://epic.org/issues/ai/screening-scoring/>.

<sup>27</sup> Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, GW Law Faculty Publications & Other Works (2021), [https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2790&context=faculty\\_publications](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2790&context=faculty_publications).

<sup>28</sup> See, e.g., Fed. Trade Comm’n, *Serving Communities of Color: A Staff Report on the Federal Trade Commission’s Efforts to Address Fraud and Consumer Issues Affecting Communities of Color* at 40 (Oct. 2021), [https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report\\_oct\\_2021-508-v2.pdf](https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf).

<sup>29</sup> Civ. Code § 1798.185(a)(15)(A).

continue until and even after the project has been deployed.”<sup>30</sup> Or, as the OMB warns federal agencies, a risk assessment

is not a time-restricted activity that is limited to a particular milestone or stage of the information system or [personally identifiable information] life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles. Accordingly, a PIA shall be considered a living document that agencies are required to update whenever changes to the information technology, changes to the agency’s practices, or other factors alter the privacy risks associated with the use of such information technology.”<sup>31</sup>

We urge the agency to require the completion of a risk assessment as soon as a business takes material steps toward data processing that will “present[] significant risk to consumers’ privacy or security” so that the risks to individuals can be prevented or mitigated *before* any processing begins. Allowing risk assessments to be postponed until the last minute (or even until after data processing has begun) would turn the assessments into a simple box-checking exercise and facilitate the whitewashing of harmful data practices.<sup>32</sup> We also urge the agency to require covered businesses to review, update, and resubmit privacy risk assessments (1) well in advance of any change to a business’s data processing activities that might alter the resulting risks to individuals’ privacy, and (2) in any event, no less than once per six month period.

Finally, it is important that both the CPPA and the business submitting a risk assessment publish the full results of the assessment promptly, conspicuously, and by means that are readily accessible to interested members of the public. In addition to forcing an institution to evaluate and

---

<sup>30</sup> *Privacy Impact Assessment*, *supra* note 17, at 5–6.

<sup>31</sup> *OMB Circular*, *supra* note 22, app. II at 10.

<sup>32</sup> *See, e.g.*, EPIC, *EPIC v. U.S. Postal Service* (2021), <https://epic.org/documents/epic-v-u-s-postal-service/> (detailing the U.S. Postal Service’s failure to complete a privacy impact assessment before deploying facial recognition and social media surveillance tools); EPIC, *EPIC v. Commerce* (2020), <https://epic.org/documents/epic-v-commerce-census-privacy/> (detailing the Census Bureau’s failure to complete a privacy impact assessment before attempting to add the citizenship question to the 2020 Census); EPIC, *EPIC v. Presidential Election Commission* (2019), <https://epic.org/documents/epic-v-presidential-election-commission/> (detailing the failure of the Presidential Advisory Commission on Election Integrity to complete a privacy impact assessment before initiating a nationwide collection of state voter data).

mitigate the harms of data processing, a risk assessment “also serves to inform the public of a data collection or system that poses a threat to privacy.”<sup>33</sup> Although the CPRA already requires the agency to “provide a public report summarizing the risk assessments filed with the agency,”<sup>34</sup> we believe the underlying assessments should be presumptively public, subject only to the narrow redactions necessary to protect data security and trade secrets. This added degree of transparency will significantly enhance the data protection benefits of the CPRA without imposing significant additional burdens on the businesses that are already required to produce risk assessments.

**III. The agency should embrace a broad definition of automated decisionmaking technology, maximize the disclosure of information about such systems, and minimize the burden on individuals to opt out.**

We urge the CPPA to adopt regulations that will (1) include broad, rights-enhancing definitions of “automated decisionmaking technology” and “profiling”; (2) ensure easy access to information about the use and logic of automated decisionmaking systems; and (3) make it as easy as possible for individuals to opt out of such systems.

***a. The meaning of ‘automated decisionmaking technology’ and ‘profiling’***

The agency should construe the terms “automated decisionmaking technology” and “profiling” broadly given the range of systems that can cause algorithmic harm. In defining automated decisionmaking technology, the agency should clarify that this term not only includes systems that *make* decisions unilaterally, but also systems that provide recommendations, support a decision, or contextualize information. We particularly recommend Rashida Richardson’s definition of automated decision systems, which encompasses “any tool, software, system, process, function,

---

<sup>33</sup> EPIC, *supra* note 20.

<sup>34</sup> Civ. Code § 1798.199.40(d)



program, method, model, and/or formula designed with or using computation to automated, analyze, aid, augment, and/or replace [] decisions, judgments, and/or policy implementation.”<sup>35</sup>

One of the most dangerous functions of automated decisionmaking is profiling. Profiling includes any form of automated processing of personal information used “to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.”<sup>36</sup> In applying this definition, the agency must be sensitive to the increasing prevalence of profiling and the special impacts of this practice in hiring, criminal justice, credit, and the provision of public benefits.

The following is a non-exhaustive list of systems and tools that qualify as automated decisionmaking technology in commercial settings, many of which also constitute profiling:

- Analysis of voice or facial expressions during a job interview for traits like “dependability,” “emotional intelligence,” and “cognitive ability”;<sup>37</sup>
- Mortality risk predictions that inform COVID-19 care, kidney transplants, and other health care determinations;<sup>38</sup>
- Education services that monitor the internet activity of K-12 students;<sup>39</sup>

---

<sup>35</sup> Rashida Richardson, *Defining and Demystifying Automated Decision Systems*, 81 Md. L. Rev. 19 (forthcoming 2022), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3811708](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811708).

<sup>36</sup> Civ. Code § 1798.3.85(a)(16).

<sup>37</sup> Alex Engler, *Auditing Employment Algorithms for Discrimination*, Brookings Inst. (Mar. 12, 2021), <https://www.brookings.edu/research/auditing-employment-algorithms-for-discrimination/>.

<sup>38</sup> Mohammed Pourhomayoun & Mahdi Shakbi, *Predicting Mortality Risk In Patients With COVID-19 Using Machine Learning To Help Medical Decision-Making*, 20 Smart Health 100178 (2021).

<sup>39</sup> Benjamin Herold, *Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming.*, Educ. Week (May 30, 2019), <https://www.edweek.org/leadership/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05>; Mark Keierleber, *'Don't Get Gaggled': Minneapolis School District Spends Big On Student Surveillance Tool, Raising Ire After Terminating Its Police Contract*, The74 (Oct. 18, 2020), <https://www.the74million.org/article/dont-get-gaggled-minneapolis-school-district-spends-big-on-student-surveillance-tool-raising-ire-after-terminating-its-police-contract/>.

- Exam proctoring tools using facial recognition and automated processing to identify potential instances of cheating;<sup>40</sup>
- The calculation of credit scores based on thousands of opaque data sources;<sup>41</sup>
- Recommendation algorithms on services like YouTube and Facebook;<sup>42</sup>
- “Fit scores,” which yield a simplistic analysis a person’s diet, exercise, and habits that may be computed by or delivered to insurance companies; and<sup>43</sup>
- Systems that purport to detect moods and emotions.<sup>44</sup>

Some of the most dangerous applications of profiling are facilitated by private companies but used in government settings such as law enforcement and the provision of public benefits. These include:

- Predictions of where a crime might occur next or the likelihood that an individual may commit a crime, which inform police resource allocation;<sup>45</sup>
- “Gang databases” that collect and combine sensitive information, subjective inputs, and social media information to categorize individuals as potentially gang-affiliated;<sup>46</sup>

---

<sup>40</sup> Privacy Center, Respondus (2021) <https://web.respondus.com/privacy/privacy-additional-monitor/>.

<sup>41</sup> See Aaron Klein, *Reducing Bias In AI-BASED Financial Services*, Brookings Inst. (July 10, 2020), <https://www.brookings.edu/research/reducing-bias-in-ai-based-financial-services/>; Kevin Peachey, *Sexist And Biased? How Credit Firms Make Decisions*, BBC (Nov. 18, 2019), <https://www.bbc.com/news/business-50432634>.

<sup>42</sup> Debashis Das, Laxman Sahoo & Sujoy Datta, *A Survey Recommendation System*, 160 Int’l J. Comput. Applications 0975-8887 (2017).

<sup>43</sup> See generally Stewart Rogers, *Data science, machine learning, and AI in fitness – now and next*, Neoteric (Aug. 19, 2021), <https://neoteric.eu/blog/data-science-machine-learning-and-ai-in-fitness-now-next/>.

<sup>44</sup> Alexa Hagerty & Alexandra Albert, *AI Is Increasingly Being Used To Identify Emotions—Here’s What’s At Stake*, The Conversation (Apr. 15, 2021), <https://theconversation.com/ai-is-increasingly-being-used-to-identify-emotions-heres-whats-at-stake-158809>.

<sup>45</sup> See Caroline Haskins, *Academics Confirm Major Predictive Policing Algorithm Is Fundamentally Flawed*, Vice (Feb. 14, 2019), <https://www.vice.com/en/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed>.

<sup>46</sup> See Rashida Richardson & Amba Kak, *It’s Time For A Reckoning About This Foundation Piece Of Police Technology*, Slate (Sept. 11, 2020), <https://slate.com/technology/2020/09/its-time-for-a-reckoning-about-criminal-intelligence-databases.html>.

- Fraud detection and prevention services, which monitor activities of benefit recipients and score the likelihood that they are committing unemployment or other type of benefit fraud;<sup>47</sup>
- The use of facial recognition systems to confirm public benefit eligibility; and<sup>48</sup>
- The application of connected prescription drug monitoring programs.<sup>49</sup>

We encourage the CPPA to incorporate these examples when construing the terms “automated decisionmaking technology” and “profiling.”

***b. Consumer access to information about automated decisionmaking systems***

The CPRA instructs the agency to create regulations that will govern how access and opt-out rights operate. To operationalize these rights, we urge the agency to focus on ensuring access to “meaningful information about the logic involved in . . . decision-making processes,” as the CPRA requires.<sup>50</sup>

There are two primary barriers to meaningful access to information about automated decisionmaking and profiling: (1) a lack of awareness that a system is being used at all, and (2) a lack of detail about the system sufficient to allow an individual to opt out. Accordingly, the agency must ensure that the use of automated decisionmaking tools is conspicuously disclosed and that accurate information about those systems is made available to individuals in a timely and user-friendly fashion.

---

<sup>47</sup> See Ashesh Anad, *How Is AI Used In Fraud Detection?*, Analytic Steps (Sept. 21, 2021), <https://www.analyticsteps.com/blogs/how-ai-used-fraud-detection>.

<sup>48</sup> Mia Sato, *The Pandemic Is Testing The Limits of Facial Recognition*, MIT Tech. Rev. (Sept. 28, 2021), <https://www.technologyreview.com/2021/09/28/1036279/pandemic-unemployment-government-face-recognition/>.

<sup>49</sup> See generally Daniel B. Neill & William Herlands, *Machine Learning For Drug Overdose Surveillance*, 36 J. Tech in Hum. Servs. 8-14 (2018).

<sup>50</sup> Civ. Code § 1798.185(a)(16).



The CPPA must decide (1) what information must be made available to provide meaningful access and provide individuals with a real opportunity to opt out; (2) the process of how companies should report this information and ensure its availability to consumers; (3) whether the developer of a system and/or the user of that system should be responsible for disclosure; (4) how the consumer should be given access to this information; and (5) methods for enforcement and consequences for insufficient or misleading information. We urge the agency to mandate, at minimum, that a business disclose the purpose of an automated decisionmaking system; how the system is being used; the factors the system relies on; a plain-language explanation of the logic of the system;<sup>51</sup> the sources and life cycle of the data processed by the system, including any brokers or other third-party sources; and how the system has been evaluated for accuracy and fairness, including links to any audits, validation studies, or impact assessments.

In a growing number of countries, automated decisionmaking systems are required to undergo algorithmic impact assessments. In Canada, for example, businesses input information about automated decisionmaking systems into a standardized survey, which allows for the evaluation of system based on design attributes, the sensitivity of data processed, and the system's connection to areas requiring additional considerations and protections.<sup>52</sup> This type of form is something the CPPA could use to collect and ensure uniform reporting of key information about automated decisionmaking systems. The Canadian assessment asks each business to evaluate the stakes of the decisions that a system makes, the vulnerability of subjects, and whether the system is a predictive tool.<sup>53</sup> The tool also allows for multiple answer options and detailed explanations of responses. In some cases, the Canadian tool requires a business to identify the downstream processes of a system.

---

<sup>51</sup> For example, in a predictive profiling system or automated decisionmaking system, the explanation should include data sources and how particular inputs affect determinations (*e.g.*, if a criminal arrest in the last three years increases a “risk” classification by two points).

<sup>52</sup> Canada Digit. Servs., *Algorithmic Impact Assessment* (2021) <https://open.canada.ca/aia-eia-js/?lang=en>.

<sup>53</sup> *Id.*

This includes asking (1) whether the system will only be used to assist a decision-maker; (2) whether the system will be making a decision that would otherwise be made by a human; (3) whether the system will be replacing human judgment; (4) whether the system will be used by the same entity that developed it; and (5) for details about the system's economic and environmental impacts.<sup>54</sup> The CCPA should consider requiring similar reporting from businesses that deploy or sell automated decisionmaking systems.

Finally, meaningful access requires *actual* notice that automated decisionmaking is being used and easy retrieval of information about the system prior to, during, and after its use. Depending on the context, this could take the form of icon, banner, pop-up, or other type of conspicuous warning. We urge the agency to set clear minimum baselines and methods of disclosure in order to secure meaningful information for California residents about each automated decisionmaking or profiling system.

***c. The right to opt out of automated decisionmaking systems***

The right to opt out of automated decisionmaking systems under the CPRA is groundbreaking, but that right cannot be fully realized without key disclosures and protections. Individuals must be given complete information about the use and operation of automated decisionmaking systems, a user-friendly method to exercise opt-outs, a clear explanation about the scope of each opt-out they exercise, and confidence that their decisions to opt out will be honored.

The agency should pay special attention to the implementation of opt-outs by companies that process personal data across multiple platforms or websites. For example, Facebook/Meta Platforms' operations include Facebook, Instagram, WhatsApp, Oculus, and Facebook Login on third-party sites. Without strong regulations, a conglomerate like Facebook may make it difficult to opt out of

---

<sup>54</sup> *Id.*

automated decisionmaking systems across all its platforms (or even to determine how broadly a given opt-out extends in the first place).<sup>55</sup> We urge the agency to establish an easy method of opting out of automated decisionmaking systems across all of a company's properties.

For an opt-out mechanism to be effective, it must be simple and accessible. The CCPA already imposes certain consumer control mechanisms on covered entities, including the requirement to provide a "do not sell or share my personal information" link. Companies must also recognize Global Privacy Control as a valid consumer request to opt out of the sale of an individual's personal information.<sup>56</sup> Universal "do not track" regimes make opting out more accessible and should be implemented whenever possible. In order to streamline the CPRA opt-out process and maximize individual control over personal data, the agency should consider requiring covered entities to respect a universal opt-out signal for automated decisionmaking systems, as well.

**IV. Any exceptions to consumer-directed limits on the use and disclosure of sensitive personal information should be narrowly drawn.**

The agency should construe any exceptions to the CPRA's consumer-directed limits on use and disclosure of sensitive personal information narrowly to ensure that Californians' privacy rights are fully respected. While rare circumstances may justify nonconsensual disclosure of a resident's sensitive personal information, the CPPA must not allow exceptions to swallow the rule. In drafting its regulations, the agency should avoid the pitfalls of the Privacy Act of 1974 (Privacy Act)'s "routine-use" exception.<sup>57</sup> Any exceptions should be narrow, rare, and enumerated, and the CPPA should take an active role in enforcing that narrow language.

---

<sup>55</sup> See Steven Melendez, *Ready To Quit Facebook? It's Harder To Opt-Out Than You Think*, Fast Company (Oct. 6, 2021), <https://www.fastcompany.com/90683647/facebook-whistleblower-quitting-data-collection>.

<sup>56</sup> Cal. Dep't of Justice, *California Consumer Privacy Act (CCPA)*, <https://oag.ca.gov/privacy/ccpa>.

<sup>57</sup> 5 U.S.C. § 552a.



The Privacy Act provides a cautionary tale about the danger of vague and ill-enforced exceptions to data protection laws. The Privacy Act prohibits federal agencies from disclosing records they maintain “to any person, or to another agency” without the consent of the “individual to whom the record pertains.”<sup>58</sup> However, the routine use exception permits an agency to disclose private data without consent if the agency determines that disclosure is “compatible with the purpose for which [the information] was collected.”<sup>59</sup> The agency needs only to publish a proposed routine use in the Federal Register for that use to become a presumptively valid exception.<sup>60</sup>

The routine use exception has significantly diminished the Privacy Act’s efficacy, giving agencies excessive power to define which of their activities are exempt from the statute. Agencies regularly claim extremely broad routine uses, taking advantage of the “compatibility” standard’s vagueness. For example, the National Security Agency (NSA) declared that the purpose of its Operations Records database is to “maintain records” related to the NSA’s mission.<sup>61</sup> What use or disclosure of data would not be compatible with “maintaining records”? Very few: the NSA claims it may disclose or use private data without consent whenever it is “compatible with” providing or obtaining intelligence or other information related to national security.<sup>62</sup> Similarly, the Department of Defense proposed creating a database of tens of millions of Americans for recruiting purposes but claimed as “routine uses” seemingly non-related activities, including providing data to law enforcement agencies for investigation and national security uses.<sup>63</sup> These wide-ranging “routine

---

<sup>58</sup> *Id.* § 552a(b).

<sup>59</sup> *Id.* § 552a(a)(7).

<sup>60</sup> *Id.* § 552a(e)(4) (agencies “publish in the Federal Register . . . each routine use of the records contained in the system, including the categories of users and the purpose of such use.”).

<sup>61</sup> System of Records, 80 Fed. Reg. 63,749 (Oct. 21, 2015); *see also* Comments of EPIC to the Nat’l Sec. Agency, GNSA 18 Operations Records System of Records Notice, Docket ID: DoD-2015-OS-0100 (Nov. 20, 2015), <https://www.epic.org/privacy/nsa/EPIC-NSA-SORN-Comments-2015.pdf>.

<sup>62</sup> *Id.*

<sup>63</sup> Notice to Add a System of Records, DHRA 04--Joint Advertising and Market Research Recruiting Database., 70 Fed. Reg. 29,486; *see also* Comments of EPIC on the DHRA 04 Joint Advertising and

uses” stretch the definition of “compatible” and have contributed to a gradual erosion of the Privacy Act’s protections.

Moreover, the federal agency charged with Privacy Act oversight, the OMB, has also failed to constrain agencies’ overbroad application of the routine use exception.<sup>64</sup> The Privacy Act delegates enforcement powers to the OMB director, but the agency has issued guidance only sporadically,<sup>65</sup> has failed to keep up with changes in case law, and has given its blessing to practices that are arguably inconsistent with the Privacy Act.<sup>66</sup>

The CPPA can ensure that any exceptions to the CPRA’s user-directed limits do not swallow the rule by drawing carve-outs narrowly and carefully policing their use by businesses. For example, the Electronic Communications Privacy Act (ECPA) has an exception for data uses or disclosures “necessary incident to the rendition of [the] service.”<sup>67</sup> By instituting a more searching review of stated uses, ECPA’s “necessary” standard has proven more privacy protective than the Privacy Act’s “compatib[ility]” language.<sup>68</sup> The CPPA should also regulate businesses’ reliance on use and disclosure exceptions more aggressively than OMB has regulated federal agencies’ assertions of the routine use exception.

If any specific exceptions to consumer-directed use and disclosure limitations are proposed in response to the CPPA’s current invitation for comments, we would be happy to respond to such proposals through supplemental comments or at a later stage of the regulatory process.

---

Marketing Research Recruiting Database to Dep’t of Def. (June 22, 2005), <https://epic.org/privacy/profiling/dodrecruiting.html>.

<sup>64</sup> See Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exception*, 40 Am. U. L. Rev. 957, 983–98 (1991).

<sup>65</sup> See The White House, *Privacy* (2021), <https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/> (listing two OMB memoranda on the Privacy Act in the past 20 years).

<sup>66</sup> *Id.* at 984.

<sup>67</sup> 18 U.S.C. § 2511(2)(a)(i).

<sup>68</sup> Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417, 1482–83 (2009).

## **V. Conclusion**

We thank the CPPA for the opportunity to comment on the forthcoming CPRA regulations and look forward to working with the agency in the future to protect the privacy of all Californians.

Respectfully submitted,

Electronic Privacy Information Center  
Consumer Action  
Consumer Federation of America  
New America's Open Technology Institute



---

**From:** Hilary Cain [REDACTED]  
**Sent:** 11/8/2021 2:11:49 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** Alliance for Automotive Innovation Comments (PRO 01-21)  
**Attachments:** Auto Innovators CPRA Comments FINAL 11.8.21.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Good Afternoon –

Please find attached comments from the Alliance for Automotive Innovation in response to the invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020.

Feel free to reach out if you have any questions or need any additional information.

Cheers,  
Hilary

**Hilary M. Cain**  
Vice President – Technology, Innovation, & Mobility Policy  
[REDACTED]

**Alliance for Automotive Innovation**  
1050 K Street, NW - Suite 650 Washington, DC 20001  
[autosinnovate.org](https://autosinnovate.org) - [twitter](#) - [linkedin](#)



November 8, 2021

**SUBMITTED ELECTRONICALLY VIA EMAIL**

Debra Castanon  
California Privacy Protection Agency  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

**Re: Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)**

Dear Ms. Castanon:

The Alliance for Automotive Innovation (“Auto Innovators”) appreciates the opportunity to provide feedback to the California Privacy Protection Agency (“Agency”) in response to its invitation for preliminary comments on proposed rulemaking under the *California Privacy Rights Act* (“CPRA”). We certainly share your goals of protecting consumer privacy and look forward to continued engagement and collaboration with you on these important issues.

Auto Innovators is the singular, authoritative, and respected voice of the automotive industry. Focused on creating a safe and transformative path for personal mobility, Auto Innovators represents the manufacturers that produce nearly 99 percent of cars and light trucks sold in the United States. In addition to motor vehicle manufacturers, members of Auto Innovators include original equipment suppliers, technology companies, and others within the automotive ecosystem. The auto industry is the nation’s largest manufacturing sector, contributing \$1.1 trillion to the United States economy and representing 5.5 percent of the country’s GDP. As a significant engine for our nation’s economy, the auto sector is responsible for 10.3 million jobs and \$650 billion in paychecks annually.

Our member companies are committed to protecting consumer privacy and have long been responsible stewards of their customers’ information. In fact, in 2014, the auto industry came together to develop the *Privacy Principles for Vehicle Technologies and Services*. The Principles are enforceable by the Federal Trade Commission and represent a proactive and unified commitment by automakers to protect identifiable information collected through in-vehicle technologies. They distinguish the auto industry from other industries as one that is dedicated to safeguarding consumer privacy.

While we appreciate the goal of creating a uniform and inclusive privacy law, we also recognize that consumer privacy is not a one-size-fits-all proposition. We continue to believe that comprehensive consumer privacy laws should account for the significant variation that exists among sectors and the implications that such variation has on consumer privacy. Our comments below highlight the unique

impacts that the CPRA and its implementing regulations may have on the auto industry and its ability to deliver a cleaner, safer, and smarter transportation future.<sup>1</sup>

As the Agency embarks on this important and consequential rulemaking, we respectfully request that sufficient lead time be provided between the finalization of the regulations and the effective date of the regulations. Our member companies take their compliance obligations seriously and need adequate time to align their processes and mechanisms with any new regulatory requirements. To that end, we request that the regulations be finalized at least 12 months before any new obligations or responsibilities take effect. In addition, to ensure sufficient input from stakeholders, we also request that any draft regulations be released for a public comment period of at least 90 days.

### **Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses**

We appreciate that the CPRA recognizes that not all processing of personal information presents a significant risk to consumers' privacy or security and only requires an annual cybersecurity audit and regular risk assessment for the subset of processing activities that pose such a risk. In determining what processing presents a significant risk to consumers' privacy and security, we suggest that the Agency focus on processing that involves "sensitive personal information" as defined in §1798.140(ae).

The Agency should not set out or establish overly prescriptive requirements as to the content of or process for conducting such audits or assessments. Instead, businesses should be provided flexibility in implementing these audit and assessment requirements to appropriately tailor them to their size and complexity, including the nature and scope of processing activities and expectations of customers. In addition, businesses should be expressly permitted to rely on and leverage well-respected and applicable standards and best practices, such as the National Institute of Standards and Technology's Cybersecurity Framework, with respect to any cybersecurity audit requirement.

We also discourage the Agency from specifying a regular cadence for the risk assessments. If the Agency seeks to establish a trigger for the risk assessments, the Agency should consider requiring businesses to update their risk assessment when there is a material change in their processing activities that is likely to have an impact on consumer privacy. Moreover, in determining when such risk assessments should be submitted to the Agency, we encourage the Agency to carefully balance the value of such submissions against the burden that such submissions may impose on businesses and the Agency. Rather than requiring every relevant business in California to periodically submit risk assessments to the Agency, the Agency should consider limiting risk assessment submissions to those requested by the Agency in conjunction with a relevant investigation or inquiry.

As you are aware, the CPRA does not require cybersecurity audits to be submitted to the Agency. Since a cybersecurity audit may reveal sensitive information about how a business defends itself against

---

<sup>1</sup> The auto industry joins other sectors in expressing practical concerns with some other aspects of the CPRA. This includes the expiration of the exemption for applicant, employee, and independent contractor data and the removal of the opportunity for a business to cure an alleged violation before an administrative enforcement action can be brought. These concerns can, and should, be addressed in a way that furthers the purpose and intent of the CPRA and look forward to working with the Agency and other policymakers in California to that end.



a potential cybersecurity attack and such information – if disclosed – could expose the business to an increased risk of attack, this is the appropriate approach.

In the instance that an assessment or audit is provided to or shared with the Agency, the assessment or audit itself and any proprietary information contained within it or reviewed in conjunction with it must be treated as confidential information. This includes ensuring that audits are exempt from disclosure to the public under the Public Records Act.

### **Automated Decisionmaking**

On its own, the term “automated decisionmaking technology” captures a broad range of use cases, including use cases that do not have significant impacts on consumer privacy. For example, the artificial intelligence that underpins automated driving systems and other advanced safety systems continuously make automated decisions about what actions the vehicle will take to safely respond to and navigate the driving environment. Disabling or reducing the effectiveness of these systems by providing opt-out rights could have significant and unintended motor vehicle safety implications. For example, if a consumer opts out of automated decisionmaking that supports a crash avoidance system, that system will no longer be available to help avoid or mitigate the impact of a crash. Moreover, in the case of this type of complex machine-learning system, it is rarely possible to provide meaningful information to consumers about the logic involved in the decisionmaking processes.

As you are aware, CPRA specifically mentions “profiling” as an area of automated decisionmaking technology to be addressed by regulations. We recommend that the Agency limit the scope of automated decisionmaking technology covered by the regulations to profiling. If the Agency opts to include automated decisionmaking technology beyond profiling in the regulation, the Agency should consider broadening its applicability to only include decisionmaking technology with significant economic or legal impact for a consumer, such as decisions about housing, lending, educational opportunities, or employment.

Any requirements to disclose that automated decisionmaking technologies are in use should be incorporated into the existing disclosure requirements in §1798.110. To the maximum extent possible, the Agency should avoid requiring separate and disparate disclosures for various aspects of the CPRA.

Finally, we recommend that any right to request access to specific pieces of information related to automated decisionmaking technologies be limited to personal information. In other words, if the information is not stored by the business in a way that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, it should not be subject to an access request. This limitation would be aligned and entirely consistent with the right to access information in §1798.110 of the CPRA.

### **Consumers Right to Delete, Right to Correct, and Right to Know**

Auto Innovators acknowledges the interest in providing consumers with a right to correct inaccurate personal information. We continue, however, to have concerns about how this right can be effectively exercised in some contexts, including with respect to vehicle-generated data. Some of the data that is collected from vehicles is data generated by vehicle systems and components, including sensors. An accuracy challenge from a consumer related to this type of vehicle data is likely to create unnecessary and unresolvable challenges for vehicle or component manufacturers.

To that end, we suggest that the Agency limit the right to request correction of personal information that has been provided directly by the consumer to the business in order to receive services. We also recommend that the Agency allow businesses to deny a consumer's request to correct personal information if the consumer fails to provide sufficient information to investigate the accuracy of the challenged personal information or when the business has reason to believe that the personal information is accurate. Moreover, we recommend that the Agency clarify that a business is not required to correct information that it has received from a third party. In these cases, the business should be permitted to refer the consumer to the third party from which it received the personal information for correction.

The Agency should set out reasonable limitations on the frequency with which a consumer can request that personal information be corrected. For example, the Agency should allow businesses to deny a consumer's request to correct personal information if the consumer has requested that the same information be corrected multiple times in an abbreviated period of time. At a minimum, a business's obligation to correct inaccurate information should be aligned with a business's disclosure obligations under §798.130(b).

### **Consumers' Right to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information**

Unlike a mobile phone or a social media account, vehicles are often used by individuals other than the vehicle owner (e.g., a spouse, family member, friend or neighbor, rental car customer, etc.). In almost all cases, an auto company does not know which consumer is using a particular vehicle at a particular point in time and would therefore not know when to honor a consumer's opt-out preference. As it is unclear how a global opt-out preference signal would work or translate effectively to the vehicle environment, it is premature for the Agency to require that all businesses accept a global opt-out preference signal. As CPRA provides other mechanisms by which consumers can effectively exercise their opt out rights, the Agency can take additional time to consider the broad implications of requiring all businesses, including those within the auto industry, to accept a global opt-out preference signal.

### **Information to be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)**

Much of the data that is generated and collected from vehicles is from onboard computer systems and sensors and relates to the operation and function of the vehicle and its systems. This data is very technical in nature and is of little use to the average consumer. In addition, this information frequently contains detailed data elements related to each vehicle system and component over the life of the vehicle. Since the average life of a vehicle is nearly 12 years, the volume of the data that may be responsive to a request for specific pieces of information would be vast and likely overwhelming for the consumer. For this reason, the Agency should deem disclosure of operational data for a device owned or used by a consumer beyond the 12-month window as involving a disproportionate effort. In addition, the Agency should consider permitting a business to deny a consumer's request if the consumer requests the same information multiple times.

As noted above, in most cases, an auto company does not know which consumer is driving a particular vehicle at a particular point in time. As a result, an auto company is generally unable to associate specific vehicle data with a person who was driving the vehicle when that vehicle data was generated. This poses significant, practical challenges for auto companies with respect to consumer requests for access to vehicle data and creates the potential for significant harm to consumers. For example, the sharing

of vehicle geolocation data with a consumer who was not using the vehicle at the time the geolocation data was generated may create privacy or even safety risks (e.g., an abusive individual seeking information about where his or her spouse has driven a vehicle.) For this reason, we urge the Agency to specifically confirm that a business is not required to provide access to specific pieces of personal information if it cannot verify that the personal information being requested relates specifically to that consumer or, in the case of data generated by a device, that the consumer was the consumer using the device when the requested personal data was generated.

Consumer privacy remains critically important to our member companies. We appreciate the opportunity to provide this feedback and input and look forward to continuing to work with the Agency on this and other privacy-related matters.

Sincerely,

A solid black rectangular box used to redact the signature of Hilary M. Cain.

Hilary M. Cain  
Vice President  
Technology, Innovation, & Mobility Policy



---

**From:** Sarah Barrows [REDACTED]  
**Sent:** 11/8/2021 2:29:35 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Sarah Barrows [REDACTED]; Jill Menning [REDACTED]; Catherine Dang [REDACTED]; Ashley Narsutis [REDACTED]; Castanon, Debra@CPPA [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b9766af8eba04290bfa5ae3e150c60e7-Castanon, D]  
**Subject:** PRO 01-21  
**Attachments:** 08NOV2021\_CPPA Comment\_\_Sarah E. Barrows\_FINAL.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Dear California Privacy Protection Agency  
Attn: Debra Castanon

Attached please find a copy of my November 8, 2021 comments.

An electronic version is also available for view by Debra Castanon [here](#).

Please advise if others need access to the electronic version of the document.

Sincerely, Sarah

Sarah Barrows  
Sr. Director, Privacy, Product & Policy Counsel



### **Statement of the Issue**

The current draft of the CCPA and CPRA negatively impact the ability for businesses to market to other businesses. This is due in part to the definitions of personal information and IP address.

The current CPRA will limit the ability of businesses to grow, acquire new (business) customers, and effectively market their products competitively. The CPRA places a particular burden on small and emerging businesses who may not have the capital, connections and employee resources to publicize their products in efficient ways aimed at growing their business in an economically friendly and targeted manner. In addition, with the pandemic impact of a large volume of professionals now working from home and other remote locations, the potential to co-mingle professional identifiers with personal identifiers presents new challenges and burdens to businesses who otherwise intend to comply with the CPRA.

NextRoll is an data-driven marketing technology company that utilizes AI and analytics capabilities to help two specific marketing sectors: direct-to-consumer products and services under the AdRoll business unit, and business-to-business ("b2b") marketing via the RollWorks business unit of NextRoll.

The following suggestions address and promote business-to-business marketing that will allow businesses to find new customers (businesses), market their products effectively, and remain competitive *without* invading consumers' privacy.

### **Initial Proposed Solutions**

- The definition of "personal information" in section 1798.140(v) *et seq.* should be revised to carve out business and professional identifiers with appropriate safeguards in instances where professionals work from home or other remote scenarios and who use person devices and/or personal home internet services to conduct professional business:
  - Specifically, 1798.140(v) (1) could be revised to include the additional language in underlined red font below:
    - (v) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household while not engaged in professional work or



visiting business solutions domains or business oriented publications and information. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household while not engaged in professional work: (A) Identifiers such as a real name, alias, residential postal address, unique personal identifiers and/or on line identifiers unconnected to an individual's professional or business capacity, residential Internet Protocol address not associated with a company domain or professional business, and not collected or used to contact or market to an individual outside non-holiday business days Monday-Friday from the hours of 9AM to 5PM in the state of California\*, personal email address not distributed by a professionals' employer or business and intended for the use of professional activity, account name, social security number, driver's license number, passport number, or other similar non-professional or business identifiers. (B) Any categories of personal information described in subdivision (e) of [Section 1798.80](#) except that "employment" can refer the company name or domain name of the company where an individual is employed so long as the company employs 100 or more individuals and/or the company is part of a company consortium consisting of multiple companies in the same industry that individually employ less than 100 individuals, but collectively employ at least 100 employees. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, consumer products or services purchased, obtained, or considered for individual or household use and not professional or business use, or other purchasing or consuming histories or tendencies related solely to consumer products or services not intended for business or professional use. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing or history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement consisting of 95% or more consumer, non-professional products or services intended for business and not individual or household use. (G) Geolocation data that is more precise than City or



State. (H) Audio, electronic, visual, thermal, olfactory, or similar Information. (I) Professional or employment-related Information that is not current for 12-months or whose current status is unknown. (J) Education information, defined as information that is not publicly available personally Identifiable information as defined In the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99). (K) Inferences drawn from any of the Information identified in this subdivision to create a profile about a consumer and not a professional acting in their professional or business capacity and which reflects~~ing~~ the consumer's preferences characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, aptitudes, and the consumer's behavior and/or preferences for business goods and services to be used in the consumer's professional or business capacity.

- In addition, the CPPA should revisit the February 10, 2020 California Attorney General modifications and explain why the guidance was stricken thus clarifying where the IP address is or is not personal information.
  - Specifically, as reported by the [IAPP](#), in the relevant excerpt from the IAPP article, and specifically with reference to the portion highlighted in yellow below:
    - The CCPA's definition of personal information expressly contemplates including IP addresses. An IP address alone may not allow a business to identify a particular consumer or household; however, in many — if not most — cases, an ISP can link an IP address with a name, home address, phone number, email address and even payment information. To be successful, certain statutes require requests for an ISP to link an IP address to an individual to be accompanied by a court order, subpoena or a law enforcement warrant. Unfortunately, it is unclear whether such efforts would be considered “reasonably capable” of linking an IP address to an individual or household such that all IP addresses are personal information under the CCPA.
    - On Feb. 10, the California attorney general issued its first set of modifications to its proposed CCPA regulations. These modifications included the following guidance:
      - “[I]f a business collects the IP addresses of visitors to its websites but does not link the IP address to any particular consumer or household, and could not reasonably link the IP



address with a particular consumer or household, then the IP address would not be 'personal information.'

- This guidance was critical in clarifying that the CCPA's "reasonableness" inquiry was focused on the receiving entity itself — not on the ability of third parties, such as ISPs, to link information to individuals or consumers. In other words, if the business did not link the IP address to a consumer or household, and the business could not reasonably link the IP address with a particular consumer or household, the IP address would not be personal information. This interpretation aligns with the reality that even if businesses wished to link IP addresses to individuals or households, many would lack the information needed to do so themselves and would be unlikely to succeed in compelling an ISP to do so for them. However, when the attorney general revised its draft regulations for a second time March 11, the guidance was struck without explanation. See article [here](#).
- In response to the CCPA's final request for 'other comments', the CPPA should provide guidance on IP addresses. It is increasingly difficult to market to businesses since remote work became more common during the pandemic—a trend unlikely to change as workers with the potential to remain remote adopt hybrid or fully remote options at their workplaces. The CPPA should provide guidance on where an IP address is and is not personal information that specifically carves out the use of IP address in marketing towards businesses.
  - The CPPA could work with the California state legislature to require a subpoena, court order or law enforcement warrant to accompany any and all requests to link an IP address with a name, home address, phone number, email address and even payment information.
  - In addition or in alternative to a court order, subpoena or warrant, companies of 100+ employees offering goods or services to individuals residing in California and seeking to engage in marketing products and services to businesses and/or companies offering goods and services to individuals residing in California seeking the opportunity to receive digital advertising via internet advertising could provide the residential IP Addresses of the relevant employees at their respective companies who work at home or remotely so long as the non-holiday, Monday-Friday business hours of 9AM-5PM Pacific are observed (with accompanying penalties for companies failing to comply with these safeguards/requirements).

Sincerely,

/s

Sarah E. Barrows

*Senior Dir. Privacy, Product & Policy Counsel at NextRoll, Inc.*



---

**From:** McArthur, Webb [REDACTED]  
**Sent:** 11/8/2021 2:27:31 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Eric Ellman [REDACTED]  
**Subject:** PRO 01-21 - Comments of the Consumer Data Industry Association  
**Attachments:** CDIA CPPA CPRA Preliminary Rulemaking Comment Letter.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

To whom it may concern:

Attached are comments of the Consumer Data Industry Association ("CDIA") on PRO 01-21.

Please contact us if you have any further questions.

Webb McArthur  
Associate | Admitted in the District of Columbia, Maryland, and Virginia  
Hudson Cook, LLP  
Direct: [REDACTED] | Cell: [REDACTED]  
1909 K St., NW | 4th Floor | Washington, DC 20006

Hudson Cook's COVID-19 Resources

HUDSON  
COOK

The information contained in this transmission may be privileged and may constitute attorney work product. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Webb McArthur at [REDACTED] or [REDACTED] and destroy all copies of the original message and any attachments.

\* \* \* \*



Consumer Data Industry Association  
1090 Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: [REDACTED]

[CDIAONLINE.ORG](http://CDIAONLINE.ORG)

November 8, 2021

*Via Electronic Delivery to [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)*

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

**RE: Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act (PRO 01-21)**

Dear Ms. Castanon,

The Consumer Data Industry Association submits this comment letter in response to the invitation of the California Privacy Protection Agency ("CPPA") for preliminary comments on proposed rulemaking under the California Privacy Rights Act ("CPRA").

The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA").

CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA appreciates the CPPA's broad invitation to comment at the beginning of the rulemaking process. As we describe in greater detail below, CDIA members provide identity verification and fraud prevention services to their customers, and such services involve the processing of personal information, including sensitive personal information. CDIA strongly urges the CPPA to ensure that consumer rights related to automated processing, correction, and notice at collection do not interfere with security and integrity activities, service providers and contractors are permitted to combine personal information obtained from multiple sources, and all businesses are permitted to engage in identity verification and fraud detection activities, including those required by law and collective standard. Finally, CDIA urges the CPPA to advocate for the repeal of employment and business to business communication exemption sunsets and issue a policy statement providing for the consistent interpretation of the CPRA with similar state laws.

To assist the agency in promulgating clear and effective regulations that allow businesses to best support customers and consumers, CDIA offers the following comments on the topics as presented in the Invitation for Preliminary Comments:

## **I. Automated Decisionmaking**

The Invitation for Preliminary Comments states, in part:

### *2. Automated Decisionmaking*

*The CPRA provides for regulations governing consumers' "access and opt-out rights with respect to businesses' use of automated decisionmaking technology." Civil Code, § 1798.185(a)(16).*

*Comments on the following topics will assist the Agency in creating these regulations:*

- a. What activities should be deemed to constitute "automated decisionmaking technology" and/or "profiling." Civil Code, §§ 1798.185(a)(16) and 1798.140(z).*

CDIA strongly urges the CPPA to exclude activities to ensure "security and integrity" from "automated decisionmaking" activities. "Security and integrity," as the CPRA defines that term, includes activities related to detecting security incidents, detecting fraud or other illegal action, and verifying identity.

Civil Code, § 1798.140(z) defines the term "profiling" as automated processing "to evaluate certain aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, behavior, location or movements."



CDIA members provide a wide range of products and services related to identity verification and fraud detection. Businesses regularly need to engage in identity verification and fraud detection efforts, in some circumstances by law or collective standard but otherwise to reduce risk of harm to the business and to consumers. By preventing fraud and identity theft on consumers, such efforts further consumer privacy.

“Profiling” under the CPRA refers to particular methods of analyzing personal information to predict personal aspects, like work performance, financial status, preferences, and location. Efforts to detect fraud and verify identity are distinct from “profiling” activities because such efforts attempt to confirm what a consumer told the business in order to reduce risk, a “business purpose” under the CCPA and CPRA.

If the CPPA were to include “security and integrity” activities in its conception of automated processing such that consumers would have access and opt out rights, businesses would be impeded from appropriately engaging in fraud detection and identity theft efforts. Consumers intending to commit fraud could simply opt out of automated processing, and a business might not be able to prevent the intended fraud. Fraudsters could also exercise access requests in order to learn how such business detects fraud, which if shared, could prevent such business from appropriately detecting fraud not only for the consumer making such a request, but for consumers generally.

Accordingly, CDIA strongly urges the CPPA to exclude activities relating to “security and integrity” as defined by the CPRA from “profiling” or automated processing.

## **II. Consumer Right to Correct**

The Invitation for Preliminary Comments states, in part:

### *4. Consumers’ Right to Delete, Right to Correct, and Right to Know*

*The CCPA gives consumers certain rights to manage their personal information held by businesses, including the right to request deletion of personal information; the right to know what personal information is being collected; the right to access that personal information; and the right to know what categories of personal information are being sold or shared, and to whom. See Civil Code, §§ 1798.105, 1798.110, 1798.115, and 1798.130. The CPRA amended the CCPA to add a new right: the right to request correction of inaccurate personal information. See Civil Code, §§ 1798.106 and 1798.130.*

*The Attorney General has adopted regulations providing rules and procedures to facilitate the right to know and the right to delete. See Code Regs., tit. 11, §§ 999.308((c), 999.312–313, 999.314(e), 999.318, 999.323–326, and 999.330(c). The CPRA additionally provides for regulations that establish rules and procedures to facilitate the new right to correct. 2 See Civil Code, § 1798.185(a)(7).*

*Comments on the following topics will assist the Agency in creating these regulations:*

...

- b. How often, and under what circumstances, a consumer may request a correction to their personal information. See Civil Code, § 1798.185(a)(8).*

...

- d. When a business should be exempted from the obligation to take action on a request because responding to the request would be “impossible, or involve a disproportionate effort” or because the information that is the object of the request is accurate. Civil Code, § 1798.185(a)(8)(A).*

First, CDIA urges the CPPA to clarify by regulation that a consumer does not have a right to correct personal information processed by a business for “security and integrity” activities. The CPRA, at Civil Code, § 1798.106(a), provides that consumers have the right to request correction of personal information maintained by a business, “taking in account the nature of the personal information and the purposes of the processing of personal information.”

Businesses maintain personal information for “security and integrity” activities, either on their own or by way of a service provider, using such information to detect identity theft or other fraud instances by verifying personal information received by the business. If consumers are permitted to modify the personal information that a business uses to compare newly-received information against, fraudsters may easily be able to bypass checks and commit identity theft against a consumer or other fraud. Businesses need to be able to maintain personal information for such security and integrity activities without having to change that information. The Right to Delete, at Civil Code, § 1798.105(d)(2), includes an exception to “[h]elp ensure security and integrity,” and the Right to Correct needs an equivalent exception. CDIA urges the CPPA to clarify that the Right to Correct’s provision for “taking account the nature of the personal information and the purposes of the processing of the personal information” includes denying a right to correct personal information maintained for “security and integrity” purposes.

Second, CDIA urges the CPPA to clarify that a business should be exempted from the obligation to take action on a request to correct where the personal information cannot be verified through official documentation. If a request cannot be verified through official documentation, like it could for a request to update an address or correct the spelling of a name, then responding to the request would be “impossible” and the business would not be able to confirm that the “object of the request is accurate.” For example, a consumer should not have the right to “correct” a business’ customer service notes, which might reflect an employee’s understanding of a phone conversation between the employee and the consumer.

An employee might document that the consumer made a particular request and that, as a result, the business had a particular response to that request. A consumer being able to change such record would make it impossible for a business to keep accurate records of what it understood happened in a conversation with a consumer. Accordingly, CDIA urges the CPPA to clarify that absent the ability to verify the object of the correction request through official documentation, regardless of whether requesting such documentation is permissible or whether the business attempted to verify the information, the business should be exempted from the obligation to take action on the request.

### **III. Consumer Right to Limit the Use of Sensitive Personal Information**

The Invitation for Preliminary Comments states, in part:

*5. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information*

*The CCPA gives consumers the right to opt out of the sale of their personal information by covered businesses. See Civil Code, § 1798.120(a). In 2020, the Attorney General adopted regulations to implement consumers' right to opt out of the selling of their personal data under the CCPA. See Code Regs., tit. 11, §§ 999.306, 999.315, and 999.316. The CPRA now provides for additional rulemaking to update the CCPA rules on the right to opt-out of the sale of personal information, and to create rules to limit the use of sensitive personal information, and to account for other amendments. See Civil Code, §§ 1798.185(a)(4) and 1798.185(a)(19)–(20).*

*Comments on the following topics will assist the Agency in creating these regulations:*

- a. What rules and procedures should be established to allow consumers to limit businesses' use of their sensitive personal information. See Civil Code, § 1798.185(a)(4)(A).*

The CPRA, at Civil Code, § 1798.121(a), limits consumers' right to direct a business that collects sensitive personal information to limit its use of that information by expressly permitting businesses to help to ensure "security and integrity" and to perform services on behalf of the business, including verifying customer information. CDIA urges the CPPA not to place limitations on these permitted uses when it adopts regulations addressing how consumers may limit business' use of their sensitive personal information. In particular, CDIA urges the CPPA not to limit the CPRA's express authorization for businesses to engage in "security and integrity" activities and other business services.

When businesses and their service providers, including CDIA members, engage in efforts to detect fraud and verify identity, they may use elements of sensitive personal information, including social security numbers, other identification numbers, or financial



account numbers, in particular, comparing information provided by the consumer to information made available for verification and fraud detection efforts. Such efforts are critical for businesses to be able to prevent loss and protect consumer privacy.

If consumers were able to limit the use of sensitive personal information for “security and integrity” activities, like fraud detection, or other business services like verifying customer information, businesses would be less able to prevent identity theft and other fraud, and all consumers would suffer because of such increased fraud risks and the potential increase in cost of services resulting from greater losses. CDIA thus urges the CPPA not to limit the CPRA’s express authorization for businesses to engage in “security and integrity” activities and other business services.

#### **IV. Business Purposes for which Entities May Combine Personal Information and Use Personal Information on Own Behalf**

The Invitation for Preliminary Comments states, in part:

*8. Definitions and Categories*

*The CCPA and CPRA provide for various regulations to create or update definitions of important terms and categories of information or activities covered by the statute.*

*Comment on the following topics will assist the Agency in deciding whether and how to update or create these definitions and categories:*

...

- e. Further defining the business purposes for which businesses, service providers, and contractors may combine consumers’ personal information that was obtained from different sources. See Civil Code, § 1798.185(a)(10).*

CDIA strongly urges the CPPA to deem that efforts to security “security and integrity” as that term is defined by the CPRA are a business purpose for which businesses, service providers, and contractors are permitted to combine consumers’ personal information obtained from different sources.

CDIA members provide “security and integrity” services, like fraud detection and identity verification services, to their business customers and may do choose to do so under the CPRA’s “service provider” or “contractor” models. In order to provide such services, fraud detection and identity verification providers often have a need to combine multiple sets of personal information collected from multiple sources. These vendors provide their services through various data processing methods, including by comparing inquiry data with data available elsewhere, by detecting anomalies in provided data, and by otherwise analyzing

multiple data sets, all with the goal of detecting—and thus preventing—identity theft, fraud, and other illegal actions on businesses. These efforts reduce business costs and protect consumers, whether such consumers are business customers or not, and thus further consumer privacy.

CCPA regulations currently permit service providers to retain, use, and disclose personal information obtained in the course of detecting data security incidents and protecting against fraudulent or illegal activity. See Cal. Code Regs. tit. 11, § 999.314(c)(4). Fraud detection and identity verification service providers need to be able to retain, use, and disclose personal information to provide their critical services and prevent fraud on businesses and on consumers. Without the ability to retain, use, and disclose personal information, such service providers would not be able to offer fraud detection and prevention services because such services necessarily involve verifying the accuracy of personal information provided to businesses. The CPPA should retain this express permission for service providers to use, retain, and disclose personal information in connection with security and integrity functions and expand it to apply to “contractors” under the CPRA.

The CPPA should also expressly include “security and integrity” activities within the business purposes for which businesses and their service providers and contractors may combine personal information obtained from multiple services. Service providers offering fraud detection and prevention services need to be able to combine, and thus compare, personal information obtained from multiple sources and on behalf of multiple business clients to be able to accurately verify personal information and prevent fraud. If fraud prevention services providers are not permitted to combine personal information from multiple sources, or if consumers are permitted to opt out of such processing, fraud prevention services providers will be unable to provide their critical services. By permitting service providers to combine personal information for “security and integrity” activities, businesses will be able to utilize commercial fraud detection and identity verification products and reduce the risk of identity theft and other fraud on both businesses and consumers.

## **V. Establishing Exceptions Necessary to Comply with State or Federal Law**

The Invitation for Comments also requests any additional comments in relation to the CPPA’s initial rulemaking. The CPPA is tasked with updating existing regulations and adopting new regulations. See, e.g., Civil Code, § 1798.185.

Civil Code, § 1798.185(a)(3) instructs the:

*Establishing [of] any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.*

The goals of the CPRA and CCPA to protect and further consumer privacy emphasize the importance—and the *growing* importance—of fraud detection products. Fraud detection products protect not only businesses against fraud by criminals, but they also protect consumers from identity fraud. These products work by utilizing a large volume of data, and removing one consumer's data from the universe of available data would affect not only that consumer, but all consumers.

The CPRA authorizes the CPPA to establish exceptions necessary to comply with state or federal law as needed. Businesses of various sorts and sizes are required to engage in customer due diligence (CDD), know your customer (KYC), or other identity theft and fraud check expectations by law, regulation, guidance, or other collective standard. Businesses engage identity verification and fraud detection providers like CDIA members to comply with such requirements or expectations. In the context of such varied CDD, KYC, and other fraud detection requirements and expectations, CDIA strongly urges the CPPA to adopt an express exception to CCPA and CPRA requirements that provides that the law is not to be interpreted to prevent or limit a business' efforts to ensure "security and integrity" as the law defines those activities. Such a provision would assist in business' efforts to comply with law and other standards and would further consumer privacy by permitting businesses to engage in appropriate efforts, including through the use of commercial fraud detection services, to combat identity theft, protect consumer personal information, and ensure consumer privacy.

## **VI. Purpose Limitation Exception for "Security and Integrity" Activities**

The Invitation for Comments also requests any additional comments in relation to the CPPA's initial rulemaking. The CPPA is authorized to adopt additional regulations as necessary to further the purposes of the CCPA and CPRA. See, e.g., Civil Code, § 1798.185(b).

CDIA urges the CPPA to clarify that "security and integrity" activities are not purposes for which businesses are required to disclose to consumers under Civil Code, § 1798.100(a)(1) and (2), and that not disclosing such "security and integrity" purposes would not prevent a business from using personal information for such purposes, per Civil Code, § 1798.100(c).

As noted, many CDIA members provide critical fraud protection services. Disclosing the nature of those services any related data collection may compromise the success of such efforts where the disclosure would inform fraudsters as to the type of fraud and identity theft checks engaged in by a particular business. Furthermore, limitations on the ability of fraud detection providers to use crucial data, including in the absence of disclosure to the consumer, will also undermine these important services.

CDIA urges the CPPA to clarify that "security and integrity" activities are not purposes that businesses are required to disclose to consumers under Civil Code, § 1798.100(a)(1) and (2). Furthermore, CDIA urges the CPPA not to apply the purpose limitation requirements in § 1798.100(c) to data used for "security and integrity." Rather, data should be made available for



those purposes regardless of the notice provided at collection in order to maximize available information to protect against fraud and to avoid providing opportunities for fraudsters to avoid detection, uses that further consumer privacy.

## **VII. Repealing or Delaying the Enforcement of Employment Context and Business to Business Communications Exemptions Sunsets**

The Invitation for Comments also requests any additional comments in relation to the CPPA's initial rulemaking. The CPPA is authorized to adopt additional regulations as necessary to further the purposes of the CCPA and CPRA. See, e.g., Civil Code, § 1798.185(b).

The CPRA sunsets these exemptions on January 1, 2023, and businesses lack clear guidance as to how to extend rights to consumers with regard to personal information not processed in the context of providing products or services to those consumers while navigating other laws, like state employment laws. CDIA urges the CPPA to advocate to the legislature the repeal of these sunsets, but in the absence of such action, CDIA urges the CPPA to delay enforcement of the law with regard to personal information processed in these contexts. In the absence of a repeal of these sunsets or a delay in enforcement, we encourage the CPPA to carefully consider the extent to which CPRA rules will apply to personal information currently covered by these exemptions given competing privacy considerations, particularly the privacy of other employees who may be referenced in employee records.

## **VIII. Urging Uniformity with Similar State Laws**

The Invitation for Comments also requests any additional comments in relation to the CPPA's initial rulemaking. The CPPA is authorized to adopt additional regulations as necessary to further the purposes of the CCPA and CPRA. See, e.g., Civil Code, § 1798.185(b).

CDIA urges the CPPA to adopt a policy statement by regulation that it will align its regulatory interpretations with provisions of similar state privacy and data protection laws, including the Virginia Consumer Data Privacy Act and the Colorado Privacy Act, wherever possible. The CPRA instructs the CPPA to cooperate with other similar state agencies to ensure consistent application of privacy protections. See Civil Code, § 1798.199.40(i). Accordingly, CDIA urges the CPPA to endeavor to interpret the CPRA consistently with the laws enforced by those other state agencies.

Businesses subject to these laws are facing an increasingly large and complex landscape of privacy laws relating to consumer data, and consumers across the nation will benefit from similar protections and rights. Accordingly, it would benefit consumers for the CPPA to interpret the CPRA consistently with such other laws. For example, CDIA encourages the CPPA to adopt consistent interpretations to what is considered "personal information" and "deidentified information," and CDIA urges consistent approaches to

interpreting provisions permitting businesses to engage in “security and integrity” activities without limitation. We also urge the CPPA to consider providing businesses right reasonable abilities to cure deficiencies in CPRA compliance, just as other state laws provide. Finally, CDIA urges the CPPA to work with other state agencies to ensure that businesses can provide consistent disclosures to residents of all states.

\* \* \*

Thank you for the opportunity to share our views on the anticipated rulemaking under the CPRA. Please contact us if you have any questions or need further information based on comments.

Sincerely,



Eric J. Ellman  
Senior Vice President, Public Policy & Legal Affairs

---

**From:** Latifah Alexander [REDACTED]  
**Sent:** 11/8/2021 2:37:28 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** Preliminary Comments on Proposed Rulemaking - CPRA  
**Attachments:** CPPA CPRA Invitation to Comment Letter.pdf  
**Importance:** High

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Hi,

I'm not sure if you have the attached letter on California Privacy Rights Act of 2020.

Thank you,



**Latifah Alexander**  
Legislative Administrative Assistant  
California Bankers Association  
1303 J Street, Suite 600 | Sacramento, CA 95814  
[REDACTED]  
F: (916) 438-4319  
Connect: [Website](#) | [Twitter](#) | [LinkedIn](#)





November 8, 2021

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**RE: Invitation for Preliminary Comments on Proposed Rulemaking -- California Privacy Rights Act of 2020**

Dear Ms. Castanon:

The California Bankers Association (CBA) appreciates the opportunity to submit comments in response to the invitation by the California Privacy Protection Agency (Agency) for preliminary comments on proposed rulemaking under the California Privacy Rights Act (CPRA) of 2020. CBA is one of the largest banking trade associations in the United States advocating on legislative, regulatory, and legal matters on behalf of banks doing business in California.

The importance of protecting consumer data and privacy are not new concepts for banks who have operated for decades under protections established by laws like the Gramm-Leach-Bliley Act and California Financial Information Privacy Act. As the Agency prepares to issue regulations in accordance with the CPRA, we appreciate the opportunity to provide preliminary input.

**Risk Assessments & Audits**

With respect to the CPRA's requirement that businesses submit regular risk assessments regarding their processing of personal information and the Agency's authority to audit businesses' compliance with the law, we urge the Agency to exempt banks which are already highly regulated and subject to supervision and frequent examination by banking regulators.

State and federally chartered banks already have at least three independent regulators. For example, state-chartered banks are presently regulated by the California

Department of Financial Protection and Innovation, the federal Consumer Financial Protection Bureau (CFPB), and the Federal Deposit Insurance Corporation (FDIC). This level of oversight includes frequent, routine examinations by regulatory agencies of the safety and soundness of these organizations and compliance with various laws whether focused on consumer protection or otherwise.

Moreover, banks' cybersecurity risk assessments contain highly sensitive information which needs to be tightly protected; any disclosure, whether inadvertent or intentional, could expose the bank, its operations, and its customers to undue risk.

### **Automated Decision-making**

Federal banking regulators are currently contemplating the use of automated decision-making and whether additional rules are necessary governing the technology. More specifically, on March 31, 2021, the Board of Governors of the Federal Reserve System, CFPB, FDIC, National Credit Union Administration, and OCC published notice in the *Federal Register* for the purpose of:

“...gathering information and comments on financial institutions' use of artificial intelligence (AI), including machine learning (ML). The purpose of this request for information (RFI) is to understand respondents' views on the use of AI by financial institutions in their provision of services to customers and for other business or operational purposes; appropriate governance, risk management, and controls over AI; and any challenges in developing, adopting, and managing AI. The RFI also solicits respondents' views on the use of AI in financial services to assist in determining whether any clarifications from the agencies would be helpful for financial institutions' use of AI in a safe and sound manner and in compliance with applicable laws and regulations, including those related to consumer protection.”

Accordingly, the Agency should refrain from applying automated decision-making regulations to banks until federal regulators take action or should ensure that the Agency's regulations do not conflict with federal requirements.

The definition of automated decision-making needs to be better developed. If a precise definition is not promulgated, it could produce unintended litigation results, where over-inclusive claims are brought. The regulations should distinguish between decision-making technology which is 100 percent automated versus partially automated with

some human intervention and a potential manual/override process, which should be outside the defined coverage. Further, if personal information is not processed through the automated decision-making technology, it should be treated as out of scope for purposes of the CPRA.

### **Right to Correct**

The CPRA requires regulations that establish rules and procedures to facilitate a consumer's right to correct inaccurate personal information. When drafting regulations, the Agency should consider permitting businesses to utilize existing protocols that allow consumers to correct personal information and should accordingly provide flexibility for businesses to direct consumers to established channels and processes utilizing existing protocols. Requiring businesses to create new CPRA-specific channels for submitting and/or receiving personal information correction requests would create operational complexity with no added value to the consumer.

For regulated financial institutions, the potential for fraud risk is a critical concern. Given the extensive customer and employee/user authentication and identity theft prevention requirements to which financial institutions are already subject, and in light of the significant risk of fraud, financial institutions should be allowed to require all customers, prospective customers, employees, and third parties to use existing channels subject to established security and authentication protocols for any personal information correction requests.

The Agency should also distinguish between personal information that is active and in use, which could be subject to the right to correct, versus personal information that is archived for recordkeeping purposes and is not in use (i.e., historical, inactive, or point-in-time records), which would be outside the right to correct.

The right to correct provisions need clarification on the 45/90-day response/completion of correction timelines. Please clarify if the clock commences when the business "verifies the identity of the requester" versus when the business verifies "that the correction request is valid" (such as when evidence of a name change through a new driver's license is provided).



### **Right to Limit the Use and Disclosure of Sensitive Personal Information**

We request that the Agency provide greater clarity to what is meant by “inferring characteristics of a consumer.” As a general matter, sensitive personal information should be collected and used on a need-to-know basis for legitimate purposes. The proposed regulations should take into consideration existing laws that require the collection of sensitive personal information and the unintended consequences to consumers if the use of such sensitive personal information is limited.

### **Specific Pieces of Information**

With respect to a business’ requirement to disclose specific pieces of information, the regulations should take into consideration the challenge associated with a business accessing and retrieving archived personal information when endeavoring to respond to a request to disclose specific pieces of information. The Agency should distinguish between personal information that is active and in use, which could be subject to the requirement to disclose specific pieces of information, versus archived personal information that is archived for recordkeeping purposes and not in use (i.e., historical, inactive, or point-in-time records), which should be outside the requirement to disclose specific pieces of information. The regulations should avoid use of overly stringent thresholds such as making such disclosures except where “impossible,” and rely instead on commercially reasonable practices.

Thank you again for the opportunity to offer preliminary comments. We welcome any questions you may have regarding our letter.

Sincerely,

A solid black rectangular box used to redact the signature of Kevin Gould.

Kevin Gould  
SVP/Director of Government Relations

KG:la

---

**From:** Kevin Gould [REDACTED]  
**Sent:** 11/8/2021 2:12:04 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 -- PRO 01-21  
**Attachments:** CPPA CPRA Invitation to Comment Letter.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Thank you for the opportunity to provide preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020. Please let us know if you have any questions regarding our attached comment letter. Thank you.



**Kevin Gould**  
SVP, Director of Government Relations  
California Bankers Association  
1303 J Street, Suite 600 | Sacramento, CA 95814  
[REDACTED]  
F: (916) 438-4310  
Connect: [Website](#) | [Twitter](#) | [LinkedIn](#)



November 8, 2021

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**RE: Invitation for Preliminary Comments on Proposed Rulemaking -- California Privacy Rights Act of 2020**

Dear Ms. Castanon:

The California Bankers Association (CBA) appreciates the opportunity to submit comments in response to the invitation by the California Privacy Protection Agency (Agency) for preliminary comments on proposed rulemaking under the California Privacy Rights Act (CPRA) of 2020. CBA is one of the largest banking trade associations in the United States advocating on legislative, regulatory, and legal matters on behalf of banks doing business in California.

The importance of protecting consumer data and privacy are not new concepts for banks who have operated for decades under protections established by laws like the Gramm-Leach-Bliley Act and California Financial Information Privacy Act. As the Agency prepares to issue regulations in accordance with the CPRA, we appreciate the opportunity to provide preliminary input.

**Risk Assessments & Audits**

With respect to the CPRA's requirement that businesses submit regular risk assessments regarding their processing of personal information and the Agency's authority to audit businesses' compliance with the law, we urge the Agency to exempt banks which are already highly regulated and subject to supervision and frequent examination by banking regulators.

State and federally chartered banks already have at least three independent regulators. For example, state-chartered banks are presently regulated by the California

Department of Financial Protection and Innovation, the federal Consumer Financial Protection Bureau (CFPB), and the Federal Deposit Insurance Corporation (FDIC). This level of oversight includes frequent, routine examinations by regulatory agencies of the safety and soundness of these organizations and compliance with various laws whether focused on consumer protection or otherwise.

Moreover, banks' cybersecurity risk assessments contain highly sensitive information which needs to be tightly protected; any disclosure, whether inadvertent or intentional, could expose the bank, its operations, and its customers to undue risk.

### **Automated Decision-making**

Federal banking regulators are currently contemplating the use of automated decision-making and whether additional rules are necessary governing the technology. More specifically, on March 31, 2021, the Board of Governors of the Federal Reserve System, CFPB, FDIC, National Credit Union Administration, and OCC published notice in the *Federal Register* for the purpose of:

“...gathering information and comments on financial institutions' use of artificial intelligence (AI), including machine learning (ML). The purpose of this request for information (RFI) is to understand respondents' views on the use of AI by financial institutions in their provision of services to customers and for other business or operational purposes; appropriate governance, risk management, and controls over AI; and any challenges in developing, adopting, and managing AI. The RFI also solicits respondents' views on the use of AI in financial services to assist in determining whether any clarifications from the agencies would be helpful for financial institutions' use of AI in a safe and sound manner and in compliance with applicable laws and regulations, including those related to consumer protection.”

Accordingly, the Agency should refrain from applying automated decision-making regulations to banks until federal regulators take action or should ensure that the Agency's regulations do not conflict with federal requirements.

The definition of automated decision-making needs to be better developed. If a precise definition is not promulgated, it could produce unintended litigation results, where over-inclusive claims are brought. The regulations should distinguish between decision-making technology which is 100 percent automated versus partially automated with



some human intervention and a potential manual/override process, which should be outside the defined coverage. Further, if personal information is not processed through the automated decision-making technology, it should be treated as out of scope for purposes of the CPRA.

### **Right to Correct**

The CPRA requires regulations that establish rules and procedures to facilitate a consumer's right to correct inaccurate personal information. When drafting regulations, the Agency should consider permitting businesses to utilize existing protocols that allow consumers to correct personal information and should accordingly provide flexibility for businesses to direct consumers to established channels and processes utilizing existing protocols. Requiring businesses to create new CPRA-specific channels for submitting and/or receiving personal information correction requests would create operational complexity with no added value to the consumer.

For regulated financial institutions, the potential for fraud risk is a critical concern. Given the extensive customer and employee/user authentication and identity theft prevention requirements to which financial institutions are already subject, and in light of the significant risk of fraud, financial institutions should be allowed to require all customers, prospective customers, employees, and third parties to use existing channels subject to established security and authentication protocols for any personal information correction requests.

The Agency should also distinguish between personal information that is active and in use, which could be subject to the right to correct, versus personal information that is archived for recordkeeping purposes and is not in use (i.e., historical, inactive, or point-in-time records), which would be outside the right to correct.

The right to correct provisions need clarification on the 45/90-day response/completion of correction timelines. Please clarify if the clock commences when the business "verifies the identity of the requester" versus when the business verifies "that the correction request is valid" (such as when evidence of a name change through a new driver's license is provided).

### **Right to Limit the Use and Disclosure of Sensitive Personal Information**

We request that the Agency provide greater clarity to what is meant by “inferring characteristics of a consumer.” As a general matter, sensitive personal information should be collected and used on a need-to-know basis for legitimate purposes. The proposed regulations should take into consideration existing laws that require the collection of sensitive personal information and the unintended consequences to consumers if the use of such sensitive personal information is limited.

### **Specific Pieces of Information**

With respect to a business’ requirement to disclose specific pieces of information, the regulations should take into consideration the challenge associated with a business accessing and retrieving archived personal information when endeavoring to respond to a request to disclose specific pieces of information. The Agency should distinguish between personal information that is active and in use, which could be subject to the requirement to disclose specific pieces of information, versus archived personal information that is archived for recordkeeping purposes and not in use (i.e., historical, inactive, or point-in-time records), which should be outside the requirement to disclose specific pieces of information. The regulations should avoid use of overly stringent thresholds such as making such disclosures except where “impossible,” and rely instead on commercially reasonable practices.

Thank you again for the opportunity to offer preliminary comments. We welcome any questions you may have regarding our letter.

Sincerely,

A solid black rectangular box used to redact the signature of Kevin Gould.

Kevin Gould  
SVP/Director of Government Relations

KG:la

---

**From:** Melanie Tiano [REDACTED]  
**Sent:** 11/8/2021 2:39:45 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** PRO 01-21 -- CTIA Comments  
**Attachments:** CTIA CPRA Rulemaking Preliminary Comments 11.08.21.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Good evening,

Attached are CTIA's comments in response to the Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21).

Please let me know if you have any questions.

Thank you,

Melanie Tiano



Melanie K. Tiano  
Assistant Vice President, Cybersecurity and Privacy  
1400 16<sup>th</sup> Street, NW  
Washington, DC 20036  
[REDACTED]

Before the  
**California Privacy Protection Agency**

In the Matter of

California Privacy Rights Act of 2020  
Rulemaking Process

)  
)  
)  
)  
)  
)

Invitation for Preliminary  
Comments on Proposed Rulemaking

**COMMENTS OF CTIA**

Gerard Keegan  
Vice President, State Legislative Affairs

Melanie K. Tiano  
Assistant Vice President, Cybersecurity and  
Privacy

Lisa Volpe McCabe  
Director, State Legislative Affairs

**CTIA**  
1400 16th St. NW, Suite 600  
Washington, DC 20036  
(202) 736-3200  
[www.ctia.org](http://www.ctia.org)

November 8, 2021



## TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION.....	4
I. Processing that Presents a Significant Risk to Consumers’ Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses – Cal. Civ. Code § 1798.185(a)(15).....	6
A. When does a business’s processing of personal information present a “significant risk to consumers’ privacy or security”?.....	7
1. “Significant risk” should be defined to address substantial, specific, and enumerated risks. ....	7
2. The triggers to conduct a cybersecurity audit or risk assessment should directly align with the cybersecurity or privacy risk creating the obligation. ....	8
B. What should a business that performs an annual cybersecurity audit be required to do, including what should it cover in its audit and what processes are needed to ensure that its audit is “thorough and independent”? .....	9
1. CPRA standards for cybersecurity audits should be consistent with California’s existing statutory data security requirements.....	10
2. The Agency should permit businesses to rely on widely-accepted, rigorous cybersecurity frameworks as a safe harbor to demonstrate compliance with CPRA cybersecurity audit standards. ....	10
3. The Agency should permit businesses to leverage existing cybersecurity audit procedures, including appropriately-structured internal audit processes. ....	11
4. Cybersecurity audits should only be required to address the specific activity that triggered the audit.....	12
C. What should businesses that submit a risk assessment to the Agency be required to do, including what should they cover in their risk assessment, how often should they submit a risk assessment, and how should they weigh the risks and benefits of processing consumers’ personal information and sensitive personal information?.....	12
1. The Agency should require a generalized risk assessment that enables meaningful oversight without creating cybersecurity and privacy risks. ....	13
2. A risk assessment, if required, should only be due every two to three years to avoid unnecessarily imposing burdens on businesses and the Agency. ....	15

3.	The Agency should implement appropriate safeguards to protect any information obtained in a risk assessment. ....	15
II.	Automated Decision-making – Cal. Civ. Code § 1798.185(a)(16) .....	16
A.	What should be the scope of consumers’ opt-out rights with regard to automated decision-making, and what processes should consumers and businesses follow to facilitate opt outs?.....	16
1.	The delegation of rulemaking authority to create a new right to opt out of automated decision-making is unconstitutional. ....	16
2.	If the Agency nonetheless creates a right to opt out of automated decision-making, the right should advance consumer privacy without unnecessarily restricting businesses and innovation.....	18
III.	Audits Performed by the Agency – Cal. Civ. Code § 1798.185(a)(18).....	23
A.	What should the scope of the Agency’s audit authority be?.....	23
1.	The scope of the Agency’s audit power should be limited to the practices found to be in substantive violation of CPRA through an adjudication arising from a claim brought by the Agency.....	23
2.	Moreover, any required disclosure of information by a business in response to an Agency’s audit should be consistent with and limited to CCPA record-keeping requirements.....	25
B.	What processes should the Agency follow when exercising its audit authority, and what criteria should it use to select businesses to audit? .....	25
1.	CTIA proposes that the Agency establish appropriate procedural protections for audits that protect both subject companies as well as the legitimacy of audit procedures.....	26
2.	The Agency should implement safeguards to protect personal, confidential and proprietary data processed in connection with the Agency’s audit. ....	27
CONCLUSION.....		27

Before the  
**California Privacy Protection Agency**

In the Matter of	)	
	)	
California Privacy Rights Act of 2020	)	Invitation for Preliminary
Rulemaking Process	)	Comments on Proposed Rulemaking
	)	
	)	

**INTRODUCTION**

CTIA<sup>1</sup> appreciates the opportunity to provide these comments in response to the California Privacy Protection Agency (the “Agency’s”) invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (“CPRA”). CTIA understands the demanding statutory deadlines governing this process and commends the efforts of the Agency to proactively seek public input from stakeholders in developing regulations.

We submit that in developing proposed rules, the Agency should focus on clarifying the rights and obligations of CPRA so that businesses, many of which are already working diligently to build CPRA compliance, can drive positive privacy outcomes for consumers, rather than using the rulemaking to expand or create new standards that go beyond the express scope of CPRA or its rulemaking grant. CTIA’s comments address the following topics identified by the Agency as topics for public comment:

- Processing that Presents a Significant Risk to Consumers’ Privacy or Security:  
Cybersecurity Audits and Risk Assessments Performed by the Businesses.<sup>2</sup>

---

<sup>1</sup> CTIA® ([www.ctia.org](http://www.ctia.org)) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association’s members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

<sup>2</sup> Cal. Civ. Code § 1798.185(a)(15).

- Automated Decision-making.<sup>3</sup>
- Audits Performed by the Agency.<sup>4</sup>

---

<sup>3</sup> Cal. Civ. Code § 1798.185(a)(16).

<sup>4</sup> Cal. Civ. Code § 1798.185(a)(18).



***I. Processing that Presents a Significant Risk to Consumers' Privacy or Security:  
Cybersecurity Audits and Risk Assessments Performed by Businesses – Cal. Civ. Code §  
1798.185(a)(15)***

CPRA authorizes the Agency to issue regulations requiring businesses “whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to 1) perform annual cybersecurity audits; and 2) submit to the Agency regular risk assessments regarding their processing of personal information.<sup>5</sup>

As discussed in more detail below, CTIA’s recommendations are as follows:

- The Agency should define “significant risk” narrowly, and identify specific activities that would trigger the obligation to either conduct a cybersecurity audit (if processing presents a specified cybersecurity risk), or a risk assessment (if processing presents a specified privacy risk).
- The Agency should apply a risk-based approach to businesses’ obligation to conduct a cybersecurity audit, and permit businesses to use widely-accepted cybersecurity frameworks and engage independent auditors to conduct their audits. Cybersecurity audits should only be required to address the processing activities that triggered the audit obligation.
- For specified activities that trigger risk assessment obligations, the Agency should require businesses to submit a generalized risk assessment every two to three years. Further, the Agency should implement appropriate safeguards to protect any personal, confidential, or proprietary information contained within, or obtained in connection with, the risk assessment.

---

<sup>5</sup> Cal. Civ. Code § 1798.185(a)(15).

**A. When does a business’s processing of personal information present a “significant risk to consumers’ privacy or security”?**

“Significant risk” should be defined narrowly to focus on substantial and specific risks that would enable meaningful oversight by the Agency. The Agency should require businesses to conduct a cybersecurity audit only when engaging in specific enumerated activities that present a cybersecurity risk, and to conduct a risk assessment only when engaging in specified activities that present a privacy risk.

**1. “Significant risk” should be defined to address substantial, specific, and enumerated risks.**

CTIA acknowledges the important role that the Agency will play in protecting consumers from processing activities that present a significant risk to consumers’ privacy and security. CTIA believes that the Agency’s oversight of cybersecurity audits and risk assessments should result in meaningful protection for consumers.

Thus, we encourage the Agency to define “significant risk” such that it truly captures enumerated processing activities that present specific risks of substantial and identified harm to consumers. This would enable focused assessments and audits that meaningfully increase consumer privacy and security, while also facilitating the Agency’s oversight function. In contrast, an overly broad definition of “significant risk” would end up requiring an incalculable number of businesses – many of which will be small- to medium-sized enterprises located around the world – to swamp the Agency with assessments, including in cases where there may be little to no risk to consumers. It is unclear how this would increase consumer privacy or security protection. Instead, it could potentially frustrate the Agency’s opportunity for meaningful oversight over business activities that have the potential to substantially and adversely impact consumer privacy.

For instance, CPRA requires the Agency to “provide a public report summarizing the risk assessments filed with the Agency.”<sup>6</sup> It would be difficult to conduct this reporting if faced with an avalanche of risk assessments, and Agency resources could be unnecessarily diverted not only from meaningful reporting, but from other oversight tasks as well.

**2. The triggers to conduct a cybersecurity audit or risk assessment should directly align with the cybersecurity or privacy risk creating the obligation.**

CPRA authorizes the Agency to identify activities that create “significant risk to the security of personal information” and thus trigger an obligation to conduct a cybersecurity audit.<sup>7</sup> It also authorizes the Agency to identify processing that creates “risks to privacy of the consumer” and thus triggers an obligation to conduct a “risk assessment.”<sup>8</sup> Accordingly, the “significant risk” that triggers a cybersecurity audit should be a cybersecurity risk, while the “significant risk” that triggers a risk assessment should be a privacy risk. Cybersecurity risks are inherently different in kind than privacy risks, and are identified, classified, and remediated under different frameworks. Organizations follow entirely different processes for auditing cybersecurity than they employ for assessing privacy risks, and often have separate functions devoted to security and privacy. In practical terms, cybersecurity audits can be far more burdensome and expensive for companies than risk assessments, particularly for smaller or medium-sized enterprises. Lastly, from a policy perspective, it would be inconsistent with existing privacy laws to require businesses to conduct a full-fledged cybersecurity audit in response to a ‘pure privacy’ risk, when (as discussed below) neither European nor U.S. state privacy statutes require this.

---

<sup>6</sup> Cal. Civ. Code § 1798.199.40(d).

<sup>7</sup> Cal. Civ. Code § 1798.185(a)(15)(A).

<sup>8</sup> Cal. Civ. Code § 1798.185(a)(15)(B).

CPRA and existing privacy laws already take this privacy/security distinction into account when defining the triggers for privacy assessments versus security audits. For example, CPRA states that the “factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.”<sup>9</sup> In comparison, while the EU’s General Data Protection Regulation (the “GDPR”) requires privacy-side assessments whenever any activity creates a “high risk” to individual privacy in light of “the nature, scope, context and purposes of the processing,”<sup>10</sup> on the security side, the GDPR does not expressly mandate cybersecurity audits. It instead only indicates they should be implemented as part of an organization’s “technical and organizational” security measures if “appropriate” in light of “the costs of implementation,” the “nature, scope, context and purposes of processing,” and “the risk[s] of varying likelihood and severity” for individuals.<sup>11</sup> The Agency should similarly acknowledge the distinction between cybersecurity and privacy risks, and align a business’s obligation to conduct security and privacy assessments with specified security risks for cybersecurity audits, or privacy risks for risk assessments.

**B. What should a business that performs an annual cybersecurity audit be required to do, including what should it cover in its audit and what processes are needed to ensure that its audit is “thorough and independent”?<sup>12</sup>**

Consistent with existing California law, a risk-based standard should be applied to cybersecurity audits. Businesses should be permitted to use well-accepted cybersecurity

---

<sup>9</sup> Cal. Civ. Code § 1798.185(a)(15)(A) (emphasis added).

<sup>10</sup> Art. 35 GDPR.

<sup>11</sup> Art. 32 GDPR.

<sup>12</sup> Cal. Civ. Code § 1798.185(a)(15)(A).



frameworks and engage independent auditors to conduct any CPRA-required cybersecurity audits. Audits should only be required to address the specific activity that triggered the audit obligation.

**1. CPRA standards for cybersecurity audits should be consistent with California’s existing statutory data security requirements.**

CPRA itself requires businesses to implement security that is “in accordance with [Civil Code] Section 1798.81.5,” and which consists of “reasonable procedures and practices appropriate to the nature of the personal information to protect [] personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.”<sup>13</sup> Audit standards should thus orient to a risk-based standard consistent with CPRA and Civil Code Section 1798.81.5, by testing for security that is “reasonable ... and ... appropriate” to the “nature of the personal information” processed by an organization.

**2. The Agency should permit businesses to rely on widely-accepted, rigorous cybersecurity frameworks as a safe harbor to demonstrate compliance with CPRA cybersecurity audit standards.**

To enable “reasonable” and “appropriate” auditing that is “independent and thorough,” CTIA encourages the Agency to permit businesses to use existing, independent, and widely utilized cybersecurity frameworks to conduct CPRA cybersecurity audits. Entire industries already rely on, and businesses regularly conduct audits pursuant to, frameworks such as the International Organization for Standardization (“ISO”) 27000 series certification, the National Institute of Standards and Technology (“NIST”) Cybersecurity Framework, the Payment Card Industry Data Security Standard (“PCI DSS”), and the Service Organization Control (“SOC”) Trust Service Principles. These frameworks embody decades of experience, and are continuously

---

<sup>13</sup> Cal. Civ. Code § 1798.100(e) (requiring businesses to implement reasonable security pursuant to Cal. Civ. Code § 1798.81.5) (emphasis added).

updated to reflect emerging risks and accepted controls. They are well-known, rigorous, and developed by independent, third-party agencies and organizations with expertise in cybersecurity.<sup>14</sup> Additionally, these frameworks are often recognized as industry-standard. Requiring businesses to audit to different standards could impair their ability to meet industry security standards, or their ability to meet security standards they have contractually committed to observe.

Indeed, some states have already enacted statutory safe harbors for companies whose security programs reflect these existing cybersecurity frameworks.<sup>15</sup> We would encourage the Agency to consider similar recognition of these frameworks in the context of CPRA cybersecurity audits. Auditing to ISO, NIST, PCI DSS, SOC, or similar standards should be sufficient to be considered a “reasonable” and “appropriate” approach to security audits under CPRA. Further, these frameworks already set the standard for detail and rigor, and are validated by third-party organizations or – in the case of NIST – by a U.S. federal government agency. They should thus be sufficient to meet CPRA’s requirement for “thorough and independent” audit standards.

### **3. The Agency should permit businesses to leverage existing cybersecurity audit procedures, including appropriately-structured internal audit processes.**

In terms of the process for conducting the audits, we submit the Agency should permit businesses to leverage existing cybersecurity audit procedures to comply with CPRA audit requirements. Many businesses already audit their cybersecurity using reputable independent

---

<sup>14</sup> See, e.g., *The NIST Cybersecurity Framework and the FTC*, Federal Trade Commission: Protecting America’s Consumers, <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc> (last visited Oct. 26, 2021) (“From the perspective of the staff of the Federal Trade Commission, NIST’s Cybersecurity Framework is consistent with the process-based approach that the FTC has followed since the late 1990s, the 60+ law enforcement actions the FTC has brought to date, and the agency’s educational messages to companies....”).

<sup>15</sup> See, e.g., Ohio Rev. Code Ann. §§ 1354.01-05 (providing an affirmative defense against a claim brought under Ohio law or in Ohio state courts and that alleges that the failure to implement reasonable information security controls resulted in a data breach for businesses that create, maintain and comply with a written cybersecurity program that reasonably conforms to an industry recognized cybersecurity framework); Utah Code Ann. §§ 78B-4-701-706 (same).

third-party auditors. This form of auditing is widely recognized as thorough and independent, so much so that it is often a component of enforcement orders that privacy regulators impose on companies.<sup>16</sup>

Additionally, as other California statutes already recognize, CPRA should recognize that audits conducted by a company's employees can also be independent and thorough as long as the company maintains appropriate internal structures around the audit function. For instance, the California Insurance Code permits internal audits, stating that "[t]o ensure that an internal audit remains objective, the internal audit function shall be organizationally independent," and that the "internal audit function shall not defer ultimate judgment on audit matters to others."<sup>17</sup> Permitting internal auditing would offer significant relief to smaller and mid-sized companies.

**4. Cybersecurity audits should only be required to address the specific activity that triggered the audit.**

CTIA encourages the Agency to ensure that CPRA audit regulations stay within the scope of delegated rulemaking. CPRA ties cybersecurity auditing obligations to processing activities that present "significant risk" to consumers' security. Accordingly, any audit obligation should be limited to the specific "significant-risk activity" that has triggered an audit obligation. Otherwise, the Agency would exceed its authority to issue rules that apply to the processing of consumers' personal information in ways that create "significant risk," and risk-assessment rulemaking would go beyond the express grant in CPRA.

**C. What should businesses that submit a risk assessment to the Agency be required to do, including what should they cover in their risk assessment, how often**

---

<sup>16</sup> See, e.g., Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 9, in: *U.S. v. Vivint Smart Home, Inc.*, No. 2:21-cv-00267-TS (N.D. Utah Apr. 29, 2021) (requiring security assessments to be conducted by a "qualified, objective, independent third-party professional").

<sup>17</sup> Cal. Ins. Code §§ 900.3(a) and (c).

**should they submit a risk assessment, and how should they weigh the risks and benefits of processing consumers’ personal information and sensitive personal information?**

Risk assessments submitted to the Agency should only be required to evaluate the specific activity that triggered the risk assessment obligation. Businesses should do this in a generalized and concise fashion to enable effective Agency review, with assessments to be submitted every two or three years. The Agency should implement safeguards to protect the personal, confidential, or proprietary information disclosed in connection with a risk assessment.

**1. The Agency should require a generalized risk assessment that enables meaningful oversight without creating cybersecurity and privacy risks.**

As stated above, CTIA encourages the Agency to structure risk assessment requirements so that they provide increased protection for consumers, while enabling effective oversight by the Agency. To this end, risk assessments that are required to be submitted to the Agency should only have to address activities that could create significant harm to consumers, and should be kept at a reasonably concise level of detail and length. As an example, the Virginia Consumer Data Protection Act requires “data protection assessments” to set forth (i) the benefits of a specific processing activity, and (ii) the potential risks of that processing activity, as mitigated by safeguards.<sup>18</sup> This can be done in a generalized and concise format, without granular detail that potentially includes confidential, proprietary, or protected technology, operations, or personal information.

This approach would serve two purposes recognized within CPRA. First, as discussed above, being inundated by overly detailed risk assessments could impede the Agency’s oversight

---

<sup>18</sup> Va. Code Ann. § 59.1-576.



activities by preventing the Agency from meaningfully assessing submissions. It could also hinder the Agency's development of the reports on risk assessments it is obligated to publish under Civil Code Section 1798.199.40(d). We respectfully submit that the Agency's oversight activities would be better served through receipt of concise, focused risk assessments that facilitate straightforward review. If the Agency deems further detail necessary, it can request that detail from businesses using its more specific authorities under CPRA.<sup>19</sup>

Second, a more generalized approach to risk assessments can help to avoid inadvertently exposing confidential or proprietary information, or creating unnecessary security risks for operations or personal information. CPRA itself contemplates that excessive detail in risk assessments could give rise to these very risks. For instance, CPRA's risk assessment provisions state that "[n]othing in this section shall require a business to divulge trade secrets"<sup>20</sup>, recognizing that details about a business's data processing in a risk assessment may reveal or implicate business operations, strategies, or know-how that is proprietary. CPRA also expressly recognizes that risk assessments could become an inadvertent 'threat vector' for proprietary information by stating that the Agency's public reporting on risk assessments must "ensur[e] that data security is not compromised."<sup>21</sup> CPRA's drafters thus understood that risk assessments could contain confidential, proprietary, or personal information, and that the Agency needed to take care not to expose this information in its public reporting. With that in mind, a more generalized approach to risk assessments – one that would not require businesses to disclose granular detail reflecting proprietary information – would be consistent with these statutory objectives.

---

<sup>19</sup> See, e.g., Cal. Civ. Code §§ 1798.199.45 (permitting the Agency to investigate possible violations of CPRA upon the sworn complaint of any person or on the Agency's own initiative); 1798.199.55 (allowing the Agency to hold a hearing to determine if a violation of CPRA has occurred when the Agency determines there is probably cause its belief). See also, Cal. Civ. Code § 1798.199.40(l) (permitting Agency to perform "acts necessary or appropriate in the exercise of its power, authority, and jurisdiction").

<sup>20</sup> Cal. Civ. Code § 1798.185(a)(15)(B).

<sup>21</sup> Cal. Civ. Code § 1798.199.40(d).

**2. A risk assessment, if required, should only be due every two to three years to avoid unnecessarily imposing burdens on businesses and the Agency.**

For similar reasons, we believe it is not advisable for the Agency to require businesses to submit a risk assessment on an annual basis. From a business perspective, this could be a significant burden without a clear benefit for consumer privacy, particularly if an assessed activity does not significantly change over a twelve-month period. Additionally, reviewing an annual tidal wave of risk assessments could unnecessarily burden the Agency. We believe it will both adequately protect California consumers, and be less burdensome, for both the Agency and for businesses, if businesses are to submit a risk assessment every two to three years on a staggered basis. This will not negatively impact Agency oversight. As indicated above, if the Agency requires further information prior to a business's next risk assessment submission, the Agency can employ its additional inquiry and/or investigative powers under CPRA.

**3. The Agency should implement appropriate safeguards to protect any information obtained in a risk assessment.**

Lastly, we encourage and trust that the Agency will implement safeguards appropriate to protect any personal information, or any confidential or proprietary information, contained or obtained in connection with risk assessments. These could include widely-accepted measures such as retention periods appropriate for security risks associated with storing risk assessments, as well as access controls that reflect the internal functional divisions within the Agency. Additionally, as compelled disclosures to the Agency, it would be appropriate for risk assessments to be exempted from FOIA requests under California law, and for CPRA rules to specify that nothing in or

provided in connection with a risk assessment results in a waiver of any evidentiary or other privilege available to a submitting party, as other U.S. state privacy laws have done.<sup>22</sup>

## ***II. Automated Decision-making – Cal. Civ. Code § 1798.185(a)(16)***

CPRA provides for regulations governing consumers’ “access and opt-out rights with respect to businesses’ use of automated decision-making technology.”<sup>23</sup> As described below, CTIA respectfully submits that the delegation of rulemaking authority to create a novel right to opt out of automated decision-making is unconstitutional because CPRA itself does not enact, create, or provide for such an opt-out right. If, despite this, the Agency nonetheless develops such regulations, it should create an opt-out right narrowly tailored to protect against substantial identified harms to advance consumer privacy and avoid dampening innovation.

### **A. What should be the scope of consumers’ opt-out rights with regard to automated decision-making, and what processes should consumers and businesses follow to facilitate opt outs?**

#### **1. The delegation of rulemaking authority to create a new right to opt out of automated decision-making is unconstitutional.**

CPRA states that the Agency is authorized to issue regulations concerning an “opt-out right[]” with respect to “businesses’ use of automated decision-making technology, including profiling ... .”<sup>24</sup> However, CPRA itself does not enact, create, or provide for such an opt-out right. Any delegation of rulemaking to the Agency to govern an opt-out right that was never enacted by the legislature, or approved by voters, is an unconstitutional delegation of authority.

---

<sup>22</sup> See Colo. Rev. Stat. § 6-1-1309(4) (deeming data protection assessments confidential and exempt from public inspection and copying under the state’s freedom of information act and stating that the disclosure of such assessments pursuant to a request from the state attorney general does not constitute a waiver of any attorney-client privilege or work-product protection that might exist with respect to the assessment and any information contained in the assessment); Va. Code Ann. § 59.1-576(C) (same).

<sup>23</sup> Cal. Civ. Code § 1798.185(a)(16).

<sup>24</sup> Cal. Civ. Code § 1798.185(a)(16).

“[A]n unconstitutional delegation of authority occurs when a legislative body (1) leaves the resolution of fundamental policy issues to others *or* (2) fails to provide adequate direction for the implementation of that policy.”<sup>25</sup> The CPRA Ballot Initiative clearly acknowledges that the ability of consumers to control how their personal information is used is a fundamental policy issue. It expressly states that “[c]onsumers should be entitled to a clear explanation of the uses of their personal information ... and to control ... it, including by allowing consumers to limit businesses’ use of their sensitive personal information ..., [and] to opt-out of the sale and sharing of their personal information ... .”<sup>26</sup> The California legislature and voters addressed this policy issue exclusively by granting consumers the rights to opt out of (i) data sales, (ii) the sharing of personal information, and (iii) certain uses of sensitive personal information. In contrast, neither the legislature nor the voters enacted a right to opt out of automated decision-making in relation to the statutorily-recognized consumer interest in controlling personal information. It would thus be unconstitutional for the Agency to now create that right, even if CPRA purports to grant the Agency the power to do so, as it would “leave a fundamental policy issue to others”. Like the rights to opt out of data sales and the sharing of personal information, and the right to limit uses of sensitive personal information, any new opt-out right, like other fundamental policy issues, must go through a process of enactment by elected officials or by the voters themselves.

Further, even if the California legislature or voters had enacted a new right to opt out of automated decision-making to address a fundamental policy issue – which neither did – rulemaking on this right would remain unconstitutional for the separate reason that CPRA fails to provide the Agency with any meaningful direction to implement the new right to opt out of

---

<sup>25</sup> *Gerawan Farming, Inc. v. Agricultural Labor Relations Bd.*, 405 P.3d 1087, 1100 (Ca. Sup. Ct. 2017) (citing *Carson Mobilehome Park Owners’ Assn. v. City of Carson*, 672 P.2d 1297, 1300 (Ca. Sup. Ct. 1983)).

<sup>26</sup> The CPRA Ballot Initiative, Section 2.H.



automated decision-making.<sup>27</sup> Instead, the Agency must create this opt-out right out of whole cloth. This is in stark contrast to the guidance for creation of other rights, such as the right to opt out of sales or data sharing of personal information, where CPRA provides substantial guidance for developing the opt-out rights by authorizing the Agency to “facilitate and govern the submission of a request by a consumer to opt-out of the sale or sharing of personal information...to ensure that consumers have the ability to exercise their choices without undue burden and to prevent business from engaging in deceptive or harassing conduct ....”<sup>28</sup> CPRA provides no such guidance to implement the right to opt out of automated decision-making.

**2. If the Agency nonetheless creates a right to opt out of automated decision-making, the right should advance consumer privacy without unnecessarily restricting businesses and innovation.**

If the Agency does issue regulations establishing a right to opt out of automated decision-making, CTIA recommends that the right be limited to protecting against substantial and specified harms to consumers, without unnecessarily restricting businesses and dampening the development of automated decision-making technologies that can provide benefits to consumers and businesses alike.

Indeed, automated decision-making has been beneficial in many ways that positively impact consumers. For instance, consumers can now purchase practically any product they want using their mobile phones thanks in significant part to fraud-prevention technology that runs on automated decision engines. Consumers can also apply for and receive a broad range of financial products and services fully online, without needing to go through the burdensome process of physically going to a bank and negotiating with bank staff/loan officers. This has been a broadly

---

<sup>27</sup> See *Gerawan Farming* and *Carson Mobilehome Park Owners*, *supra* note 25.

<sup>28</sup> Cal. Civ. Code § 1798.185(4)(A).

positive outcome for consumers, and it has happened in substantial part due to financial services providers' automating decisions related to core services such as opening accounts, issuing credit cards, and issuing loans.

It bears remembering that the goal of automated decision-making is to *eliminate* the potential biases and inconsistencies that human decisions have traditionally entailed, and thus *improve* outcomes for consumers, businesses, and society. Proper use of automated decision-making technology can also allow businesses to improve business processes, save costs, better allocate resources, and increase productivity. The above benefits are just a few examples of positive consumer outcomes stemming from automated decision technology, and we encourage the Agency not to issue rules that unnecessarily impede technologies that can help create more of these outcomes in the future.

As such, an overly broad right to opt out of *all* automated decisions would be unnecessary to protect privacy interests and would hamper the use and development of automated decision-making, thereby placing at risk the benefits that such processing provides to businesses and consumers. Regulations should take a risk-based approach, focusing on outcomes from automated decisions that have a substantial and potentially adverse impact on individuals. Accordingly, any right to opt out of automated decisions should apply to (i) solely automated decisions that (ii) are based on "profiling," as the term is defined under CPRA, and (iii) result in enumerated legal or similarly significant effects concerning consumers.

First, the right to opt out of automated decision-making should only apply to decisions that are made on a solely automated basis. If the opt-out right is not limited to "solely" automated decisions, it will become overbroad. Rights to opt out of automated decisions are intended to insert a level of human review over what would otherwise be a fully automated decision, thus enabling

the potential for a human corrective action, if needed, as automated decision engines are optimized. However, if consumers can opt out of decisions that involve *any* degree of automated decision-making – even if it is only used to assist a human-made decision – it will be incredibly disruptive to business and also negatively impact consumers. Businesses would need to offer something akin to a “solely manual” decision, *i.e.*, a decision wherein a human decides with no aid from automated processes. This is simply infeasible, and amounts to something akin to a manual, page-by-page review of the consumer’s file to make a decision. This introduces its own risks, such as human error, inconsistency, and inattention, as well as the risks of human-driven unfairness and discrimination that automated decisions are intended to reduce.<sup>29</sup>

While CTIA broadly agrees that automated decisions do not, by themselves, eliminate these potential risks, the proper approach to eliminate such risks is a layer of human review over automated decisions, not an overcorrection “back in time” to a solely human review. This layer of human review, which would be triggered by a consumer’s opt-out request, will provide a safeguard to ensure that the logic of the decision being made is applied consistently and fairly, while still allowing businesses to utilize technology to increase efficiency. It also enables automated decision technology to be improved over time through continuous human oversight, while protecting consumers from adverse impacts in the process.

Second, the opt-out right should be limited to solely automated decisions based on profiling. “Profiling” is a broadly defined term under CPRA that refers to any form of automated processing to evaluate certain personal aspects of an individual and to make predictions about individuals

---

<sup>29</sup> See Larry Long, *How the Right Automation Road Map Helps Overcome Human Error*, Forbes (Nov. 9, 2018), <https://www.forbes.com/sites/forbestechcouncil/2018/11/09/how-the-right-automation-road-map-helps-overcome-human-error/?sh=490e4be3647f> (explaining how automation can help overcome human error and challenges and biases).

based on that processing.<sup>30</sup> Limiting the right to opt out of automated decision-making to decisions based on profiling would create broad protections for consumers and certainty as to the scope of such a right. Without a ‘profiling’ limitation on opt-out rights, the scope of the right would be boundless. Any decision based on software-encoded rules could trigger the right, and this would reach deeply into situations that have no implications for consumer privacy.

As an example, businesses may use automated decision technology to flag in real time when activities associated with user accounts may be suspicious, thus signaling a compromised account that requires a protective response. Permitting opt-outs from these uses of automated decision technology would be devastating to businesses and consumers alike. Consumers would be put at *greater* risk, and businesses would be unable to run core functions demanded by consumers, all without providing any benefit to consumer privacy.

Notably, all other existing U.S. state privacy laws have limited the right to opt out to decision-making based on profiling.<sup>31</sup> Automated decisions based on profiling are more likely to have the kinds of impacts privacy statutes may properly regulate, given that they rely on personal information about a specific consumer and predictions drawn about that consumer to support decisions. We thus encourage the Agency to limit opt-out rights to automated decision-making based on “profiling” as defined under CPRA.

Third, the right to opt out of automated decision-making should only apply to decisions that result in legal or similarly significant effects concerning consumers. Any opt-out right should be

---

<sup>30</sup> Cal. Civ. Code § 1798.140(z) (“profiling” means “any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.”).

<sup>31</sup> Colo. Rev. Stat. § 6-1-1306(a)(a)(I)(C) (providing consumers the right to opt out of *profiling* in furtherance of decisions that produce legal or similar effects concerning a consumer) (emphasis added); Va. Code Ann. § 59.1-573(A)(5) (same).



scoped such that it focuses on specific harms that automated decisions may create for consumers, not the mere use of automated decision technology. An overbroad approach would create an unnecessary burden on businesses and disincentivize the advancement of decisioning technology, without actually furthering consumer privacy interests.

In order to trigger opt-out rights, an automated decision should have a legal or equally substantial effect on the consumer that, if adverse and incorrect, would be recognized as a harm to the consumer. For instance, if a consumer's application for a housing is denied by a platform, the consumer would suffer a substantial harm if unable to ascertain that the application was denied in compliance with applicable law and application policies. Given the importance of the determination, the consumer would likely want, and it is broadly accepted as appropriate, for a human to be involved in the decision-making process. The consumer should have a right to opt out of this decision if it were made solely using automated processing so as to trigger such human review. But by the same token, if a brand uses a prior purchase to infer that a consumer's favorite color is red, so that the brand can offer them goods that come in red, the consumer suffers no significant harm if this decision is incorrect. People incorrectly guess the preferences of their friends, family, and colleagues every day, without anyone feeling harmed in the process. Any opt-out right that would interfere with these types of decisions that do not create consumer harm would fail to protect a consumer privacy interest.

Further, we encourage the Agency to align with Colorado and Virginia by enumerating the specific instances in which a decision is deemed to have a "legal or similarly significant effect[.]".<sup>32</sup>

---

<sup>32</sup> See Colo. Rev. Stat. § 6-1-1306(1)(a)(I)(C) (providing a right to opt out of "profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer"); Va. Code Ann. § 59.1-573(A)(5)(iii) (same); see also GDPR, Art. 22 ("[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"). While we have identified Colorado and Virginia as existing models for an opt-out right, we note for completeness that Colorado's opt-out right may be subject to further refinements in the future. Colorado's Privacy Act has been recognized by Colorado governor Jared Polis as needing revisions to "strike the

We suggest that this be limited to automated decisions that result in the grant or denial of services that other state privacy laws have deemed significant, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, healthcare services or access to basic necessities, such as food and water.<sup>33</sup> California voters have recognized that “[t]o the extent it advances consumer privacy and business compliance, the [California Privacy Rights Act] should be compatible with privacy laws in other jurisdictions.”<sup>34</sup>

### ***III. Audits Performed by the Agency – Cal. Civ. Code § 1798.185(a)(18)***

CPRA gives the Agency the authority to audit businesses’ compliance with the law.<sup>35</sup> CTIA recommends that the Agency’s audit power be triggered by and limited to addressing practices found through an Agency adjudication to constitute a substantive CPRA violation. Also, any recordkeeping requirements imposed on businesses in connection with a CPRA audit should be consistent with CCPA recordkeeping requirements. Further, the Agency should be required to establish appropriate protections to safeguard companies, the legitimacy of the Agency’s audit process, and any information acquired in connection with the audits.

#### **A. What should the scope of the Agency’s audit authority be?<sup>36</sup>**

**1. The scope of the Agency’s audit power should be limited to the practices found to be in substantive violation of CPRA through an adjudication arising from a claim brought by the Agency.**

CPRA tasks the Agency with ensuring that the “rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy, while

---

appropriate balance between consumer protection while not stifling innovation and Colorado’s position as a top state to do business.” SB-21-190 Signing Statement (July 7, 2021).

<sup>33</sup> Va. Code Ann. § 59.1-571.

<sup>34</sup> The CPRA Ballot Initiative, Section 3.C.8.

<sup>35</sup> See Cal. Civ. Code § 1798.199.65.

<sup>36</sup> See Cal. Civ. Code § 1798.185(a)(18).

giving attention to the impact on business and innovation.” The Agency should develop criteria for when and how it is permitted to exercise its audit powers, including defining the scope of its powers. Without an explicit trigger of when the Agency is permitted to conduct an audit, there is a risk that some businesses will be unfairly or disparately targeted, or that audits will lack the appearance of fair and equal treatment. A defined trigger would minimize the appearance of impropriety and protect the legitimacy of the Agency’s authority to enforce compliance with CPRA. And, considering the number of companies around the world that are subject to CPRA, these criteria should also serve the Agency by conserving its resources and applying them to situations that create significant consumer privacy or security risk. A defined trigger would also avoid the Agency using resources to audit businesses that have shown no signs of materially violating CPRA. The Agency’s resources would be better directed towards auditing specific businesses that may potentially pose a significant risk to consumer privacy and cybersecurity interests.

Thus, we submit that the Agency should only be permitted to audit a business when an adjudication arising from a claim brought by the Agency establishes that the business has substantively violated CPRA, and that the scope of the Agency’s audit power should be limited to addressing the substantial violations of CPRA that triggered the Agency’s audit. This places the audit power squarely within the Agency’s privacy-protection mission, enabling it to work with a business to identify policies, practices, and controls needed to remove a CPRA violation and thus protect consumer privacy on a going-forward basis. Any other approach is not consistent with the overall scheme and structure of CPRA, which provide ample authority for inquiries and investigations concerning compliance. It would thus be an unnecessary burden to issue a

regulation allowing the Agency to audit a business in a “free ranging” fashion, without being limited to the specific situation that gave rise to the audit in the first place.

**2. Moreover, any required disclosure of information by a business in response to an Agency’s audit should be consistent with and limited to CCPA record-keeping requirements.**

The existing CCPA regulations require a business to maintain records of CCPA consumer requests and how the business responded to the requests for at least twenty-four months.<sup>37</sup> Likewise, businesses subject to an audit should not be required to produce information beyond the prior two years. The California Attorney General thought that a two-year record-keeping requirement was reasonable for purposes of the CCPA Regulations, and we agree. A regulation that requires businesses subject to an audit to produce information beyond the prior two years would be inconsistent with the CCPA Regulations and could present a security risk to the extent businesses are required to maintain records containing personal information that the businesses no longer need to offer goods and services to consumers.

**B. What processes should the Agency follow when exercising its audit authority, and what criteria should it use to select businesses to audit?**

The Agency should be required, when exercising its audit authority, to establish appropriate procedural safeguards to protect companies and the legitimacy of the auditing process, including permitting businesses to select independent third-party auditors (subject to the Agency’s veto), and proper protections for any data acquired in connection with an Agency’s audit.

---

<sup>37</sup> Cal. Code Regs. tit. 11, § 999.317(b).



**1. CTIA proposes that the Agency establish appropriate procedural protections for audits that protect both subject companies as well as the legitimacy of audit procedures.**

In addition to the substantive protections discussed in Subsection A above, CTIA advances that the Agency’s audit rules should require a majority of Agency members to vote in favor of an audit to determine whether the adjudication revealed violations of CPRA justifying the Agency’s use of its resources to audit the business. This vote should be memorialized in a written resolution that cites the relevant evidence and defines the scope of the audit. The Agency might follow the lead of the Federal Trade Commission and require audits to be performed only in instances wherein an enforcement action against a business revealed significant privacy or security weaknesses.<sup>38</sup>

There can be a conflict of interest created when an Agency is empowered to audit a business’s CRPA compliance, while also being authorized to investigate potential violations, “determine if a [CPRA] violation has occurred,” and issue fines.<sup>39</sup> This could create a range of complex privilege issues for any investigation or enforcement proceedings that would be connected to an audit. One way to address any potential concerns, is to allow businesses to select reputable, independent third-party auditors to conduct the audit. The Agency could have the right to veto an auditor selected by a business, provided that the Agency has legitimate justifications for doing so. This process would avoid the inherent conflict of interest in an agency with investigatory and enforcement powers conducting the audit itself.

---

<sup>38</sup>See, e.g., Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 9, in: *U.S. v. Vivint Smart Home, Inc.*, No. 2:21-cv-00267-TS (N.D. Utah Apr. 29, 2021) (requiring security assessments to be conducted by a “qualified, objective, independent third-party professional”); *Zoom Video Communications, Inc.*, FTC Docket No. C-4731, FTC File No. 192 3167 at 7-8 (Jan. 19, 2021) (decision and order) (same).

<sup>39</sup> Compare Cal. Civ. Code § 1798.199.40 (granting the Agency the power to audit businesses to ensure compliance) with Cal. Civ. Code § 1798.199.45 (granting the Agency the power to investigate possible violations) and § 1798.199.55 (authorizing the Agency to hold a hearing to determine if a violation has occurred and issue a cease and desist order and an administrative fine if a violation has occurred).

**2. The Agency should implement safeguards to protect personal, confidential and proprietary data processed in connection with the Agency's audit.**

We also submit that the regulations should ensure the confidentiality and security of all information disclosed by a business to the Agency in connection with an audit, given the certainty that confidential, proprietary, and personal information will be at stake. Similar to the above discussion regarding risk assessments, audits can create a data security compromise risk by requiring access to personal information, and potentially to IT systems, to be provided to a third party. We trust the Agency will implement robust safeguards for any data acquired in connection with audits.

**CONCLUSION**

CTIA appreciates the Agency's consideration of these comments and stands ready to provide any additional information that would be helpful.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan  
Vice President, State Legislative Affairs

Melanie K. Tiano  
Assistant Vice President, Cybersecurity  
and Privacy

Lisa Volpe McCabe  
Director, State Legislative Affairs

**CTIA**

1400 16th St. NW, Suite 600  
Washington, DC 20036  
(202) 736-3200

November 8, 2021

---

**From:** Thomas Daly [REDACTED]  
**Sent:** 11/8/2021 2:44:45 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Adam Judelson [REDACTED]; Will McKissick [REDACTED]; Nate Munger  
[REDACTED]  
**Subject:** PRO 01-21 – Response to Invitation for Preliminary Comments on Proposed Rule making Under the CPRA on behalf  
of mePism Inc  
**Attachments:** 11-08-21 mePrism Preliminary Comments on Proposed Rulemaking Under CPRA - PRO 01-21 (1).pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Dear California Privacy Protection Agency Board,

Please find attached for your review and consideration preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020 on behalf of mePrism, Inc. pursuant to the invitation for comments dated September 22, 2021.

Kind regards,  
Tom Daly

**Tom Daly**  
Founder and CEO  
mePrism  
[REDACTED]





2011 Palomar Airport Rd Suite 101  
Carlsbad, CA 92011  
Tel: (760) 765-5767

November 8, 2021

**VIA E-MAIL (REGULATIONS@CPPA.CA.GOV)**

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

Re: PRO 01-21 - Response to Invitation for Preliminary Comments on Proposed Rulemaking  
Under the California Privacy Rights Act of 2020

Dear Ms. Castanon:

We would like to thank and congratulate the California Privacy Protection Agency (the "Agency") for its work so far in standing up the new agency and the proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA). On behalf of mePrism, Inc., we would like to respectfully submit these comments on the proposed rulemaking under the CPRA pursuant to the invitation from the Agency on September 22, 2021.

mePrism is an online tool aimed at assisting consumers in taking control of their online data by facilitating the collection of their data from across the web and exercising control over how their data can be used and, if they desire, sold. At mePrism, we believe that a consumer's online data is their own and that consumers have a fundamental right to privacy and the freedom to make choices over their data without hidden influence. In order to help consumers facilitate these rights in a broad fashion, mePrism serves as an authorized agent under the California Consumer Privacy Act of 2018 (CCPA) and the CPRA. As a result, mePrism has a front row seat to how some of the biggest companies in the world are responding to consumer requests submitted by consumers and through lawful, authorized agents. Based on these experiences, mePrism submits these preliminary comments in order to help guide the Agency in the development of new regulations and in updating existing regulations.

**Overview**

The CCPA and CPRA give California consumers several new rights over the information businesses collect and store about them. Specifically, under the law, consumers can tell businesses to stop selling their personal information, to supply the consumer with a copy of their information, correct their information, or, under certain circumstances, delete it all together. The law also permits consumers to ask a third party, or "authorized agent," to help them exercise their rights by contacting businesses on their behalf. Notably, if a consumer wants to fully capitalize on their rights under the CCPA and CPRA, the ability to utilize an authorized agent is incredibly important given the hundreds

(maybe thousands) of companies that may hold data about a single individual. In today's increasingly digital world, it is nearly impossible for an individual to find and contact each company one by one to comprehensively exercise their rights. mePrism is built to address this conundrum in an automated fashion and is intended, with a single integrated platform, to allow consumers to protect their privacy and effectively control their data throughout the online ecosystem. As we have seen over nearly two years, however, exercising rights on behalf of consumers as an authorized agent comes with many distinct challenges exacerbated by businesses that selectively or narrowly interpret the CCPA and end up completely frustrating consumers' choices.

In the preambles, the CPRA sets out that its implementation is guided by several overarching principles, including:

- Consumers should know who is collecting their personal information, how it is being used, and to whom it is disclosed, so that they have the information necessary to exercise meaningful control over businesses' use of their personal information. CPRA, Sec. 3, (A)(1).
- Consumers should have access to their personal information and should be able to correct it, delete it, and take it with them from one business to another. Consumers *or their authorized agents* should be able to exercise these options through easily accessible self-serve tools. CPRA, Sec. 3, (A)(3) & (4) (Emphasis added).
- Businesses should specifically and clearly inform consumers about how they collect and use personal information and how they can exercise their rights and choice. Businesses should provide consumers *or their authorized agents* with easily accessible means to allow consumers and their children to obtain their personal information, to delete it, or correct it, and to opt-out of its sale and the sharing across business platforms, services, businesses and devices, and to limit the use of their sensitive personal information. CPRA, Sec. 3, (B)(1) & (4) (Emphasis added).

Additionally, and importantly, the CPRA anticipates that the law "should enable pro-consumer new products and services and promote efficiency of implementation for business." CPRA, Sec. 3, (C)(5). In order for third party authorized agents (like mePrism, who are developing new products to both facilitate consumer choice and effectuate efficient implementation of the CPRA for businesses) to operate and aid consumers in taking control of their online data, regulations should be adopted with a forward-looking view to help consumers broadly control their data through the use of authorized agents.

We look forward to draft regulations that will help bring a measure of clarity and practical guidance to businesses working with consumers and their designated authorized agents to facilitate their rights under the CPRA. To that end, we submit the following recommendations:

### **Audits Performed by the Agency (Public Comment Topic #3)**

When a consumer makes a request to access or delete information, the consumer has no way to determine whether the business has fully complied with the request. In this regard, we suggest two approaches:

First, we note the Agency has the authority to audit a business's compliance with the CPRA. This audit authority can serve as a valuable tool to ensure compliance. In selecting businesses for audit, we suggest the Agency randomly select businesses based on complaints received from consumers. Selecting businesses randomly based on complaints received allows for efficient use of the Agency's auditing authority, especially when funding is limited. It would also protect consumers'

personal information from disclosure to an auditor as those consumers making the complaint can elect to share their personal information with the auditor for purposes of investigating the complaint. In conducting the audit, those businesses selected should be required to provide access to its internal IT systems such that the business's response can be compared against the actual data maintained on the consumer that is subject to the law. Such an approach would also allow the Agency, using its audit authority, to confirm and ensure businesses are fully complying with their obligations under the law.

Additionally, consumers have the right to request deletion of their information, correct their information, and to opt-out of the sale and sharing of their information. The law, however, only provides for consumers to request their data but two times in a year. Should a consumer seek to confirm if a business has complied with their request to delete or correct their data, the consumer would potentially be required to use up those two requests to know. To the extent consumers are afforded more than two opportunities to correct information pursuant to the law, it may be necessary for consumers to have more than two chances to request the business provide them with a copy of their data to confirm correction or deletion. Further, if the consumer has already made two requests within a year (e.g., in order to confirm correction) and the consumer later seeks to port their data to another business, the consumer may be denied the opportunity to obtain a copy of their data to port simply because they already utilized their two requests. This would be fundamentally unfair for the consumer and does not comport with the spirit of the CPRA. As such, we suggest regulations be drafted that exempt requests to know when they follow (e.g. within 45 days) a consumer request to correct, delete, or opt-out. Such an exemption would allow the consumer to conduct their own "audit" to ensure a business's compliance with the law.

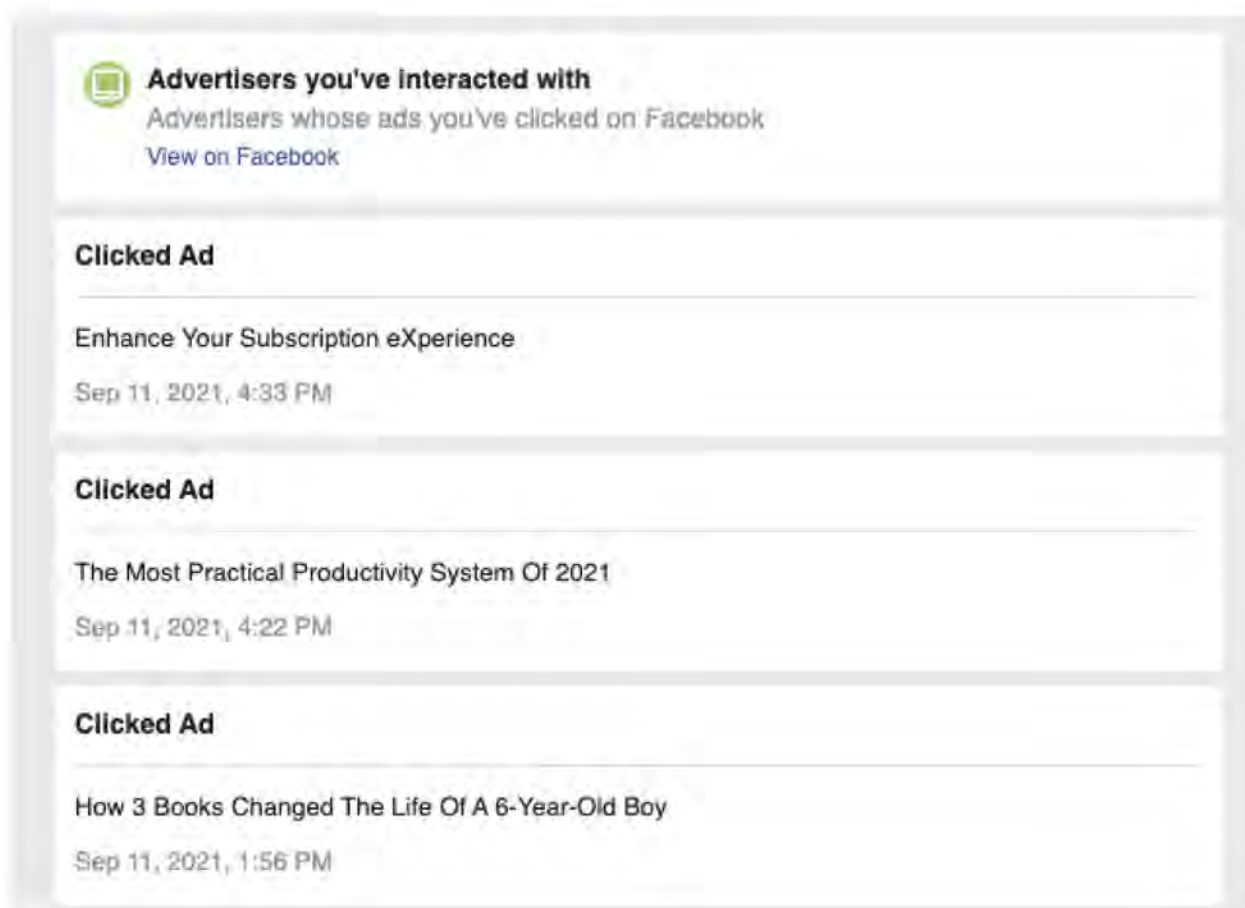
#### **Definitions and Categories (Public Comment Topic #8 h)**

The CPRA requires businesses to disclose the "specific pieces" of personal information the business has collected about a consumer pursuant to a verified consumer request. CPRA Sec. 1798.110(a)(5) & (b). As evidenced by actual examples set out below, in practice, some of the largest businesses in the world respond to verified requests to know by providing wholly inadequate or incomplete responses that are not understandable or useable to the average consumer. **The regulations adopted by the Agency should clarify that businesses are expected to respond in such a manner that will allow consumers to understand and use the information received from the business.** This, after all, is the very essence of the CPRA.

On behalf of consumers as an authorized agent, mePrism has made requests and experienced:

- **Facebook**, in response to requests to know and access information, will provide information on advertisements shown to a particular consumer. The information shared with the consumer, however, only provides the text of the advertisement shown or clicked. Facebook does not provide information on the advertiser (i.e., who purchased the advertisement) in a way that can be linked to the text of the advertisement shown to the consumer. Online advertisements are tailored to consumers based on their digital footprint. As such, access to the information that facilitates a consumer's understanding of who is targeting them for delivery of advertisements is just as important as understanding what data is collected about them. The CPRA is a tool that empowers consumers to understand how and why their information is being used, including being used to target, discriminate, or make decisions about them. Indeed, the CPRA requires businesses to disclose the categories of third parties to whom the business discloses the consumer's personal information. CPRA Sec. 1798.130 (a)(3)(B)(ii). Businesses such as Facebook, however, are preventing consumers from fully utilizing the CPRA as a tool by

failing to provide access to the most valuable information they maintain on the consumer. The screenshot below shows the information Facebook makes available to consumers about advertisements the consumer has interacted with on the platform. Notably absent is any information related to the purchaser of the advertisement.



The screenshot displays a section titled "Advertisers you've interacted with" with a sub-header "Advertisers whose ads you've clicked on Facebook" and a link "View on Facebook". Below this, three individual ad entries are listed, each with a "Clicked Ad" header. The first ad is for "Enhance Your Subscription eXperience" with a timestamp of "Sep 11, 2021, 4:33 PM". The second ad is for "The Most Practical Productivity System Of 2021" with a timestamp of "Sep 11, 2021, 4:22 PM". The third ad is for "How 3 Books Changed The Life Of A 6-Year-Old Boy" with a timestamp of "Sep 11, 2021, 1:56 PM".

**Advertisers you've interacted with**  
Advertisers whose ads you've clicked on Facebook  
[View on Facebook](#)

---

**Clicked Ad**

---

Enhance Your Subscription eXperience  
Sep 11, 2021, 4:33 PM

---

**Clicked Ad**

---

The Most Practical Productivity System Of 2021  
Sep 11, 2021, 4:22 PM

---

**Clicked Ad**

---

How 3 Books Changed The Life Of A 6-Year-Old Boy  
Sep 11, 2021, 1:56 PM

- **Facebook** also provides information to consumers about activity and visits it tracks off of Facebook. The information provided, however, is limited to the name of the third party business and an assigned ID number. No further information is provided, which means the consumer is provided with meaningless information. This response does not comply with the requirement to disclose the specific pieces of personal information collected as the information provided, without context, is meaningless to the consumer. The screenshot below is an example of such a situation with the ID information redacted to protect the identity of the consumer.





### Your Off-Facebook Activity

Your activity from the businesses and organizations you visit off of Facebook

#### Activity received from mercurynews.com

ID	XXXXXXXXXXXXXXXXXX
Event	PAGE_VIEW
Received on	September 13, 2021 at 11:31 AM
ID	XXXXXXXXXXXXXXXXXX
Event	PAGE_VIEW
Received on	September 13, 2021 at 11:31 AM

- **Spotify** responds to requests to know by providing consumers with a file called “Marquee.json” with an attribute called “MarqueeReachableAudience.” There is no further information about the about the file or the information contained therein. As with the Facebook example above, without context, the information provided to the consumer is meaningless.

```
1  {
2    "marqueeReachableAudience": [
3      "Lady Gaga"
4    ]
5  }
```

The above examples are just a small sample of the types of responses received from covered businesses that show how businesses are circumventing the rights of the consumers and the spirit of the law by providing responses that are not complete, difficult to understand, or completely meaningless. The CPRA requires businesses respond to a request to know specific pieces of information by providing the information in a “format that is easily understandable to the average consumer.” CPRA Sec. 1798.130 (a)(3)(B)(iii). Providing responses to requests to know with information that is not understandable to anyone but the business or that does not allow the consumer to easily use the information downstream with another product or service does not comply with the law or discharge the business’s obligations under the law.

The CPRA also requires businesses respond to a request to know specific pieces of information by providing the information, “to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer’s request without hindrance.” *Id.* By way of brief example, Twitter responds to requests to know by providing data in the form of a JavaScript website. While this format can be useful in some instances to consumers in that it is easy to read, it is not a format that allows for easy downstream use “without hinderance” with other digital services or products.

**Regulations should be drafted that require businesses provide data in machine-readable and transmittable formats, e.g., JSON, XML, or via application programming interfaces (APIs), at the consumer’s option.** Such common, readily useable formats would facilitate the consumer’s use of the data received from the business with other digital products and services.<sup>1</sup> Indeed, the businesses that collect the largest amount of consumer data, e.g., Google and Facebook, already have APIs developed and in use that allow for secure, easy exchanges of data. Regulations that would require those businesses to utilize existing APIs to share information collected with consumers (or their authorized agents) at the consumer’s option would allow easy use and transmission of the information to other downstream digital products and services and fulfill the purpose behind giving consumers rights over their data.<sup>2</sup>

**Regulations should also be drafted requiring businesses to meet minimum standard practices already in place for sharing digital information when responding to requests.** In practice, when companies share digital information, they typically abide by common, expected courtesies such as explaining the contents of large file exports. This is usually done by providing descriptions of how to read or navigate the information within the file. This is a standard practice commonly used in large data transfers. In interacting with third party authorized agents on behalf of consumers, the regulations should encourage businesses to engage in an interactive process with the authorized agent to facilitate file transfers or have a designated way for authorized agents to redress issues of file transfer protocols. Unlike many consumers, third party authorized agents like mePrism are experts at “speaking the language” and can serve as a tool to help consumers quickly and efficiently access, manage and control their data. The processes to facilitate those conversations between authorized agents and businesses, however, does not exist and as a result, consumers are unable to exercise their rights under the law through the use of third party agents. As such, regulations should be adopted that encourage businesses to cooperate with third party agents and at a minimum, provide responses to requests that explain the contents of large file exports so that the information can be utilized by another entity without hinderance.

Further, when the business refuses to cooperate with the consumer or the authorized agent, consumers should have a mechanism to request redress for inadequate responses through the Agency. We are aware that the California Attorney General currently has a mechanism in place to report CCPA consumer complaints: <https://oag.ca.gov/contact/consumer-complaint-against-business-or-company>. To the extent the Agency enforces the CPRA either alongside the California AG

---

<sup>1</sup> For example, a consumer could choose to share their Amazon purchasing history with Nordstrom to receive improved recommendations.

<sup>2</sup> Again, this is particularly true in the case where a business is interacting with third party authorized agents. Currently, there is no transparent process or standard around third party authorized agents requesting or receiving API access to consumer data. Notably, businesses, such as Google and Facebook, allow consumers to export their information to other products and services such as Dropbox or Microsoft OneDrive via an API. However, there is no way for third party authorized agents to request similar API access. Where API access is already in use, regulations should specify that businesses must be required to provide such access when requested by a consumer or their authorized agent. This would facilitate the consumer’s use of third party authorized agents in an efficient and fair manner.

or on its own, a similar mechanism should be adopted by the Agency. We further suggest that consumer complaints be made public (with identifying information appropriately redacted) to further incentivize businesses to address and resolve the complaints, potentially without the need for intervention by the Agency or the California AG. Businesses should also be given an opportunity to respond publicly and where the Agency or the California AG does intervene to resolve a dispute, the final rulings or resolutions can also be made public. Making the complaints, responses, and rulings public will encourage self-compliance with the CPRA and also serve to provide guidance to other businesses in implementing their own compliance plans.

#### **Additional Comments (Public Comment Topic #9)**

##### *Resolving Identity Verification Issues*

The CPRA is clear that consumers can utilize authorized agents to help them exercise their rights under the law. Some businesses, however, have thwarted this part of the law by making it *impossible* for consumers to make a request through an authorized agent. By way of specific example, when some Facebook users attempt to log into their account by way of an authorized agent to make a request to access information, the authorized agent is met with an error advising they are not permitted to log in due to security restrictions. The authorized agent, however, has no alternate method to provide positive identity verification on behalf of the consumer, *thus effectively making it impossible for many consumers to exercise their rights through an authorized agent*. Again, this is an issue due to the fact that Facebook (and other businesses) do not have a way to engage in an interactive process with the authorized agent to otherwise request access to the information via other methods, including programmatic methods like APIs, regularly used by the business to transfer data.

In another example, a prominent data broker *permits consumers to purchase their own data (and the data of other consumers) from the business*, but when a request is made pursuant to the CCPA, the data broker responds that they have no way of verifying the person's identity without asking for several more pieces of personal information, ostensibly to confirm the person's identity. This approach acts as an effective deterrent to consumers seeking to know what data businesses hold on them. The consumer must now decide whether to potentially provide *more* information to a data broker in order to obtain a copy of their data or request deletion.

**To address these issues, regulations should be adopted to encourage covered businesses to use or adopt an identity management solution.** Alternatively, where the business provides its own identity management solution, then that system must be made available and considered sufficient validation for an authorized agent to use and validate the identity of a user.

Notably, this is not the first time businesses have had to grapple with identity verification issues when a consumer requests access to their information for their own use and for use with downstream digital products and services. Indeed, the financial services sector previously faced a similar situation and successfully met the needs of consumers requesting access to information and the banks' need for security by developing standards and reaching agreement around identity verification, API access, and security. This resulted in adoption of common interoperability standards through the Financial Data Exchange (FDX) and the emergence of powerful platforms such as Mint (acquired by Intuit), Plaid, and Akoya, each of which has fueled the creation of more businesses that improve the consumer's experience and unlock new market efficiencies that have grown the economy. The emergence of these data sharing and aggregation tools allow consumers to move their financial data securely between platforms, aggregate their financial data from different service providers in a usable ways, and improve the security of data transfer across the entirety of the financial services ecosystem by utilizing agreed-upon identity management and verification solutions. These are the very issues faced by CCPA- and CPRA-covered businesses that are now trying to implement the new

rights granted to consumers under the law. We encourage the Agency to look to the financial services sector to adopt regulations that will encourage the same type of secure sharing solutions.

Moreover, the California AG has already set precedent that technical specifications and new products developed in response to the CCPA and intended to enhance consumer privacy rights can be mandated for adoption by covered businesses. See *Office of the Attorney General of California, Frequently Asked Questions (FAQs): What is the GPC?*, <https://oag.ca.gov/privacy/ccpa> (stating covered businesses must honor the Global Privacy Control). As California is a thought leader in privacy and enhancing the consumer experience, the adoption of standards or frameworks around identity verification and management is of paramount importance to resolve the issues for consumers attempting to achieve control over their data through the use of new products and third party services. Indeed, adopting identity validation protocols will facilitate consumer rights under the law and also simultaneously ease the burden on businesses by removing the (substantial compliance) concern of identity verification. As such, we suggest adopting regulations that will help guide or formulate standards around identity verification management.

#### *Clarification of “Sale” Under the CPRA*

In the California AG’s prior promulgation of regulations, it declined to provide guidance as to what constitutes a “sale” under the CCPA. The California AG commented that it prioritized drafting regulations that operationalize and assist in the immediate implementation of the law due to the time constraints and efforts to meet the July 1, 2020 deadline set by the CCPA. See *Office of the Attorney General of California, Final Statement of Reasons, Appendix A: Summary and Response to Comments Submitted During 45-Day Period, Comment #43*, <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf>.

With the anticipated effective date for the CPRA in 2023, the Agency should take this opportunity to provide guidance as to what constitutes a “sale” under the CPRA. Businesses have taken very diverse approaches to whether conduct constitutes a “sale” under the CCPA. This includes businesses in the digital advertising industry, where there appears to be a lack of consensus of whether digital advertising is a “sale.” Some digital advertising businesses have declared that they believe their receipt of consumer data falls within the “service provider” exception and is therefore not a “sale” (despite that the parties in those relationships often use the personal information received for their own purposes) to other digital advertising businesses acknowledging sales and adhering to ad industry frameworks. Other businesses have implicitly acknowledged “sales” by offering new services that purport to avoid activities constituting a “sale.” Given the widely different approaches by businesses as to what constitutes a “sale,” it is clear more guidance is needed for businesses, particularly those in the digital advertising industry, to determine when certain conduct constitutes a “sale.”

[Intentionally left blank]



## **Conclusion**

mePrism appreciates the Agency's work on new regulations for the CPRA and appreciates the opportunity to provide comments at this preliminary stage. We urge the Agency to adopt rules that will provide clear guidance to businesses for implementing the many consumer-protective aspects of the CPRA, including those that can clarify the role and expectations around authorized agents acting on behalf of consumers to exercise rights.

If we can answer any questions or provide any further resources, please feel free to contact us at any time.

Very truly yours,

Tom Daly  
Founder CEO  
mePrism, Inc.

---

**From:** David LeDuc ([REDACTED])  
**Sent:** 11/8/2021 2:47:54 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Fatiha Tabibpour ([REDACTED])  
**Subject:** PRO 01-21 -- Comments from the Network Advertising Initiative  
**Attachments:** PastedGraphic-2.tiff; CPRA Preliminary Comments\_NAI\_8Nov2021.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Dear California Privacy Protection Agency,

Thank you for the opportunity to provide preliminary comments on proposed rulemaking under the California Privacy Rights Act ("CPRA"). Please find the enclosed comments from the Network Advertising Initiative (NAI). If we can provide any additional information, or otherwise assist your office as it engages in the rulemaking process, please do not hesitate to contact Leigh Freund, President & CEO ([REDACTED]) or myself, David LeDuc, Vice President, Public Policy ([REDACTED]).

Best regards,

David LeDuc

David LeDuc  
Vice President, Public Policy  
Network Advertising Initiative  
409 7th Street, NW, Suite 250  
Washington, DC 20004  
[REDACTED]



November 8, 2021

Attn: Debra Castanon  
California Privacy Protection Agency  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

Dear California Privacy Protection Agency,

On behalf of the Network Advertising Initiative (“NAI”), thank you for the opportunity to provide preliminary comments on proposed rulemaking under the California Privacy Rights Act (“CPRA”).

### **Overview of the NAI**

Founded in 2000, the NAI is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising in multiple media, including web, mobile, and TV.

All NAI members are required to adhere to the NAI’s FIPPs-based,<sup>1</sup> privacy-protective Code of Conduct (the “NAI Code”), which continues to evolve and recently underwent a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy.<sup>2</sup> Member compliance with the NAI Code is promoted by a strong accountability program. It includes a comprehensive annual review by the NAI staff of each member company’s adherence to the NAI Code, advising companies about how to best comply with the Code and guidance and implement privacy-first practices, penalties for material violations, and potential referral to the Federal Trade Commission (FTC). Annual reviews cover member companies’ business models, privacy policies and practices, and consumer-choice mechanisms.

Several key features of the NAI Code align closely with the underlying goals and principles of the CPRA. For example, the NAI Code requires members to provide consumers with an easy-to-use mechanism to opt out of different kinds of Tailored Advertising,<sup>3</sup> and requires members to disclose to consumers the

---

<sup>1</sup> See FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

<sup>2</sup> See NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter NAI CODE OF CONDUCT], [https://www.networkadvertising.org/sites/default/files/nai\\_code2020.pdf](https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf).

<sup>3</sup> See, e.g., *id.* § II.C.1.a. The NAI Code of Conduct defines Tailored Advertising as “the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device. Tailored Advertising includes Interest-Based Advertising, Cross-App Advertising, Audience-Matched Advertising, Viewed Content Advertising, and Retargeting. Tailored Advertising does not include Ad Delivery and

kinds of information they collect for Tailored Advertising, and how such information is used.<sup>4</sup> The NAI Code's strong privacy protections also go further than the CPRA in some respects. For example, the NAI Code includes outright prohibitions against the secondary use of information collected for Tailored Advertising for certain eligibility purposes, such as credit or insurance eligibility, regardless of whether such information is ever sold, and even when a consumer has not opted out of Tailored Advertising.<sup>5</sup>

**I. Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses**

The NAI supports the requirement for businesses that process personal information to conduct regular cybersecurity audits and data risk assessments. These risk assessments are also required by new privacy laws in Virginia and Colorado—referred to as Data Protection Assessments (“DPAs”)—and are essential for responsible data processing that minimizes risk posed by the collection and processing of personal information.

The NAI's long-standing Code and self-regulatory program predate both these legal requirements and those established in Europe under Article 35 of the European General Data Protection Regulation (“GDPR”). The Code is in essence a program to identify and minimize privacy risks surrounding the collection and use of consumer data for digital advertising purposes. The NAI's compliance team actively works with companies to assess practices, and as these practices evolve and new privacy risks are identified, we regularly update our Code and associated guidance documents, raising the bar to ensure that NAI members are upholding the highest standards among industry.<sup>6</sup> In response to the new state law legal requirements for risk assessments around various types of data and practices, the NAI has begun a process of mapping the requirements to digital advertising practices, with the goal to help companies tailor their own assessments building from core NAI compliance requirements as the foundation.

New requirements for risk assessments will ultimately help level the playing field, extending privacy risk mitigation practices to the entire digital advertising ecosystem, rather than just companies who voluntarily comply with enhanced NAI requirements. However, a set of disparate requirements across multiple states threatens to create an environment where businesses are overwhelmed in their efforts to comply, with no discernable privacy benefit to consumers. The CPRA generally recognizes this by directing the California Privacy Protection Agency (“Agency”) to cooperate with other states and countries “to ensure consistent application of privacy protections.”<sup>7</sup>

Therefore, the NAI urges the Agency to develop and implement regulations that seek to harmonize to the greatest extent possible with the other state laws. We also offer the following recommendations regarding data risk assessments and cybersecurity audits.

---

Reporting, including frequency capping or sequencing of advertising creatives.” *Id.* § I.Q. Capitalized terms used but not defined herein have the meanings assigned to them by the NAI Code of Conduct. *See generally id.* § I.

<sup>4</sup> *Id.* § II.B.

<sup>5</sup> *Id.* § II.D.2.

<sup>6</sup> *See* NETWORK ADVERTISING INITIATIVE, 2020 ANNUAL REPORT (2020), [https://www.networkadvertising.org/sites/default/files/nai\\_annualreport-20\\_nolivetype\\_final.pdf](https://www.networkadvertising.org/sites/default/files/nai_annualreport-20_nolivetype_final.pdf); NETWORK ADVERTISING INITIATIVE, 2019 ANNUAL REPORT (2019), [https://www.networkadvertising.org/sites/default/files/nai\\_annualreport\\_19\\_no-live\\_type\\_final.pdf](https://www.networkadvertising.org/sites/default/files/nai_annualreport_19_no-live_type_final.pdf).

<sup>7</sup> *See* CAL. CIV. CODE § 1798.199.40(j).



## **Data Risk Assessments**

First, in seeking to harmonize risk assessment requirements with other state laws, the Agency should identify a consistent set of criteria for assessments to provide for the performance of a single assessment by businesses. The Agency should maintain a clear emphasis on processing that presents a heightened risk of harm to consumers. The new laws in Colorado and Virginia are largely consistent in their identification of activities requiring the performance of a risk assessment, so aligning with these two laws would not only be a practical step, but also a relatively efficient process. Similarly, Europe's GDPR requires the performance of data protection impact assessments (DPIAs) for data processing that "is likely to result in a high risk to the rights and freedoms of natural persons."<sup>8</sup> The law sets out three categories in which DPIAs are always required: systematic and extensive profiling with significant effects, processing of sensitive data on a large scale, and systematic monitoring of public areas on a large scale.<sup>9</sup>

Second, while the CPRA makes references to submission of risk assessments on a regular basis, the NAI recommends that the Agency clarify the requirement for performance of annual risk assessments, and allow the Agency to request risk assessments when they are relevant to an investigation or inquiry. This approach would conform with Virginia's privacy law, which provides for submission to the Attorney General upon request when there is an ongoing investigation of a business, and the assessment is relevant to that investigation.<sup>10</sup> This is also consistent with the approach taken under the GDPR, where businesses are required to conduct data impact assessments and to make these records available to a European data protection authority in the event of an audit or investigation arising from the controller's use of the data.<sup>11</sup> Importantly, it helps the Agency balance its resources more effectively by not creating an unnecessary overburden through an automatic production without cause.

Third, while the CPRA appropriately requires businesses to conduct risk assessments only after the law comes into effect on July 1, 2023, the Act does not explicitly clarify that data in a businesses' possession *prior* to the effective date would also not be subject to risk assessments moving forward. We therefore ask that the CPRA regulations clarify by adopting language consistent with the Colorado Privacy Act ("CPA"), which explicitly clarifies the application of the requirement to personal data that a business "*acquired on or after*" the CPA's effective date.<sup>12</sup> This approach is clear and efficient, providing

---

<sup>8</sup> "Art. 35 GDPR - Data Protection Impact Assessment." GDPR.eu, 23 July 2020, <https://gdpr.eu/article-35-impact-assessment/>.

<sup>9</sup> "When Is a Data Protection Impact Assessment (DPIA) Required?" European Commission - European Commission, 18 Dec. 2019, [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en).

<sup>10</sup> See VA. CODE ANN. § 59.1-576 (2021). "The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-574." *Id.*

<sup>11</sup> GOV'T OF IR., GUIDANCE NOTE: GUIDE TO DATA PROTECTION IMPACT ASSESSMENTS (DPIAs) (2019), [https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29\\_Oct19\\_0.pdf](https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf) at 17.

<sup>12</sup> COLO. REV. STAT. § 6-1-1309 (2021).

businesses the opportunity to establish forward-looking assessments and have greater confidence in their compliance efforts.

Finally, the assessments should be confidential, and the rules should recognize that privileged information or trade secrets will be redacted. This presents a practical approach to help companies maintain confidentiality of business practices.

### ***Cybersecurity Audits***

The CPRA implementing regulations should clarify that businesses are required to conduct cybersecurity audits on an annual basis, and they should establish clear requirements for retention of audit records. The requirement for cybersecurity audits should maintain a risk-based approach, where businesses can certify that they have implemented and adhere to policies and procedures designed to identify types of personal information and processing practices that present the greatest risk for the consumer's privacy or security. It should be a priority for the Agency to maintain consistency with existing security requirements and practices in California law,<sup>13</sup> as well as those promoted by the FTC, and requirements recently enacted in other state privacy laws.

The NAI recommends that the regulations align with current California law, enabling business to utilize existing certifications, such as the ISO 27000 series certification and those that leverage the NIST Cybersecurity Framework. Companies should retain the ability to develop and conduct their own internal cybersecurity program and engage third-party auditors. The Agency can also look to the programs established in cases where audits are required pursuant to consent decrees established by the FTC. Finally, businesses should retain the ability to either select independent third-party auditors of their choice in accordance with a set of qualifications established by the Agency or to conduct internal audits provided there are policies and other safeguards in place to ensure independence. On the latter point, California law already contemplates the ability of companies to conduct independent yet internal audits in the insurance context.<sup>14</sup>

## **II. Audits Performed by the Agency**

The CPRA grants audit authority to the Agency, but it does not provide significant direction regarding the performance of audits. The NAI encourages the Agency to develop implementing regulations that provide an audit performed by the Agency must be triggered by evidence that a business has violated substantive provisions of the CPRA, creating either harm or a substantial risk of harm to consumers. The Agency should also confirm that its audit authority is separate and distinct from its enforcement authority for CPRA enforcement actions. Finally, the regulations should also require a majority of Agency members to vote in favor of an audit and to issue a resolution that cites the relevant evidence and defines the scope of the audit. The scope should be limited to addressing practices directly related to the misuse of personal information that necessitated the audit. Alternatively, the Agency might follow the lead of the Federal Trade Commission and require audits to be performed after an enforcement action against a business has been completed. The NAI urges the Agency to ensure that any audits required under the law are protected by strict confidentiality provisions that prevent disclosure to or use by third parties.

---

<sup>13</sup> See CAL. CIV. CODE § 1798.81.5 (2021).

<sup>14</sup> See CAL. INS. CODE § 900.3 (2021).

### **III. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information**

The NAI has a long history of promoting consumers' ability to exercise choice over uses of their data for digital advertising. Enabling consumers to express their preferences and exercise control through easy-to-use choice mechanisms is a foundational element of tailored advertising that we have championed for decades.

In crafting the provision regarding opt-out preference signals, the authors of the CPRA provided explicitly the option for businesses to have a choice whether to honor these signals, or to instead offer consumers the ability to opt-out through a link on their website or digital property.<sup>15</sup> In the case of relying on links to opt out, consumers determine on a case-by-case basis which businesses they will allow to sell or share their personal information. In the case of opt-out preference signals, users can set their preference to be applied across all businesses they interact with, for instance through a browser signal transmitting a consumer's preference across all websites that they don't want their personal information to be shared or sold.

Despite this flexibility created by the CPRA, we expect that many companies will elect to honor both approaches to maximize consumer choices about their data, and to minimize confusion for consumers who elect to activate opt-out preference signals. However, if technology companies who serve as intermediaries through which consumers access internet-based products and services seek to make decisions about selling and sharing personal information on behalf of consumers by using default-on settings, businesses will doubt the integrity of these signals as an expression of a genuine consumer choice. The regulations can play a valuable role in encouraging businesses to honor opt-out preference signals by ensuring that they reflect actual consumer choices.

To that end, the CPRA places specific parameters around the Agency's promulgation of such rules. Namely, the opt-out signal or mechanism must "ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal **cannot unfairly disadvantage another business.**"<sup>16</sup> According to the CPRA, the Agency must also ensure such opt-out preference signals or controls "clearly represent a consumer's intent and [are] **free of defaults constraining or presupposing such intent.**"<sup>17</sup>

We urge the Agency to develop regulations that reflect these important priorities established by the CPRA to ensure consumer choices are genuine, that opt-out preference signal regulations do not favor certain businesses over others, remove businesses' ability to communicate the consequences of opt out choices to consumers, or stand in the way of true and informed consumer choices. Also, the regulations should recognize that in many cases, an opt-out preference signal should only apply to a specific

---

<sup>15</sup> According to the CPRA, businesses "**may elect**" to either "(a)... [p]rovide a clear and conspicuous link on the business's internet homepage(s) titled 'Do Not Sell or Share My Personal Information'" **or** (b) allow consumers to "opt-out of the sale or sharing of their personal information... through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]" The CPRA makes this business choice explicitly clear by stating: "**A business that complies with subdivision (a) of this Section is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or (b).**" *Id.* § 1798.135(a)-(b) (emphasis added).

<sup>16</sup> *Id.* at § 1798.185(19)(A)(i) (emphasis added).

<sup>17</sup> *Id.* at § 1798.185(19)(A)(iii) (emphasis added).

browser, device or platform from which the signal is sent. This would be applicable in cases where the entity sending the signal is not known by the business receiving the signal, rather only a pseudonymous identifier is used by the business to identify a consumer, and the business does not take steps to associate that identifier with the specific consumer. Finally, the regulations should recognize that opt-out preference signals will in some cases present conflicting preferences by a consumer who has otherwise agreed to the business selling or sharing their data, and they should provide guidance that retains flexibility for businesses to resolve these discrepancies.

#### **IV. Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information**

For many years, the NAI has set the highest industry standard for defining sensitive data categories, and for requiring opt-in consent for the use of such data for advertising and marketing purposes. For instance, our definition has long included mental health and sexual orientation, even before European policymakers adopted a broad definition of sensitive personal information--referred to as special category data--under the GDPR. We recently further expanded the scope of sensitive data with the adoption of our 2020 Code of Conduct to also include new types of data that are increasingly being collected through mobile phones and connected devices, such as sensor data, and personal directory data that consumers enter or compile on their own devices. For all of this data, NAI member companies and their partners are required to obtain opt-in consent with clear and conspicuous notice about the sharing and use of this data for advertising and marketing purposes.

While the NAI definition of sensitive data closely aligns with the definition established by the CPRA, there are some categories of data where we diverge, notably regarding the inclusion of data that reveals a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership. We recognize and agree that many consumers have increased sensitivity around these data types, and that they present an increased likelihood of leading to disparate outcomes, particularly when processed for eligibility determinations. For that reason, the NAI prohibits the use of any data collected for advertising and marketing to be used for eligibility determinations. This approach preserves the ability of companies to tailor advertising based on these categories, but it mitigates the potential for harmful outcomes through these practices.

Indeed, there are many cases where these data types are utilized to reach at-risk communities and promote products and services that are beneficial to these populations. Most recently, tailored advertising was effectively deployed by health organizations to reach at-risk populations and educate them about the value of COVID vaccines.<sup>18</sup> Advertising for educational institutions and services is another key area where identification of these data types can have beneficial outcomes, such as promoting racial or ethnic diversity.

The NAI strongly shares the objectives of the CPRA to increase consumers' control over the use of their sensitive data, and more importantly to mitigate harmful outcomes around the processing of these data types. However, we encourage the Agency to also be mindful of the beneficial uses of this data, and to craft rules that do not unnecessarily limit opportunities presented by tailored advertising. As currently drafted, the CPRA definition of sensitive personal information is unclear as to the application of inferences. The NAI believes that this category should include data which is used to make such specific

---

<sup>18</sup> Dan Diamond, *It's Up to You: Ad Campaign to Encourage Coronavirus Vaccinations Get Underway*, THE WASHINGTON POST, (Feb. 25, 2021), <https://www.washingtonpost.com/health/2021/02/25/covid-vaccine-ad-council/>.



inferences, not that which merely *could* be used. This latter approach would encompass a much broader set of data, and it would alter the objectives and construct of the bill, which appropriately provides for different treatment of a narrower set of data categories.

With respect to the treatment of inferences, the guidance provided by the UK Information Commissioner's Office (ICO) regarding special category data, as defined consistently under the GDPR, establishes the following intent standard that could be applied effectively for the CPRA.

"It may be possible to infer or guess details about someone which fall within the special categories of data. Whether or not this counts as special category data ... depends on how certain that inference is, and whether you are deliberately drawing *that* inference."<sup>19</sup>

Advertising and marketing to individuals who have similar shopping and lifestyle interests could reveal, for instance, a similar race or ethnicity, but if those are neither declared by a user, nor intentionally inferred by a business to reach members of the population, the data should not be treated as sensitive data. The same guidance contains an example referring to collection of surnames and images relating to inferences and educated guesses based on those data categories, noting that if used for profiling it would likely constitute special category data.<sup>20</sup> Therefore, a practical interpretation for the CPRA would be to require opt-outs of selling and sharing sensitive personal information to profiling and targeted advertising practices that deliberately seek to target sensitive information categories, rather than merely those that could have the effect of disproportionately reaching individuals in these categories unknowingly. After all, large data sets can be processed in different ways, either seeking to reveal or target certain categories of individuals, to avoid drawing those specific inferences, or even with the goal of avoiding unintended disparate outcomes of the data processing. The regulations should therefore clarify this distinction, with the goal of incentivizing processing that avoids the use of sensitive data or making inferences about sensitive data categories, while still enabling uses of the data that can be beneficial to consumers and to businesses.

For example, in our *Guidance for NAI Members: Health Audience Segments*, the NAI distinguished between companies inferring that a consumer may have a certain health condition, a practice which requires a consumer's express consent, and generalized demographic targeting based on such demographic factors as age and gender to select the decile of the population that is most likely to be affected by a condition.<sup>21</sup> This approach was designed to balance the objective of reaching populations with valuable advertising and information, against potential privacy risks.

Taken in the context of the CPRA, the law's various provisions combine to enable privacy risk analysis and increase privacy protections for consumers, even when consumers do not exercise their right to limit the use and disclosure of their sensitive personal information. That is, the requirements for businesses to conduct data privacy risk assessments is crucial in helping to identify cases of processing personal information, even in the absence of sensitive personal information, that pose a heightened risk

---

<sup>19</sup> *What is special category data?*, INFORMATION COMMISSIONER'S OFFICE, GUIDE TO THE GENERAL DATA PROTECTION REGULATION, (emphasis added) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7>.

<sup>20</sup> *Id.*

<sup>21</sup> See generally *Guidance for NAI Members: Health Segment Audiences*, NETWORK ADVERTISING INITIATIVE (2020), [https://thenai.org/wp-content/uploads/2021/07/nai\\_healthtargeting2020.pdf](https://thenai.org/wp-content/uploads/2021/07/nai_healthtargeting2020.pdf).

of harm to a consumer, and to identify whether the risks to privacy of the consumer outweigh the benefits.

## **V. Regulation and Enforcement of Dark Patterns**

The vast majority of websites, apps and digital media services leverage data-driven advertising in order to maximize ad revenue. Indeed, data driven advertising is the leading driver of free and low-cost content across the digital ecosystem. These businesses therefore have an incentive to inform consumers about these practices, and to encourage them to share their data. At the same time, consumers have long expressed support for ad-supported content that is made available for free or low cost.<sup>22</sup> Ultimately, the interests of consumers and businesses are often aligned in this regard, and consumers are well served by websites and apps that engage tailored advertising and employ responsible data practices—this scenario is a win-win for consumers and business, and worth preserving.

The NAI’s industry-leading self-regulatory program was founded with the mission to promote transparency around these mechanisms, and choice for consumers about the use of their data, as well as establishing use limitations to protect consumers from unexpected and harmful outcomes. The NAI has long promoted—and even required through our Code and self-regulatory program—notice and choice interfaces that are presented to consumers regarding their data collection should be clear, meaningful, and free from deceptive practices that manipulate consumers into making certain elections. Most recently, with the introduction of our 2020 Code of conduct, the NAI developed industry leading requirement, along with detailed guidance, that directs companies seeking the collection of consumer location data and other sensitive data to present clear and meaningful disclosures about the sharing and uses of the data for advertising and marketing purposes in conjunction with obtaining a user’s consent.<sup>23</sup>

The concept of dark patterns was first identified in 2010, defined broadly as “tricks used in websites and apps that make users do things they otherwise would not necessarily do, such as buying or signing up for something.”<sup>24</sup> These practices, which span much more broadly than the collection of consumers’ personal information, have received well deserved attention and enforcement as policymakers at various levels seek to discourage and enforce against them. Thus far, most cases where the FTC has brought enforcement actions, have been focused on business practices that lead to upselling consumers on services and subscriptions such as the enforcement case against Age of Learning, Inc. that involved misrepresentation with respect to membership cancellation leading many to renew their membership without clear consent.<sup>25</sup>

---

<sup>22</sup> NAI’s 2019 consumer survey revealed that nearly 60% of respondents prefer their online content to be paid for by advertising, while another question sought feedback from consumers on how much they currently pay for online content and how much they would be willing to pay. Nearly 90% said they are unwilling to pay a significant amount of money to continue receiving apps and online content that they currently receive for free. The survey provided a strong affirmation that the ad-supported content model is ideal for most consumers. See Network Advertising Initiative, *NAI Consumer Survey on Privacy and Digital Advertising*, NETWORK ADVERTISING INITIATIVE (Oct. 22, 2019), <https://www.networkadvertising.org/blog-entry/nai-consumer-survey-privacy-and-digital-advertising/>.

<sup>23</sup> See *Guidance for NAI Members: Opt-In Consent*, NETWORK ADVERTISING INITIATIVE (2019), [https://thenai.org/wp-content/uploads/2021/07/nai\\_optinconsent-guidance19.pdf](https://thenai.org/wp-content/uploads/2021/07/nai_optinconsent-guidance19.pdf).

<sup>24</sup> DARK PATTERNS, <http://www.darkpatterns.org>

<sup>25</sup> *Fed. Trade Comm’n. v. Age of Learning, Inc.*, No. 2:20-cv-7996 (C.D. Cal. Sept. 8, 2020), <https://www.ftc.gov/enforcement/cases-proceedings/172-3186/age-learning-inc-abcmouse>

Despite the leadership of the NAI and other self-regulatory efforts across the digital advertising industry, consumers are all too often subject to deceptive and unfair practices around data collection. As a result, we are currently placing even greater emphasis on our efforts to educate businesses and discourage these practices. To that end, we are developing more detailed recommendations that draw from the ongoing discussions at the FTC, as well as CCPA and CPRA requirements, and perspectives from other key stakeholders.

At the same time, California regulators and other policymakers are right to focus specifically on enforcing against deceptive and unfair practices associated with consumer data collection. The CPRA, and the preceding regulations pursuant to the CCPA, define dark patterns as a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.<sup>26</sup> With respect to consumer requests to opt out of the sale of their personal information as authorized under California law, the California Office of the Attorney General (“OAG”) has directed through regulations that businesses must make the process easy for consumers to execute and must follow a minimal number of steps.<sup>27</sup> Moreover, a business must not use a method “designed with the purpose or [having] the substantial effect of subverting or impairing” the consumer’s choice.<sup>28</sup>

The NAI concurs with the scoping of this definition, and we share the goal of maintaining user autonomy over their own decisions about the use of their data, in this case pertaining to the sale or sharing of their data by each business with which they interact. Notices and choice interfaces that are presented to consumers should be clear, meaningful, and free from deceptive practices that manipulate consumers into making certain decisions. At the same time, businesses should retain the flexibility to present user information, choices, and notices to consumers in ways that are practical for each particular business, and the consumer, to facilitate informed choices about whether their data may be sold by a business, as long as these practices don’t amount to deception or tricks, and that user autonomy is not undermined. To achieve this important balance, the NAI offers the following recommendations for the Agency.

***The Agency should clarify current CCPA regulations to ensure that businesses can perform consumer education and communicate effectively with their consumers.***

Under the current proposed regulations, a business may not require consumers to click through or listen to reasons why they should not submit a request to opt out before confirming their request.<sup>29</sup> The NAI concurs with the objectives of this regulation: a consumer should not be forced to unreasonably click through a lengthy list of reasons that unnecessarily hinders their ability to submit their request to opt out. However, this should not prohibit businesses from providing concise meaningful and truthful notices or disclosures that inform users about their decisions, including informing users about the potential harms related to an opt out, as long as these are truthful and do not obstruct a consumer’s intentions to opt out. Additionally, as various states enact differing opt-out requirements, it could be a necessary service to consumers for businesses to explain differences in these requirements.

For example, prior to the delivery of a privacy-related permission request, a business could reasonably provide a concise explanation of the types of sales or sharing that it engages in, and notify its consumers that it relies on the use of this data to monetize free or low-cost products and services. As long as this is

---

<sup>26</sup> CAL. CIV. CODE § 1798.140(l) (2021).

<sup>27</sup> CAL. CODE REGS. tit. 11, § 999.315(h) (2021).

<sup>28</sup> *Id.*

<sup>29</sup> CAL. CODE REGS. tit. 11, § 999.315(h)(3) (2021).



not done in a way that impairs or unnecessarily delays the consumer's decision to opt-out of the sale or sharing of their information, this does not undermine a consumer's ability to easily make an informed choice. Ensuring the regulations strike this balance is important for the Agency to tailor the regulations to avoid a conflict with First Amendment free speech principles.

***The Agency should avoid developing technical specifications or specific user interfaces that prescribe how choices should be offered.***

The Agency's proposed regulations include a non-exhaustive list of examples of dark patterns.<sup>30</sup> These examples involve overly complicated or lengthy processes for opting out of selling personal information, confusing or misleading language, and requiring consumers to click through a list of reasons to not opt out.<sup>31</sup> Taking this totality-of-the-circumstances approach, rather than seeking to develop or prohibit specific user interfaces, is the right approach. Ultimately, what could constitute a dark pattern in one circumstance, such as a multi-click interface on a website, could actually serve consumers more effectively if offered on small screen devices that ease consumer choice through clear interfaces.

***The Agency should be mindful of so-called "light patterns" or "bright patterns."***

In contrast to dark patterns, "light patterns" or "bright patterns" have been referred to as practices that make it easy for consumers to navigate, read, and follow directions or make choices in general. Alternatively, it could be described as a practice that makes a proactive choice on behalf of consumers, with their best intentions in mind.<sup>32</sup> These "best intentions" are not uniform across the consumer experience, and therefore these practices should be approached carefully. For example, according to a 2019 NAI survey, 60 percent of consumers prefer to have online content sponsored by advertising, rather than paying subscription fees for individual websites and apps.<sup>33</sup> A user interface that assumes data-driven advertising is not in the best interest of consumers fails to contemplate negative market externalities to those consumers, such as an increase in fees and subscription-based digital content.

***The Agency should be guided by the findings, recommendations, and enforcement activities of the Federal Trade Commission.***

As the federal administrative body that oversees consumer protection throughout the FTC has produced a body of opinions and rulemakings that should guide the Agency in how it defines and regulates dark patterns. In particular, the Agency should be mindful of the FTC's regulations regarding deceptive acts or practices, and whether any omissions or misrepresentations are material. Under well-established FTC standards, an act or practice is deceptive if it (1) is *likely* to mislead the consumer; (2) is one a *reasonable* consumer would consider misleading; and (3) is a *material* misrepresentation.<sup>34</sup> For a

---

<sup>30</sup> CAL. CODE REGS. tit. 11, § 999.315(h)(1)-(5) (2021).

<sup>31</sup> *Id.*

<sup>32</sup> See, e.g., Coleman, Aidan, *Light and Dark UX Patterns*, Medium, *Prototypr*, 26 May 2019, [blog.prototypr.io/light-and-dark-ux-patterns-19ffcaa50e9a](https://blog.prototypr.io/light-and-dark-ux-patterns-19ffcaa50e9a).

<sup>33</sup> Network Advertising Initiative, *NAI Consumer Survey on Privacy and Digital Advertising*, NETWORK ADVERTISING INITIATIVE (Oct. 22, 2019), <https://www.networkadvertising.org/blog-entry/nai-consumer-survey-privacy-and-digital-advertising/>.

<sup>34</sup> Letter from James C. Miller, Chairman, Federal Trade Commission, to the Hon. John D. Dingell, Member of Congress (Oct. 14, 1983) ([https://www.ftc.gov/system/files/documents/public\\_statements/410531/831014deceptionstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf)).



misrepresentation to be material, it must be one that is likely to affect a consumer's choice or conduct regarding a product.<sup>35</sup>

These are practices and regulations businesses in California—and the entire United States—have been adhering to for decades. Businesses are familiar with the requirements and have modeled their best practices around them. Importantly, in recent years the FTC has considered dark patterns to be an example of a deceptive act or practice and have been pursuing enforcement actions accordingly.<sup>36</sup> By following the FTC's standards, the Agency can ensure its regulations are consistent with federal law.

**VI. Updates or additions, if any, that should be made to the categories of “personal information” given in the law.**

There is broad agreement around the inclusion of an internet protocol address (IP address) as a data type that could be considered personal information. The CPRA definition of personal information includes persistent identifiers such as an IP address, but only if it “identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” This definition aligns generally with the conclusion reached by the FTC dating back to their 2012 Privacy Report, which also focused on the ability to link these to specific individuals.

While it is true that in many cases businesses can and do associate IP addresses with specific individuals or households, many fundamental uses of IP are not related to identifying a specific individual or household, such as monitoring website traffic, identifying a general location of a consumer, such as the state in which they live, and even deterring malicious activity. Additionally, many IP addresses do not function at a personal or household level, rather they are associated with businesses or even communities, such as in the case of public Wifi networks. IP addresses can therefore be used for many practical purposes without creating privacy risks, particularly when combined with additional privacy-protective tools and policies, such as anonymization, encryption, and restricted forms of access. In recognition of this, the February 2020 modified proposed regulations, the California Attorney General added an example stating that “if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be ‘personal information.’”<sup>37</sup>

Unfortunately, the final CCPA regulation removed this helpful language. The NAI recommends that the Agency restore the example and clarify that IP addresses, when used with appropriate practices and controls, cannot be reasonably linked to a particular consumer or household.

---

<sup>35</sup> *Id.*

<sup>36</sup> *See, e.g., In re Zoom, Inc.*, F.T.C. No. C-4731 (2021) (complaint).

<sup>37</sup> CAL. CODE REGS. tit. 11, § 999.302(a) (2021).

## **VII. Agency Enforcement**

The NAI offers the following recommendations regarding the Agency's enforcement of the CPRA.

### ***Delay enforcement sufficient to provide business compliance following adoption of final regulations***

The CPRA empowers the agency to begin enforcement in January 2023, a date that is now less than 14 months away. While it was the goal of the CPRA for enforcement to begin on this date, the legislation underestimated the task of establishing a new Agency, and the process for development and finalization of implementing regulations. The NAI recognizes the need for timely enforcement, but it is also imperative that businesses be given sufficient time to update their policies and practices to comply with the regulation. We therefore request that the Agency provide a delay in enforcement as necessary, or exercise leniency in enforcement for an appropriate period of time to provide for a reasonable duration for businesses to come into compliance.

### ***Maintain 30-day cure period for businesses first offense when demonstrating reasonable efforts to comply***

The CPRA presents many significant updates and changes from the CCPA, and pending regulations are expected to also provide new direction for businesses across a wide range of processing consumers' personal information. The mandatory cure period established by the CCPA was removed from the statute to address concerns that companies would wait to comply with key requirements of the CCPA until they received a warning, and to take the opportunity to comply only after being called out by Californian regulators. While the NAI concurs that this is an outcome that should be discouraged, a cure period provides a valuable tool for companies seeking to comply, enabling well-intentioned companies from being penalized.

Although the CPRA removes the requirement for a "30-day cure period," the Agency maintains the ability to utilize its discretion to apply this approach in cases it deems appropriate, such as cases where companies are demonstrating a good-faith effort to comply with the law, and where reasonable measures could bring that company into compliance quickly. The goal of the CPRA, and all data privacy and security laws and regulations, is to enhance privacy and security for consumers. The NAI therefore recommends that the Agency retain the use of a 30-day cure period for first-time enforcement with a particular business, particularly in cases where the business has demonstrated a reasonable attempt to comply with the CPRA and implementing regulations and is not a repeat offender.

## **VIII. Conclusion**

Again, the NAI appreciates the opportunity to submit preliminary comments to the Agency on the rulemaking process for the CPRA. We look forward to reviewing a draft of the regulations and providing specific comments at a later date. In the meantime, if we can provide any additional information, or otherwise assist your office as it engages in the rulemaking process, please do not hesitate to contact me at [REDACTED] or David LeDuc, Vice President, Public Policy, at [REDACTED].

\*\*\*\*\*

Respectfully Submitted,

[REDACTED]  
**Leigh Freund**  
President and CEO  
Network Advertising Initiative (NAI)

---

**From:** Emory Roane [REDACTED]  
**Sent:** 11/8/2021 2:29:37 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**Subject:** PRO 01-21  
**Attachments:** 2021-11-08-Privacy-Rights-Clearinghouse-privacycoalition-CPPA-Comments.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

Subject: PRO 01-21

To the California Privacy Protection Agency,

We are a coalition of civil society, privacy and consumer advocacy organizations working in California dedicated to improving privacy protections, and we appreciate the California Privacy Protection Agency ("the Agency") invitation to comment on the proposed rulemaking under the California Privacy Rights Act of 2020 ("CPRA").

We respectfully ask that the Agency ensure implementing CPRA regulations do not erode California Consumer Privacy Act ("CCPA") protections, and recommend the Agency require businesses to include a "Do Not Sell My Personal Information" link on the business's webpage *and* honor a consumer's privacy choice exercised through a browser signal, setting or plug-in. Additionally, we encourage the Agency to craft regulations that give consumers easy ways to exercise their rights in every context and on every device. To that end, we ask the Agency to require businesses to respect existing, widely-deployed privacy settings and signals on multiple platforms, and to interpret those signals in accordance with consumer intent rather than requiring signals to be specifically tailored to the language of CPRA.

Global privacy settings have the obvious benefits to consumers of being simple to understand and easy to enable, and we believe that regulations which foster the adoption of such controls will help CPRA deliver on its intent. However, the ways that businesses interpret privacy settings may not always be clear or intuitive to consumers. For example, a consumer who has enabled a privacy setting in their browser may believe that they have opted out of sale with respect to every business they interact with on the Web, when, in fact, not every business will be able to associate that signal with the consumer's identity on other platforms. We request that the Agency give consumers ways to know whether, and to what extent, their privacy settings are respected.

-

**Implementing regulations should continue to require businesses to include a "Do Not Sell My Personal Information" link and treat user-enabled global privacy controls as valid Requests to opt out**



Current CCPA regulations require businesses to treat user-enabled global privacy controls, such browser plugins or privacy settings, as valid requests to opt out of the sale of information to third parties.<sup>1[1]</sup> Critically, this is independent of the requirement that businesses include a prominently placed link on their webpage that reads, “Do Not Sell My Personal Information” so that consumers may easily exercise their privacy choices.<sup>2[2]</sup> While the CPRA could be read to make this protective requirement optional<sup>3[3]</sup> we strongly recommend preserving both mechanisms for consumers to opt out. Allowing companies to decide which consumer choices to honor would, in addition to directly contravening the Findings and Declarations, and Purposes and Intent of the CPRA,<sup>4[4]</sup> negatively impact consumer privacy protections and reduce the effectiveness of the CCPA.

The existence of the “Do Not Sell My Personal Information” link conveys to a concerned consumer – and to watchdog organizations like the undersigned – essential information regarding a business’s privacy practices and its likely level of compliance with the CCPA. Put simply, both consumers and watchdogs can tell, merely by looking for a “Do Not Sell My Personal Information” Link, whether a company sells consumers’ personal information under the law. This at-a-glance information helps inform consumer choices *and* enforcement actions. Indeed, the existence or absence of the link is one of the most easily auditable requirements of the CCPA. The office of the Attorney General, recognizing the value of such a clear indicator of compliance, developed the Consumer Privacy Interactive Tool to allow consumers to easily report obviously non-compliant businesses.<sup>5[5]</sup> Among the 27 CCPA enforcement actions the Office of the Attorney General has spoken about publicly, nearly 30% (8 of the 27) included violations of the requirement to include a “Do Not Sell My Personal Information” link.<sup>6[6]</sup>

The CCPA requires consumers exercise their rights individually on a business-by-business basis – an onerous task made only somewhat less burdensome by the “Do Not Sell My Personal Information” link and the acceptance of user-enabled global privacy controls. Unsurprisingly, research suggests that consumers are already having difficulty exercising their privacy choices under the CCPA. A Consumer Reports study in 2020 attempted to act as an intermediary between 124 consumers in California and 21 large companies that deal in personal information – and found barriers to exercising those choices with almost all 21 companies.<sup>7[7]</sup> As part of reporting on the study, Consumer Reports spoke to Joshua Browder, founder of DoNotPay, a company that has been trying to act as an authorized agent for Californians exercising CCPA rights. According to Joshua, “It’s been a huge challenge. . . Every day it’s like an arms race.”<sup>8[8]</sup> The CCPA’s requirement that large businesses share annual metrics about consumer requests received, denied and complied with (in whole and in part)<sup>9[9]</sup> further illustrates that consumers are, for the most part, unaware of their CCPA rights. Equifax, one of the largest data brokers in the country, which *exposed* the information of 150 million Americans in 2017, reported that only 623 consumers exercised their Right to Know, and 1,205 consumers exercised their Right to Opt Out in 2020 (an estimated 0.0000015% of the total 800 million users that the business collects and aggregates).<sup>10[10]</sup>

Consumers, in other words, need more help. The Agency should therefore ensure that implementing the CPRA does not result in a rejection of the intent and purposes of the proposition: to strengthen privacy protections for

---

Californians and set a protective floor which cannot be eroded. Allowing a business to omit a “Do Not Sell My Personal Information” link would do just that, resulting in CCPA opt-out options and other notices of privacy choices being buried in a website’s privacy policy. It could also hamstring enforcement actions, leaving the Agency unable to rely on watchdog organizations and consumer alerts made through the Consumer Privacy Interactive Tool. Allowing a business to refuse a consumer’s opt-out request made through a user-enabled global privacy control would erect yet another barrier to consumers exercising their privacy rights. As the rest of the country looks on, the California Privacy Protection Agency’s first actions as enforcement authority should *not* include substantially weakening Californians’ existing privacy protections.

### **The Agency should require businesses to comply with clear, widely deployed opt-out controls.**

In order to make opt-out signals as useful as possible to consumers, businesses should be required to comply with opt-out technologies that are easy to use and widely deployed. Regulations should account for the different contexts in which consumers interact with businesses.

On the Web, the Global Privacy Control (GPC)<sup>11[11]</sup> is specifically designed to convey a user’s intent to opt out of sharing and sale, and it has achieved widespread adoption, including endorsement from the California Attorney General.<sup>12[12]</sup> Technically, it is a simple HTTP header that can be appended to every request that a device makes. It is simple for both client-side software and businesses to implement, and it works whether a user is logged in to a service or interacting with a website anonymously. Businesses should be required to treat a GPC=1 signal coming from a consumer as an opt out of sharing and sale.

Other contexts will require businesses to accept different kinds of opt-out controls. Consumers spend a significant amount of time interacting with mobile phones, often via third-party apps, and the surveillance business model in mobile apps works similarly to the way it does on the Web. Apps collect information about their users, then disclose it to third-party advertisers and data brokers for monetization. However, users enjoy less control over their experience on mobile devices than they do on the Web. Most major web browsers allow users to install “extensions” which customize the way the browser works—for example, by adding a “GPC=1” header to every outgoing request. This allows for rapid development and deployment of novel privacy-preserving tools. But there is no comparable “extension” ecosystem on iOS and Android. For the most part, users can only configure apps in ways that are explicitly allowed by developers of the apps or the operating system itself.

Fortunately, there are existing operating system-level and application-level privacy controls on both iOS and Android. These controls should be considered opt-out requests under CPRA whenever that is practical.

Android has a system-wide preference labeled “Opt out of Ads Personalization,” which users can choose to enable in their settings. Apps installed on a user’s phone can access that user’s opt-out preference with a simple query. This setting is described as follows: “Instruct apps not to use your advertising ID to build profiles or show you personalized ads.” Android terms restrict how developers can use other persistent identifiers, like IMEI number, and bar developers from selling personal data at all.<sup>13[13]</sup> Therefore, a consumer choosing to “opt out of ads personalization” is led to believe that the setting will prohibit any sale, or sharing for the purpose of advertising profiling, of their personally-identifiable information. Businesses should respect this signal as a clear opt out of sharing and sale.

---

Similarly, on iOS, Apple requires apps to ask permission to “track” users before accessing device identifiers, and app store policy prohibits apps from tracking users in other ways without receiving such permission.<sup>14[14]</sup> Therefore, a user’s refusal to grant an app permission to “track” them should be interpreted as a request to opt out of sharing and sale under CPRA.

### **The Agency should not require opt-out signals to be designed specifically for CPRA compliance.**

The Agency should require businesses to comply with any privacy signals that a user reasonably believes to be an expression of their intent to opt out. We continue to oppose the text of the final CCPA regulations at Section 315(d)(1): “Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information.” As we’ve explained, many users already enable privacy controls which convey their desire for protections equivalent to, or stronger than, the opt-out rights granted by CPRA. If the Agency requires each valid opt-out signal to be molded around the exact language present in CPRA, it will lead to a confusing, fractured set of competing technical standards that all convey more-or-less the same thing.

For both the opt out of sharing and sale, and the opt out of use of sensitive personal information, businesses should accept any signal that is widely adopted and that indicates a consumer’s desire to exercise rights which are equivalent to, or encompass, their CPRA rights. Businesses should not be able to ignore signals which do not precisely match the language of the statute. For example, a signal which specifies that a user wants to opt out of “tracking” or “profiling” should be interpreted as an expression of their intent to opt out of sharing and sale as well.

Rather than require operating system developers to create new, distinct tools to help users opt out of sharing, sale, and secondary use, the Agency should prefer to encourage businesses to respect existing, widely-deployed privacy controls. Users should not be forced to toggle several different settings on each device they own in order to protect their personal information.

### **Regulations should minimize consumer confusion and ensure that businesses process opt-out signals in a transparent way**

We strongly support the inclusion of user-enabled global privacy controls in the CCPA regulations and CPRA ballot initiative. Ensuring that consumers can easily and effectively communicate their privacy choices is enshrined in the intents and purposes of the CPRA. Those purposes rightly stress the importance of consumer control, the ability to opt out of the sale of information to third parties, and specifically references the ability to make privacy choices through authorized agents, as well as browser and device settings and signals.<sup>15[15]</sup> Unfortunately, the current implementation threatens to leave consumers with a mistaken impression of how effectively they have controlled their personal information – and we encourage the Agency to address this confusion in implementing CPRA regulations.

CCPA regulations require that a business treat user-enabled global privacy controls as an opt-out request for *that device* or, if known, for the consumer submitting the request.<sup>16[16]</sup> For consumers interacting with a business’s website without a logged-in experience or a direct connection with the business, user-enabled privacy controls might only apply to the device or browser that consumer was using at the time, and not to the

---

whole body of personal information that the business may possess about the consumer. To be clear, user-enabled privacy controls should **always** be accepted as an opt-out request, and businesses should treat these controls as opt-out requests for the device or browser when the individual consumer is not known. Our concern lies with consumers who may be relying on the belief that a device-level privacy setting has effectively communicated an opt-out request for *all* of their personal information.

Such a consumer would, upon visiting a business's website with a browser setting configured, be given no indication that a GPC signal was received, whether the business honors browser signals, or whether the opt-out request has been interpreted as an opt out for the *device* or for them personally. This consumer, operating under the belief that they have already opted out of the sale of their information to third parties, may not take additional steps to exercise their opt-out rights under the law. They would not know to scour the business's privacy policy for CCPA information or attempt to submit a verified consumer request. This is also a problem for watchdogs trying to hold businesses to account: if a business does not indicate what kind of signals it accepts, or how it processes those signals, it is hard to verify that the business is properly complying with CPRA.

At the very least, businesses should include information in their privacy policies about which privacy settings, controls, and signals they accept, and how those technical opt-out mechanisms are applied. For example, a business which accepts GPC via a website should indicate both how it interprets the GPC signal (as an opt out of sharing/sale, opt out of processing sensitive personal information, or both) and how far that signal extends (whether the business attempts to apply it to a specific user's account, to a specific browser, or only to the interaction in which the signal is received).

Furthermore, it would be extremely helpful for consumers to receive active feedback from a business when the business successfully processes an opt-out setting or signal. The CPRA requires implementing regulations *not* mandate a "notification or pop-up in responses to the consumer's opt-out preferences signal,"<sup>17[17]</sup> which is important to prevent businesses from degrading the experience of consumers who do use such signals. However, the absence of *any* kind of visual signifier or feedback from the business could make it difficult for consumers to "set and forget" a control like GPC and trust that it will serve as an effective communicator of their privacy preferences.

We request the Agency explore additional methods by which consumers could be informed as to the effectiveness of their choices exercised through global settings or opt-out signals. Rather than a pop-up notification, this could be in the form of a flag or label, unobtrusively located near the "Do Not Sell My Personal Information" link, or could be communicated back to the user's browser or device in some form. Another possibility is described in the draft GPC specification, which provides a way for websites that comply with GPC to communicate that fact by posting data at a "well known" URL. The data hosted at the URL allows browser extensions and similar tools to automatically audit a business's compliance with GPC.<sup>18[18]</sup>

Additionally, we recommend that the annual reporting requirements for large businesses be expanded to include a delineation in reported opt-out requests made through browser signals which were interpreted as requests made by the consumer, opt-out requests made through browser signals which were interpreted as requests made by the device or browser, and opt-out requests made through alternative mechanisms.



Once again, the undersigned organizations appreciate the opportunity to comment on this initial rulemaking procedure. We welcome any comments, are available for additional feedback and look forward to continuing to work with the Agency as we move forward towards the ever-approaching date of CPRA implementation.

Sincerely,

Privacy Rights Clearinghouse  
Access Humboldt  
Becca Cramer-Mowder, ACLU California Action  
Jacob Snow, Senior Staff Attorney, ACLU Foundation of Northern California  
Common Sense Media  
The Consumer Federation of America  
The Electronic Frontier Foundation  
Media Alliance  
Oakland Privacy

---

<sup>19</sup>[1] 11 CA ADC § 999.315

<sup>20</sup>[2] Cal Civ. Code § 1798.135(a)(1), and 11 CA ADC § 999.306(b)(1)

<sup>21</sup>[3] Cal Civ. Code § 1798.135(b)(1)

<sup>22</sup>[4] “Rather than diluting privacy rights, California should strengthen them over time.” The California Consumer Privacy Act of 2018, A.B. 375, §2(E);

“Consumers need stronger laws to place them on a more equal footing when negotiating with businesses in order to protect their rights” *Id.* At §2(H);

“The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy” *Id.* At §3(C)(1)

“The law should be amended, if necessary, to improve its operation, provided that the amendments do not compromise or weaken consumer privacy” *Id.* At §3(C)(6)

<sup>23</sup>[5] Consumer Privacy Interactive Tool, <https://oag.ca.gov/consumer-privacy-tool> (last visited Nov. 8, 2021)

<sup>24</sup>[6] CCPA Enforcement Case Examples, <https://www.oag.ca.gov/privacy/ccpa/enforcement> (last visited Nov. 8, 2021)

<sup>25</sup>[7] Kaveh Waddell, *Why It's Tough to Get Help Opting Out of Data Sharing*, Consumer Reports, (March 16, 2021) <https://www.consumerreports.org/privacy/why-its-tough-to-get-help-opting-out-of-data-sharing-a7758781076/>

<sup>26</sup>[8] *Id.*

<sup>27</sup>[9] 11 CA ADC § 999.317(g)

<sup>28</sup>[10] California Residents Privacy Statement and Notice at Collection, <https://www.equifax.com/privacy/privacy-statement/#CaliforniaResidents> (last visited Nov. 8, 2021)

<sup>29[11]</sup> Global Privacy Control (GPC) Unofficial Draft 11 October 2021, <https://globalprivacycontrol.github.io/gpc-spec/> (last visited Nov. 8, 2021)

<sup>30[12]</sup> Kate Kaye, California's attorney general backs call for Global Privacy Control adoption with fresh enforcement letters to companies, Digiday (July 16, 2021) <https://digiday.com/marketing/californias-attorney-general-backs-call-for-global-privacy-control-adoption-with-fresh-enforcement-letters-to-companies/>

<sup>31[13]</sup> User Data, Google, <https://support.google.com/googleplay/android-developer/answer/10144311?hl=en> (last visited Nov. 8, 2021)

<sup>32[14]</sup> App privacy details on the App Store, Apple, <https://developer.apple.com/app-store/app-privacy-details/> (Last visited Nov. 8, 2021)

<sup>33[15]</sup> The California Privacy Rights Act of 2020, Proposition 24, §3(A)(2),(4) and §3(B)(1),(4) and §3(C)(1),(3),(4),(5),(6)

<sup>34[16]</sup> 11 CA ADC § 999.315(C)

<sup>35[17]</sup> Cal Civ. Code 1798.185(a)(20)(B)(v)

<sup>36[18]</sup> 4.1 GPC Support Representation, Global Privacy Control (GPC) Unofficial Draft 11 October 2021, <https://globalprivacycontrol.github.io/gpc-spec/#gpc-support-representation> (Last visited Nov. 8, 2021)

Emory Roane  
Policy Counsel  
Privacy Rights Clearinghouse  
3033 5<sup>th</sup> Avenue, Suite 223  
San Diego, CA 92103  
[privacyrights.org](https://privacyrights.org)  
@privacytoday

---





November 8, 2021

California Privacy Protection Agency  
Attn: Debra Castanon  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

Subject: PRO 01-21

To the California Privacy Protection Agency,

We are a coalition of civil society, privacy and consumer advocacy organizations working in California dedicated to improving privacy protections, and we appreciate the California Privacy Protection Agency (“the Agency”) invitation to comment on the proposed rulemaking under the California Privacy Rights Act of 2020 (“CPRA”).

We respectfully ask that the Agency ensure implementing CPRA regulations do not erode California Consumer Privacy Act (“CCPA”) protections, and recommend the Agency require businesses to include a “Do Not Sell My Personal Information” link on the business’s webpage *and* honor a consumer’s privacy choice exercised through a browser signal, setting or plug-in. Additionally, we encourage the Agency to craft regulations that give consumers easy ways to exercise their rights in every context and on every device. To that end, we ask the Agency to require businesses to respect existing, widely-deployed privacy settings and signals on multiple platforms, and to interpret those signals in accordance with consumer intent rather than requiring signals to be specifically tailored to the language of CPRA.

Global privacy settings have the obvious benefits to consumers of being simple to understand and easy to enable, and we believe that regulations which foster the adoption of such controls will help CPRA deliver on its intent. However, the ways that businesses interpret privacy settings may not always be clear or intuitive to consumers. For example, a consumer who has enabled a privacy setting in their browser may believe that they have opted out of sale with respect to every business they interact with on the Web, when, in fact, not every business will be able to associate that signal with the consumer’s identity on other platforms. We request that the Agency give consumers ways to know whether, and to what extent, their privacy settings are respected.

**Implementing regulations should continue to require businesses to include a “Do Not Sell My Personal Information” link and treat user-enabled global privacy controls as valid Requests to opt out**

Current CCPA regulations require businesses to treat user-enabled global privacy controls, such browser plug-ins or privacy settings, as valid requests to opt out of the sale of information to third parties.<sup>1</sup> Critically, this is independent of the requirement that businesses include a prominently placed link on their webpage that reads, “Do Not Sell My Personal Information” so that consumers may easily exercise their privacy choices.<sup>2</sup> While the CPRA could be read to make this protective requirement optional<sup>3</sup> we strongly recommend preserving both mechanisms for consumers to opt out. Allowing companies to decide which consumer choices to honor would, in addition to directly contravening the Findings and Declarations, and Purposes and Intent of the CPRA,<sup>4</sup> negatively impact consumer privacy protections and reduce the effectiveness of the CCPA.

The existence of the “Do Not Sell My Personal Information” link conveys to a concerned consumer – and to watchdog organizations like the undersigned – essential information regarding a business’s privacy practices and its likely level of compliance with the CCPA. Put simply, both consumers and watchdogs can tell, merely by looking for a “Do Not Sell My Personal Information” Link, whether a company sells consumers’ personal information under the law. This at-a-glance information helps inform consumer choices *and* enforcement actions. Indeed, the existence or absence of the link is one of the most easily auditable requirements of the CCPA. The office of the Attorney General, recognizing the value of such a clear indicator of compliance, developed the Consumer Privacy Interactive Tool to allow consumers to easily report obviously non-compliant businesses.<sup>5</sup> Among the 27 CCPA enforcement actions the Office of the Attorney General has spoken about publicly, nearly 30% (8 of the 27) included violations of the requirement to include a “Do Not Sell My Personal Information” link.<sup>6</sup>

The CCPA requires consumers exercise their rights individually on a business-by-business basis – an onerous task made only somewhat less burdensome by the “Do Not Sell My Personal Information” link and the acceptance of user-enabled global privacy controls.

---

<sup>1</sup> 11 CA ADC § 999.315

<sup>2</sup> Civil Code § 1798.135(a)(1), and 11 CA ADC § 999.306(b)(1)

<sup>3</sup> Civil Code § 1798.135(b)(1)

<sup>4</sup> “Rather than diluting privacy rights, California should strengthen them over time.” The California Consumer Privacy Act of 2018, A.B. 375, §2(E);

“Consumers need stronger laws to place them on a more equal footing when negotiating with businesses in order to protect their rights” *Id.* At §2(H);

“The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy” *Id.* At §3(C)(1)

“The law should be amended, if necessary, to improve its operation, provided that the amendments do not compromise or weaken consumer privacy” *Id.* At §3(C)(6)

<sup>5</sup> Consumer Privacy Interactive Tool, <https://oag.ca.gov/consumer-privacy-tool> (last visited Nov. 8, 2021)

<sup>6</sup> CCPA Enforcement Case Examples, <https://www.oag.ca.gov/privacy/ccpa/enforcement> (last visited Nov. 8, 2021)



Unsurprisingly, research suggests that consumers are already having difficulty exercising their privacy choices under the CCPA. A Consumer Reports study in 2020 attempted to act as an intermediary between 124 consumers in California and 21 large companies that deal in personal information – and found barriers to exercising those choices with almost all 21 companies.<sup>7</sup> As part of reporting on the study, Consumer Reports spoke to Joshua Browder, founder of DoNotPay, a company that has been trying to act as an authorized agent for Californians exercising CCPA rights. According to Joshua, “It’s been a huge challenge. . . Every day it’s like an arms race.”<sup>8</sup> The CCPA’s requirement that large businesses share annual metrics about consumer requests received, denied and complied with (in whole and in part)<sup>9</sup> further illustrates that consumers are, for the most part, unaware of their CCPA rights. Equifax, one of the largest data brokers in the country, which *exposed* the information of 150 million Americans in 2017, reported that only 623 consumers exercised their Right to Know, and 1,205 consumers exercised their Right to Opt Out in 2020 (an estimated 0.0000015% of the total 800 million users that the business collects and aggregates).<sup>10</sup>

Consumers, in other words, need more help. The Agency should therefore ensure that implementing the CPRA does not result in a rejection of the intent and purposes of the proposition: to strengthen privacy protections for Californians and set a protective floor which cannot be eroded. Allowing a business to omit a “Do Not Sell My Personal Information” link would do just that, resulting in CCPA opt-out options and other notices of privacy choices being buried in a website’s privacy policy. It could also hamstring enforcement actions, leaving the Agency unable to rely on watchdog organizations and consumer alerts made through the Consumer Privacy Interactive Tool. Allowing a business to refuse a consumer’s opt-out request made through a user-enabled global privacy control would erect yet another barrier to consumers exercising their privacy rights. As the rest of the country looks on, the California Privacy Protection Agency’s first actions as enforcement authority should *not* include substantially weakening Californians’ existing privacy protections.

### **The Agency should require businesses to comply with clear, widely deployed opt-out controls.**

In order to make opt-out signals as useful as possible to consumers, businesses should be required to comply with opt-out technologies that are easy to use and widely deployed. Regulations should account for the different contexts in which consumers interact with businesses.

---

<sup>7</sup> Kaveh Waddell, *Why It's Tough to Get Help Opting Out of Data Sharing*, Consumer Reports, (March 16, 2021) <https://www.consumerreports.org/privacy/why-its-tough-to-get-help-opting-out-of-data-sharing-a7758781076/>

<sup>8</sup> *Id.*

<sup>9</sup> 11 CA ADC § 999.317(g)

<sup>10</sup> California Residents Privacy Statement and Notice at Collection, <https://www.equifax.com/privacy/privacy-statement/#CaliforniaResidents> (last visited Nov. 8, 2021)



On the Web, the Global Privacy Control (GPC)<sup>11</sup> is specifically designed to convey a user's intent to opt out of sharing and sale, and it has achieved widespread adoption, including endorsement from the California Attorney General.<sup>12</sup> Technically, it is a simple HTTP header that can be appended to every request that a device makes. It is simple for both client-side software and businesses to implement, and it works whether a user is logged in to a service or interacting with a website anonymously. Businesses should be required to treat a GPC=1 signal coming from a consumer as an opt out of sharing and sale.

Other contexts will require businesses to accept different kinds of opt-out controls. Consumers spend a significant amount of time interacting with mobile phones, often via third-party apps, and the surveillance business model in mobile apps works similarly to the way it does on the Web. Apps collect information about their users, then disclose it to third-party advertisers and data brokers for monetization. However, users enjoy less control over their experience on mobile devices than they do on the Web. Most major web browsers allow users to install “extensions” which customize the way the browser works—for example, by adding a “GPC=1” header to every outgoing request. This allows for rapid development and deployment of novel privacy-preserving tools. But there is no comparable “extension” ecosystem on iOS and Android. For the most part, users can only configure apps in ways that are explicitly allowed by developers of the apps or the operating system itself.

Fortunately, there are existing operating system-level and application-level privacy controls on both iOS and Android. These controls should be considered opt-out requests under CPRA whenever that is practical.

Android has a system-wide preference labeled “Opt out of Ads Personalization,” which users can choose to enable in their settings. Apps installed on a user's phone can access that user's opt-out preference with a simple query. This setting is described as follows: “Instruct apps not to use your advertising ID to build profiles or show you personalized ads.” Android terms restrict how developers can use other persistent identifiers, like IMEI number, and bar developers from selling personal data at all.<sup>13</sup> Therefore, a consumer choosing to “opt out of ads personalization” is led to believe that the setting will prohibit any sale, or sharing for the purpose of advertising profiling, of their personally-identifiable information. Businesses should respect this signal as a clear opt out of sharing and sale.

Similarly, on iOS, Apple requires apps to ask permission to “track” users before accessing device identifiers, and app store policy prohibits apps from tracking users in other

---

<sup>11</sup> Global Privacy Control (GPC) Unofficial Draft 11 October 2021, <https://globalprivacycontrol.github.io/gpc-spec/> (last visited Nov. 8, 2021)

<sup>12</sup> Kate Kaye, California's attorney general backs call for Global Privacy Control adoption with fresh enforcement letters to companies, Digiday (July 16, 2021) <https://digiday.com/marketing/californias-attorney-general-backs-call-for-global-privacy-control-adoption-with-fresh-enforcement-letters-to-companies/>

<sup>13</sup> User Data, Google, <https://support.google.com/googleplay/android-developer/answer/10144311?hl=en> (last visited Nov. 8, 2021)



ways without receiving such permission.<sup>14</sup> Therefore, a user's refusal to grant an app permission to "track" them should be interpreted as a request to opt out of sharing and sale under CPRA.

**The Agency should not require opt-out signals to be designed specifically for CPRA compliance.**

The Agency should require businesses to comply with any privacy signals that a user reasonably believes to be an expression of their intent to opt out. We continue to oppose the text of the final CCPA regulations at Section 315(d)(1): "Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information." As we've explained, many users already enable privacy controls which convey their desire for protections equivalent to, or stronger than, the opt-out rights granted by CPRA. If the Agency requires each valid opt-out signal to be molded around the exact language present in CPRA, it will lead to a confusing, fractured set of competing technical standards that all convey more-or-less the same thing.

For both the opt out of sharing and sale, and the opt out of use of sensitive personal information, businesses should accept any signal that is widely adopted and that indicates a consumer's desire to exercise rights which are equivalent to, or encompass, their CPRA rights. Businesses should not be able to ignore signals which do not precisely match the language of the statute. For example, a signal which specifies that a user wants to opt out of "tracking" or "profiling" should be interpreted as an expression of their intent to opt out of sharing and sale as well.

Rather than require operating system developers to create new, distinct tools to help users opt out of sharing, sale, and secondary use, the Agency should prefer to encourage businesses to respect existing, widely-deployed privacy controls. Users should not be forced to toggle several different settings on each device they own in order to protect their personal information.

**Regulations should minimize consumer confusion and ensure that businesses process opt-out signals in a transparent way**

We strongly support the inclusion of user-enabled global privacy controls in the CCPA regulations and CPRA ballot initiative. Ensuring that consumers can easily and effectively communicate their privacy choices is enshrined in the intents and purposes of the CPRA. Those purposes rightly stress the importance of consumer control, the ability to opt out of the sale of information to third parties, and specifically references the ability to make privacy choices through authorized agents, as well as browser and device settings and signals.<sup>15</sup> Unfortunately, the current implementation threatens to leave consumers with a mistaken impression of how

---

<sup>14</sup> App privacy details on the App Store, Apple, <https://developer.apple.com/app-store/app-privacy-details/> (Last visited Nov. 8, 2021)

<sup>15</sup> The California Privacy Rights Act of 2020, Proposition 24, §3(A)(2),(4) and §3(B)(1),(4) and §3(C)(1),(3),(4),(5),(6)

effectively they have controlled their personal information – and we encourage the Agency to address this confusion in implementing CPRA regulations.

CCPA regulations require that a business treat user-enabled global privacy controls as an opt-out request for *that device* or, if known, for the consumer submitting the request.<sup>16</sup> For consumers interacting with a business’s website without a logged-in experience or a direct connection with the business, user-enabled privacy controls might only apply to the device or browser that consumer was using at the time, and not to the whole body of personal information that the business may possess about the consumer. To be clear, user-enabled privacy controls should **always** be accepted as an opt-out request, and businesses should treat these controls as opt-out requests for the device or browser when the individual consumer is not known. Our concern lies with consumers who may be relying on the belief that a device-level privacy setting has effectively communicated an opt-out request for *all* of their personal information.

Such a consumer would, upon visiting a business’s website with a browser setting configured, be given no indication that a GPC signal was received, whether the business honors browser signals, or whether the opt-out request has been interpreted as an opt out for the *device* or for them personally. This consumer, operating under the belief that they have already opted out of the sale of their information to third parties, may not take additional steps to exercise their opt-out rights under the law. They would not know to scour the business’s privacy policy for CCPA information or attempt to submit a verified consumer request. This is also a problem for watchdogs trying to hold businesses to account: if a business does not indicate what kind of signals it accepts, or how it processes those signals, it is hard to verify that the business is properly complying with CPRA.

At the very least, businesses should include information in their privacy policies about which privacy settings, controls, and signals they accept, and how those technical opt-out mechanisms are applied. For example, a business which accepts GPC via a website should indicate both how it interprets the GPC signal (as an opt out of sharing/sale, opt out of processing sensitive personal information, or both) and how far that signal extends (whether the business attempts to apply it to a specific user’s account, to a specific browser, or only to the interaction in which the signal is received).

Furthermore, it would be extremely helpful for consumers to receive active feedback from a business when the business successfully processes an opt-out setting or signal. The CPRA requires implementing regulations *not* mandate a “notification or pop-up in responses to the consumer’s opt-out preferences signal,”<sup>17</sup> which is important to prevent businesses from degrading the experience of consumers who do use such signals. However, the absence of *any* kind of visual signifier or feedback from the business could make it difficult for consumers to

---

<sup>16</sup> 11 CA ADC § 999.315(C)

<sup>17</sup> Cal Civil Code § 1798.185(a)(20)(B)(v)



“set and forget” a control like GPC and trust that it will serve as an effective communicator of their privacy preferences.

We request the Agency explore additional methods by which consumers could be informed as to the effectiveness of their choices exercised through global settings or opt-out signals. Rather than a pop-up notification, this could be in the form of a flag or label, unobtrusively located near the “Do Not Sell My Personal Information” link, or could be communicated back to the user’s browser or device in some form. Another possibility is described in the draft GPC specification, which provides a way for websites that comply with GPC to communicate that fact by posting data at a “well known” URL. The data hosted at the URL allows browser extensions and similar tools to automatically audit a business’s compliance with GPC.<sup>18</sup>

Additionally, we recommend that the annual reporting requirements for large businesses be expanded to include a delineation in reported opt-out requests made through browser signals which were interpreted as requests made by the consumer, opt-out requests made through browser signals which were interpreted as requests made by the device or browser, and opt-out requests made through alternative mechanisms.

Once again, the undersigned organizations appreciate the opportunity to comment on this initial rulemaking procedure. We welcome any comments, are available for additional feedback and look forward to continuing to work with the Agency as we move forward towards the ever-approaching date of CPRA implementation.

Sincerely,

Privacy Rights Clearinghouse  
Access Humboldt  
Becca Cramer-Mowder, ACLU California Action  
Jacob Snow, Senior Staff Attorney, ACLU Foundation of Northern California  
Common Sense Media  
The Consumer Federation of America  
The Electronic Frontier Foundation  
Media Alliance  
Oakland Privacy

---

<sup>18</sup> 4.1 GPC Support Representation, Global Privacy Control (GPC) Unofficial Draft 11 October 2021, <https://globalprivacycontrol.github.io/gpc-spec/#gpc-support-representation> (Last visited Nov. 8, 2021)

---

**From:** David Reid ([REDACTED])  
**Sent:** 11/8/2021 4:11:39 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Don Maurice ([REDACTED]); [REDACTED]; 'Eric Rosenkoetter' ([REDACTED])  
**Subject:** RMAI Comments on the Proposed Rulemaking Under the California Privacy Rights Act of 2020  
**Attachments:** RMAI Comments to CPRA Proposed Rulemaking 20211108.pdf

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

California Privacy Protection Agency:

Attached, please find the Receivables Management Association International's comments on the Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21).

Please do not hesitate to reach out with any questions you may have.

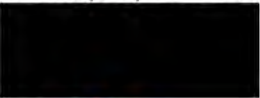
Sincerely,

David Reid

**David E. Reid**   
General Counsel



1050 Fulton Avenue, Suite 120  
Sacramento, CA 95825  
Office: (916) 482-2462



Linked  profile

**About the Receivables Management Association International** – The Receivables Management Association International (RMAI) is a nonprofit trade association that represents the Receivables Management Industry. RMAI's [Receivables Management Certification Program](#) and [Code of Ethics](#) protect consumers and businesses by setting the gold standard through uniform industry best practices. RMAI provides networking, education, and business development opportunities through events and communications. RMAI also maintains a highly effective grassroots advocacy program at the state and federal levels. Founded in 1997, RMAI is headquartered in Sacramento, California.



November 8, 2021

Debra Castanon  
California Privacy Protection Agency  
915 Capitol Mall, Suite 350A  
Sacramento, CA 95814

*Sent via email:* regulations@coppa.ca.gov

Re: RMAI Comments on the Proposed Rulemaking Under the California Privacy Rights Act  
of 2020  
(Proceeding No. 01-21)

Dear Ms. Castanon:

The Receivables Management Association International (“RMAI”) appreciates this opportunity to submit the following comments regarding the Proposed Rulemaking Under the California Privacy Rights Act of 2020 (“CPRA”).

## I. BACKGROUND

RMAI is the nonprofit trade association that represents more than 570 companies that purchase or support the purchase of performing and non-performing receivables on the secondary market. The existence of the secondary market is critical to the functioning of the primary market in which credit originators extend credit to consumers. An efficient secondary market lowers the cost of credit extended to consumers and increases the availability and diversity of such credit.

RMAI is an international leader in promoting strong and ethical business practices within the receivables management industry. RMAI requires all its member companies who are purchasing receivables on the secondary market to become certified through RMAI’s Receivables Management Certification Program (“RMCP”)<sup>1</sup> as a requisite for membership. The RMCP is a comprehensive and uniform source of industry standards that has been recognized by the collection industry’s federal regulator, the Consumer Financial Protection Bureau, as “best practices.”<sup>2</sup>

In addition to requiring that certified companies comply with local, state, and federal laws and regulations concerning collection activity,<sup>3</sup> the RMCP goes above and beyond the requirements

---

<sup>1</sup> RMAI, *RMAI Receivables Management Certification Program*, <https://rmassociation.org/certification> (last accessed March 2, 2019).

<sup>2</sup> Consumer Financial Protection Bureau, *Small Business Review Panel for Debt Collector and Debt Buyer Rulemaking, Outline of Proposals Under Consideration*, July 28, 2016, p. 38, [http://files.consumerfinance.gov/f/documents/20160727\\_cfpb\\_Outline\\_of\\_proposals.pdf](http://files.consumerfinance.gov/f/documents/20160727_cfpb_Outline_of_proposals.pdf) (last accessed March 2, 2019).

<sup>3</sup> The federal laws to which member companies are subject include but are not limited to the Fair Debt Collection Practices Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Electronic Funds Transfer Act, Telephone Consumer Protection Act, the Family Educational Rights and Privacy Act and the Health Insurance Portability and Accountability Act.



of local, state, and federal laws and regulations by requiring its member companies to comply with additional requirements not addressed by existing laws and regulations. The debt buying companies certified by the RMCP hold approximately 80 percent of all purchased receivables in the country, by RMAI's estimates.

RMCP certified companies are subject to vigorous and recurring independent third-party audits to demonstrate to RMAI their compliance with the RMAI Certification Program. This audit includes an onsite inspection of the certified companies to validate full integration of RMCP standards into the company's operations. Following a company's initial certification, review audits continue to be conducted every two to three years.

RMAI's Certification Program was recognized by a resolution of the Michigan State Senate as "exceed[ing] state and federal laws and regulations through a series of stringent requirements that stress responsible consumer protection through increased transparency and operational controls..."<sup>4</sup>

At the state level, since 2013, RMAI has worked with legislators and regulators in California, Connecticut, Colorado, Maine, Maryland, Minnesota, New York, Oregon, Washington, and West Virginia toward the enactment of enhanced laws and regulations regarding the collection of purchased consumer debts.

## II. COMMENTS

### 1. *Civil Code, § 1798.185(a)(15) - Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses*

#### a. **When a business's processing of personal information presents a "significant risk to consumers' privacy or security."**

RMAI believes that when consumers provide their personal information to an entity covered by the Fair Debt Collections Practices Act, (15 U.S.C. § 1692, *et seq.*), the Fair Credit Reporting Act (15 U.S.C. § 1681, *et seq.*), the Gramm-Leach-Bliley Act (15 U.S.C.S. §§ 6801-6809) the Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001, *et seq.*), the Health Insurance Portability and Accountability Act of 1996 or the Family Educational Rights and Privacy Act (20 U.S.C. § 1232, *et seq.*), the processing of personal information does not present a significant risk to consumers' privacy or security. First, the CPRA recognizes that such covered entities already are subject to expansive regulatory frameworks designed to protect consumers' privacy and security. Second, the CPRA expressly exempts personal information subject to certain of these federal laws. However, in some instances these same entities may process both personal information subject to and not subject to these federal laws for the same consumer. RMAI understands the non-exempt personal information is *de minimus* in these instances. Therefore,

---

<sup>4</sup> Michigan Senate Resolution 33, adopted March 26, 2015.  
[https://www.legislature.mi.gov/\(S\(c0155hrzl15jmpuaxb4uv0gf\)\)/mileg.aspx?page=getobject&objectname=2015-SR-0033&query=on](https://www.legislature.mi.gov/(S(c0155hrzl15jmpuaxb4uv0gf))/mileg.aspx?page=getobject&objectname=2015-SR-0033&query=on) (last accessed March 2, 2019).



entities who process both exempt and non-exempt personal information related to the same consumers should not be deemed to pose a “significant risk” to consumers’ privacy or security.

**2. Civil Code, § 1798.185(a)(16) – Automated Decisionmaking**

- a. What activities should be deemed to constitute “automated decisionmaking technology” and/or “profiling.”**
- b. When consumers should be able to access information about businesses’ use of automated decisionmaking technology and what processes consumers and businesses should follow to facilitate access.**
- c. What information businesses must provide to consumers in response to access requests, including what businesses must do in order to provide “meaningful information about the logic” involved in the automated decisionmaking process.**
- d. The scope of consumers’ opt-out rights with regard to automated decisionmaking, and what processes consumers and businesses should follow to facilitate opt outs.**

As noted above, our members process personal information subject to various federal laws that the CPRA exempts but in some instances these same entities may also process personal information for the same consumers that is non-exempt. RMAI believes such non-exempt personal information is *de minimus* and exempted personal information is largely if not exclusively used to drive automated decisionmaking. Therefore, to the extent a business uses exempt personal information as part of its automated decisionmaking:

- a. it should not be “deemed to constitute ‘automated decisionmaking technology’ and/or ‘profiling;’
- b. consumers should not be “able to access information about [such] businesses’ use of automated decisionmaking technology;”
- c. such business should not be required to provide consumers with information concerning “automated decisionmaking technology” including ““meaningful information about the logic’ involved in the automated decisionmaking process;” and,
- d. consumers should not be permitted to opt-out of automated decisionmaking used by such businesses.

**3. Civil Code, § 1798.199.65– Audits Performed by the Agency**

- a. What the scope of the Agency’s audit authority should be.**

Because RMAI members process personal information subject to various federal laws that the CPRA exempts, they should not be subject to audits performed by the Agency. Specifically, businesses that process personal information exempt from the CPRA should not be subject to Agency audits notwithstanding that they may also process personal information for the same consumers that is not subject to the federal law exemptions.

4. *Civil Code, § 1798.106 – Consumers’ Right to Delete, Right to Correct, and Right to Know*

- a. The new rules and procedures, or changes to existing rules and procedures, needed for consumers to make requests to correct inaccurate personal information.
- b. How often, and under what circumstances, a consumer may request a correction to their personal information.
- c. How a business must respond to a request for correction, including the steps a business may take to prevent fraud.
- d. When a business should be exempted from the obligation to take action on a request because responding to the request would be “impossible, or involve a disproportionate effort” or because the information that is the object of the request is accurate.
- e. A consumer’s right to provide a written addendum to their record with the business, if the business rejects a request to correct their personal information.

RMAI supports the ability of consumers to correct inaccurate personal information that businesses may maintain. The RMCP includes numerous standards designed to ensure that RMAI’s members receive, maintain and share personal information that is materially accurate and complete.

- a. Generally, the items required to be explained in the privacy policy regarding the right to delete, § 999.308(c)(2), can be applied to the right to correct, as can the general response concepts in § 999.313(a) and (b), and the identity verification processes described in §§ 999.323, 999.324 and 999.325.

However, just as the exceptions in § 1798.105(d) can prevent the deletion of personal information in certain circumstances, there must opportunity for a business to confirm that the “corrected” information provided by a consumer is, in fact, correct. This is essential, for example, with respect to personal information related to consumer financial services and transactions.

The onus of confirmation should not fall solely on the business. RMAI suggests that the rules allow a business to require a consumer to provide documentation substantiating the information, and if the substantiation is insufficient, or if the business cannot confirm the information independently, it may deny the request to correct the information with an explanation to the consumer.

5. *Civil Code, §§ 1798.185(a)(4) and 1798.185(a)(19)–(20) – Consumers’ Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information*

As noted above, our members process personal information subject to various federal laws that the CPRA exempts. As RMAI has noted in its past, entities that process such exempt personal information should not be required to provide consumers with a disclosure which states a consumer has the right to opt-out of the sale or sharing of personal information. Such a notice would certainly confuse the consumer recipient because the information subject to the exemption is not covered by the CPRA.

6. *Civil Code, § 1798.121 - Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information*

For the same reasons noted in RMAI's comments to Topic 5, to the extent that personal information exempted by the CPRA is processed by our members, our members should not be required to provide consumers with a disclosure of consumers' rights to limit the use and disclosure of "sensitive personal information." Such a notice would certainly confuse the consumer recipient because the information subject to the exemption is not covered by the CPRA.

### III. CONCLUSION

RMAI thanks the California Privacy Protection Agency for its many thoughtful questions concerning rulemaking under the CPRA and for its consideration of these comments.

Please let me know if you have questions or if I can be of any assistance.

Sincerely,



David E. Reid  
RMAI General Counsel

---

**From:** Alan Sege [REDACTED]  
**Sent:** 11/8/2021 5:04:41 PM  
**To:** Regulations [/o=ExchangeLabs/ou=Exchange Administrative Group  
(FYDIBOHF23SPDLT)/cn=Recipients/cn=68b5b9696958418b8130c949930f1d78-CPPA Regula]  
**CC:** Ryan Hatch [REDACTED]; Tara Klamrowski [REDACTED]  
**Subject:** PRO 01-21  
**Attachments:** 21 11 8 clean final CPRA comment on scraping.pdf  
**Importance:** High

[EXTERNAL]: [REDACTED]

**CAUTION:** THIS EMAIL ORIGINATED OUTSIDE THE DEPARTMENT OF CONSUMER AFFAIRS!  
**DO NOT:** click links or open attachments unless you know the content is safe.  
**NEVER:** provide credentials on websites via a clicked link in an Email.

---

Dear Debra Castanon:

Attached here is our submission for preliminary comments on the proposed rulemaking under the California Privacy Rights Act of 2020.

All the Best,

Alan Sege  
13323 West Washington, Blvd., Suite 302  
Los Angeles, CA 90066  
[REDACTED]



**Comment: Does the CPRA Permit Email and CRM Scraping by Database Companies?**

Submitted November 8, 2021

**INTRODUCTION**

We submit the following comments (“Comments”) to the California Privacy Protection Agency (“CalPPA”) on the topic of Direct Data Extraction (defined below) practices and whether such practices are legal under the California Privacy Rights Act of 2020 (“CPRA”). We refer to a growing practice by database companies who embed special software in their customers’ computer systems, to scrape personal information from email “signatures” and other communications sent by unknowing Consumers<sup>1</sup> as “Direct Data Extraction.” Here is an illustration of how Direct Data Extraction works, using the example of scraping an actual email sent by an unknowing Consumer:<sup>2</sup>

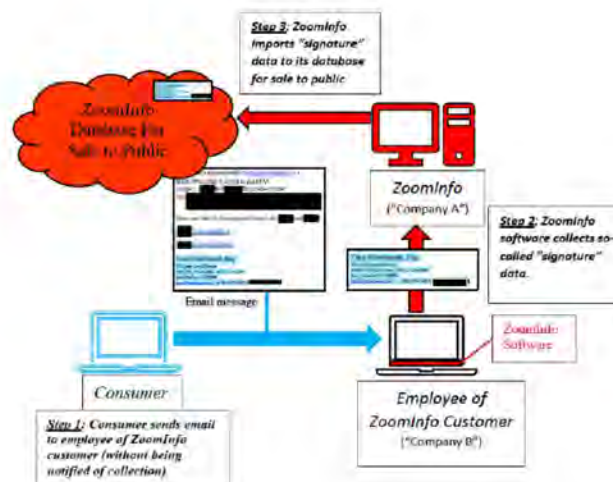


Figure 1: Direct Data Extraction Operation for Email Scraping<sup>3</sup>

<sup>1</sup> As used herein, “Consumer” means “a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.” § 1798.140(i). Note, this definition does not make a distinction between the Consumer sending an email message to an employee of Company B from their computer at work or from a personal computer at home.

<sup>2</sup> That Consumer is a co-author of this petition, Tara Klamrowski, Esq.

<sup>3</sup> Figure 1 is based on a conservative interpretation of the “signature data” scraping process ZoomInfo describes in its February 26, 2020 Form S-1, available at <https://sec.report/Document/0001628280-20-002344> (visited March 26, 2021) (emphasis added),

As shown above, database companies like ZoomInfo collect and upload the Consumer's personal information into their own databases, for sale to the public for marketing purposes, without ever notifying the Consumer at or before the point of collection. This practice appears to circumvent the important obligation under the CPRA for businesses who control the collection of personal data to inform Consumers "at or before the point of collection" that their personal information (and separately, their "Sensitive Personal Information")<sup>4</sup> is being collected for such purposes, and that this information will be sold or shared.

Many long-established data brokers and database companies avoid engaging in this practice, while their competitors boast achieving a competitive advantage by engaging in Direct Data Extraction. The database industry needs clarity from CalPPA to level the playing field between those in the database industry who are already engaging in these practices that may violate the CPRA, and those who have refrained from engaging in such practices.

### **ISSUE TO BE CONSIDERED**

An issue (the "Issue") that should be addressed by the California Privacy Protection Agency (the "Agency") is whether it is a violation of the CPRA for a database company ("Company A") to collect a Consumer's name, phone number, email address, employment information and other personal information directly from emails or other communications sent by that Consumer to a person employed by a business customer ("Company B") of Company A, where Company A scrapes personal information from the emails or communications through a computer interface into Company B's email or communication systems, and then sells the Consumer's personal information to the public without the Consumer being informed at or before the point of collection?<sup>5</sup>



*Figure 2: Map Illustrating that California Does Not Exempt "Business Data" from the CPRA (Presented by ZoomInfo CEO Henry Schuck, and Created by ZoomInfo)*

see Exhibit A, and its "ZoomInfo FAQs Community Edition" section of its website, located at <https://www.zoominfo.com/b2b/faqs/community-edition>, attached hereto as Exhibit B. But, it is unclear how much of a Consumer's email message ZoomInfo *actually* limits itself to collecting from the applicable email service API or email client on Company B's employee's computer.

<sup>4</sup> The CPRA specifically requires businesses to notify Consumers if they collect "Sensitive Personal Information", as that term is defined in the CPRA. §1798.100(a)(2).

<sup>5</sup> Specifically, these Comments relate to topics numbered 4, 5, 6, and 9 in the CalPPA Invitation for Comments (defined below).

## **THE CALIFORNIA PRIVACY PROTECTION AGENCY'S AUTHORITY TO SOLICIT COMMENTS**

This Comment including the Issue is submitted under the CPRA.<sup>6</sup> On September 22, 2021, the CalPPA invited preliminary comments on proposed rulemaking under the CPRA.<sup>7</sup> The writers present this Issue in response to that invitation.

We are attorneys who advise database and software companies on issues including the Issue presented herein, and we, therefore, have a legitimate business interest in seeking and obtaining clarity on the legality of Direct Data Extraction, which impacts these industries. Previously, we have, on behalf of clients, requested guidance from the Office of Attorney General (“OAG”) on the Issue, understanding that the OAG would provide guidance on such pressing questions as provided under the CCPA itself (Cal. Civ. Code, § 1798.155). But the OAG responded in writing that they are not actually providing such guidance, although the law provides for it.

In the absence of guidance from the OAG under the outgoing law, now more than ever, database businesses need clarity from the new commission’s rulemaking to level the playing field between those database and technology competitors are already engaging in these questionable practices that may violate the CPRA, and those who have, in light of the Issue under the CCPA and the upcoming CPRA, refrained from engaging in the practices described herein.

### **PRACTICES FOR WHICH RULEMAKING IS SOUGHT**

We seek guidance or rulemaking from the CalPPA on whether database and software companies may, without violating the CPRA, engage in the following three methods for collecting personal information about Consumers:

- “Email Scraping,” meaning collecting personal information from private emails sent by Consumers to persons working at customers of database companies;
- “CRM Scraping,” meaning collecting personal information received from Consumer communications into Customer Relationship Management (“CRM”) systems, such as Salesforce.com; and
- “List Scraping,” meaning collecting personal information from lists of data submitted by businesses to database companies for the purpose of matching or validating their personal information and other data,

(the practices collectively referred to as “Direct Data Extraction”).

Direct Data Extraction practices are used by certain database companies to extract data in real-time *directly* from ordinary emails and other communications sent by unaware Consumers to

---

<sup>6</sup> Cal. Civ. Code, § 1798.100 – 1798.199.

<sup>7</sup> See California Privacy Protection Agency. (2021). Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020, Proceeding No. 01-21 (“CalPPA Invitation for Comments”).



other parties. Such practices may drastically reduce the cost of collecting and verifying business data in California, because they directly access communications sent by the Consumers without first providing any notice to the Consumers that their information is being collected and later sold. But there is a serious risk that these practices violate the CPRA, and specifically its requirement that database companies inform Consumers “at or before the point of collection” that their personal information is being collected, used, shared, and sold.

Appendix A shows profiles from the ZoomInfo database of professionals in occupations that require maintaining confidentiality, like attorneys. One of them is Alicia Hancock, a Deputy Attorney General litigation attorney right in California’s Office of the Attorney General, and her profile, publicized by ZoomInfo, is her personal cell phone number. *See* Appendix A, p.2. Another of them is our colleague, attorney Tara Klamrowski. One day, Ms. Klamrowski sent an email to a client including privileged information about the contents of client’s corporate minute book. Of course, when she sent the e-mail, she had no way of knowing whether her client was a ZoomInfo subscriber. Moreover, her decision to send her client an email was not initiated by any ZoomInfo website or any disclosure to her that her client or ZoomInfo was collecting personal information. But apparently, ZoomInfo scraped her e-mail harvesting not just her name, title and phone number, but client confidential information. And they included the client confidential information in their business database for sale. *See Id.*, p.1.

We seek clarity from CalPPA on whether it is lawful for database companies to engage in the Direct Data Extraction that companies such as ZoomInfo and Dun & Bradstreet are already using.

### **DIRECT DATA EXTRACTION METHODS**

The three Direct Data Extraction methods at issue here can generally be described as follows.

#### **E-Mail Scraping**

Software supplied by a database company (Company A), such as ZoomInfo or Dun & Bradstreet, is inserted directly into the email system of its business customers (Company B). The software works by monitoring emails sent into and out of email servers of Company B such as Google’s Gmail, or Microsoft’s Outlook.com, or by installing plug-ins into the email server or client applications such as Outlook on end user computers at Company B. Company A’s computer programs attempt to scrape e-mail “signature” information (signature data) from inbound e-mails, sent from unknowing Consumers in what they think are private or at least personal one-on-one communications to Company B.

As intended, the computer software will retrieve what it has determined to be the Consumers’ “signature” data, comprising his or her name, address, phone number, email address, company name, and title — the type of information certain database companies claim is typically found on a “business card.” However, the software is not perfect, and can also scrape information that is not part of an email “signature.” This may include content such as attorney-client privileged communications, trade secrets, or phone numbers and email of top-level business executives, law



enforcement officials, and government employees, all of which is highly-sensitive.<sup>8</sup> We have located examples of such information in ZoomInfo's databases, and provide examples in Appendix A.<sup>9</sup> But for the direct scraping of this type of information from emails, such information would never be made available to the general public.

As noted, Company A's scraping computer software operates behind-the-scenes where Consumers are unaware that their email communications to an employee Company B could end up in a third-party database for sale to the public. Further, in these circumstances, the Consumers' personal information is scraped and collected from the *recipients'* email at Company B, without any attempt to inform these Consumers at or before the point of collection. The personal information of these Consumers is then included in a database and made available for sale to the public by Company A, in widely-available products such as those offered by ZoomInfo and Dun & Bradstreet.

### CRM Scraping

In addition to email, another source of personal information is customer relationship management ("CRM") environments. When a Consumer contacts Company B or its employees, such as by email, webform, phone call or in-person, the Consumer's personal information is typically updated in Company B's CRM system, such as Salesforce.

As with email, database companies (like Company A) integrate their tools into Salesforce, or other CRM environments involving their business customers (Company B). This is ostensibly done to add new sales prospects to Company A's business data lists, or for Company B to augment and validate its own database of Consumers' personal information. However, as a condition of receiving this service, Company B must also agree to give Company A access to all of the personal information about Company B's Consumers taken from Company B's CRM system, so that Company A can collect and add the information into its own commercial databases for sale to the public. As with E-Mail Scraping as described above, all of this happens without first providing any notice to Consumers.

### List Scraping

List Scraping is similar to CRM Scraping, except that the business customers of Company B send their business customer lists directly to the database companies (like Company A), rather than Company A having access to Customer B's CRM systems. Company A collects the information sent by business customers of Company B into its commercial database to be offered for sale to the public. As with E-Mail Scraping and CRM Scraping, Company A collects personal information without first providing any notice to consumers.

---

<sup>8</sup> The definition of "Sensitive Personal Information" under the CPRA includes, "[T]he contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication." §1798.140(ae)(1)(E).

<sup>9</sup> Appendix A hereto contains examples of highly-sensitive information found in the databases of companies who practice Direct Data Extraction methods. These databases are made available for sale to the public.

### Direct Data Extraction Disclosures

ZoomInfo and Dun & Bradstreet are two well-known database companies that practice Direct Data Extraction methods. Their public disclosures describe at a high level their use of Direct Data Extraction methods.

#### ZoomInfo Disclosures

In ZoomInfo's disclosures to the U.S. Securities and Exchange Commission ("SEC"), ZoomInfo mentions processing "email signatures," which it describes as a "rich source of data" and part of over 50 million daily updates, or "hundreds of millions" of data points:

"Our contributory network captures data on over 50 million email signatures, email deliverability and contact update records daily. We obtain email signatures, which are rich sources of data, through integrations with email systems, and also obtain unattributed data through integrations with our customers' CRM and sales & marketing automation systems. This gives us visibility into hundreds of millions of confirmatory and disqualifying signals each month, allowing us to keep our data and our customers' data cleaned in real time and create accuracy scores for the content."<sup>10</sup>

In the same SEC disclosures, ZoomInfo states that its customers supply data as part of a "contributory network," and that free access to ZoomInfo's database is conditioned on such participation:

"All of our free Community Edition users must participate in our contributory network to get access to data. Similarly, many of our paying customers participate in our contributory network to improve the quality of the data within their CRM and similar systems. Community Edition users may cease to participate in our contributory network after deciding not to renew our Community Edition version."<sup>11</sup>

More information on the "contributory network" is provided on ZoomInfo's website. There, ZoomInfo states that users of their free edition "install our local application that connects to their email service provider," that the "application then identifies business contact information that is used to ... add new records to the ZoomInfo platform," and that such information "includes name, company job title, business phone, and email address."<sup>12</sup> ZoomInfo represents that "[b]efore being added to ZoomInfo, every professional receives a notification with instructions on how to claim, manage, update, or remove their profile."<sup>13</sup> But even assuming this is true, at

---

<sup>10</sup> February 26, 2020 Form S-1 of ZoomInfo Technologies Inc., p. 133, available at <https://sec.report/Document/0001628280-20-002344> (visited March 26, 2021) (emphasis added), relevant excerpts attached as Exhibit A.

<sup>11</sup> *Id.*, p. 31 (emphasis added).

<sup>12</sup> <https://www.zoominfo.com/ce/ce-download> (visited April 29, 2021), attached as Exhibit C.

<sup>13</sup> *Id.*



no time before ZoomInfo has already accessed that information and therefore “collected”<sup>14</sup> it has ZoomInfo’s notification actually informed the Consumer “at or before the point of collection,” as required by the CPRA. And it has not informed the Consumer that it has collected Sensitive Personal Information — the contents of a Consumer’s email message. Namely, this type of notification is not an immediate alert that a Consumer automatically receives from ZoomInfo in response to sending an email to an employee of Company B.

ZoomInfo admits that it collects personal information, stating that the “Personal Information Collected” comprises “Name, Internet Protocol address, Business email address, Job title and department, Business phone numbers (general, direct and fax), Business related postal address of consumer, Social Networking URLs.”<sup>15</sup>

In its Privacy Policy, ZoomInfo describes its use of List Scraping:

“As part of the Site, ZoomInfo may make available to its customers certain “Integrations”. In using ZoomInfo’s Integrations, such as ZoomInfo’s SFNA and web browser extensions, Business Information from customer’s CRM, MAT, or sales enablement software may be transmitted to ZoomInfo for purposes of matching or cleansing customer’s data against ZoomInfo’s database as a feature of the Site. In that event, ZoomInfo may retain and store such Business Information for purposes of identifying potential contacts to supplement the Site, verifying the accuracy of such Business Information, removing out-of-date Business Information from the Site, or otherwise improving ZoomInfo’s research processes and the content provided through the Site. Information so received will not be attributable to the source. In the event that any customer wishes to opt out of ZoomInfo’s use of such information, they may do so by visiting the ‘Privacy Center’ within the ZoomInfo Salesforce Native Application and adjusting the appropriate controls.”<sup>16</sup>

List Scraping is further described in the Terms and Conditions shown in a splash screen for ZoomInfo’s DiscoverOrg product “application” plug-in to Salesforce, stating that ZoomInfo “may supplement its database” with information submitted by users of its software applications:<sup>17</sup>

---

<sup>14</sup> The CPRA defines “collects,” “collected,” or “collection” to mean “buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means.” Cal. Civ. Code, § 1798.140(f).

<sup>15</sup> ZoomInfo Privacy Statement – California, available at <https://www.zoominfo.com/about-zoominfo/ccpa-privacy-statement> (visited April 29, 2021), attached as Exhibit D.

<sup>16</sup> ZoomInfo Privacy Policy, available at <https://www.zoominfo.com/about-zoominfo/privacy-policy> (visited April 29, 2021), attached as Exhibit E.

<sup>17</sup> See Terms and Conditions splash screen for ZoomInfo App Exchange product DiscoverOrg, accessed on March 22, 2021, attached as Exhibit F.

## Terms and Conditions

I understand and agree that my use of this application is governed by the license terms and conditions available at [discoverorg.com/ltc](https://discoverorg.com/ltc) and the privacy policy available at [discoverorg.com/privacy-policy](https://discoverorg.com/privacy-policy), or by the terms of a separate written agreement between my organization and DiscoverOrg. ###I understand that when using this application, DiscoverOrg will attempt to research and verify business contact information submitted by you through match, cleanse, append, or update requests to supplement, and DiscoverOrg may supplement its database to the extent it is able to verify such information. I understand that DiscoverOrg may also use email deliverability information, on an anonymous basis, to remove out-of-date information from its database.



Finally, as an implicit acknowledgment of the obvious risks it has taken, ZoomInfo warns investors that its data collection practices could be found to violate the California Consumer Privacy Act (“CCPA”) <sup>18</sup> and other data privacy laws, resulting in “enforcement actions and significant penalties against us”:

“Certain of our activities could be found by a government or regulatory authority to be noncompliant or become noncompliant in the future with one or more data protection or data privacy laws, even if we have implemented and maintained a strategy that we believe to be compliant.... CCPA allows for fines of up to \$7,500 per violation (affected individual). Our actual or alleged failure to comply with applicable privacy or data security laws, regulations, and policies, or to protect personal data, could result in enforcement actions and significant penalties against us, which could result in negative publicity or costs, subject us to claims or other remedies, and have a material adverse effect on our business, financial condition, and results of operations..... Because the interpretation and application of many privacy and data protection laws are uncertain, it is possible that these laws may be interpreted and applied in a manner that is inconsistent with our existing data management practices or the features of our products and services.”<sup>19</sup>

### *Dun & Bradstreet Disclosures*

Dun & Bradstreet’s disclosures likewise confirm that it engages in Direct Data Extraction methods similar to ZoomInfo by collecting personal information from senders of emails and including that information for sale in its “Data Cloud” product:

“When a user opts into the installation of D&B Email IQ, the application will access limited data from the emails and calendar invites the user sends and receives in their email environment. The data collected will be limited to email addresses found in the “To” and “From” fields of the emails, as well as the business card information contained in an email signature. The signature of an

<sup>18</sup> ZoomInfo has not updated its “ZoomInfo Privacy Statement — California” to refer to the CPRA.

<sup>19</sup> *Id.*, p. 25 (emphasis added).



email may include data elements such as name, job title and department, company name, email address, telephone number, fax number, company address, corporate URL, and social networking URL. Data collected via the application may be incorporated into the Dun & Bradstreet Data Cloud and be used to enhance and improve our products by enabling businesses to manage their financial risks, protect against fraud and dishonesty, know who they are doing business with, meet their compliance and regulatory obligations and better understand organizations, industries and markets. Where permitted under applicable law, this information may also be used for sales and marketing purposes.”<sup>20</sup>

The Direct Data Extraction methods engaged in by ZoomInfo and Dun & Bradstreet present serious questions regarding compliance with the CPRA, which is relevant to the rulemaking topics published by the CalPPA for public comments.

### ANALYSIS

It seems likely that Direct Data Extraction methods violate the CPRA because the database companies who practice such methods do not inform Consumers that their personal information is being collected at or before the point of collection, which appears to be at odds with the obligations imposed by the CPRA.

*First*, with Direct Data Extraction methods, Consumers are never informed at or before the point of collection that their names, phone numbers, email addresses, and other personal information are being collected from private emails they send. Nor are Consumers informed that the personal information and Sensitive Personal Information being collected is being included in a commercial database for sale to, and also shared for free with, the public. Without being informed, Consumers do not know to exercise their right to opt-out or delete the personal information.

Moreover, the Consumer communications being scraped are person-to-person communications by Consumers to individual people working for another business. The person receiving the Consumer’s communication will have no idea that Sensitive Personal Information from their own emails or communications is being scraped by a third-party database company, as they are never so informed.

Businesses engaging in Direct Data Extraction may, therefore, be violating the CPRA, which requires that Consumers be informed “at or before the point of collection” that their personal information and Sensitive Personal Information is being collected:

“A business that controls the collection of a consumer’s personal information shall, *at or before the point of collection*, inform consumers of the following: (1) The categories of personal information to be collected and the purposes for which

---

<sup>20</sup> Dun & Bradstreet Privacy Notice, available at <https://www.dnb.com/utility-pages/privacy-policy.html> (visited March 24, 2021) (emphasis added).



the categories of information are collected or used and whether that information is sold or shared,”<sup>21</sup> (emphasis added).

There is a similar, separate notification required specifically for the collection of Sensitive Personal Information.<sup>22</sup> These requirements to inform Consumers are meant to ensure that Consumers can exercise their “right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”<sup>23</sup>

Consider the following use case involving Alice and Bob, who work at different companies. Bob’s employer is a customer of ZoomInfo, the business database company that enables Email, CRM and List Scraping and other Direct Data Extraction methods. Alice and her employer are not customers of ZoomInfo. Alice sends an email to Bob reasonably believing that the content of her email will not be made available to the public. The ZoomInfo software scans Alice’s email for the purpose of collecting her name, phone number, mailing address, email address, job title, employer, and other personal information, and to send that information to ZoomInfo’s servers for inclusion in a publicly-available database. All of this happens *without ever informing Alice*. Alice, not being informed, does not know to exercise her right to delete the personal information that was just collected.

This use case involving Alice and Bob appears to be at odds with the CPRA’s requirement that businesses notify consumers “*at or before the point of collection*” as to the categories of personal information the business is collecting and the purposes for which the categories of personal information shall be used.<sup>24</sup> Yet it happens daily to consumers across California, and up to 50 million times each day according to ZoomInfo. Accordingly, we submit these Comments for CalPPA’s consideration as to whether this practice is actually permitted under the CPRA.

**Second**, we raise the question for CalPPA’s consideration of whether an exception for data brokers contained in regulations promulgated by the OAG applies to Direct Data Extraction and exempts data brokers from complying with the CPRA’s continuing requirement to inform consumers at the point of collection. Under the exception (the “Data Broker Exception”), a registered data broker “does not need to provide a notice at collection to the consumer” if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.<sup>25</sup> The companies who engage in Direct Data Extraction, such as ZoomInfo and Dun & Bradstreet, have generally registered as “data brokers,” such that they would likely try to rely on this exception.<sup>26</sup>

---

<sup>21</sup> Cal. Civ. Code § 1798.100(a) (emphasis added).

<sup>22</sup> See *Id.* at § 1798.100(a)(2).

<sup>23</sup> *Id.* at § 1798.105(a).

<sup>24</sup> *Id.* at § 1798.100(a).

<sup>25</sup> California Consumer Privacy Act Regulations, § 990.305(e).

<sup>26</sup> See <https://oag.ca.gov/data-broker/registration/185627> for ZoomInfo (visited March 24, 2021), attached as Exhibit G, and <https://oag.ca.gov/data-broker/registration/189043> for Dun & Bradstreet (visited April 1, 2021), attached as Exhibit H.

However, the Data Broker Exception cannot apply to an information collecting practice that entails a “direct relationship” with a Consumer. This is because “data broker” is defined as “a business that knowingly collects and sells to third parties the personal information of a consumer *with whom the business does not have a direct relationship*.”<sup>27</sup> While the term “direct relationship” is not defined in the CPRA, CCPA or in the OAG’s Regulations, Direct Data Extraction methods require the database company’s software tools to have a *direct* connection to the email and CRM systems of their customers, so that they can collect data from those systems in real time. ZoomInfo uses Direct Data Extraction to collect information from consumers — even though carried out by listening in on their customers’ communications systems — constitutes a “direct relationship.” And the “Data Broker” Exception does not apply to this practice, since that exception is explicitly limited to information about consumers with whom the data broker does not have a “direct relationship.” Given this conflict, we question whether the Data Broker Exception actually exempts Direct Data Extraction.

**Third**, whether or not the personal information being scraped is of the kind that might exist on a “business card” or in an “email signature,” as the database companies claim, is irrelevant because the CPRA makes no distinctions in this regard.<sup>28</sup> In fact, the CPRA explicitly includes the contents of a consumer’s email message in the definition of Sensitive Personal Information.<sup>29</sup>

This fact is admitted by ZoomInfo’s CEO Henry Schuck himself, in presenting a map showing the “State by State Breakdown” of whether privacy laws “Apply[] to third party business data,” showing California **in bright red** to signify that its privacy laws “Apply[] to third party business data”<sup>30</sup>:



<sup>27</sup> *Id.* at § 1798.99.80(d) (emphasis added).

<sup>28</sup> *See, e.g.*, “Data Privacy with [ZoomInfo CEO] Henry Schuck,” <https://videos.zoominfo.com/watch/8VPp6w31xTCS17Y1MB3Psx>, at minute 2:50, stating that ZoomInfo collects “the information that exists on a business card.”

<sup>29</sup> *Id.*, §1798.140(ae)(1)(E).

<sup>30</sup> *Id.*, minute 3:27, attached as Exhibit I.



The CPRA, of course, has no carve-out for business-card information,<sup>31</sup> but instead defines “personal information” broadly to mean “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”<sup>32</sup> This includes, but is not limited to, “a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers,” plus a person’s “telephone number.”<sup>33</sup> “Personal information” even includes “professional or employment-related information,” which includes precisely the kind of professional and employment information that would ordinarily exist on a person’s business card or email signature.<sup>34</sup> And Sensitive Personal information includes, “the contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication.”<sup>35</sup> Because this information is meant to be protected by the CPRA, we question whether scraping so-called “business information” is different from scraping “Personal Information” as defined in § 1798.140(v)(1) of the CPRA.

***Fourth***, attempts to inform consumers *after* their data has already been *collected* seem to be an attempt to un-ring the bell after the law has been violated. ZoomInfo engages in this practice, as explained by its CEO, by sending notices to consumers after their personal information has already been collected: “So at the end of Q4 in 2019 and into this month in January [2020], we went out and we gave every California resident who we had collected information on notice that we had collected their information....”<sup>36</sup> ZoomInfo does not, for example, send Consumers an immediate, automatic notice in response to an email the Consumer sends to an employee of Company B, alerting the Consumer that it has collected, i.e., accessed, the Consumer’s personal information.

ZoomInfo’s practice of giving post-collection notice is also described on ZoomInfo’s website, which states that they “collect” information in Step 2 but do not send notification until Step 3<sup>37</sup>:

---

<sup>31</sup> In what appears to be an attempt to reassure the Consumer that it collects only “business contact information,” ZoomInfo claims that they “filter out” personal email addresses, such as those from “Gmail, Hotmail, Yahoo, etc.” However, we are not aware of a definitive or generally accepted industry process, practice, or methodology to filter and separate personal email addresses from business email addresses. A company may use a pre-compiled list of major Consumer email providers for comparison, but this does not account for personal email addresses outside of those major providers.

<sup>32</sup> Cal. Civ. Code, § 1798.140(v).

<sup>33</sup> *Id.* at § 1798.140(v)(1) (defining “Personal information”), and (aj) (defining “Unique Personal Identifier”).

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*, § 1798.140(ae)(1)(E).

<sup>36</sup> *See Id.*, minute 1:48.

<sup>37</sup> *See Exhibit J.*





But the essence of the CPRA’s “at or before the point of collection” requirement appears to be the opposite of ZoomInfo’s purported *post*-collection notification. ZoomInfo also appears to re-define what it means to “collect” information under the CPRA by narrowing the act of collecting to the point when the personal information is “added to ZoomInfo”, but in the CPRA “collects” includes “accessing” or “receiving” information.<sup>38</sup> Moreover, ZoomInfo’s attempts to notify consumers after-the-fact appears to be altogether ineffective, as consumers report that such notices, which are broadcasted as email, are filtered as spam or phishing attempts.<sup>39</sup> Accordingly, we question whether attempts to inform consumers after their data has already been collected actually satisfy the obligations under § 1798.100(a).

***Fifth*** and lastly, if ZoomInfo (or other such companies) are not required to inform Consumers with whom they have a direct relationship, then the Data Broker Exception promulgated by the OAG is on its face inconsistent with the CPRA’s mandate that “a business that controls the collection of a consumer’s personal information (and Sensitive Personal Information) shall, at or before the point of collection, inform consumers of the following: (1) The categories of personal information to be collected and the purposes for which the categories of information are collected or used and whether that information is sold or shared.”<sup>40</sup> This result fails to inform any Consumers at or before the point of collection that their personal information is being collected. Any reading of the OAG’s Data Broker Exception can only be understood within the context of the self-evident *limitation* on the Attorney General’s authority — to “further the purposes of” the CPRA. Because of this failure, we seek guidance on whether the Data Broker Exception vitiates the CPRA’s key public safeguard — the obligation to inform consumers at or before the point of collection.

## **CONCLUSION**

We respectfully request that the CalPPA consider the Issue raised in this Comment — of whether a database company may engage in Direct Data Extraction without violating the CPRA. If we can provide any additional information for your consideration, please do not hesitate to reach out to us.

<sup>38</sup> *Id.* at § 1798.140(f).

<sup>39</sup> See Exhibit K.

<sup>40</sup> Cal. Civ. Code § 1798.100(a).

Submitted by:



Alan Sege, Esq.  
Alan Sege Esq., PC



Ryan Hatch, Esq.  
Hatch Law, PC



Tara Klamrowski, Esq.  
Alan Sege Esq., PC



## Exhibit A

S-1 1 zoominfos-1.htm S-1

As filed with the Securities and Exchange Commission on February 26, 2020.

Registration No. 333-

**UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
Washington, D.C. 20549**

**FORM S-1  
REGISTRATION STATEMENT  
UNDER  
THE SECURITIES ACT OF 1933**

**ZoomInfo Technologies Inc.**

(Exact name of registrant as specified in its charter)

Delaware  
(State or other jurisdiction of  
incorporation or organization)

7372  
(Primary Standard Industrial  
Classification Code Number)  
805 Broadway Street, Suite 900  
Vancouver, Washington 98660  
Telephone: (800) 914-1220

(I.R.S. Employer  
Identification No.)

(Address, including zip code, and telephone number, including area code, of registrant's principal executive offices)

Anthony Stark  
General Counsel  
ZoomInfo Technologies Inc.  
805 Broadway Street, Suite 900  
Vancouver, Washington 98660  
Telephone: [REDACTED]

(Name, address, including zip code, and telephone number, including area code, of agent for service)

Copies to:

Richard A. Fenyes  
Simpson Thacher & Bartlett LLP  
425 Lexington Avenue  
New York, New York 10017  
Telephone: [REDACTED]

Marc D. Jaffe  
Jason M. Licht  
Stelios G. Saffos  
Latham & Watkins LLP  
885 Third Avenue  
New York, New York 10022  
Telephone: [REDACTED]

Approximate date of commencement of proposed sale to the public: **As soon as practicable after this Registration Statement is declared effective.**

If any of the securities being registered on this Form are to be offered on a delayed or continuous basis pursuant to Rule 415 under the Securities Act of 1933, check the following box. ☐

If this Form is filed to register additional securities for an offering pursuant to Rule 462(b) under the Securities Act, please check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

If this Form is a post-effective amendment filed pursuant to Rule 462(c) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

If this Form is a post-effective amendment filed pursuant to Rule 462(d) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☐

Accelerated filer ☐

Non-accelerated filer ☒

Smaller reporting company ☐

Emerging growth company ☒

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 7(a)(2)(B) of the Securities Act. ☐

**CALCULATION OF REGISTRATION FEE**

Title of Each Class of Securities to be Registered	Proposed Maximum Aggregate Offering Price <sup>(1)(2)</sup>	Amount of Registration Fee
Class A Common Stock, par value \$0.01 per share	\$500,000,000	\$64,900

(1) Estimated solely for the purpose of determining the amount of the registration fee in accordance with Rule 457(o) under the Securities Act of 1933.

(2) Includes shares of Class A common stock that are subject to the underwriters' option to purchase additional shares.

The Registrant hereby amends this Registration Statement on such date or dates as may be necessary to delay its effective date until the Registrant shall file a further amendment which specifically states that this Registration Statement shall thereafter become effective in accordance with Section 8(a) of the Securities Act of 1933 or until this Registration Statement shall become effective on such date as the Securities and Exchange Commission, acting pursuant to said Section 8(a), may determine.



Excerpt from Page 133

## Our Data Sources

We have a number of data sources, including proprietary sources, that enrich our platform as detailed below.

### *Contributory Network*

Our free users and many of our paying customers contribute data that enhances our platform. Many of our paying customers participate in our contributory network to improve the quality of the data within their CRM and sales & marketing automation systems. Similarly, all of our free Community Edition users participate in our contributory network to get access to data. Our contributory network captures data on over 50 million email signatures, email deliverability and contact update records daily. We obtain email signatures, which are rich sources of data, through integrations with email systems, and also obtain unattributed data through integrations with our customers' CRM and sales & marketing automation systems. This gives us visibility into hundreds of millions of confirmatory and disqualifying signals each month, allowing us to keep our data and our customers' data cleaned in real time and create accuracy scores for the content. In addition to enriching our existing data, these types of records often provide us with additional data and actionable insights, such as professionals getting promoted, changing jobs or leaving companies.

### *Unstructured Public Information*

Our patented and proprietary technologies extract and parse unstructured information found on webpages, newsfeeds, blogs, and other public sources, and then match that information with entities that we have previously identified. The conversion of unstructured data to actionable insights at massive scale is highly valuable to our customers. We monitor over 45 million web domains everyday.

### *Data Training Lab*

We have developed hundreds of processes, largely automated, to gather information from sources, such as PBX directories, website traffic and source code, and proprietary surveys. Our researchers develop proprietary libraries that map raw data points to additional information to generate useful insights. For example, we enhance technology to gather a telephone number extension at a particular company and location by leveraging our library to generate a full direct dial phone number, by appending the correct area code and prefix. Combining these libraries with the wealth of information we gather from our contributory network and unstructured public and generally available information allows us to provide proprietary data points for customers.

### *Generally Available Information*

We purchase a limited amount of data from third-party vendors (e.g., other data brokers) to be used in our platform. Our technology typically adds value to this data by combining it with our proprietary insights. In 2019, we spent less than \$3 million on such data, with spend decreasing year over year.

## Benefits of Our Platform

- ***Significant and Measurable Revenue Improvement.*** The highly accurate and deep intelligence on existing and prospective customers, coupled with analytics and prioritization engines that we provide, increases revenue for our customers. Proving this to our customers is easy, because we integrate with the systems that they use to attribute revenue at the end of each month, quarter, and year. In some cases, the return on investment ("ROI") that we generate can exceed 100 times the annual spend on the ZoomInfo platform. For example, a tier 1 global bank with initial spend of approximately \$17,000 in 2006, expanded to approximately 1,000 licenses and increased spend to approximately \$1.45 million annually as of December 31, 2019 after thirteen of their top users generated approximately \$46 million in net new money in the first 12 months of use. Similarly, a telecom giant that uses the ZoomInfo platform to empower its salesforce with attribute insights had initial spend of approximately \$6,000 in 2017, grew to spend of approximately \$1.1 million as of December 31, 2019 and used the ZoomInfo platform to drive approximately \$43 million in closed business attributable to ZoomInfo in 24 months.
- ***Unmatched Accuracy, Depth, and Coverage of Data.*** We gather data from millions of sources to power our AI- and ML-driven platform. We are able to provide a guarantee of 95%+ accuracy as a result of our focus

Excerpt from Page 31

Our ability to attract new customers and increase revenue from existing customers depends in large part on our ability to continually enhance and improve our platform and the features, integrations, and capabilities we offer, and to introduce compelling new features, integrations, and capabilities that reflect the changing nature of our market to maintain and improve the quality and value of our products and services, which depends on our ability to continue investing in research and development and our successful execution and our efforts to improve and enhance our platform. The success of any enhancement to our platform depends on several factors, including timely completion and delivery, competitive pricing, adequate quality testing, integration with existing technologies, and overall market acceptance. Any new features, integrations, or capabilities that we develop may not be introduced in a timely or cost-effective manner, may contain errors, failures, vulnerabilities, or bugs or may not achieve the market acceptance necessary to generate significant revenue. If we are unable to successfully develop new features, integrations, and capabilities to enhance our platform to meet the requirements of current and prospective customers or otherwise gain widespread market acceptance, our business, results of operations, and financial condition would be harmed.

Moreover, our business is subscription-based, and therefore our customers are not obligated to and may not renew their subscriptions after their existing subscriptions expire or may renew at a lower price, including if such customers choose to reduce their data access rights under their subscription, reduce the products or services to which they have access, or reduce their number of users. Most of our subscriptions are sold for a one-year term, though some organizations purchase a multi-year subscription plan. While many of our subscriptions provide for automatic renewal, our customers may opt-out of automatic renewal and customers have no obligation to renew a subscription after the expiration of the term. Our customers may or may not renew their subscriptions as a result of a number of factors, including their satisfaction or dissatisfaction with our products and services, decreases in the number of users at the organization, our pricing or pricing structure, the pricing or capabilities of the products and services offered by our competitors, the effects of economic conditions, or reductions in our paying customers' spending levels. In addition, our customers may renew for fewer subscriptions, renew for shorter contract lengths if they were previously on multi-year contracts, or switch to lower cost offerings of our products and services. It is difficult to predict attrition rates given our varied customer base of enterprise, mid-market, and SMB customers. Our attrition rates may increase or fluctuate as a result of a number of factors, including customer dissatisfaction with our services, customers' spending levels, mix of customer base, decreases in the number of users at our customers, competition, pricing increases, or changing or deteriorating general economic conditions. If customers do not renew their subscriptions or renew on less favorable terms or fail to add more users, or if we fail to expand subscriptions of existing customers, our revenue may decline or grow less quickly than anticipated, which would harm our business, results of operations, and financial condition.

Additionally, some of our customers may have multiple subscription plans simultaneously. For example, large enterprises with distributed procurement processes where different buyers, departments, or affiliates make their own purchasing decisions based on distinct product features or separate budgets. Companies who are our existing customers may also acquire another organization that is already on our subscription plan or complete a reorganization or spin-off transaction that results in an organization subscribing to multiple subscription plans. If organizations that subscribe to multiple subscription plans decide not to consolidate all of their subscription plans or decide to downgrade to lower priced or free subscription plans, our revenue may decline or grow less quickly than anticipated, which would harm our business, results of operations, and financial condition.

***A slowdown or decline in participation in our contributory network and/or increase in the volume of opt-out requests from individuals with respect to our collection of their data could lead to a deterioration in the depth, breadth, or accuracy of our data and have an adverse effect on our business, results of operations, and financial condition.***

We have a number of sources contributing to the depth, breadth, and accuracy of the data on our platform including our contributory network. All of our free Community Edition users must participate in our contributory network to get access to data. Similarly, many of our paying customers participate in our contributory network to improve the quality of the data within their CRM and similar systems. Community Edition users may cease to participate in our contributory network after deciding not to renew our Community Edition version. Our paying customers, including those who have migrated from the Community Edition, may elect not to participate for various reasons, including their sensitivity to sharing information within our contributory network or their determination that the benefits from sharing do not outweigh the potential harm from sharing. If we are not able to attract new participants or maintain existing participants in our contributory network, our ability to effectively gather new data and update and maintain the accuracy of our database could be adversely affected. Additionally, CCPA and other legal and regulatory changes are making it easier for



## Exhibit B

## ZOOMINFO FAQs

# Community Edition

ZoomInfo's Community Edition grants users limited use of our product in exchange for business data. Learn exactly which information we collect, and how we secure it.

[Business FAQs](#) [Technical/Data FAQs](#) [Community Edition FAQs](#)

## What is ZoomInfo Community Edition?

What is the ZoomInfo Contact Contributor, and what are its system requirements?

What info does Contact Contributor submit?

Will my contacts know ZoomInfo received their info from me?

Isn't sharing contacts a privacy violation?

Can I pick the contacts I want to share?

Does Contact Contributor read my email messages?

Why is ZoomInfo offering free access?

How much does Community Edition cost?

Does Contact Contributor modify my address book?

Can I get free access if I'm already a ZoomInfo subscriber?

How do I sign in to Community Edition?

How do I unsubscribe from Community Edition?

How do I uninstall Contact Contributor?

[Free Trial](#)

## What is ZoomInfo Community Edition?

Community Edition is a program that gives you free, ongoing access to ZoomInfo's database of millions of B2B profiles, and contact information for the people you want to reach in return for sharing your business contacts with ZoomInfo. Community Edition works with either Microsoft Outlook or Google Apps for Business. [Join the ZoomInfo community today!](#)

## Who can use ZoomInfo Community Edition?

Anyone who uses a supported version of Microsoft Outlook or Google Apps for Business to send and receive business-related emails is eligible to take part in the ZoomInfo Community Edition program. Current or past subscribers to one of ZoomInfo's premium services are not eligible to take part in the Community Edition program and accounts created by such users will be deactivated. In addition, ZoomInfo only allows three employees of a single company to access the ZoomInfo Database with ZoomInfo Community Edition.

If you are an Outlook user, you must successfully install the ZoomInfo Contact Contributor software and start sharing contacts before you can access ZoomInfo Community Edition. If you are a Google Apps for Business user, you must provide ZoomInfo with access to your email account before you can access ZoomInfo Community Edition. Your username will be deactivated if you uninstall the software, revoke access to your email account, or violate the ZoomInfo terms of service.

Sales people and recruiters find the ability to search for professionals by name and/or job title and/or company to be most useful. Jobseekers can also make use of ZoomInfo Community Edition to find contacts within companies and industries where they would like to find a position.

## How will ZoomInfo Community Edition help me get business done faster?

Community Edition members can search the entire ZoomInfo Database, which includes over 10 million businesses (from start-ups to the largest organizations in the world) and 125 million business professionals. You can also access contact information for a certain number of contacts each month. Every day, ZoomInfo adds 2,000 businesses and 30,000 employees and updates 20,000 businesses and 300,000 employees.

## What if I have more questions?

Just shoot an email to [zoominfohelp@zoominfo.com](mailto:zoominfohelp@zoominfo.com). We'll get back to you within one business day!

## What is the ZoomInfo Contact Contributor, and what are its system requirements?

Contact Contributor is a lightweight software application for Microsoft Outlook or Google Apps for Business that Community Edition users install to facilitate the submission of business contacts to ZoomInfo. This software works with Microsoft Outlook 2003, 2007, 2010, 2013 or 2016 on a system running Windows 10, Windows 8, Windows 8.1, Windows 7, Windows XP or Windows Vista. Sorry, but Outlook 64-bit, Outlook Express, Outlook Web App and Mac computers are not currently supported. Click [here](#) for more information about sharing your business contacts through Google Apps for Business.

If you do not use a supported operating system or Google Apps for Business, you can still get access to ZoomInfo! Consider a subscription that [fits your business needs](#).

## What info does Contact Contributor submit?

Contact Contributor shares only *business* contact information, essentially the information a person would normally include on a business card: Name, Company, Title, Email Address, and Phone Number. Personal email address (such as those from Gmail, Hotmail, Yahoo, etc.) are filtered out. Contact Contributor operates locally, and only business contact information is shared with ZoomInfo. The body of your email is never seen by ZoomInfo; in fact, it never leaves your email.

## Will my contacts know ZoomInfo received their info from me?

Information shared via the Contact Contributor is completely anonymous as to the source. Additionally, we send an email notification directly to each contact as they are added to our product and inform them of their ability to opt out of our database.

## Isn't sharing contacts a privacy violation?

ZoomInfo takes privacy very seriously, which is why we provide notifications to each new contact that we gather for our database. We have also created an automated self-service privacy center so that anyone can opt out of our database at any time, regardless of region. Meanwhile, we do not collect any sensitive personal information from Community Edition users; simply business contact information of the type that hundreds of millions of business professionals share every day, online, on their business cards, and otherwise.

## Can I pick the contacts I want to share?

No. When you take part in the ZoomInfo Community Edition program, you agree to share all of the business contacts in your email database, including names and email addresses found in email headers and job titles, company names, phone numbers, and locations found in email signatures. Personal contacts that are connected with ISPs and free email accounts will be ignored by our system. If you would like to access the ZoomInfo Database without sharing your business contacts, consider a subscription to [one of the packages on the ZoomInfo platform](#).



## Does Contact Contributor read my email messages?

Absolutely not. Contact Contributor operates locally on your email client and looks only at address book entries, email headers, and email signatures to capture basic business contact information. All other information is excluded.

## Why is ZoomInfo offering free access?

We are on a mission to map the business landscape in near real time, and dramatically improve the quality of B2B information. In return for your help, you are given free access to ZoomInfo Community Edition as long as you allow ZoomInfo to access your email account and continue contributing business contacts. Join the [ZoomInfo Community](#) today.

## How much does Community Edition cost?

ZoomInfo Community Edition is absolutely free. Really! As long as you are sending and receiving business emails through a supported version of Microsoft Outlook or Google Apps for Business and contributing your contacts with ZoomInfo, you can access the ZoomInfo Database and the industry's most powerful search tools for free. How's that for a great exchange?

## Does Contact Contributor modify my address book?

No. The ZoomInfo Contact Contributor creates and uses its own data structure and does not modify any of your information.

## Can I get free access if I'm already a ZoomInfo subscriber?

We're sorry, but ZoomInfo Community Edition is only available to people who are not current or past ZoomInfo subscribers.

## How do I sign in to Community Edition?

We'll send your ZoomInfo Community Edition username and password via email after you successfully provide access to your email account and start sharing your business contacts. Your login details will be sent to the email address connected with Outlook or Google Apps for Business where you have given ZoomInfo access to your email account. Once you have your username and password, [login here](#).

## How do I unsubscribe from Community Edition?



If you have granted ZoomInfo access to your Google Apps account in order to participate in the ZoomInfo Community Edition, you can choose to deactivate your community membership by revoking access in the settings of your Google account. To do this, follow the instructions on the Google Accounts help section [here](#).

## How do I uninstall Contact Contributor?

You can access the uninstaller program by going to Start > Programs > ZoomInfo Contact Contributor > Uninstall. But why would you want to lose all the great benefits of ZoomInfo Community Edition?

### What happens when I uninstall Contact Contributor?

When you uninstall the ZoomInfo Contact Contributor, you will be immediately unsubscribed from and lose access to ZoomInfo Community. ZoomInfo will no longer have access to information about your business contacts once you uninstall the ZoomInfo Contact Contributor. However, you are not able to 'unshare' the information you had already shared up to that point, and ZoomInfo will retain that previously shared information.

# Get your free trial today

Free Trial



#### POPULAR FEATURES

Sales Solutions  
Marketing Solutions  
Company Contact Search  
Buyer Intent Data  
CRM Lead Enrichment

#### B2B DATABASE

Our Data  
Data Transparency  
Update Your Company  
Claim Profile  
Browse Directories

#### COMPANY

About Us  
Our Leadership  
Investor Relations  
FAQs  
Careers  
Contact Us

#### MORE RESOURCES

ZoomInfo Videos  
Newsroom  
Engineering Blog  
COVID-19 Newsfeed  
Recipes for Success  
Privacy Center

Free Trial

Login

866.904.9666



## Exhibit C

# ZoomInfo's Code of Community: Promising Transparency to Build Trust

Learn how ZoomInfo collects, manages, and respects Community Edition data

Business contact and company data changes at an incredible speed, which creates a real challenge for B2B professionals trying to reach new and existing customers.

ZoomInfo has created a proprietary engine that leverages human research, machine learning, and artificial intelligence across a diverse portfolio of data sources to continuously collect, validate, and manage the most comprehensive database of B2B intelligence available today.

One of the ways we collect and validate our data is through our Community Edition contributory network.

## Download Community Edition

- ☐ I agree to the [Terms of Service](#) and [Privacy Policy](#). I understand that I will receive a subscription to ZoomInfo Community Edition at no charge in exchange for downloading and installing the ZoomInfo Contact Contributor utility, which, among other features, involves sharing my business contacts as well as headers and signature blocks from emails that I receive.

[Get Started](#)



# What is Community Edition?

In exchange for free access to ZoomInfo, Community Edition users agree to share their business contacts to help ZoomInfo keep our platform updated. And in turn, we continuously keep their address book up-to-date with verified business information.

## How the Community Edition works:

1

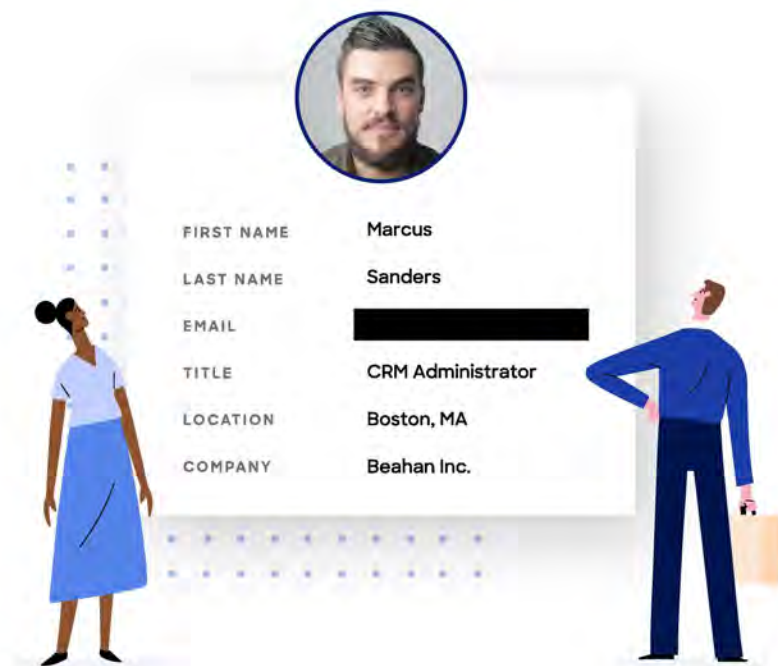
Once a community user agrees to the terms of service, authenticates themselves, and creates an account, they install our local application that connects to their email service provider.

2

Our application then identifies business contact information that is used to validate existing or add new records to the ZoomInfo platform. The information we collect is what is customarily found on a business card and includes name, company job title, business phone, and email address.

3

Before being added to ZoomInfo, every professional receives a notification with instructions on how to claim, manage, update, or remove their profile.



## What type of information does ZoomInfo collect from Community Edition?

Our algorithms and processes are designed to collect business contact information. **We do not process or capture any additional content from emails sent to or received by our Community Edition users.**

The type of business contact information we collect is what you would customarily find on a business card. In today's digital world this information now lives in email signatures and email contact books. And 99% of the information we collect from our Community Edition users simply acts as part of our system of checks and balances; confirming information that already exists on professional profiles in ZoomInfo.

## ZoomInfo's Code of Community

To build a community, you must respect it first. Our code is a promise. We're here to do more than deliver the best B2B intelligence available on the planet;



we're here to ensure that that way we collect, verify, publish, and secure data is transparent and ethical.

In the spirit of ZoomInfo's Code, here are certain types of information that we choose not to process.

### Information we do not collect:

- We do not use our cookies to track individuals across the web
- We do not track personal browsing history
- We do not read the subject lines or content of email communications
- We do not look at your calendar for meetings or attendees
- We do not mine our community for relationship data
- We do not collect contact information or user geolocation data from our mobile application

### Information we anonymize:

- We anonymize web-traffic logs and do not store or sell person-level intent
- We do not associate community users with their shared contacts
- We do not associate customers to shared contacts
- We de-identify market research survey respondent data

### How ZoomInfo proactively enables data privacy for individuals:

- Between our self-service Privacy Center, available 24/7, and personalized notification emails with instructions for how to verify, claim, update or remove profiles, we make it easy for individuals to discover and manage their ZoomInfo profile.
- We publish the date the notification email was sent to the contact

on their ZoomInfo profile

- We make it easy for individuals to opt out of our platform, with a self-service Privacy Center
- We make it easy for customers to see who has opted out of ZoomInfo
- We make it easy for customers to filter out individuals on the Do Not Call list
- We make it easy for customers to exclude their opt-out/unsubscribe lists from our platform
- Lastly, we don't hide behind complicated terms of services

Our algorithms are designed to solely collect business contact information and business contact information alone. And we've implemented privacy practices that go above and beyond those of our peers and what's required by law.







## How does Community Edition fit into the latest thoughts on data privacy?

As an ISO 27001 certified company, ZoomInfo takes data privacy and security very seriously. We have strict policies in place to ensure the data we collect always complies with the latest legislation.

ZoomInfo is self-certified to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks to comply with data transfer requirements from the European Union, United Kingdom, and/or Switzerland to the United States.

ZoomInfo's proactive approach to notifying users and our robust Privacy center ensures that users can always [claim, manage and remove their professional and/or company profiles](#) found in our database. The Privacy Center also offers a deep dive into the [latest privacy regulations](#) and provides an [expanded suite of tools, guides, and best practices for companies](#) to stay in compliance with existing and upcoming US and global legislation.

We have an in-house privacy team dedicated to providing individuals like you and our customers excellent support regarding compliance with privacy regulations. And, as part of our commitment to data privacy, we are continuously adding new notifications and features to our Privacy Center.

[Learn more about how ZoomInfo collects data](#) →

## Popular ZoomInfo Privacy Resources

4/29/2021

For your reference, click these links to read our Privacy Policy, Terms of Use and commonly asked questions about our services and technology.

[ZoomInfo Privacy Policy](#) →

[ZoomInfo Terms & Conditions](#) →

[ZoomInfo Community Edition Terms & Conditions](#) →

[ZoomInfo Privacy FAQs](#) →



[Free Trial](#)

#### POPULAR FEATURES

[Sales Solutions](#)

[Marketing Solutions](#)

[Company Contact Search](#)

[Buyer Intent Data](#)

[CRM Lead Enrichment](#)

#### COMPANY

[About Us](#)

[Our Leadership](#)

[Investor Relations](#)

[FAQs](#)

[Careers](#)

[Contact Us](#)

#### B2B DATABASE

[Our Data](#)

[Data Transparency](#)

[Update Your Company](#)

[Claim Profile](#)

[Browse Directories](#)

#### MORE RESOURCES

[ZoomInfo Videos](#)

[Newsroom](#)

[Engineering Blog](#)

[COVID-19 Newsfeed](#)

[Recipes for Success](#)

[Privacy Center](#)

[Login](#)

4/29/2021

866.904.9666

© 2021 ZoomInfo Technologies LLC

[Privacy Policy](#)

[Terms of Use](#)

[Cookies](#)

[Status](#)

[Do Not Sell My Personal Information](#)



## Exhibit D



# Privacy Statement – California

This PRIVACY STATEMENT FOR CALIFORNIA RESIDENTS supplements the information contained in the [ZoomInfo Privacy Policy](#). ZoomInfo has adopted this statement to comply with the California Consumer Privacy Act of 2018 (the “CCPA”) and other California privacy laws, and it applies solely to “consumers” as that term is defined in the CCPA. Any terms defined in the CCPA have the same meaning when used in this statement.

## Information ZoomInfo Collects

ZoomInfo collects personal information. We have collected the categories of personal information indicated below within the last twelve (12) months:

- Identifiers
  - Personal Information Collected:
    - Name
    - Internet Protocol address
    - Business email address
    - Job title and department
    - Business phone numbers (general, direct and fax)
    - Business related postal address of consumer
    - Social Networking URLs
  - Categories of Sources from which this Personal Information was Collected:
    - Publicly available information
    - First-hand research

- Submissions from ZoomInfo's customers or freemium product users
- Third-party data vendors
- Directly and indirectly from activity on ZoomInfo's website
- Directly and indirectly from our customers or their representatives
- Directly from vendors and other contractual counterparties
- Through communications with prospective customers and other businesses and their representatives
- Purpose for Collection of this Personal Information:
  - To fulfill or meet the purpose for which the information is provided.
  - To provide the consumer with information, products or services that the consumer requests from ZoomInfo.
  - To provide the consumer with email alerts, event registrations and other notices concerning ZoomInfo products or services, or events or news, that may be of interest to the consumer.
  - To carry out ZoomInfo's obligations and enforce ZoomInfo's rights arising from any contracts entered into between ZoomInfo and a ZoomInfo customer or other contractual counterparty, including for billing and collections.
  - To improve ZoomInfo's website and present its contents to the consumer.
  - For testing, research, analysis and product development.
  - As necessary or appropriate to protect the rights, property or safety of ZoomInfo, our customers or others.
  - To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
  - As described to the consumer when collecting such consumer's personal information or as otherwise set forth in the CCPA.



- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of ZoomInfo's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by ZoomInfo is among the assets transferred.
- To modify, enhance, or improve ZoomInfo's services and/or provision such services to ZoomInfo customers.
- To include in ZoomInfo's database of business contacts, which ZoomInfo licenses to its customers for such customers to use for business-to-business sales and marketing and recruiting.
- Categories of Third Parties with whom this Personal Information is Shared:
  - ZoomInfo affiliates
  - Service Providers
  - ZoomInfo customers
- Personal Information Categories Listed in the California Customer Records Statute
  - Personal Information Collected:
    - Name
    - Business address
    - Business telephone number
    - Employment
    - Employment status
  - Categories of Sources from which this Personal Information was Collected:
    - Publicly available information.
    - First-hand research.
    - Submissions from ZoomInfo's customers or freemium product users.

- Third-party data vendors.
- Directly and indirectly from activity on ZoomInfo's website.
- Directly and indirectly from our customers or their representatives.
- Directly from vendors and other contractual counterparties.
- Through communications with prospective customers and other businesses and their representatives.
- Purpose for Collection of this Personal Information:
  - To fulfill or meet the purpose for which the information is provided.
  - To provide the consumer with information, products or services that the consumer requests from ZoomInfo.
  - To provide the consumer with email alerts, event registrations and other notices concerning ZoomInfo products or services, or events or news, that may be of interest to the consumer.
  - To carry out ZoomInfo's obligations and enforce ZoomInfo's rights arising from any contracts entered into between ZoomInfo and a ZoomInfo customer or other contractual counterparty, including for billing and collections.
  - To improve ZoomInfo's website and present its contents to the consumer.
  - For testing, research, analysis and product development.
  - As necessary or appropriate to protect the rights, property or safety of ZoomInfo, our customers or others.
  - To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
  - As described to the consumer when collecting such consumer's personal information or as otherwise set forth in the CCPA.
  - To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of ZoomInfo's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar



proceeding, in which personal information held by ZoomInfo is among the assets transferred.

- To modify, enhance, or improve ZoomInfo's services and/or provision such services to ZoomInfo customers.
- To include in ZoomInfo's database of business contacts, which ZoomInfo licenses to its customers for such customers to use for business-to-business sales and marketing and recruiting.
- Categories of Third Parties with whom this Personal Information is Shared:
  - ZoomInfo affiliates
  - Service Providers
  - ZoomInfo customers
- Internet or Other Similar Network Activity
  - Personal Information Collected:
    - Information on a consumer's interaction with a website, application, or advertisement
    - Internet Protocol address
  - Categories of Sources from which this Personal Information was Collected:
    - Directly and indirectly from activity on ZoomInfo's website.
    - Directly and indirectly from our customers or their representatives.
    - Through communications with prospective customers and other businesses and their representatives.
  - Purpose for Collection of this Personal Information:
    - To carry out ZoomInfo's obligations and enforce ZoomInfo's rights arising from any contracts entered into between ZoomInfo and a ZoomInfo customer or other contractual counterparty, including for billing and collections.

- To improve ZoomInfo's website and present its contents to the consumer.
- For testing, research, analysis and product development.
- As necessary or appropriate to protect the rights, property or safety of ZoomInfo, our customers or others.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to the consumer when collecting such consumer's personal information or as otherwise set forth in the CCPA.
- To modify, enhance, or improve ZoomInfo's services and/or provision such services to ZoomInfo customers.
- Categories of Third Parties with whom this Personal Information is Shared:
  - ZoomInfo affiliates
  - Service Providers
- Professional or Employment-Related Information
  - Personal Information Collected:
    - Business email
    - Business telephone number
    - Business physical address
    - Current or past job history
    - Title
  - Categories of Sources from which this Personal Information was Collected:
    - Publicly available information.
    - First-hand research.
    - Submissions from ZoomInfo's customers or freemium product users.
    - Third-party data vendors.



- Directly and indirectly from activity on ZoomInfo's website.
- Directly and indirectly from our customers or their representatives.
- Directly from vendors and other contractual counterparties.
- Through communications with prospective customers and other businesses and their representatives.
- Purpose for Collection of this Personal Information:
  - To fulfill or meet the purpose for which the information is provided.
  - To provide the consumer with information, products or services that the consumer requests from ZoomInfo.
  - To provide the consumer with email alerts, event registrations and other notices concerning ZoomInfo products or services, or events or news, that may be of interest to the consumer.
  - To carry out ZoomInfo's obligations and enforce ZoomInfo's rights arising from any contracts entered into between ZoomInfo and a ZoomInfo customer or other contractual counterparty, including for billing and collections.
  - To improve ZoomInfo's website and present its contents to the consumer.
  - For testing, research, analysis and product development.
  - As necessary or appropriate to protect the rights, property or safety of ZoomInfo, our customers or others.
  - To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
  - As described to the consumer when collecting such consumer's personal information or as otherwise set forth in the CCPA.
  - To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of ZoomInfo's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar



proceeding, in which personal information held by ZoomInfo is among the assets transferred.

- To modify, enhance, or improve ZoomInfo's services and/or provision such services to ZoomInfo customers.
- To include in ZoomInfo's database of business contacts, which ZoomInfo licenses to its customers for such customers to use for business-to-business sales and marketing and recruiting.
- Categories of Third Parties with whom this Personal Information is Shared:
  - ZoomInfo affiliates
  - Service Providers
  - ZoomInfo customers

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing prior notice.

## Disclosure or Sale of Personal Information and the Right to Opt-Out

We sell personal information collected for our database to our customers. This database may contain information about consumers' business personas including name, employer, job title, email address, phone number, office address, social media or professional profile link, and work or educational history. This information is sold to ZoomInfo's customers for the purpose of business-to-business sales and marketing and recruiting and is provided subject to license agreements that limit its use to those purposes.

A consumer has the right to opt out of the sale of that consumer's personal information by ZoomInfo by visiting our [Privacy Center](#) and submitting a request to remove the consumer's profile or delete the consumer's data. A consumer may also contact us by calling 833-901-0859 or by email to [privacy@zoominfo.com](mailto:privacy@zoominfo.com). In order to submit a request, a consumer or an authorized agent will be required to demonstrate that such person has control of an email inbox associated with the profile in question. If such person cannot,



then we may be contacted regarding other means of verifying such person's identity or the authorization of a third party to exercise a consumer's rights on that consumer's behalf.

In the preceding twelve (12) months, we have sold or disclosed the following categories of personal information for a business purpose:

Category A: Identifiers

Category A: California Customer Records personal information categories.

Category I: Professional or employment-related information.

For avoidance of doubt, the personal information disclosed and/or sold by ZoomInfo within the identified categories is limited to business contact information related to a consumer's profile as an employee of its employer. No sensitive personal information (i.e. Social Security number, passport number, medical or financial information) is collected, shared, disclosed, or sold by ZoomInfo.

We do not sell the personal information of minors under 16 years of age.

## A Consumer's Other CCPA Rights and Choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes a consumer's CCPA rights and explains how to exercise those rights.

### Access to Specific Information and Data Portability Rights

A consumer has the right to request that we disclose certain information to that consumer about ZoomInfo's collection and use of that consumer's personal information over the past 12 months. Once we receive and confirm a consumer's verifiable consumer request, we will disclose:

- The categories of personal information we collected about that consumer.
- The categories of sources for the personal information we collected about that consumer.
- Our business or commercial purpose for collecting or selling that personal

- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about that consumer (also called a data portability request).

## Deletion Request Rights

A consumer has the right to request that ZoomInfo delete any of its personal information that we have collected and retained, subject to certain exceptions. Once we receive and confirm a consumer's verifiable consumer request, we will delete (and direct our service providers and/or customers to delete) that consumer's personal information from our records, unless an exception applies.

We may deny a consumer's deletion request if retaining the information is necessary for us or our service providers or customers to:

- 1 Complete the transaction for which we collected the personal information, provide a good or service that a consumer requested, take actions reasonably anticipated within the context of our ongoing business relationship with that consumer, or otherwise perform our contract with that consumer.
- 2 Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- 3 Debug products to identify and repair errors that impair existing intended functionality.
- 4 Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- 5 Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
- 6 Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if a consumer previously provided informed consent.



- 7 Enable solely internal uses that are reasonably aligned with consumer expectations based on a consumer's relationship with us.
- 8 Comply with a legal obligation.
- 9 Make other internal and lawful uses of that information that are compatible with the context in which a consumer provided it.

## Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Calling us at 833-901-0859.
- Visiting [Privacy Center](#)
- Contacting us at [privacy@zoominfo.com](mailto:privacy@zoominfo.com)

Only a consumer or a person registered with the California Secretary of State that a consumer authorizes to act on a consumer's behalf, may make a verifiable consumer request related to a consumer's personal information. A consumer may also make a verifiable consumer request on behalf of that consumer's minor child.

A consumer may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows ZoomInfo to reasonably verify a consumer is the person about whom we collected personal information or an authorized representative.
- Describe a consumer's request with sufficient detail that allows ZoomInfo to properly understand, evaluate, and respond to it.

We cannot respond to a consumer's request or provide a consumer with personal information if we cannot verify the consumer's identity or authority to make the request and confirm the personal information relates to that consumer. Making a verifiable consumer request does not require a consumer to create an account with us. We will only use personal information provided in

a verifiable consumer request to verify the requestor's identity or authority to make the request.

## Response Timing and Format

We endeavor to respond to a verifiable consumer request within 45 days of its receipt. If we require more time (up to 90 days), we will inform the consumer of the reason and extension period in writing. We will deliver our written response by mail or electronically. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide a consumer's personal information that is readily useable and should allow a consumer to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to a consumer's verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell the consumer why we made that decision and provide the consumer with a cost estimate before completing that consumer's request.

## Non-Discrimination

We will not discriminate against a consumer for exercising any CCPA rights.

## Changes to Our Privacy Statement

We reserve the right to amend this privacy statement at our discretion and at any time. When we make changes to this privacy statement, we will provide notification by email or through a notice on our website homepage.

## §999.317(g)(1) Metrics

During the previous calendar year, ZoomInfo received the following number of requests from residents of California:

--	--	--	--



The number of requests to know that the business received, complied with in whole or in part, and denied;	N/A*	N/A*	N/A*
The number of requests to delete that the business received, complied with in whole or in part, and denied;	N/A*	N/A*	N/A*
The number of requests to opt-out that the business received, complied with in whole or in part, and denied;	N/A*	N/A*	N/A*

\*The Effective Date of the CCPA is January 1, 2020 and, therefore, we do not have prior year metrics at this time.

We anticipate our median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out will be three (3) business days based on similar operations, however, given the effective date of the CCPA, we do not have these metrics at this time.

## Contact Information

If there are any questions or comments about this statement, our [Privacy Policy](#), the ways in which we collect and use a consumer's personal information, how to receive a copy of the Privacy Policy and/or this statement in an alternative format (for consumers with a disability), a consumer's choices and rights regarding such use, or wish to exercise consumer rights under California law, please do not hesitate to contact us at:

ZoomInfo

Attn: Privacy

805 Broadway, Suite 900

Vancouver, WA 98660

Phone: 360-718-5630

Email: [privacy@zoominfo.com](mailto:privacy@zoominfo.com)

*This statement was last updated on November 20, 2019.*



Free Trial

#### POPULAR FEATURES

[Sales Solutions](#)

[Marketing Solutions](#)

[Company Contact Search](#)

[Buyer Intent Data](#)

[CRM Lead Enrichment](#)

#### COMPANY

[About Us](#)

[Our Leadership](#)

[Investor Relations](#)

[FAQs](#)

[Careers](#)

[Contact Us](#)

#### B2B DATABASE

[Our Data](#)

[Data Transparency](#)

[Update Your Company](#)

[Claim Profile](#)

[Browse Directories](#)

#### MORE RESOURCES

[ZoomInfo Videos](#)

[Newsroom](#)

[Engineering Blog](#)

[COVID-19 Newsfeed](#)

[Recipes for Success](#)

[Privacy Center](#)

[Login](#)

[866.904.9666](#)

© 2021 ZoomInfo Technologies LLC

[Privacy Policy](#)

[Terms of Use](#)

[Cookies](#)

04/29/2021

Status

Do Not Sell My Personal Information



## Exhibit E



# ZoomInfo Privacy Policy



Updated: March 22, 2021

**ZoomInfo Privacy Policy** – ZoomInfo understands that you care about how information about you is used. This privacy policy (the “Policy”) explains how we collect information pertaining to businesses and business people (“Business Information”) and all other types of information through our website and online services (the “Site”); how we maintain, use and share that information; and how you can manage the way information about you is handled.

“ZoomInfo” for purposes of this Privacy Policy includes DiscoverOrg Data, LLC, a Delaware limited liability company, and its affiliates, including Zoom Information, Inc.

For individuals residing in the EEA or Switzerland, please [click here](#) to find out more information.

For residents of the State of California, please [click here](#) to find out more about your rights under the California Consumer Privacy Act of 2018 (“CCPA”).

## Where does ZoomInfo get the Business Information for its Public Profiles?

ZoomInfo creates profiles of business people and companies, which we call “Public Profiles,” from different sources. Once we have collected Business Information about a person or company, we combine multiple mentions of the same person or company into a Public Profile. The resulting directory of Public Profiles (the “Directory”) is then made available to the users of the Site and our customers and strategic partners.

ZoomInfo obtains the data for its Public Profiles in several ways including:

- 1 Our search technology scans the web and gathers publicly-available information.
- 2 We license information from other companies.
- 3 Users contribute Business Information about themselves or other people and companies. (See “ZoomInfo Contact Contributor,” below)
- 4 Through market research surveys and phone interviews conducted by our in-house research team.

## How does the ZoomInfo Community and the ZoomInfo Contact Contributor Work?

ZoomInfo offers a service called ZoomInfo Community. To subscribe to ZoomInfo Community, you are required to install software offered on the Site, known as the ZoomInfo Contact Contributor (the “Software”) or otherwise provide ZoomInfo with access to your email account. When you subscribe to ZoomInfo Community, you allow ZoomInfo to access certain Business Information stored by the application that your computer uses to manage your email and contacts, known as an “email client” (e.g., Microsoft Outlook) or stored by a provider of cloud services for email (e.g. Google Apps). If required to access this Business Information stored on your computer’s email and contact application(s), you may need to provide ZoomInfo with the necessary username and password information. We use this Business Information to improve the size and quality of our Directory. In exchange for allowing this access, you receive a subscription to ZoomInfo Community at no charge under specified terms and conditions (available at [/about-zoominfo/ce-terms-conditions](#)).

From the contacts within your email client and “signatures” within email messages, we collect the following Business Information, if available, for each person:

- Name
- Email address
- Job title and department
- Business phone numbers (general, direct and fax)
- Company name
- Postal address of company
- Business related postal address of person



- Corporate website URLs
- Social Networking URLs

From the headers of your emails, we collect:

- The date the email message was sent or received
- Email addresses, names and job titles of recipients and senders

To ensure the integrity of the Directory, we take the following steps:

- Business Information Only – ZoomInfo only wants business-related information. Therefore, any contacts that have an address from a consumer-oriented service such as Gmail, Hotmail or Yahoo are disregarded.
- Unattributed – We do not disclose who contributed particular Information using the ZoomInfo Contact Contributor software or other contribution methods. (The only exceptions: See “Disclosures to Service Providers,” “Disclosures for Legal Reasons,” and “Disclosures to a Buyer of the Company,” below.)
- Opt Out – Anyone added to the Directory may request to be removed at any time, via email, web or a toll-free number. We promptly honor such requests.

ZoomInfo does not “read” the content of your email messages; our technology automatically extracts from the messages only the data we describe in this Policy. We do not collect data from custom fields or notes in your email client.

Information from your email client will continue to be shared as described above as long as the Software remains installed. If you choose to stop sharing Information from your email client with ZoomInfo, you can uninstall the Software at any time following the instructions at [/cefaq](#). You may not, however, retroactively “unshare” the Business Information you have already made available to ZoomInfo.

## How else does ZoomInfo Collect and Use Information?

Visitors to our Site may choose to submit their name, email address and/or other information so that they can learn more about our services, register to take part in a ZoomInfo-sponsored event, or participate in a survey, contest or sweepstakes, among other things. By accessing, using, and/or submitting information through the Site, you consent to the practices described in this Policy with regard to the information collected thereby as described herein. If you do not agree with this Policy, you must delete all cookies from your browser cache after visiting the Site and refrain from visiting or using the Site.

In order to use certain ZoomInfo products and services, you may be required to register as a user. From time to time, we may use your email address to send you information and keep you informed of products and services in which you might be interested. You will always be provided with an opportunity to opt out of receiving such emails. Your contact information may also be used to reach you regarding issues concerning your use of our Site, including changes to this Policy. A more detailed description of how we may collect and use customer information is found below under “Customer Information Collected.”

If you choose to use our referral service to invite a friend to join ZoomInfo, we will ask you for your friend’s name and email address. We will automatically send your friend a one-time email inviting him or her to visit the Site. ZoomInfo will use this information for the sole purpose of sending this one-time email and will not store your friend’s name or email address.

ZoomInfo may aggregate collected information about our users in a form that does not allow users to be personally identified for the purpose of understanding our customer base and enhancing the services that we and our strategic partners and customers can provide you.

If you purchase one of our online subscription-based services, you will need to provide credit card information. We will use that information solely for the purpose of fulfilling your ZoomInfo purchase request. We will store credit card information in an encrypted form and will not sell, share or use it again without your prior consent. (The only exceptions are described in the sections below on “Disclosures to Service Providers,” “Disclosures for Legal Reasons,” and “Disclosures to a Buyer of the Company”).

ZoomInfo will use personal information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual about whom the information pertains. ZoomInfo will take reasonable steps to ensure that personal information is relevant to its intended use, accurate, complete and current.

We also collect information using cookies, as described below.

## Cookies

Most websites, including our Site, use a feature of your browser to set a small text file called a “cookie” on your computer. The site placing the cookie on your computer can then recognize the computer when you revisit the site to allow auto log in and track how you are using the site. When you visit our Site, our servers and/or those of our service providers automatically record certain information that your web browser sends, such as your web request, Internet Protocol address, browser type, referring/exit pages and URLs, number of clicks, domain names, landing pages, pages viewed, time and date of use and other information.

We may link this information to information that you submit while on our Site, which does allow you to be personally identified.

You are free to decline cookies. You can configure your browser to accept all cookies, reject all cookies, erase cookies or notify you when a cookie is set. Electing to reject or disable cookies may substantially limit your ability to use our Site.



ZoomInfo may adopt other technologies that serve similar functions as cookies. If we do so, we will disclose it in this Policy.

## Third Party Cookies

The use of cookies and similar technologies by our partners, affiliates, tracking utility company, service providers is not covered by this Policy. We do not have access or control over these cookies. Our partners, affiliates, tracking utility company and service providers may use session ID cookies in order to:

- personalize your experience
- analyze which pages our visitors visit
- provide website feature such as social sharing widgets
- measure advertising effectiveness
- track which areas of our site you visit; in order to remarket to you after you leave

To disable or reject third-party cookies, please refer to the third-party's relevant website.

## Google Analytics

We use Google Analytics, a web analytics service provided by Google, Inc., on our Site. Google Analytics uses cookies or other tracking technologies to help us analyze how users interact with and use the Site, compile reports on the Site's activity, and provide other services related to Site activity and usage. The technologies used by Google may collect information such as your IP address, time of visit, whether you are a return visitor, and any referring website. The Site does not use Google Analytics to gather information that personally identifies you. The information generated by Google Analytics will be transmitted to and stored by Google and will be subject to Google's privacy policies. To learn more about Google's partner services and to learn how to opt out of tracking of analytics by Google click [here](#).

## Do Not Track Signals

Your browser or device may include 'Do Not Track' functionality. Our information collection and disclosure practices, and the choices that we provide to visitors, will continue to operate as described in this Policy, whether or not a Do Not Track signal is received.

## Web beacons

Our Site contains electronic images known as "web beacons" (sometimes called single-pixel gifs) and are used along with cookies to compile aggregated statistics to analyze how our site is used and may be used in some of our emails to let us know which emails and links have been opened by recipients. This allows us to gauge the effectiveness of our customer communications and marketing campaigns.

## Customer Information Collected

ZoomInfo may collect the following information from or regarding its customers: (1) personal contact information regarding users of the Services ("User Information"); (2) information uploaded to our system by a user of the Services ("Uploaded Information"); (3) and usage logs regarding the use of the Site, including logins and other actions taken, time stamps, IP address, and other usage data ("Usage Logs") (collectively, "Customer Information").

You may be a user that has been provided access to the Site through your company license agreement. Your employer may require that one or more users have global rights to access any and all information of every user that has access through the company. If you have questions or concerns regarding the rights of other individuals in your company to access your User Information, Uploaded Information, or Usage Logs, you should raise those concerns with the appropriate person at your company.

## Use of Customer Information

Customer Information may be used for ZoomInfo's legitimate business interests in connection with your use of the Site, including to respond to user inquiries and fulfill user requests, complete transactions, provide customer service, send administrative information, and to personalize user experience with the Site. We may use Customer Information to better understand our users in general and to improve the content and functionality of the Site. We may use Customer Information to contact you in the future to tell you about services, promotions, opportunities, and other general information about ZoomInfo we believe will be of interest to you. We may use Customer Information to investigate and prosecute potential breaches of ZoomInfo's security or license agreements.

ZoomInfo will not disclose Customer Information to any third party except in connection with a legitimate use as set forth herein, in connection with a bona fide legal dispute to which such information is relevant, in response to valid, compulsory legal process, or as otherwise required by law. ZoomInfo will, whenever possible, obtain confidentiality agreements from any person or entity to whom Customer Information is disclosed and ensure any recipients are committed to employing appropriate technological security measures.

ZoomInfo employs reasonable security and back-up procedures to protect Customer Information. However, in the unlikely event there is a loss or corruption of Customer Information, ZoomInfo is not responsible or liable for such loss or corruption. We encourage our users to



retain copies of all Uploaded Information on their own system.

## Customer Use of ZoomInfo Integrations

As part of the Site, ZoomInfo may make available to its customers certain "Integrations". In using ZoomInfo's Integrations, such as ZoomInfo's SFNA and web browser extensions, Business Information from customer's CRM, MAT, or sales enablement software may be transmitted to ZoomInfo for purposes of matching or cleansing customer's data against ZoomInfo's database as a feature of the Site. In that event, ZoomInfo may retain and store such Business Information for purposes of identifying potential contacts to supplement the Site, verifying the accuracy of such Business Information, removing out-of-date Business Information from the Site, or otherwise improving ZoomInfo's research processes and the content provided through the Site. Information so received will not be attributable to the source. In the event that any customer wishes to opt out of ZoomInfo's use of such information, they may do so by visiting the 'Privacy Center' within the ZoomInfo Salesforce Native Application and adjusting the appropriate controls.

## When does ZoomInfo Share Information?

### Disclosures of Public Profiles

We may make any Business Information that our users contribute for inclusion in our Directory, that we collect from public web sources or that we license from third parties available to users of the Site, to our strategic partners and to our customers.

### Disclosures to Service Providers

ZoomInfo may from time to time disclose Business Information or other collected information to service providers, solely for providing functions related to our operation of the Site and for no other purpose. For example:

- ZoomInfo uses service providers to process credit card payments on our Site. When you use a credit card to pay for ZoomInfo services, information such as your name, billing address, phone number, email address and credit card information will be submitted to service providers for verification and to manage any recurring payments.
- ZoomInfo uses software hosted by a service provider to provide us with information regarding our visitors' activities on our Site. When you visit our Site, that service provider may set cookies on our behalf and may receive information about your browsing activity on our Site.

### Disclosures for Legal Reasons

We may disclose collected information, including Business Information, to a third party if we believe in good faith that such disclosure is necessary or desirable:

(i) to comply with lawful requests, subpoenas, search warrants or orders by public authorities, including to meet national security or law enforcement requirements, (ii) to address a violation of the law, (iii) to protect the rights, property or safety of ZoomInfo, its users or the public, or (iv) to allow ZoomInfo to exercise its legal rights or respond to a legal claim.

### Disclosures to a Buyer of the Company

If our company or substantially all of our assets are acquired, or in the event of a merger or bankruptcy, information about you and/or information you provide to ZoomInfo may be among the transferred assets. You will be notified via email and/or a prominent notice on our Site of any change in ownership or uses of your personal information, as well as any choices you may have regarding your personal information.

### Other Disclosures

If you register for a ZoomInfo event with a third-party speaker, your information will generally be shared with the speaker.

If you provide information, including Business Information, in creating or updating your Public Profile, that information will be included in the Directory and thus can be viewed by third parties.

We post customer testimonials on our Site which may contain the customer's name. We always get consent from the customer prior to posting any testimonial. If you wish to update or delete your testimonial, you can contact us at [privacy@zoominfo.com](mailto:privacy@zoominfo.com).

Our Site offers publicly accessible blogs or community forums. You should be aware that any content you provide in these areas may be read, collected, and used by others who access them. You can request the removal of your personal information from our blog or community forum, by contacting us at [privacy@zoominfo.com](mailto:privacy@zoominfo.com). In some cases, we may not be able to remove your personal information, in which case we will let you know if we are unable to do so and why.

ZoomInfo may have liability to you in case of failure to comply with the law or this Policy in handling onward transfer of your Information to third parties.

## How Can You Change or Delete Your Information?

### Professional Profiles



To find out if you are in the ZoomInfo database, [search for your first name and last name](#) on the ZoomInfo home page. If you have a common name, you can limit your search based on geographical location or companies where you have worked.

Once you have located one or more ZoomInfo profiles in your name, consider these options for managing your professional profile on ZoomInfo:

### Update Your Own Professional ZoomInfo Profile

Make sure your ZoomInfo profile is up to date for recruiters and others who may want to reach you. Simply, verify your ZoomInfo profile and you can update your work history, contact information and even delete web references you do not want associated with your professional profile. You can also consolidate multiple ZoomInfo profiles in your name to create a comprehensive snapshot of your professional background. Please [Click here](#) to view, verify and update your ZoomInfo Directory profile.

### Remove Your ZoomInfo Profile Completely

If you wish to completely remove your existing individual profile from the Directory, please visit [Remove Your Zoominfo Professional Profile](#) or email [remove@zoominfo.com](mailto:remove@zoominfo.com). If you make this choice, your name, employment history, web references and contact information (including email address) will be removed from our search results as soon as possible.

## Company Profiles

To find out if your company is in the ZoomInfo database, [search for your organization](#) on the ZoomInfo home page. Once you have located the ZoomInfo profile, consider these options for managing your company profile on ZoomInfo:

### Update Your Company Profile on ZoomInfo

Simply, verify your ZoomInfo company profile to update your company description, industry, company location, and more. You can also consolidate multiple ZoomInfo profiles to create a comprehensive snapshot of your company. Please [click here](#) to view, verify and update your ZoomInfo company profile.

### Remove Your Company ZoomInfo Profile Completely

ZoomInfo is a specialized web search engine, similar to Google but focused on finding information about companies and professionals. We gather all information about companies from corporate web sites, press releases, and/or SEC documents filed with the US government. The company summaries are created automatically by ZoomInfo's software based on the information we find on those documents.

*As a company policy, ZoomInfo does not remove company information from our search engine. If any of the company information is incorrect, please update your company profile.*

If any of the company information is incorrect, please update your company profile.

## Data Retention

We will retain your information for a period of time consistent with the original purpose(s) for which we collected it, as described in this Privacy Policy. We will retain your information (i) for as long as we have an ongoing relationship with you and as needed to provide you services; (ii) as necessary to comply with our legal obligation(s); (iii) as necessary to resolve disputes or to protect ourselves from potential future disputes; or (iv) as necessary to enforce our agreements. Retention periods will be determined taking into account the amount, nature and sensitivity of your information and the purpose(s) for which it was collected. After the retention period ends, we will delete your information. Where we are unable to do so, we will ensure that appropriate measures are put in place to prevent any further use of your information.

## How Can You Opt Out of Certain Uses of Your Information?

ZoomInfo gives you the opportunity to "opt out" of having your information used for certain purposes.

If you no longer wish to receive our newsletter and promotional communications, you may opt-out of receiving them by following the instructions included in each newsletter or communication or by visiting [/unsubscribe](#). After we receive your request, we will send you an email message to confirm that you have been unsubscribed.

ZoomInfo will not share information about you that you submit when you register for our services with third parties for promotional uses unless you opt in to such sharing within your ZoomInfo account or ZoomInfo has separately acquired such information from other sources, in which case ZoomInfo will give you the opportunity to opt out via email.

If you have registered for a ZoomInfo account and opted in to share your personal information with ZoomInfo subscribers, you may opt out by signing in to your ZoomInfo account and changing your preferences by clicking "Edit" next to your contact information on the Profile page.

If you have subscribed to ZoomInfo Community and opted in to share your business contacts with ZoomInfo in exchange for free access to our premium services, you may opt out of any further sharing of business contacts by uninstalling the Software, as described on [/cefaq](#). If you uninstall the Software, your subscription to ZoomInfo Community will immediately expire and ZoomInfo will no longer collect Business Information from you through this method (however, you will not be able to 'unshare' the Business Information you have previously provided to ZoomInfo).



You may also communicate your opt-out request to ZoomInfo by telephone or postal mail by using the contact information at the bottom of this Policy.

## How Do We Keep Your Information Secure?

The security of your information is important to us. When you enter sensitive information (such as a credit card number) on our registration forms, we encrypt that information using secure socket layer technology (SSL).

We follow generally accepted industry standards to protect the information submitted to us, both during transmission and once we receive it. However, no method of Internet transmission or electronic storage is 100% secure. Therefore, while we strive to use commercially acceptable means to protect your information, we cannot guarantee its absolute security.

## Links to Other Sites

This Site contains links to other sites that are not owned or controlled by ZoomInfo. We are not responsible for the privacy practices of such other sites. We encourage when you leave our Site to be aware and to read the privacy statements of each and every web site that collects personally identifiable information. This Policy applies only to information collected by this Site or in the method(s) otherwise discussed herein.

## Social Media Widgets

Our Site includes social media features, such as the Facebook "Like" button and "Widgets", such as the "Share" button or interactive mini-programs that run on our Site. These features may collect your IP address, which page you are visiting on our site, and may set a cookie to enable the feature to function properly. Social media features and widgets are either hosted by a third party or hosted directly on our Site. Your interactions with these features are governed by the privacy policy of the company providing it.

## EU Residents

In the course of obtaining data to be included on the Site, if ZoomInfo obtains business contact information regarding an individual that ZoomInfo has reason to believe is based in the European Union, ZoomInfo will provide such individual with a notice detailing the information ZoomInfo has on such person, the purpose for which it will be used, and informing such person of their rights with respect to such information, including the right to know what information ZoomInfo possesses on them, to correct such information, or to opt out of data collection entirely. Such persons may opt out of the ZoomInfo database by visiting </update/remove> or emailing [remove@zoominfo.com](mailto:remove@zoominfo.com).

## Information for Users in Europe and Elsewhere Outside the U.S.

If you use our Site outside of the United States, you understand that we may collect, process, and store your personal information in the United States and other countries. The laws in the U.S. regarding personal information may be different from the laws of your state or country. Any such transfers will comply with safeguards as required by relevant law.

Users in the European Union (EEA) and Switzerland: If you are a resident of the EEA or Switzerland, the following information applies.

Purposes of processing and legal basis for processing: As explained above, we process personal data in various ways depending upon your use of our Sites. We process personal data on the following legal bases:

- 1 with your consent;
- 2 as necessary to perform our agreement to provide Services; and
- 3 as necessary for our legitimate interests in providing the Sites where those interests do not override your fundamental rights and freedom related to data privacy.

ZoomInfo's collection of Business Information, and the creation and licensing of ZoomInfo's Public Profiles and Directory, are within ZoomInfo's legitimate interests to organize and make available business contact information given the limited impact of this data on an individual's private life and that this information, unlike personal contact details, is widely disclosed. ZoomInfo has put in place safeguards to protect personal privacy and individual choice, including disclosures of its data processing activities, the use of consent or opt-outs wherever possible, and the implementation of a privacy center: </about-zoominfo/privacy-center>.

Right to lodge a complaint: Users that reside in the EEA or Switzerland have the right to lodge a complaint about our data collection and processing actions with the supervisory authority concerned. Contact details for data protection authorities are available [here](#).

Transfers: Personal information we collect may be transferred to, and stored and processed in, the United States or any other country in which we or our affiliates or subcontractors maintain facilities. Per the applicable requirements of the General Data Protection Regulation (GDPR), we will ensure that transfers of personal information to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. Please see "Privacy Shield Frameworks" below regarding our compliance with the EU- and Swiss-US Privacy Shields.



Individual Rights: If you are a resident of the EEA or Switzerland, you are entitled to the following rights under the GDPR. **Please note:** In order to verify your identity, we may require you to provide us with personal information prior to accessing any records containing information about you.

- The right to access and correction. You have the right to request access to, and a copy of, your personal data at no charge, as well as certain information about our processing activities with respect to your data. You have the right to request correction or completion of your personal data if it is inaccurate or incomplete. You have the right to restrict our processing if you contest the accuracy of the data we hold about you, for as long as it takes to verify its accuracy.
- The right to request data erasure. You have the right to have your data erased from our Site if the data is no longer necessary for the purpose for which it was collected, you withdraw consent and no other legal basis for processing exists, or you believe your fundamental rights to data privacy and protection outweigh our legitimate interest in continuing the processing.
- The right to object to our processing. You have the right to object to our processing if we are processing your data based on legitimate interests or the performance of a task in the public interest as an exercise of official authority (including profiling); using your data for direct marketing (including profiling); or processing your data for purposes of scientific or historical research and statistics.

## The General Data Protection Regulation (“GDPR”) 2016/679

ZoomInfo endeavors to comply with the provisions of the GDPR as to any information in its possession regarding European Union-based persons (“data subjects”). As such, ZoomInfo only processes personal information on data subjects where it has a lawful basis to do so, which may include the consent of the person (especially in the case of website visitors who provide their information), performance of a contract, compliance with a legal obligation, or the legitimate interest of the controller or a third party. ZoomInfo provides notice to all data subjects as required by GDPR Article 13 or 14, as appropriate, and honors the rights of data subjects provided in Articles 12–23, including the right to be forgotten. For any opt-out requests or other inquiries related to privacy, please visit our privacy center at [/about-zoominfo/privacy-center](#) or email [remove@zoominfo.com](mailto:remove@zoominfo.com).

## Privacy Shield Frameworks

While ZoomInfo continues to be certified by and adhere to the principles of the Privacy Shield Frameworks, in light of Court of Justice of the European Union decisions regarding the legal effect of the EU-US Privacy Shield Framework, ZoomInfo does not rely upon the framework to ensure the lawful transfer of data from EEA to non-EEA countries.

ZoomInfo complies with the EU-US Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. ZoomInfo has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the policies in this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, any rights you may have to binding arbitration before a Privacy Shield Panel, and to view our certification page, please visit <https://www.privacyshield.gov>.

For information received under the Privacy Shield, ZoomInfo and Datanyze will require third parties to whom they disclose personal information to safeguard that personal information consistent with this Policy by contract, obligating those third parties to provide at least the same level of protection as is required by the Privacy Shield Principles. EU and Swiss citizens may choose to opt-out of such disclosures. ZoomInfo may have liability to you in case of failure to comply with the law or this policy in handling onward transfer of your information to third parties.

In compliance with the Privacy Shield Principles, ZoomInfo commits to resolve complaints about your privacy and its collection or use of your personal information. European Union or Swiss individuals with inquiries or complaints regarding this Policy should first contact ZoomInfo at [privacy@zoominfo.com](mailto:privacy@zoominfo.com). European Union and Swiss individuals have the right to access their personal data.

ZoomInfo further has committed to refer unresolved privacy complaints under the Privacy Shield Principles to JAMS (Judicial Arbitration & Mediation Services), an independent alternative dispute resolution provider located in the United States and recognized for this purpose by the US Department of Commerce. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit <https://www.jamsadr.com/eu-us-privacy-shield> for more information, and to file a complaint.

The Federal Trade Commission has enforcement authority regarding ZoomInfo’s compliance with the Privacy Shield Principles.

## Your California Privacy Rights

If you are a California resident, California law permits you to request certain information regarding the disclosure of your personal information by us to third parties for the third parties’ direct marketing purposes. To make such a request, please send your request, by mail or email, to the address at the end of this Policy.

## Changes to this Policy

ZoomInfo reserves the right to modify this Policy from time to time, so please review it regularly. If we make material changes to this policy, we will notify you here, by email, and/or by means of a notice on our homepage prior to the changes becoming effective.

## Non-Privacy Shield Related Questions or Complaints

If you have an unresolved privacy data or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at <https://feedback-form.truste.com/watchdog/request>.

## Contact Us


If you have questions or concerns regarding this privacy policy, please contact us at:

ZoomInfo  
Attn: Privacy  
805 Broadway, Suite 900  
Vancouver, WA 98660  
360-718-5630  
Email: [privacy@zoominfo.com](mailto:privacy@zoominfo.com)

## Frequently Asked Questions

Want to learn more about ZoomInfo? Check out some of our FAQs. From trustworthiness and safety, to how we collect data, we are committed to answers your top questions:

- [Is ZoomInfo Trustworthy?](#)
- [Is ZoomInfo Safe?](#)
- [How Does ZoomInfo Get My Information?](#)
- [Read All FAQs](#)



POPULAR FEATURES

[Sales Solutions](#)
[Marketing Solutions](#)
[Company Contact Search](#)
[Buyer Intent Data](#)
[CRM Lead Enrichment](#)

COMPANY

[About Us](#)
[Our Leadership](#)
[Investor Relations](#)
[FAQs](#)
[Careers](#)
[Contact Us](#)

B2B DATABASE

[Our Data](#)
[Data Transparency](#)
[Update Your Company](#)
[Claim Profile](#)
[Browse Directories](#)






MORE RESOURCES

[ZoomInfo Videos](#)
[Newsroom](#)
[Engineering Blog](#)
[COVID-19 Newsfeed](#)
[Recipes for Success](#)
[Privacy Center](#)

[Free Trial](#)

[Login](#)  
866.904.9666

© 2021 ZoomInfo Technologies LLC | [Privacy Policy](#) | [Terms of Use](#) | [Cookies](#) | [Status](#) | [Do Not Sell My Personal Information](#)



## Exhibit F

## Terms and Conditions

I understand and agree that my use of this application is governed by the license terms and conditions available at [discoverorg.com/ltc](https://discoverorg.com/ltc) and the privacy policy available at [discoverorg.com/privacy-policy](https://discoverorg.com/privacy-policy), or by the terms of a separate written agreement between my organization and DiscoverOrg. #####I understand that when using this application, DiscoverOrg will attempt to research and verify business contact information submitted by you through match, cleanse, append, or update requests to supplement, and DiscoverOrg may supplement its database to the extent it is able to verify such information. I understand that DiscoverOrg may also use email deliverability information, on an anonymous basis, to remove out-of-date information from its database.

Close

## Exhibit G

State of California Department of Justice



**XAVIER BECERRA**  
*Attorney General*

# Data Broker Registration for ZoomInfo

**Data Broker Name:**

ZoomInfo

**Email Address (Accessible to the public):**

privacy@zoominfo.com

**Website URL:**

<http://www.zoominfo.com>

**Physical Address:**

805 Broadway

#900

Vancouver, WA 98660

United States

**How a consumer may opt out of sale or submit requests under the CCPA:**

Consumers may manage their data management preferences through our comprehensive privacy center: <https://www.zoominfo.com/about-zoominfo/privacy-center>

**How a protected individual can demand deletion of information posted online under Gov. Code sections 6208.1(b) or 6254.21(c)(1):**

Consumers may manage their data management preferences through our comprehensive privacy center: <https://www.zoominfo.com/about-zoominfo/privacy-center>



**Additional information about data collecting practices:**

Our data collection and management practices can be located here:

<https://www.zoominfo.com/business/about-zoominfo/privacy-policy>

**Date Approved:**

01/29/2020

[Office of the Attorney General](#)

[Accessibility](#)

[Privacy Policy](#)

[Conditions of Use](#)

[Disclaimer](#)

© 2021 DOJ

## Exhibit H

State of California Department of Justice



**OFFICE OF THE**  
*Attorney General*

# Data Broker Registration for Dun & Bradstreet, Inc

**Data Broker Name:**

Dun & Bradstreet, Inc

**Email Address (Accessible to the public):**

PrivacyOfficer@dnb.com

**Website URL:**

<https://www.dnb.com/utility-pages/privacy-policy.html>

**Physical Address:**

103 JFK Parkway

Short Hilla, NJ 07078

United States

**How a consumer may opt out of sale or submit requests under the CCPA:**

A consumer may opt out of sale or submit requests under the CCPA by going to the California Resident Section of our Privacy Notice and filling out the corresponding forms: <https://www.dnb.com/utility-pages/privacy-policy.html#title-twenty>

**How a protected individual can demand deletion of information posted online under Gov. Code sections 6208.1(b) or 6254.21(c)(1):**

A protected individual can demand deletion of their personal information posted online by filling out a Right to Deletion Form, available at: <https://www.dnb.com/utility-pages/privacy-policy.html#title-twenty>

**Additional information about data collecting practices:**

For additional information about our data collection practices, please see: • Our Privacy Notice, available at: <https://www.dnb.com/utility-pages/privacy-policy.html> • The California Resident section of our Privacy Notice, available at: <https://www.dnb.com/utility-pages/privacy-policy.html#title-twenty> If you would like to see the CCPA categories of information we collect, please look under the California Resident section of our Privacy Notice for the text: “Please see below for the categories of personal information about California consumers that we have collected, sold and disclosed for a business purpose over the past 12 months.” And click on “Additional Information”

**Date Approved:**

04/29/2020

[Office of the Attorney General](#)[Accessibility](#)[Privacy Policy](#)[Conditions of Use](#)[Disclaimer](#)

© 2021 DOJ



## Exhibit I

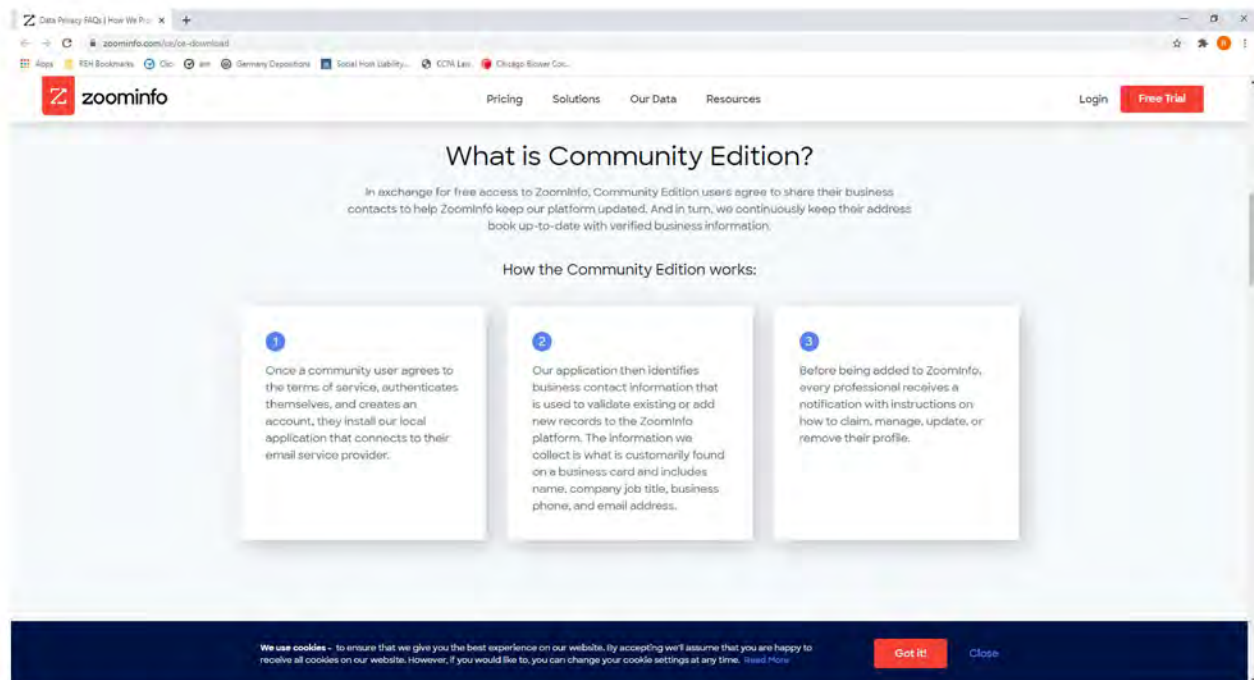


### Data Privacy with Henry Schuck

Hear from our CEO Henry Schuck on what data privacy means to us, and what Zoominfo is doing to stay on the forefront of data privacy in 2020 and

“Data Privacy with Henry Schuck,” available at <https://videos.zoominfo.com/watch/8VPp6w31xTCS17Y1MB3Psx>, minute 3:27 (Visited March 26, 2021).

## Exhibit J



See <https://www.zoominfo.com/ce/ce-download> (Visited March 26, 2021).



## Exhibit K

## Personal Information Notice

This notice is to inform you of the collection, processing, and sale of certain personal information or personal data about you ("personal information"). ZoomInfo is a provider of contact and business persona information regarding business professionals for direct marketing purposes. Our customers are businesses trying to reach business professionals for sales and marketing and recruiting. You can opt out of our database if you want to; the best way to do so is to visit our Privacy Center at <https://www.zoominfo.com/about-zoominfo/privacy-center>. At the Privacy Center you can also submit an access request or review our privacy policy. Please continue reading below for more information about the information we collect, how we gather it, and how it is used and shared.

### Categories of Personal Information Processed

ZoomInfo profiles business organizations and the executives and professionals who work for those organizations. We may have any or all of the following categories of personal information about you, past or current:

- Name
- Company
- Office Address
- Telephone Number
- Email Address
- Job Title
- Job Function and Responsibilities
- Education
- Social Media URL

### Purpose of Processing

ZoomInfo processes this information for direct marketing purposes. The information may be licensed to our customers for their sales, marketing, or recruiting purposes, or to other organizations who may license it to their customers for the same purposes ("partners"). The information is provided to customers or partners subject to restrictive license agreements that limit the use to those specified purposes and prohibits the unauthorized use or transfer of the information. ZoomInfo's customers may obtain the information via password protected account-based access to our database. Our customers, or those of our partners, may use the information to market their services to your employer or to contact you about professional opportunities.

### Lawful Basis

ZoomInfo's processing of your personal information is based on the legitimate interest of itself and its customers to engage in direct marketing.

### Recipients

This personal information may be provided, subject to restrictive license agreements, to ZoomInfo's customers, its partners, or the customers of its partners. These recipients are business organizations who are permitted to use the information only for lawful sales, marketing, and recruiting. The substantive terms of ZoomInfo's license agreements may be reviewed at <https://www.zoominfo.com/business/about-zoominfo/LTC>.

### Period

ZoomInfo endeavors to provide the most accurate information possible to its customers. We seek to verify the accuracy of our information as frequently as

Source: [https://www.reddit.com/r/privacy/comments/hmaanz/zoominfo\\_data\\_collection\\_notice/](https://www.reddit.com/r/privacy/comments/hmaanz/zoominfo_data_collection_notice/)  
(Visited March 26, 2021)

possible and to remove information that we learn to be inaccurate. Thus, we intend to process the information we have about you for so long as it is accurate or until you instruct us to refrain from processing it.

#### Your Rights

You have the right to request that ZoomInfo (1) provide you with access to your personal information, (2) rectify or correct your personal information, (3) erase your personal information, or (4) restrict processing of your personal information, including refraining from selling it or otherwise providing it to any third parties. You also have the right to object to processing, to data portability, and to lodge a complaint with the appropriate supervisory authority in your country, if any. The foregoing rights may be subject to certain limitations pursuant to applicable law.

#### Sources of Personal Information

ZoomInfo gathers personal information from several sources, which include publicly available sources such as websites and government records, contributions from our customers, third party data providers, or through telephone interviews. Because information from several sources may be combined into one record, it may be difficult or impossible to identify the exact source of one particular piece of information.

#### Who We Are

ZoomInfo is ZoomInfo Technologies LLC, and we are located at 805 Broadway St, Suite 900, Vancouver, WA 98660. ZoomInfo is a registered data broker in the State of California.

To opt out or for more information, please visit our Privacy Center.

Regards,

ZoomInfo Privacy





Search




Free



r/privacy

**Posts**

[Wiki](#)

Posted by u/itsjustkiet 8 months ago 

## ZoomInfo Data Collection Notice

### Personal Information Notice

This notice is to inform you of the collection, processing, and sale of certain personal information that ZoomInfo collects, processes, and uses.

#### Categories of Personal Information Processed

ZoomInfo profiles business organizations and the executives and professionals who work for them.

Name

Company

Office Address

Telephone Number

Email Address

Job Title

Job Function and Responsibilities

Education

Social Media URL

#### Purpose of Processing

ZoomInfo processes this information for direct marketing purposes. The information may be used to contact you about our products and services.

#### Lawful Basis

ZoomInfo's processing of your personal information is based on the legitimate interest of ZoomInfo to provide our products and services to our customers.

#### Recipients

This personal information may be provided, subject to restrictive license agreements, to our sales and marketing personnel.

#### Period

ZoomInfo endeavors to provide the most accurate information possible to its customers and to delete or anonymize your information when it is no longer needed.

#### Your Rights

You have the right to request that ZoomInfo (1) provide you with access to your personal information and (2) delete or anonymize your information.

#### Sources of Personal Information

ZoomInfo gathers personal information from several sources, which include publicly available information, information provided by you, and information provided by third parties.

#### Who We Are





Search



To opt out or for more information, please visit our Privacy Center.

Regards,

ZoomInfo Privacy

I recieved this email today from ZoomInfo, a data collection partner for Zoom I'm assuming and reading it through I feel like this is blatant shady data collection practices. Am I wrong/crazy here?

4 Comments Award Share ...

99% Upvoted



**This thread is archived**

New comments cannot be posted and votes cannot be cast

**SORT BY BEST**



alwayssonnyhere 8 months ago

Found an article on this from University of Michigan IT Dept. (a google search away). They classified this as Marketing Spam. Zoom Info is unrelated to Zoom. Appears they collect data by scrapping web pages and then turn around and offer access to their database to paying customers. So this is part regulatory compliance and part sales pitch.

I would say that this is a legitimate business with legal but questionable business module and practices.

1 Give Award Share Report Save



mr\_em\_el 6 months ago

<https://www.zoominfo.com/b2b/faqs>

If you look at their FAQ, they have an outlook extension that people download "to get free access" that harvests all of their contacts' info. So if you email someone who has that extension installed, it captures your contact info and publishes it in Zoominfo's database. Seems like voluntary malware to me.

1 Share ...



redredredred1 5 months ago

This website classified that email as a phishing scam:

<https://www.itsc.cuhk.edu.hk/newsdetails/phishing-alert-notice-of-personal-information-processing-this-is-not-an-advertisement/>

1 Give Award Share Report Save

## Appendix A

1

← → ↺

app.zoominfo.com/#/apps/profile/person/1255316114?url=%2Fapps%2Fsearch%2Fresults%2Fperson%3Fquery%3Dey/maWx0ZXJzlp/7ln8hc3RQb3NpdGlvbi6W3siZCI6IkN1cnJlbnQgb3IgaGFzdCBDb21wYW55Iiwidil6ijMifV0slmzQ2VydGlmaWVkJjpbey/kjoiS...

Apps Investment Work Google RUN powered by A...

zoominfo

Search for companies, contacts, industries, etc.

Advanced Search

Lists Intent WebSights Alerts Enhance Events FormComplete

Contact Search - Alicia Hancock

A

Alicia Hancock

Deputy Attorney General

in

U.S. Department of Justice

www.usdoj.gov

(202) 514-2000 in

950 Pennsylvania Ave Washington, D.C., District of Columbia 20530, United States

Law Firms & Legal Services

10,000+

\$ \$5.2 Billion

Export Tag Contact

Suggest Contact Update

Contact Profile Overview Org Chart Employees Technologies and Attributes Scoops News Similar Companies

in

Contact Details

(Direct)

(HQ)

(Mobile)

Notice Provided Date: March 31, 2020

Social Networks

in

Location

Local 300 S Spring St, Ste 1702, Los Angeles, California, 90013, United States

HQ 950 Pennsylvania Ave, Washington, D.C., District of Columbia, 20530, United States

Employment History

Current

Deputy Attorney General

U.S. Department of Justice

Former

Attorney

O'Melveny

Show more

Web References

O'Melveny & Myers LLP | Professionals

http://www.ommm.com/professionals/List.aspx?LastName=H

Alicia Hancock Counsel

Momentum - AbilTo Blog

http://abilto.com/blog/tag/momentum

Counsel Alicia Hancock, who works in O'Melveny's Century City, California, office, was one of the first lawyers at the firm to enroll. "It was a big help because my consultant asked practical question...

Read More

ABA Journal - AbilTo Blog

http://abilto.com/blog/tag/aba-journal


Alicia Hancock was the first lawyer to use the new program. She met with a counselor by video conference before and after her maternity leave, the story says. She came away with tips on organization a...

Read More

13 Z

2





**Jonathan Malek**  
ShareALG Litigation FilesOffice DocumentsNuVisionEshaghi

Anaya Law Group

[www.anayalawgroup.com](http://www.anayalawgroup.com)  
(805) 230-9222

2629 Townsgate Rd, Ste 140 Westlake Village, California 91361, United States

Law Firms & Legal Services

1 - 10

\$ \$1.1 Million

Export

Tag Contact

Suggest Contact Update

**Contact Details**

(Direct)

(HQ)

(Mobile)

(Business)

(Supplemental)

Notice Provided Date: January 4, 2020

**Location**

Local 2629 Townsgate Rd, Ste 140, Westlake Village, California, 91361, United States

HQ 2629 Townsgate Rd, Ste 140, Westlake Village, California, 91361, United States

**About**

Jonathan Malek is the ShareALG Litigation FilesOffice DocumentsPinnacleLeal at Anaya Law Group based in Westlake Village, California.

**Employment History**

Current

ShareALG Litigation FilesOffice DocumentsNuVisionEshaghi Anaya Law Group

**Education**

California State University, Northridge

Show more

**Web References**

2016-02-16

<http://www.metnews.com/articles/2016/elec021616.htm>

Jonathan A. Malek, 36, filed his declaration of intent to run for Office No. 11, the seat left open by Judge Michelle Rosenblatt. Malek said he was running because "I believe I can provide justice to..."

Read More





## Alexander Robertson

Work Product OR Otherwise Privileged OR Confidential Attorney



Robertson & Associates



www.arobertsonlaw.com



(818) 851-3850 in



32121 Lindero Canyon Rd, Ste 200 Westlake Village, California 91361, United States



Law Firms & Legal Services



11 - 50



\$5.7 Million

Export

Tag Contact

Suggest Contact Update



Contact Profile



Overview



Org Chart



Employees



Technologies and Attributes



Similar Companies



Tags



Settings



12

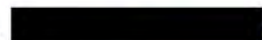
### Contact Details



Direct)

HQ)

Mobile)



(Business)



Notice Provided Date: January 6, 2020

### Social Networks

in

### Location



Local 32121 Lindero Canyon Rd, Ste 200, Westlake Village, California, 91361, United States

HQ

32121 Lindero Canyon Rd, Ste 200, Westlake Village, California, 91361, United States

### Employment History

Current



Work Product OR Otherwise Privileged OR Confidential Attorney  
Robertson & Associates

### Education

Pepperdine University  
Bachelor of Arts

### Web References

Mediators for Hotel, Restaurant, Hospitality Legal Cases 2008-09-17

<http://www.hospitalitylawyer.com/mediators.asp>

Alexander Robertson, IV Expand/Collapse Robertson & Vick, LLP26050 Mureau Rd, Suite 102 Calabasas, CA, 91302(818) 878-1800 , PhoneEmail: arobertson@rvcdlaw.comAlex has maintained a national construct...

[Read More](#)

George D. Calkins II, Esq., JAMS Mediator and Arbitrator

<https://www.jamsadr.com/calkins/>

- Alexander Robertson, IV, Esq. Robertson & Vick LLP

George Calkins Mediator Arbitrator Neutral and Dispute Resolution, CA, NV, AZ Los Angeles

[Read More](#)



zoominfo

Search for companies, contacts in business, etc.

Advanced Search

Lists

Intent

WebSights

Alerts

Enhance

Events

FormComplete

Update

AS

Contact Search - Sam Chun Kwak



Sam Chun Kwak

In-House Opinion of Back-Up Manager  
in



Latham & Watkins



www.lw.com



(424) 653-5500



10250 Constellation Blvd, Ste 1100 Los Angeles, California 90067, United States

Law Firms & Legal Services

1,001 - 5,000

\$3.8 Billion

Export

Tag Contact

Suggest Contact Update

Contact Profile

Overview

Org Chart

Employees

Technologies and Attributes

Scoops

News

Similar Companies

Tags

### Contact Details



Direct

(HQ)



(Business)

Notice Provided Date: June 1, 2020

### Social Networks

in

### Location



Local Third Ave, Ste 1000885, New York City, New York, 10022, United States

HQ

10250 Constellation Blvd, Ste 1100, Los Angeles, California, 90067, United States

Salesforce


Sync Date

### Employment History

Current



In-House Opinion of Back-Up Manager  
Latham & Watkins



**Isabel Díaz**  
Project Spectrum Latam Cash Plan  
in



**DLA Piper**  
www.dlapiper.com  
(410) 580-3000 in twitter facebook youtube

6225 Smith Avenue Baltimore, Maryland 21209, United States

Law Firms & Legal Services

1,001 - 5,000



\$2.8 Billion



[Export](#) [Tag Contact](#)


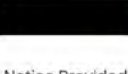
[Suggest Contact Update](#)

- Contact Profile
- Overview
- Org Chart
- Employees
- Technologies and Attributes
- Scoops
- News
- Similar Companies
- Tags

### Contact Details

  (Direct)

  (HQ)

  (Business)

Notice Provided Date: June 27, 2020

### Social Networks

in

### Location


Local Chile

HQ 6225 Smith Avenue, Baltimore, Maryland, 21209, United States

### Salesforce

Sync Date

### Employment History

- Current  Project Spectrum Latam Cash Plan  
DLA Piper





**Piper Alderman**  
The Sustainable Finance Disclosure Regulation



DLA Piper  
www.dlapiper.com  
(410) 580-3000

6225 Smith Avenue Baltimore, Maryland 21209, United States  
Law Firms & Legal Services  
1,001 - 5,000  
\$2.8 Billion

Export Tag Contact

Suggest Contact Update

- Contact Profile
- Overview
- Org Chart
- Employees
- Technologies and Attributes
- Scoops
- News
- Similar Companies
- Tags

Contact Details

(HQ)

Social Networks

Location

Local  
HQ 6225 Smith Avenue, Baltimore, Maryland, 21209, United States

Salesforce

Sync Date

Employment History

Current



The Sustainable Finance Disclosure Regulation  
DLA Piper





**Mike McGuire**  
OPPOSED Dear Senator

 **Livable California**  
[www.livablecalifornia.org](http://www.livablecalifornia.org)  
(415) 870-1511

2940 16th St, Ste 200-1 San Francisco, California 94103, United States  
Organizations  
1 - 10

Export

Tag Contact

Suggest Contact Update

**Contact Details**

  (Direct)  
(HQ)

  (Business)  
(ntal)

Notice Provided Date: January 4, 2020

**Location**

Local California, United States

HQ 2940 16th St, Ste 200-1, San Francisco, California, 94103, United States

**Employment History**

Current

 **OPPOSED Dear Senator**  
Livable California

Former

 Supervisor  
Sonoma Land Trust

**Board Memberships & Affiliations**



Board Member  
Conservation Corps North Bay  
2018 - 2020

Show more

**Web References**

California State Legislator Contacts - Livable California 2021-01-19  
<https://www.livablecalifornia.org/california-state-legislator-contacts/>  
Mike McGuire /2

admin-155424102 - Page 3 - Livable California  
<https://www.livablecalifornia.org/author/admin-155424102/page/3/>  
In a series of letters to California state Senate and Assembly Committees, Livable California formally Opposed SB50, SB330 and AB1467  
April 14, 2019 CA Senate Gov...  
[Read More](#)

Board of Directors | Sonoma Ecology Center 2021-02-27  
<https://sonomaecologycenter.org/board/>  
Mike McGuire California State Senator





Amit Majalatti

IBM Accounts Payable - IC - Flat Files

intuit


 www.intuit.com

 (650) 944-6000    

 2700 Coast Ave Mountain View, California 94043, United States

 Financial Software, Software

 10,000+

 \$ 7.7 Billion


Export

Tag Contact

Suggest Contact Update


 Contact Profile

 Overview

 Org Chart

 Employees

 Technologies and Attributes

 Scoops

 News



 Similar Companies

 Tabs

### Contact Details


  (Direct)

(HQ)

  (Business)

 Notice Provided Date: June 24, 2020

### Location

 Local Bengaluru, Karnataka, 560002, India

HQ 2700 Coast Ave, Mountain View, California, 94043, United States

### Employment History

 Current

intuit

IBM Accounts Payable - IC - Flat Files  
Intuit





zoominfo

Search for companies, contacts, industries, etc.



Advanced Search

Lists

Intent

WebSights

Alerts

Enhance

Events

FormComplete

AS

Contact Search - Rahul Bhola



Rahul Bhola

Hello Doctor

in



CHOC Children's



www.choc.org



(714) 997-3000



1201 W. La Veta Ave. Orange, California 92868, United States

Medical & Surgical Hospitals, Hospitals & Physicians Clinics

1,001 - 5,000

\$ 802 Million

Export

Tag Contact

Suggest Contact Update



Contact Profile



Overview



Org Chart



Employees



Technologies and Attributes



Scoops



News



Similar Companies



Tags

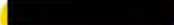
### Contact Details



(Direct)

(HQ)

(Mobile)



(Supplemental)

Notice Provided Date: January 16, 2020

### Social Networks



### Web References

Community - AAP-OC

<https://www.aap-oc.org/community/>

Presented By: Rahul Bhola, MD, MBA Section Chair, Ophthalmology, CHOC Children's Medical Director, Ophthalmology, CHOC Children's Specialists Associate Clinical Professor, University of California, Ir...

[Read More](#)

Joern B. Soltan, M.D. - University of Louisville Ophthalmology 2017-07-16

<http://www.louisvilleeyedocs.com/member/joern-b-soltan-m-d/clinical-faculty/>

Rahul Bhola, M.D. Rahul Bhola, M.D.

Rahul Bhola, M.D. - University of Louisville Ophthalmology 2017-07-16

<http://www.louisvilleeyedocs.com/member/rahul-bhola-m-d/clinical-faculty/>

### Employment History

Current



Hello Doctor

CHOC Children's

Former



Associate Clinical Professor  
University of California, Irvine

[Show more](#)

### Education

MBA

[Show more](#)



Irene Bonato

Bays Elite Investments QAP17, PDF

Austin & Austin Insurance Services



www.a-ains.com



(800) 987-1475 in

3697 Mt. Diablo Blvd, Ste 100 Lafayette, California 94549, United States

Insurance

11 - 50

\$ \$3.3 Million

Export

Tag Contact

Suggest Contact Update



Contact Profile



Overview



Org Chart



Employees



Technologies and Attributes



How



Tabs

### Contact Details



(Direct)

(HQ)



(Business)



Notice Provided Date: December 30, 2019

### Location



Local 3697 Mt. Diablo Blvd, Ste 100, Lafayette, California, 94549, United States

HQ

3697 Mt. Diablo Blvd, Ste 100, Lafayette, California, 94549, United States

### Employment History

Current

zoominfo

Bays Elite Investments QAP17, PDF  
Austin & Austin Insurance Services

### Web References

Real Estate Errors and Omissions Quote (E&O), E&O insurance for realtors in CA - Austin & Austin, Austin & Austin Insurance Services Inc - Errors & Omission Insurance (E&O)

<http://www.a-ains.com/?agent=irene>

Irene Bonato (800) 987-1475 Fax: (925) 226-7545 Irene has been with Austin & Austin Insurance Services since 1998. The experience and knowledge of the insurance industry she has gained allows her t...

[Read More](#)

Real Estate Errors and Omissions Quote (E&O), E&O insurance for realtors in CA - Austin & Austin, Austin & Austin Insurance Services Inc - Errors & Omission Insurance (E&O) 2020-04-01

<http://www.a-ains.com/meet-the-team/>

Irene Bonato

Real Estate Errors and Omissions Quote (E&O), E&O insurance for realtors in CA " Austin & Austin, Austin & Austin Insurance Services Inc " Errors & Omission Insurance (E&O)

<http://www.a-ains.com/?agent=irene>

Irene Bonato Real Estate Errors and Omissions Quote (E&O), E&O Insurance for realtors in CA - Austin & Austin, Austin & Austin Insurance Services Inc - Errors & Omission Insurance (E&O) Irene Bonato



**Bethany Lesser**  
President Trump



U.S. Department of Justice

[www.usdoj.gov](http://www.usdoj.gov)

(202) 514-2000 in twitter facebook

950 Pennsylvania Ave Washington, D.C., District of Columbia 20530, United States

Law Firms & Legal Services

10,000+

\$ \$5.2 Billion

Export

Tag Contact

Suggest Contact Update

Contact Profile Overview Org Chart Employees Technologies and Attributes News Similar Companies Tabs

### Contact Details

(Direct)  
(HQ)  
(Mobile)  
(Business)

Notice Provided Date: December 31, 2019

### Social Networks

### Location

Local 1300 J. St Ste 125, Sacramento, California, 94244, United States  
HQ 950 Pennsylvania Ave, Washington, D.C., District of Columbia, 20530, United States

### Salesforce

Sync Date

### Employment History

Current President Trump  
U.S. Department of Justice  
Former Director, Communications  
State of California



## Whitlock Bruce

To The Senior Technical Advisor & Chief Information Officer, Office of Justice Programs



U.S. Department of Justice



www.usdoj.gov



(202) 514-2000 in

950 Pennsylvania Ave Washington, D.C., District of Columbia 20530, United States

Law Firms & Legal Services

10,000+

\$5.2 Billion

Export

Tag Contact

Suggest Contact Update

Contact Profile

Overview

Org Chart

Employees

Technologies and Attributes

News

Similar Companies

Tags

### Contact Details



Direct

(HQ)



(Business)

Supplemental

Notice Provided Date: August 3, 2020

### Social Networks

in

### Location



Local 950 Pennsylvania Ave, Washington, D.C., District of Columbia, 20530, United States

HQ

950 Pennsylvania Ave, Washington, D.C., District of Columbia, 20530, United States

### Salesforce

Sync Date

### Employment History

Current



To The Senior Technical Advisor & Chief Information Officer, Office of Justice Programs  
U.S. Department of Justice

Former



Project Manager & Manager, Test  
Concentrix

Show more



Margaret Lawrence

To the Secretary and Chief Counsel  
in

Department of Health and Human Services

www.hhs.gov

(877) 696-6775

200 Independence Ave., SW Washington, D.C., District of Columbia 20201, United States

Federal, Government

10,000+

\$1.286.4 Billion

Export

Tag Contact

Suggest Contact Update

- Contact Profile

Overview

Org Chart

Employees

Technologies and Attributes

Scoops

News

Similar Companies

Tags

Contact Details

(Direct)

(HQ)

(Business)

Notice Provided Date: July 7, 2020

Social Networks

Location

Local 61 Forsyth St. SW., Sam Nunn Atlanta Federal Center, Atlanta, Georgia, 30303, United States

HQ 200 Independence Ave., SW, Washington, D.C., District of Columbia, 20201, United States

Salesforce

Sync Date

Employment History

Current To the Secretary and Chief Counsel  
Department of Health and Human Services

Board Memberships & Affiliations

To the Secretary and Chief Counsel  
Department of Health and Human Services  
2016 – 2021

15



**Amy Markopoulos**  
To The Counsel & Healthcare Fraud Unit, Fraud Section Chief  
in



**U.S. Department of Justice**  
[www.usdoj.gov](http://www.usdoj.gov)  
(202) 514-2000 in











950 Pennsylvania Ave Washington, D.C., District of Columbia 20530, United States  
Law Firms & Legal Services  
10,000+  
\$ \$5.2 Billion

Export

Tag Contact



Suggest Contact Update

**Contact Details**  
  (Direct)  
  (HQ)  
  (Mobile)  
  (Business)  
Notice Provided Date: July 31, 2020

**Social Networks**  
in

**Location**  
Local 950 Pennsylvania Ave, Washington, D.C., District of Columbia, 20530, United States  
HQ 950 Pennsylvania Ave, Washington, D.C., District of Columbia, 20530, United States

**Salesforce**  
Sync Date

**Employment History**  
Current  To The Counsel & Healthcare Fraud Unit, Fraud Section Chief  
U.S. Department of Justice  
Former  A- Fcpa  
Quirin Emanuel Trial Lawyers  
Show more

**Web References**  
Conference Sessions - The NHCAA  
<https://www.nhcaa.org/education/annual-training-conference/conference-sessions.aspx>  
Amy Markopoulos U.S. Department of Justice, Counsel to the Chief, Health Care Fraud Unit  
2012-11-05  
[http://judicialview.com/Court-Cases/Civil\\_Remedies/Fundamentalist-Church-of-Jesus-Christ-of-Latter-Day-Saints-v-Horne/11/566334](http://judicialview.com/Court-Cases/Civil_Remedies/Fundamentalist-Church-of-Jesus-Christ-of-Latter-Day-Saints-v-Horne/11/566334)  
Amy Markopoulos Sidley Austin LLP



**Jason Abend**  
President Trump Picks CBP Adviser

**U.S. Department of Defense**  
[www.defense.gov](http://www.defense.gov)  
(703) 545-6700

1400 Defense Pentagon Washington, D.C., District of Columbia 20301, United States  
Federal, Government  
10,000+  
\$ 685 Billion

Export Tag Contact

Suggest Contact Update

Contact Profile Overview Org Chart Employees Technologies and Attributes Scoops News Similar Companies Tabs

Contact Details

(HQ)

Social Networks

in

Location

Local  
HQ 1400 Defense Pentagon, Washington, D.C., District of Columbia, 20301, United States

Salesforce

Sync Date

About

Jason Abend is the President Trump Picks CBP Adviser at Department of Defense based in Washington, D.C., District of Columbia.  
Previously, Jason was the Special Agent at Federal Housing Finance Agenc...  
[Read More](#)

Employment History


Current President Trump Picks CBP Adviser  
U.S. Department of Defense  
Former Special Agent  
Federal Housing Finance Agency

Board Memberships & Affiliations

Senior Policy Advisor  
US Department of Homeland Security, Customs and Border Protection  
2017 - 2020

Web References

Longtime Pentagon Watchdog Stepping Down From Post | Patriots Voter Poll  
<https://www.patriotsvoterpoll.com/daily-hot-picks/longtime-pentagon-watchdog-stepping-down-from-post/>  
The president nominated Jason Abend, a senior policy adviser at the U.S. Customs and Border Protection agency and a former federal investigator, as the Defense Department's permanent inspector general...  
[Read More](#)  
The Wall Street Journal: Trump Removes Watchdog Who Heads Panel Overseeing Pandemic Stimulus Spending - Government Accountability Project



Richard McComb

Chief Security Officer

in

🏢 Department of Homeland Security

dhs.gov

(202) 282-8000

in

f

📍 2707 Martin Luther King Jr Ave SE Washington, D.C., District of Columbia 20528, United States

🏢 Federal, Government

👤 10,000+

💰 \$47.5 Billion

Export

Tag Contact

Suggest Contact Update

Contact Details

📞 (Direct)

(HQ)

(Mobile)

(Business)

📅 Notice Provided Date: August 4, 2020

Location

📍 Local 245 Murray Ln SW, Washington, D.C., District of Columbia, 20032, United States

HQ 2707 Martin Luther King Jr Ave SE, Washington, D.C., District of Columbia, 20528, United States

Salesforce

Sync Date

Employment History

Current  Chief Security Officer  
Department of Homeland Security

Former  Chief Security Officer  
The Management Group Associates (TMGA)  
[Show more](#)

Education

Associate degree

[Show more](#)

Board Memberships & Affiliations

 Member  
American Society for Public Administration  
[Show more](#)

Web References

Executive Briefings - The Homeland Security and Defense Business Council  
<https://www.homelandcouncil.org/executivebriefings>  
Richard McComb - Chief Security Officer, DHS

The Most Influential People in Security 2017 | 2017-09-01 | Security Magazine  
<https://www.securitymagazine.com/articles/88234-the-most-influential-people-in-security-2017>  
Richard D. McComb Richard D. McComb Richard D. McComb Richard D. McComb Chief Security Officer, Department of Homeland Security Richard McComb was appointed to the position of Chief Security Officer...

18



**Teren Hutchinson**  
Communications Security Chief  
in

**U.S. Department of Defense**  
[www.defense.gov](http://www.defense.gov)  
(703) 545-6700 in

1400 Defense Pentagon Washington, D.C., District of Columbia 20301, United States  
Federal, Government  
10,000+  
\$685 Billion

Export Tag Contact  
Suggest Contact Update

Contact Details

(HQ)  
(Mobile)  
(Supplemental)

Social Networks

in

Location

Local Stafford, Virginia, United States  
HQ 1400 Defense Pentagon, Washington, D.C., District of Columbia, 20301, United States

Salesforce

Sync Date

Employment History

Current  
Former  
Communications Security Chief  
U.S. Department of Defense  
Communications Security Chief  
HQDA Elderly Life Network

Education

Park University  
Bachelor of Science



📍 1 Rocket Rd Hawthorne, California 90250, United States

🚗 Transportation, Airlines, Airports & Air Services

👥 5,001 - 10,000

💰 \$2 Billion

[Suggest Contact Update](#)

Direct)  
(HQ)  
Mobile)

③ [REDACTED] (Business)

Local 12301 Crenshaw Blvd, Hawthorne, California, 90250, United States

HQ 1 Rocket Rd, Hawthorne, California, 90250, United States

● Current REPORTING Chief Executive Officer  
SpaceX

## B.Sc.

[Show more](#)

Member [Spaceflight Now](#)

SpaceX brings back human spaceflight to the United States 2020-07-01  
<http://sps-aviation.com/news/?id=895&catId=9&h=SpaceX-brings-back-human-spaceflight-to-the-United-States>

Elon Musk, founder and chief engineer at SpaceX said, "This is a dream come true for me and everyone at SpaceX. It is the culmination of an incredible amount of work by the SpaceX team, by NASA and by..."

Who We Are - SPI International 2020-06-06  
<https://www.spint.co.za/who-we-are/>

Elon Musk, Founder, CEO, and chief engineer/designer of SpaceX

Science & Technology | Whale Lifestyle  
<http://whalelifestyle.com/topic/science-and-technology/>

In the 14 years since Elon Musk founded SpaceX, it's managed to become a budding private space program. Employing more than 5,000 people and nabbing a highly...



zoominfo

Zoominfo is a leading provider of business intelligence and contact information.



Advanced Search

Lists

Intent

WebSights

Alerts

Enhance

Events

FormComplete

AS

Contact Search - Catherine Bidart



## Catherine Bidart

General, Opinion Unit Deputy Attorney  
in



State of California



www.ca.gov



(916) 445-2841 in



1303 10th Street, Suite 1173 Sacramento, California 95814, United States



State, Government



10,000+



\$202.1 Billion

Export

Tag Contact

Suggest Contact Update



Contact Profile



Overview



Org Chart



Employees



Technologies and Attributes



Scoops



News

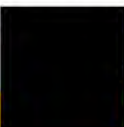


Similar Companies



Tags

### Contact Details



(Direct)

(HQ)

(Mobile)



(Business)



Notice Provided Date: December 29, 2019

### Social Networks



### Location



Local 1013 58th St, Sacramento, California, 95819, United States

HQ

1303 10th Street, Suite 1173, Sacramento, California, 95814, United States

### About

Catherine Bidart is the General, Opinion Unit Deputy Attorney at State of California based in Sacramento, California.

Previously, Catherine was the Deputy Attorney General III at U.S. Department of J...

[Read More](#)

### Employment History

Current



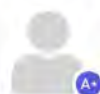
General, Opinion Unit Deputy Attorney  
[State of California](#)

Former



Deputy Attorney  
[State of California - California Department of Transportation](#)

[Show more](#)



**Lee Mollie**  
Senior Assistant Attorney General  
in

**U.S. Department of Justice**  
[www.usdoj.gov](http://www.usdoj.gov)  
(202) 514-2000 in

950 Pennsylvania Ave Washington, D.C., District of Columbia 20530, United States  
Law Firms & Legal Services  
10,000+  
\$5.2 Billion

Export Tag Contact

Suggest Contact Update

Contact Profile Overview Org Chart Employees Technologies and Attributes News Similar Companies Tabs

### Contact Details

Direct  
 HG  
 (Business)  
 (Supplemental)

Notice Provided Date: December 11, 2019

### Social Networks

in

### Location

Local 450 Golden Gate Ave, San Francisco, California, 94102, United States  
 HQ 950 Pennsylvania Ave, Washington, D.C., District of Columbia, 20530, United States

### About

Mollie Lee is the Senior Assistant Attorney General at U.S. Department of Justice based in Washington, D.C., District of Columbia.

Previously, Mollie was the Senior Assistant Attorney General at STAT...

[Read More](#)

### Employment History

Current Senior Assistant Attorney General  
U.S. Department of Justice  
 Former Senior Assistant Attorney General  
State of California

[Show more](#)

### Education

New College Of Florida  
Bachelor of Arts

### Web References

Mollie Lee | ACLU of Northern CA  
<https://www.aclunc.org/staff/mollie-lee>

Home - About - Staff - Mollie Lee Mollie Lee Senior Staff Attorney Mollie Lee Headshot Mollie Lee is a senior staff attorney at the ACLU of Northern California. In this capacity, she works on a ran...  
[Read More](#)

Staff Members | ACLU of Northern CA 2019-11-17  
<https://www.aclunc.org/about/staff>

Mollie Lee - Senior Staff Attorney



Select Filters

Open Search

Financials

Company Attributes

Type & Model

Location

Type in location

US - States

US - Metro Regions

CA - Provinces

CA - Metro Regions

International

Postal Code

Type in postal cod

Exact Results

Street Address

e.g. 100 Main Street

Suite

Specify HQ & Contact Location

All Any

Contacts Work at Location

Company HQ at Location

Scoops

10/14/20 - 4/14/21

Updated since publication

4 Filters Clear Law Firms & Legal Services ca US - States Contact Accuracy Score: 85-99

165,904 Results

0 Selected Export Tag Contacts

Accuracy: Grade Score

Contact Name	Job Title	Contact Info	Company Name	Company Industry	Accuracy	
<input type="checkbox"/> Drew Storms	To Amy Thomas Legal Assist...	D HQ B S	Wolkin Curran	Law Firms & Legal Servi...	A	...

Contact Profile Overview Org Chart Employees Technologies and Attributes Scoops News Similar Companies Tabs

**Drew Storms** Suggest Contact Update Export Tag Contact

To Amy Thomas Legal Assistant & Paralegal

**Contact Details**

(Direct)

(Business)

Person ID: -1897833916

Notice Provided Date: January 24, 2020

**Social Networks**

in

**Location**

Local 111 Maiden Ln, Fl 6, San Francisco, California, 94108, United States

HQ 111 Maiden Ln, Fl 6, San Francisco, California, 94108, United States

**Employment History**

Current To Amy Thomas Legal Assistant & Paralegal Wolkin Curran

Former Shift Manager Dimple Records

Show more

<input type="checkbox"/> Angela Rojas	-	HQ B S	Wolkin Curran	Law Firms & Legal Servi...	A	...
<input type="checkbox"/> Brandt Wolkin	Partner	HQ B S	Wolkin Curran	Law Firms & Legal Servi...	A	...













- Select Filters
- Open Search
- Contact
- Company
- Location
- Scoops
- Technologies
- Salesforce
- Exclusion
- Tags

2 Filters Clear Contact Accuracy Score: 75-99 Nury Martinez(3)

3 Results

0 Selected Export Tag Contacts

Accuracy: Grade Score

Contact Name	Job Title	Contact Info	Company Name	Company Industry	Accuracy	
<input type="checkbox"/> Nury Martinez	Council President	D HQ M B S	Los Angeles Police De...	Local, Government	A	

- Contact Profile Overview Org Chart Employees Technologies and Attributes Scoops News Similar Companies Tabs

Nury Martinez

Suggest Contact Update

Council President

Export Tag Contact

Contact Details

(Direct)

(HQ)

(Mobile)

(Business)

Person ID: 182180578

Notice Provided Date: June 25, 2020

Social Networks

in

Location

Local

200 N Spring St, Los Angeles, California, 90012, United States

HQ

100 W 1st St, Los Angeles, California, 90012, United States

About

Nury Martinez is the President at City of Los Angeles, CA based in Los Angeles, California.

Employment History

Current

Council President

Los Angeles Police Department

Former

President

City of Los Angeles, CA

Education

California State University at Northridge

Show more

Board Memberships & Affiliations

Board Member

Horizon Institute

2021 - 2021

Show more

Web References

Local Community Leaders | LAPPL - Los Angeles Police Protective League 2021-02-11

https://www.lapd.com/about/local-community-leaders

Nury Martinez 200 N. Spring Street Los Angeles, CA 90012 Telephone 213-473-7006 Fax 213-847-0549

Select Filters

2 Filters Clear Contact Accuracy Score: 75-99 Pam Black(3)

117 Results

0 Selected Export Tag Contacts

Accuracy: Grade Score

Contact Name	Job Title	Contact Info	Company Name	Company Industry	Accuracy
--------------	-----------	--------------	--------------	------------------	----------

Contact Profile Overview Org Chart Employees Technologies and Attributes Scoops News Similar Companies Tabs

Pam Black

Suggest Contact Update

Olivia Wilde's Attorney

Export Tag Contact

Contact Details

(Direct)

(HQ)

(Mobile)

(Business)

Person ID: 1453417274

Notice Provided Date: January 6, 2020

Location

Local

1801 Century Park W, Los Angeles, California, 90067, United States

HQ

1801 Century Park W, Los Angeles, California, 90067, United States

Employment History

Current

Olivia Wilde's Attorney

Ziffren Brittenham

Web References

ATTORNEYS | Ziffren Brittenham LLP 2021-03-12

<https://www.ziffrenlaw.com/attorneys/>

Pam Black Pam Black



- Select Filters
- Open Search
- Contact
- Company
- Location
- Scoops
- Technologies
- Salesforce
- Exclusion
- Tags

2 Filters Clear

Contact Accuracy Score: 75-99

Peter Cahill(3)

65 Results

0 Selected

Export


Tag Contacts

Accuracy: GradeScore

Contact NameJob TitleContact InfoCompany NameCompany IndustryAccuracy

Contact ProfileOverviewOrg ChartEmployeesTechnologies and AttributesScoopsNewsSimilar Companies

Tags



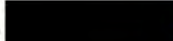
**Peter Cahill** | Suggest Contact Update


Judge


Export


Tag Contact

Contact Details

 (Direct)

 (HQ)

 (Mobile)

 (Business)

Person ID: -1525682573

Notice Provided Date: May 20, 2020

Social Networks

in

Location

Local


300 South 6th St C-714, Minneapolis, Minnesota, 55487, United States

HQ


500 N 3rd St, Fl 11, Harrisburg, Pennsylvania, 17101, United States

Employment History

Current

 Judge  
The State Bureau of Investigation

Former

 District Court Judge  
State of Minnesota - Minnesota Judicial Branch

Web References

Fourth District Judges - Hennepin County Bar Association  
<http://www.hcba.org/?page=Judges>  
Judge Cahill Chief Judge Peter Cahill Appointed to the Bench in 2007.

ZoomInfo

Search for companies, contacts, industries, etc.

Advanced Search

Contacts

Companies

Scoops

More

2 Filters

Contact Accuracy Score: 75-99

Richard Blumenthal(3)

20 Results

0 Selected

Export

Tag Contacts

Accuracy: Grade Score

Contact Name

Job Title

Contact Info

Company Name

Company Industry

Accuracy

Contact Profile

Overview

Org Chart

Employees

Technologies and Attributes

Scoops

News

Similar Companies

Tab

Richard Blumenthal

Senator

Suggest Contact Update

Export

Tag Contact

Contact Details

Location

About

Person ID: 31419954

Notice Provided Date: July 4, 2020

Social Networks

Web References

State Info- CT : Strippers Forever 2021-03-13

https://www.stripersforever.org/progress-map-state-info/state-info-ct/

Richard Blumenthal - (D - CT) 706 HART SENATE OFFICE BUILDING WASHINGTON DC 20510 (202) 224-2823

Employment History

Current

Former

Education

Board Memberships & Affiliations

1

2

3

4

5

6

7

8

9

30

Haven't found a contact that you are looking for? Submit a Research





Richard Harris

Chief Security Officer

in



Federal Bureau of Investigation

[www.fbi.gov](http://www.fbi.gov)

 (202) 324-3000    

 935 Pennsylvania Avenue, NW Washington, D.C., District of Columbia 20535, United States

 Federal, Government


 10,000+


 \$9.3 Billion


Export


Tag Contact


Suggest Contact Update



[Contact Profile](#)



[Overview](#)



[Org Chart](#)



[Employees](#)






[Technologies and Attributes](#)


[Scoops](#)


[News](#)


[Similar Companies](#)


[Tabs](#)

<div> <div>Contact Details</div> <div> <div>  <div> <div></div> <div>(Direct)</div> </div> </div> <div> <div></div> <div>(HQ)</div> </div> </div> <div> <div>  <div> <div></div> <div>(Supplemental)</div> </div> </div> </div> <div> <div>Social Networks</div> <div> <div>in</div> </div> </div> </div>	<div> <div>Location</div> <div> <div> <div>Local</div> <div>600 State St, New Haven, Connecticut, 06511, United States</div> </div> <div> <div>HQ</div> <div>935 Pennsylvania Avenue, NW, Washington, D.C., District of Columbia, 20535, United States</div> </div> </div> <div> <div>Salesforce</div> <div> <div></div> </div> </div> <div> <div>Sync Date</div> <div></div> </div> </div>	<div> <div>Employment History</div> <div> <div> <div>Current</div> <div>  <div> <div>Chief Security Officer</div> <div>Federal Bureau of Investigation</div> </div> </div> </div> <div> <div>Former</div> <div>  <div> <div>Naval ROTC Administrative Officer</div> <div>Yale University</div> </div> </div> </div> </div> </div>
---	---	---

**Web References**

**Thank You Mr. Dobson - Screen Ireland**  
<https://www.screenireland.ie/directory/view/333/thank-you-mr.-dobson/archive>

What it reveals is an underbelly of truth to Martin's eccentric fantasies, which include the search for Hitler's Silver Arrow, drug importation, forgery, stunt doubling for James Coburn and Richard Ha...

[Read More](#)

**Screen Ireland**  
<https://www.screenireland.ie/directory/1/250>

Richard Harris, Stephen Rea, Sean McGinley, Aislin McGuckin, Bríd Brennan Richard Harris, Gabriel Byrne, Samantha Morton, John Lynch, Ross McDade

**This is the Sea - Screen Ireland**  
<https://www.screenireland.ie/directory/view/206/this-is-the-sea/archive>



- Select Filters
- Open Search
- Contact
- Company
- Location
- Scoops
- Technologies
- Salesforce
- Exclusion
- Tags

3 Filters Clear Law Firms & Legal Services Contact Accuracy Score: 75-99 Starna Erickson(3)

4 Results

0 Selected Export Tag Contacts

Accuracy: Grade Score

Contact Name	Job Title	Contact Info	Company Name	Company Industry	Accuracy	
<input type="checkbox"/> Starna Erickson	Mcallister's Counsel	D HQ M B S	Zaro & Sillis	Law Firms & Legal Servi...	A	

Contact Profile Overview Org Chart Employees Technologies and Attributes Scoops News Similar Companies Tabs

Starna Erickson Suggest Contact Update

Export Tag Contact

Contact Details

(Direct)

HQ

Mobile

(Business)

Supplemental

Person ID: -1269283437

Notice Provided Date: January 25, 2020

Location

Local

1315 I St, Ste 200, Sacramento, California, 95814, United States

HQ

1315 I St, Ste 200, Sacramento, California, 95814, United States

Employment History

Current

Mcallister's Counsel

Zaro & Sillis

ZoomInfo

Search for companies, contacts, industries, etc.

Advanced Search

Contacts

Companies

Scoops

More

Save & Subscribe

Select Filters

Open Search

Contact

Company

Location

Scoops

Technologies

Salesforce

Exclusion

Tags

2 Filters

Clear

Contact Accuracy Score: 75-99

Thomas Brill(3)

23 Results

0 Selected

Export

Tag Contacts

Accuracy: Grade Score

Contact Name

Job Title

Contact Info

Company Name

Company Industry

Accuracy

Contact Profile

Overview

Org Chart

Employees

Technologies and Attributes

Scoops

News

Similar Companies

Tags

Thomas Brill

Suggest Contact Update

Export

Tag Contact

Search Case Law

Contact Details

Location

Person ID: 3284689855

Notice Provided Date: January 4, 2020

Social Networks

Web References

Employment History

Education

Thomas Brill

Suggest Contact Update

Export

Tag Contact

Search Case Law

Contact Details

Location

Person ID: 3284689855

Notice Provided Date: January 4, 2020

Social Networks

Web References

Employment History

Education

33

Haven't found a contact that you are looking for? Submit a Research