EFF Comments to the California Attorney General Regarding CCPA Rulemaking
March 8, 2019

The California Consumer Privacy Act (CCPA) grants consumers new rights in their relationships with businesses that collect and share their personal data. *See* Cal. Civil Code sec. 1798.100 *et seq*. The CCPA requires the California Attorney General (AG) to promulgate regulations to implement the CCPA, including rules regarding how businesses must handle consumers' requests to exercise their rights. *See* sec. 185.

These comments from the Electronic Frontier Foundation (EFF) address two aspects of the AG's rulemaking. First, the CCPA creates consumer rights to transparency about their personal information, but limits these rights to *verified* requests from consumers, and requires the AG to make rules on how business should determine which requests are sufficiently verified. *See* sec. 185(a)(7). EFF proposes rules that protect the privacy and security of consumers from fraudulent requests for their data, while ensuring that consumers can readily make bona fide requests.

Second, the CCPA creates a consumer right to opt-out[1] from the sale of their personal data, and requires the AG to make rules about how consumers may do so. *See* sec. 185(a)(4). Opt-out requests do not raise significant privacy and security hazards for consumers, so there is no need for verification of opt-out requests. Instead, we propose an automatic, World Wide Web-based opt-out mechanism: a "do not track" header sent by a user's web browser.

I. Verified consumer requests

Defining what constitutes a "verified consumer request" requires a careful balancing of two important considerations. On one hand, the regulations must ensure that consumers are readily able to exercise their CCPA rights with as many businesses as reasonably possible. On the other hand, these regulations must protect consumers from the risk of fraudulent requests for their data. While no verification process is perfect, the AG can create one that is both accessible and privacy-protective.

A. Background: CCPA provisions on verification of information requests

The CCPA's information access rules only apply when a business receives a "verifiable consumer request from a consumer." Specifically, this verification requirement applies to the CCPA's *right to know*, meaning the right of consumers to learn what personal information a business has about them. *See* Sec. 100(d), 110(b), and 115(b).[2] It also applies to the CCPA's

[1] Under the Privacy for All Act (A.B. 1760), consumers would have a right to opt-in consent. Businesses would need to receive a consumer's affirmative consent before selling or sharing any personal data.

[2] The recommendations in this section apply in particular to requests for specific pieces of personal information under 110(a)(5). Metadata about the kinds of information a business collects and shares, specified in 110(a)(1-4), is less sensitive, and therefore may be

right to portability, meaning the right of consumers to obtain a machine-readable set of their personal information. *See* Sec. 100(d).

The CCPA defines a "verifiable consumer request" to have two elements. *See* Sec. 140(y). First, it must be made by (a) a consumer, (b) a consumer on behalf of their minor child, or (c) "a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf." Second, the request must be one "that the business can reasonably verify," pursuant to the AG's regulations.

The CCPA requires the AG to make rules "to govern a business's determination that a request for information received by[3] a consumer is a verifiable consumer request." *See* Sec. 185(a)(7). The legislature intended these regulations "to further the purposes" of two of the CCPAs' right-to-know rules (Secs. 110 and 115), and "to facilitate . . . [the] ability to obtain information" under the CCPA's compliance rules (Sec. 130), "with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business."

The CCPA requires different approaches to verification, depending on whether the consumer already has a password-protected account with the business responding to a request. *See* Sec. 185(a)(7). First, it should "treat[] a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request." Second, it should "provid[e] a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity."

The CCPA gives the AG significant discretion in promulgating verification rules. First, the CCPA defines "verifiable consumer requests" as those "that the business can *reasonably* verify" under the AG's rules. *See* Sec. 140(y) (emphasis added). This rule of "reasonableness" empowers the AG to ensure sound outcomes. Second, the CCPA section requiring the AG to promulgate verification rules also requires the AG to take into account both (1) "administrative burden on consumers," and (2) "available technology, security concerns, and the burden on the business." *See* Sec. 185(a)(7). This empowers the AG to balance the various equities, including data security. Third, the CCPA is to be "liberally construed to effectuate its purposes" (Sec. 194), and the CCPA's core purpose is "to further Californians' right to privacy by giving consumers an effective way to control their personal information" (Finding i).

B. Verification of password-protected accounts

---

subject to less strict standards of verification by the business. While there are some situations in which it may be difficult or impossible for a business to reasonably verify a consumer request in order to disclose specific pieces of information, it should be easier for consumers to discover the types of information that are being collected about them and the categories of businesses to which their information is being sold.

[3] The word "by" is apparently a typo that should be "from."

The AG must ensure that businesses treat a consumer request as verified if it is "submitted [i] through a password-protected account maintained by the consumer with the business [ii] while the consumer is logged into the account." *See* Sec. 185(a)(7). This language applies whether the account bears the consumer's name or a pseudonym.

Taken in isolation, this language might rigidly be read to mean that every request that meets these two conditions is verified, with no exceptions. But as discussed above, the CCPA grants the AG significant discretion to promulgate well-balanced verification rules, which should include the power to limit as needed this mode of verification.

Exercising this power, the AG must attend to scenarios in which a wrongdoer might pretend to be a consumer logged into their password-protected account. For example, a thief might steal a consumer's laptop, and that laptop and one of its online accounts might both be unlocked. Also, a consumer might use a shared public computer to access their password-protected account, and might neglect to sign out when they are done, in which case a thief might use the shared computer to access the account.

To prevent such security intrusions, the AG should mandate re-authentication before a user can access their data. Specifically, the AG can require a business to require that the user log out and then present their password again, before making a request. To prevent the great harm of wrongful access to a consumer's vast trove of personal data, it is not an undue burden to require a consumer to re-input their password.

The AG should also encourage, but not require, two-factor authentication as a form of verification. Two-factor authentication (2FA) is an information security practice in which a service provider requires a user to identify themselves with both (1) something the user knows, like their password, and (2) something else the user controls, like their mobile phone or email address. Where a consumer already has 2FA enabled on an account with a business, or has voluntarily provided the business with enough information to enable 2FA, it will often be reasonable for the business to require verification by means of 2FA. This will provide additional assurance that the requester is who they say they are. Furthermore, verifying by a second factor can notify the user of fraudulent attempts to access their information if their account is compromised.

But 2FA should not be mandated across-the-board. There are recurring situations where a reasonable user might choose not to associate a "second factor" of their identity with their account. For example, whistleblowers and activists using social media could face grave harm if their pseudonymous accounts are associated with real-world identities. Likewise, survivors of spousal abuse or sex trafficking have the right to share their stories pseudonymously online without risk that their identities will be exposed. Such vulnerable people need to be able to effectively exercise their rights to know what data companies are collecting about them so, among other reasons, they can assess the threats they would face if an adversary stole their data.

Finally, because time may pass from when a person requests data to when a business makes that data accessible to the requester, the AG should require authentication not just of the person who requests data, but also of the person who later accesses it. For example, Facebook's "download your information" feature used to take a good deal of time for processing. A user had to request that Facebook assemble all of their personal data into one place through a dialog on the website. After a delay of potentially several days, the company would send the user an email with a one-time link allowing them to access their data. If the company verified identity at the time of request but not the time of access, an imposter might have gotten access to the data.

C. Verification in other scenarios

The AG must ensure that companies "provid[e] a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity." *See* Sec. 185(a)(7). This CCPA language is broad, and grants the AG an even higher level of discretion to make sound verification rules that prevent fraud while providing reasonable access.

These are examples of scenarios where the requester has no account with the business:

a) A consumer who uses their credit card to make a purchase from a business without creating an account with that business, either online (*e.g.,* as a "guest" of a website) or offline (*e.g.*, inside a bricks-and-mortar store).

b) A business that collects data *from* a consumer without the consumer's knowledge or consent, either online (*e.g.*, via third-party tracking tools) or offline (*e.g.*, via visual observation).

c) A business that collects data *about* a consumer without having any direct interaction with the consumer, by purchasing or collecting it from other parties (*e.g.*, a data broker).

If the requester has no existing account with the business, the AG should require businesses to be as certain as reasonably possible that the initiator of a request for access is, in fact, the subject of the personal data in question. There also must be oversight to ensure that businesses are not using the verification process to evade their disclosure duties. Different contexts may require somewhat different approaches.

Data associated with a real identity. The company should require proof that the requester is the consumer in question. If a consumer's data is associated with something that indirectly ties the consumer to a real identity, like a credit card number or license plate number, the company can require that the requester to prove they are the person associated with the identifier. Likewise, if a consumer's data is associated with a biometric identifier, the company can require the requester to prove they are the person identified.

Data associated with a communication address. Companies may assemble user data associated with an identifier that doubles as a secure means of communication, such as a mobile phone

number, email address, or social media profile. In these cases, the company can require proof that a requester has control of their communication address. This can be done, for example, by sending a confirmation link to the address.

Data associated with a device. Companies may collect data associated with a physical device, like a mobile phone or voice-activated smart device. In these cases, the company should require proof that the requester owns and controls the device before granting access to the data. Furthermore, the company should be reasonably certain that the requester was in control of the device at the time the data in question were collected. If a device is used by two or more consumers, a verified request should include the consent of all of these consumers.

Data associated with a unique device identifier. The AG should require heightened due diligence if a company verifies a requester's identity through their hardware identifier. For example, every Internet-accessible device is associated with a media access control (MAC) address. MAC addresses are persistent and difficult for an average consumer to change, which makes them attractive device identifiers.[4] However, it also is fairly easy for sophisticated users to "spoof" them.[5] Where applicable, companies should require proof that a device identifier has not been forged or spoofed in order to impersonate another consumer.

Data associated with online tracking tools. Some companies use cookies and other tools to track a user's online activity, without necessarily knowing the identity of the user. If the company knows the tracked user's identity, a requester can verify their identity by showing they are that known tracked user. Otherwise, if the requester can reasonably prove that they were the sole person identified by the tracking tool for the duration of the period in which data were collected, a company should consider it a verified consumer request.

Finally, the AG should ensure that any information collected by a business for the purpose of verifying a consumer request must only be used for that purpose, and should be deleted as soon as practical once that purpose is achieved. All too often, companies gather data ostensibly to protect consumer privacy, then use it to intrude on consumer privacy. For example, researchers revealed last year that Facebook collected phone numbers ostensibly for two-factor authentication, then used those phone numbers to target ads.[6]

D. Requests by agents

---

[4] In fact, some companies place tiny wireless "beacons" in physical spaces to collect MAC addresses from the devices in the vicinity. This data is used by retailers, marketers, and political consultants. *See* https://www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service, https://www.latimes.com/politics/la-na-pol-campaign-tech-privacy-20190220-story.html.

[5] *See, e.g.*, https://web.archive.org/web/20120623060142/http://www.rcmp-grc.gc.ca/ncecc-cncee/factsheets-fichesdocu/macspoof-usurpmac-eng.htm.

[6] *See, e.g.*, https://www.eff.org/deeplinks/2018/09/you-gave-facebook-your-number-security-they-used-it-ads.

The CCPA allows consumers to make a verified request indirectly through an agent. *See* Sec. 140(y). From a data security perspective, such requests by agents present a new attack vector that data thieves might attempt to exploit. A business might err not just regarding whether a particular consumer actually has the right to access the data, but also whether that consumer actually authorized a particular agent to make the request.

Thus, the AG should mandate that when a purported agent requests data from a business on behalf of a consumer, the business must require proof that the consumer actually instructed the agent to make the request. In this context especially, the AG must attend to "security concerns." *See* Sec. 185(a)(7).

E. Verification of deletion requests

In addition to the information requests discussed above, the CCPA empowers consumers to make deletion requests, subject to verification. *See* Sec. 105(c). Compared to information requests, deletion requests raise fewer privacy concerns, because fraudulent deletion requests will not result in adversaries wrongfully acquiring personal information about a target. However, information requests nonetheless raise significant information security concerns. Specifically, fraudulent deletion requests can harm a target by depriving them of access to their own personal information, which the target may have wanted to review, use, share, or store. Accordingly, verification of deletion requests should be like verification of information requests.

II. Consumer requests to opt-out of data sales

A. Background: the CCPA right to opt-out of sales of personal information

The CCPA provides: "(a) A consumer shall have the right, at any time, to direct a business that sells[7] personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out." *See* Sec. 120(a). The CCPA further provides that a business that has received an opt-out request from a consumer is barred from selling that consumer's information, unless the consumer subsequently provides "express authorization" to do so. *See* Sec. 120(d).

To implement this right to opt-out of data sales, the CCPA provides that a company must:

> Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.'

[7] Under the Privacy for All Act, the right to opt-in consent would apply to both the sale and sharing of personal information.

See Sec. 135(a)(1). After an opt-out, the CCPA requires a business to wait a year before again asking the consumer for permission to sell their data. *See* Sec. 135(a)(5). If a business collects personal information from a consumer in connection with an opt-out request, the business cannot use that information for any other purpose. *See* Sec. 135(a)(6).

The CCPA charges the AG with establishing rules and procedures "to govern business compliance with a consumer's opt-out request." *See* Sec. 185(a)(4)(B).

B. Opt-out requests present negligible security risks

Unlike the consumer requests to businesses for personal information discussed above, which present serious risks of fraudulent requests that intrude on consumer privacy and data security, consumer requests to businesses to opt-out of sales present little or no privacy or security risk. If an adversary wrongly opted a consumer out of sales of their data, the adversary would gain nothing of value. And when the wrongdoing was uncovered, the consumer could easily opt back in to sales of their data, if they wanted it. Thus, the CCPA does not require companies to verify consumer requests to opt-out from sales of their personal information.

C. Opt-out requests via the World Wide Web

The CCPA clearly requires a business to maintain a web page to handle consumer opt-out requests, and bars a business from requiring a consumer to create an account in order to make an opt-out request.

Due to the vast diversity of businesses covered by the CCPA, the average California consumer is likely to interact with hundreds or even thousands of businesses that collect and maintain personal information about them, directly or indirectly.

Many consumers will reasonably decide that they want to opt-out of the sale of their personal information *by default for all businesses they interact with*. They should be able to use automatic tools to assist them in doing so.

Fortunately, a way to do so already exists: the Do Not Track (DNT) system. It combines a technology (a browsing header that announces the user prefers not to be tracked online) with a policy framework (how companies should respond to that signal).[8]

EFF proposes that the AG require any business that interacts with consumers directly over the Internet using HTTP or HTTPS to treat an HTTP request with a DNT header set to 1 as a binding request to opt-out of data collection.

The DNT header is already widely supported by most major web browsers, including Google Chrome, Mozilla Firefox, and Opera. This will allow for immediate and widespread use of DNT as a tool for making opt-out requests. Users will be able to configure their browsers, either by

[8] *See, e.g.*, https://www.eff.org/issues/do-not-track.

themselves or with privacy-preserving extensions like EFF's Privacy Badger, to exercise their CPPA right to opt-out from data sales with all businesses they interact with online.

There should be different DNT rules depending on whether the user is logged-in or otherwise verified as the controller of an account with the business. If so, the business should be required to consider the DNT header as an affirmative request to opt-out of *all* sales of the consumer's data until the consumer decides to opt back in. If not, the business should consider it a request to opt-out only from the sale of data collected in the current session.

Conclusion

EFF thanks the California Attorney General's Office for its consideration of these comments on CPPA rulemaking concerning (1) how to verify consumer requests for personal information, and (2) how to structure consumer requests to opt-out of sales of personal information.

Respectfully,
Bennett Cyphers, Staff Technologist, bennett@eff.org
Adam Schwartz, Senior Staff Attorney, adam@eff.org