

CPPA Statement
Pre-rulemaking Stakeholder Session
5/6/22
Consumers' Rights to Limit Use of Sensitive Personal Information

By Andrew Crawford
Senior Counsel, Privacy & Data Project

Thank you to the California Privacy Protection Agency for the opportunity to join you today. My name is Andrew Crawford. I'm a senior counsel on the privacy and data project at the Center for Democracy & Technology. CDT is a nonprofit, nonpartisan 501(c)(3) organization based in Washington D.C. that advocates for civil rights and civil liberties in the digital world. For the past two years, I have focused my work around identifying and advocating for robust privacy protections for consumers' sensitive data, focusing mainly on health data.

Appropriate collection, sharing and use of sensitive data, like health data, can empower individuals and yield truly remarkable and beneficial outcomes. However, sometimes, the benefits are minimal and sensitive data collection, sharing, and use can be harmful. Specifically, when sensitive data is shared and used in ways that consumers do not want or anticipate, they lose agency over their data and face a greater likelihood of harm.

Unfortunately, there are ample examples of consumers being harmed by inappropriate collection, sharing, and use of sensitive personal information. Reproductive health apps have been found to violate their own policies when sharing sensitive health information of millions of users with third parties, including advertisers. Moreover, just this week, there are new reports detailing how data brokers sell location information about visitors to health clinics, including those that provide reproductive health services. The harms associated with the misuse of sensitive personal data can have lasting emotional and physical effects.

Today, the burden of protecting their sensitive health data falls almost entirely on consumers. It is time to rebalance these relationships and empower consumers with more control over how their sensitive information is collected, shared, and used. To take full advantage of the current opportunity to confront these very real harms, the CPPA should embrace the following priorities in subsequent rulemaking regarding sensitive personal information:

1. The CPPA should embrace a broad definition of "sensitive personal information."

I encourage the CPPA to interpret the CPRA's definition of "sensitive personal information" broadly so that it captures the full universe of sensitive data. This is especially true when approaching health data. I encourage the CPPA to focus not just on specific clinical data or data held by a hospital or doctor's office, but more so on the nature of the data and how it is used. If data is being used by businesses to

make insights and/or conclusions about consumers' physical and mental health, that data should be treated as sensitive data. Indeed, any data can be sensitive "health data" if it is used for those purposes, even if it appears unrelated on its face. Location information, web browsing history, and purchase histories can all reveal very probative details about a consumer's health.

This type of purpose- and use-based approach has several benefits. First, it benefits consumers by raising the bar for all the data that is used to impact their health and wellness. Trying to delineate certain data sets as worthy of coverage and others as not no longer makes sense for the people whose information is implicated. Second, it creates a tech-neutral standard that will stay relevant as technology evolves.

2. The CPPA should narrowly define what reasonable expectations by an average consumer are when requesting goods or services.

Under CPRA, it is up to each consumer to request that businesses limit the use of their sensitive information. Once that choice has been made, it should be meaningful and effective. The CPPA should be careful to avoid permitting exceptions that swallow the rule. To that end, you should embrace a narrow interpretation of what is reasonably expected by an average consumer who requests goods or services. As my colleague noted in an earlier session that focused on data minimization and use limitations, there are lots of examples of apps and services collecting far more information than is necessary. If not constrained, there is a real risk that "reasonable expectations" can expand to include ancillary and unrelated purposes and uses that are not reasonably expected.

You should work to ensure that irrelevant data, especially sensitive information like health data, is not collected and retained when the data is unrelated to the goods or services being requested. Specifically, the CPPA should clearly articulate that once a consumer directs a business to limit the use of her sensitive personal information, that business immediately limits collection, disclosure, or use of consumers' sensitive information to only what is necessary to provide the specific product or feature the consumer has requested - and nothing else. Those limits, which also apply to third parties and service providers should be conveyed immediately. Moreover, the original data collector should follow up with all third parties to ensure each consumer request is being honored and fulfilled. This final point is important and should be done by each business because consumers will often not know who each and every third party is. To recap, CPPA should develop robust rules that empower consumers to truly limit data collection and use practices by businesses to ensure that sensitive personal information is used for limited purposes consistent with consumer requests and expectations.

3. The consumer opt-out process should be simple and straightforward.

For consumers to truly be empowered and gain back some semblance of control of their sensitive personal information, the choice to limit businesses use of their data should be simple to identify and easy to execute. CPPA should develop rules that allow consumers to know their rights and exercise them easily.

First, timely and meaningful notice allows consumers to make informed decisions before they permit their sensitive personal information to be collected, disclosed, or used. Sensitive information, like health data, is personal and intimate and notices about it should not be relegated to a dense paragraph in a daunting multi-page privacy policy. Instead, consumers should be prominently told about their rights to limit the use and disclosure of their sensitive personal information independently of other terms and policies. Moreover, this notice and opportunity to opt out should be given before any collection or sharing has occurred.

But simply providing an initial notice is not enough. Consumers' rights to limit the use and disclosure of sensitive personal information do not vanish once they have shared data with a business - their rights continue and permit consumers to limit use and collection "at any time." CPPA should promulgate rules that provide meaningful ongoing transparency requirements, at set intervals, to allow each consumer to revisit their decision and make up-to-date decisions informed by changing data uses. Periodic notifications should be simple and digestible in order to best empower consumers to revisit their decisions, and make new ones, before, during, and after business collect some of their most sensitive personal information.

Notice should also be provided in ways that are accessible to all consumers. Any rules you develop should ensure that notices are tailored for each set of users and made easy to access and understand. Consumers are not empowered if they don't know about, or have the ability to exercise their rights to limit the collection and use of their sensitive personal information.

To wrap up, I commend the CPPA for holding these sessions. As you contemplate rules surrounding consumers' rights to limit the use and disclosure of their sensitive personal information, you should:

1. Embrace a broad definition of "sensitive personal information" with a focus on the purpose and use of data;
2. Narrowly identify what reasonable expectations by an average consumer are to prevent exceptions from swallowing the rule; and
3. Ensure that the consumer opt-out process is simple and straightforward.

Thank you for the opportunity to speak today. I look forward to continuing to follow the CPPA's efforts and I am ready and willing to assist should you have any questions or wish to follow-up on any of the points I've covered today.