PAUL HASTINGS

THE CALIFORNIA PRIVACY RIGHTS ACT (CPRA) HAS PASSED – DOES YOUR COMPANY COMPLY?

PAUL HASTINGS

TABLE OF CONTENTS

OVERVIEW OF CPRA

On November 3rd, 2020, the California Privacy Rights Act ("CPRA") was passed via a ballot initiative. The CPRA, which amends the California Consumer Privacy Act ("CCPA"), significantly broadens the control that California residents (referred to in the CPRA as "consumers") have over their personal information and imposes new obligations on businesses. Although the CPRA does not become effective until **January 1, 2023**, many of its substantive provisions have a "lookback" to January 1, 2022.

SCOPE

The CPRA, like the CCPA, protects "personal information" ("PI"). In addition, however, the CPRA introduces a new subset of PI called "sensitive personal information" and implements heightened protections for the types of information that fall within this category.

PERSONAL INFORMATION

The definition of PI under the CPRA is substantially the same as under the CCPA, meaning "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."

This definition encompasses typical "direct" identifiers (e.g., name, email address, physical address, social security number, passport number) but also online or other "indirect" identifiers, such as mobile advertising IDs, IP addresses, cookie IDs, user names, MAC addresses, or geolocation data.

SENSITIVE PERSONAL INFORMATION

The CPRA also creates a subset of PI called "sensitive personal information." As defined, this category includes the following data elements:

- Social security, state identification, passport, and driver's license numbers;
- Financial account information in combination with credentials that would allow access to an account;
- Precise geolocation information;
- Information pertaining to an individual's racial, ethnic origin, union membership, or religious or philosophical beliefs;
- The contents of emails or text messages;
- Genetic data; and
- Biometric information (when processed for the purpose of uniquely identifying a consumer), health information, or information concerning a consumer's sex life or orientation.

However, the CPRA states that where the above information is not being used for "the purpose of inferring characteristics about" a consumer, it is not sensitive PI and should be treated as standard "personal information." The CPRA does not explicitly define what constitutes "inferring characteristics about" consumers

but does clarify that any of the above data elements that are only processed "incidentally" are not considered sensitive PI.

EXCLUDED CATEGORIES OF INFORMATION

The CPRA excludes two categories of information from its definitions of PI (including sensitive PI).

First, information that is "publicly available" is excluded from the definition of PI. This includes:

- Information made available from government records;
- Information that is "made available by" a person to whom a consumer has disclosed the information, where the consumer has not restricted the information to a specific audience; and,
- Information that a business has a "reasonable basis to believe" was lawfully made available to the general public by the consumer or from "widely distributed media."

Second, the CPRA does not consider "lawfully obtained, truthful information that is a matter of public concern" to be PI.

APPLICABILITY

BUSINESSES

The CPRA applies to "businesses," essentially defined as any organization or person that does business in California and meets certain thresholds, regardless of whether the organization or person has any physical presence in California. While several of the thresholds for what constitutes a "business" remain the same as in the CCPA, the CPRA includes some important changes, as summarized below.

CCPA Requirement	CPRA Requirement
Annual gross revenues in excess of $25MM.	Annual gross revenue in excess of $25MM ***in the preceding calendar year, as determined on January 1 of the calendar year***.
Annually buys, sells, receives for a commercial purpose, or shares the PI of 50,000 or more consumers, households, or devices.	Annually buys, sells, or shares the PI of ***100,000*** or more consumers or households.
Derives 50% or more of its annual revenues from selling consumers' PI.	Derives 50% or more of its annual revenues from selling or sharing consumers' PI.

In addition, while the CCPA's requirement that entities sharing common control and common branding in order to be considered the same "business" are largely unchanged, the CPRA adds an additional requirement: namely, that the entities must also share consumers' PI.

SERVICE PROVIDERS

Like the CCPA, the CPRA also applies to "service providers," generally defined as any organization or person that processes consumers' PI on behalf of a business and pursuant to written contractual restrictions (which also must be imposed by the service provider on downstream parties that will assist it in processing the PI). One such restriction is that, subject to certain exceptions to be defined by the California Attorney General and the newly created California Privacy Protection Agency (discussed below), a service provider cannot combine PI collected from, or on behalf of, one business with information collected from, or on behalf of, other businesses.

Further, while service providers can provide "advertising and marketing services" on behalf of a business, they are prohibited from being utilized to provide "cross-context behavioral advertising" (as discussed below).

CONTRACTORS

The CPRA also applies to "contractors," defined as any organization or person "to whom a business makes available" a consumer's PI pursuant to written contractual restrictions similar to those required with service providers (which also must be imposed by the contractor on downstream parties that will assist in processing the PI).

The "contractor" definition seems to have a slightly larger scope than that of "service provider," given that a contractor is anyone to whom a business "makes available" a consumer's PI. Though clarity is needed, this definition may be intended for disclosures to those that do not believe they are processing PI "on behalf of" a business but still need to receive PI for some business purpose (e.g., disclosure of PI from an online travel agency to an airline for booking purposes).

Further, while contractors can provide "advertising and marketing services" in relation to a business, they are prohibited from being utilized to provide "cross-context behavioral advertising" (as discussed below).

THIRD PARTIES

The CPRA broadens the concept of "third parties" under California privacy law. Under the CPRA, a company is considered a "third party" unless it is (a) the business with which the consumer has intentionally interacted, or (b) a "service provider" or "contractor."

Note that the definitions of "business" and "third party" are not mutually exclusive. In other words, an organization can receive PI as a "third party" (i.e., from another business) but be obliged to protect that PI as a "business."

EXEMPTIONS

The CPRA retains the CCPA's deferment of various provisions related to PI collected in the employment context and the business-to-business (B2B) context. Under the CPRA, those exemptions will sunset on January 1, 2023.

ENFORCEMENT

The CPRA establishes the California Privacy Protection Agency (the "CPPA")—a new agency tasked with implementing and enforcing the statute. Among its mandates, the CCPA is responsible for investigating alleged violations of the CPRA and initiating administrative proceedings where appropriate. **The CPRA also eliminates the CCPA's "cure" provision with respect to administrative enforcement actions**, whereby companies could avoid CCPA liability by curing any alleged violation within 30 days of notice. The CCPA's civil penalties of up to $7,500 per each intentional violation and $2,500 for each non-intentional violation remain unchanged.

With respect to civil litigation, the CPRA broadens consumers' private right of action for data breaches. In addition to a breach of any "personal information" as that term defined in California's separate data breach law, the CPRA allows consumers to recover for the compromise of an email address and the associated password. In either case, consumers can recover the greater of $750 per incident or actual damages.

TOP 10 CHANGES

Changes to the scope, applicability, and enforcement mechanisms are far from the only changes that the CPRA implements. While the following list is not inclusive, it highlights some of the more significant additions and modifications that the CPRA includes.

1. In its "notice at collection" to consumers, businesses must disclose its retention periods for each category of PI it collects or, if not possible, the criteria used to determine that period.

2. In response to access requests, businesses are explicitly required to disclose the PI they have collected about a consumer, including any PI collected by a service provider or contractor.

3. Businesses that receive verified requests from consumers for deletion of their PI must communicate that request to (i) their service providers and contractors and (ii) any third parties to whom the businesses have "sold" or "shared" the consumer's PI, absent limited exception.

4. Consumers can request the correction of inaccurate PI that a business maintains about them.

5. Businesses cannot collect or use PI (or sensitive PI) for a purpose that is incompatible with the disclosed purpose for which the information was collected without notifying the consumer.

6. In addition to the right to opt-out of "sales," the CPRA requires businesses to provide the right to opt-out of:

    a. Use of sensitive PI outside of that which is necessary to provide the good or service requested or perform certain enumerated "business purposes" (e.g., ensuring security, "short-term transient uses" such as for contextual advertising, customer service-related uses, maintaining quality and safety, and as otherwise permitted by regulation); and

    b. "Sharing" PI, which is essentially defined as a disclosure by a business to a third party for "cross-context behavioral advertising," regardless of whether or not the disclosure is a "sale."

        i. "Cross-context behavioral advertising" is generally defined as the targeting of advertising to a consumer based on the consumer's PI obtained across various websites, applications, or services.

7. Businesses must provide certain opt-out links that, when clicked, allow consumers to exercise their various CPRA opt-out rights (to the extent applicable):

    a. A clear and conspicuous link (on the business's homepage) titled "Limit the Use of My Sensitive Personal Information"; and

b. A clear and conspicuous link on the business's homepage titled "Do Not Sell or Share My Personal Information"; or

c. In lieu of two separate links above, a "single, clearly-labeled link" on the business's homepage that allows for the opt-outs contemplated in (a) and (b) above.

Alternatively, a business can forego those hyperlinks to the extent it responds to opt-out signals sent either by, or on behalf of, a consumer (such as via a platform, technology, or mechanism). However, this option is subject to further clarification based on regulations to be promulgated by the California Attorney General and CPPA.

8. Businesses that "sell" or "share" PI with a third party must enter into agreements with those third parties that restrict the third party's use of the PI to the purposes for which it was "sold" or "shared" and that obligate the third party to provide "the same level of privacy protections" as is required under the CPRA.

9. Processing activities that present a "significant risk" to consumers' privacy or security require annual audits and periodic risk assessments. This requirement is subject to further development by regulations that are to be promulgated by the California Attorney General and the CPPA.

10. Pursuant to regulations yet to be adopted by the California Attorney General and the CPPA, businesses may need to provide an opt-out for automated decision-making about consumers, including profiling, and access rights regarding the logic used for that automated decision-making.

HOW TO GET STARTED WITH CPRA COMPLIANCE

- **Create Awareness within Your Organization**. Even if you have already been operating in compliance with the CCPA for several months, you should ensure that decision-makers and key individuals in your organization are aware of the CPRA and its impact on your business.
- **Understand the Information You Hold**. If you have not already done so, you should create data maps to document what PI you hold, how you use it, where you store it, the source of the PI, and to whom you disclose it. Among other things, this information is necessary for evaluating whether your company is a "business" or "service provider," engages in "sales" or "sharing" of PI (such as, in the latter case, to adtech partners for "cross-context behavioral advertising" purposes) and can adequately respond to the consumer rights requests mandated by the act.
- **Communicate Your Data Use Practices**. Your privacy notices, both employee and consumer-facing, should be reviewed and updated to ensure compliance with specific CPRA disclosure requirements. You should also ensure that your company is collecting and processing PI in a manner consistent with these notices.
- **Recognize the Consumer Rights Granted by the CPRA**. The CPRA adds new consumer rights and retains and refines the pre-existing CCPA rights, specifically:
  - Right to know about PI collected, disclosed, or sold, including by requesting the "specific pieces" of PI that have been collected (also known as "access requests");
  - Right to request deletion of PI;
  - Right to request correction of PI;
  - Right to opt-out of the "sale" or "sharing" of PI;
  - Right to opt-out of the use of sensitive PI; and
  - Right to non-discrimination for exercising these rights.
- **Establish Processes for Responding to Consumer Requests**. Your company should have a process for identifying the PI that is the subject of consumer requests, verifying the consumer's identity (for fraud prevention purposes), and responding in compliance with CPRA requirements on timing, as well as method and medium of delivery. Your company should also adopt procedures for identifying what data must be deleted in response to a request and what data may be retained according to any exceptions provided in the CPRA. Evaluating your response timeliness and completeness, on an ongoing basis, is critical to ensuring your continued compliance with CPRA.
- **Effective Mechanisms to Opt-Out of the "Sale" or "Sharing" of PI or Use of Sensitive PI**. Companies that "sell" or "share" PI or use sensitive PI must implement a process for consumers to opt-out accordingly, such as via the links described above. Where a company does not "sell" or "share" PI, this should be stated in the privacy notice to consumers.
- **Create a Process for Entering into and Reviewing Contracts with Service Providers, Contractors, and Third Parties**. The CPRA includes specific requirements regarding contracts between businesses and its contractors, service providers, and third parties. Your company should review any currently existing contracts and establish procedures for ensuring

that any future contracts involving the PI of consumers meet CPRA requirements.

- **Review Your Consent Mechanisms for Minors**. Companies that "sell" or "share" PI must also obtain the prior opt-in consent of consumers who are 13-15 years old. If the consumer is under the age of 13, prior consent from the consumer's parent or guardian is required.
- **Assess the Adequacy of Your Information Security Program**. The CPRA, like the CCPA, requires businesses to implement and maintain reasonable security procedures and practices to protect PI, especially due to the private right of action for data breaches. You should ensure your information security program is aligned with, and assessed against, the requirements of an established information security framework (e.g., CIS, NIST, or ISO).

HOW THE PAUL HASTINGS PRIVACY & CYBERSECURITY SOLUTIONS GROUP CAN HELP

Our Privacy and Cybersecurity Solutions Group operates as part of our Global Privacy and Cybersecurity Practice. Together, we offer a unique blend of legal and consulting expertise under a single umbrella. We have provided advice and support to hundreds of companies across all market sectors.

We can provide comprehensive CPRA compliance support, and more specifically:

- **Document Review and Development**. We can enhance your current internal policies and procedures, as well as create new documentation to support your CPRA compliance program. Our team has extensive experience in creating program documentation that is both legally sufficient to meet regulatory requirements and customized to your unique business needs and functionality. We routinely work with clients to integrate CPRA compliance efforts into the broader compliance activities of the company, and, while we have a library of tried-and-true templates, we work closely with our clients to ensure that any documents we produce are usable, workable guidelines that their businesses can easily follow.
- **Data Mapping**. Our consultants are experienced at creating detailed data maps based on your documents and data collection, storage, sharing, and destruction practices. When necessary, we also collaborate with experienced technical firms to provide support for implementation and operationalization of data mapping tools.
- **Compliance Gap Assessment**. Based on the information we obtain through our document review, data mapping and key interviews or other fact-gathering, and our day-to-day experience in supporting CPRA compliance efforts at a broad range of companies, we can provide you with an easy-to-understand, actionable assessment that provides a clear picture of where your program is now compared to where you need to be to comply with CPRA and in comparison with other similarly situated companies.
- **Remediation Roadmap Development**. Based on the compliance gap assessment, we can provide you with a prioritized, systematic guide for remediating those identified gaps. We can provide guidance on who in your organization should be responsible for implementing each action item and what additional tools or resources you may need.

OUR TEAM

Jacqueline Cooney

Leader, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1236
jacquelinecooney@paulhastings.com

John Binkley

Senior Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1862
johnbinkley@paulhastings.com

Daniel Julian

Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1231
danieljulian@paulhastings.com

Brianne Powers

Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1237
briannepowers@paulhastings.com

PAUL HASTINGS

ABOUT PAUL HASTINGS

Paul Hastings provides innovative legal solutions to many of the world's top financial institutions and Fortune 500 companies in markets across Asia, Europe, Latin America, and the United States.

We offer a complete portfolio of services to support our clients' complex, often mission-critical needs—from structuring first-of-their-kind transactions to resolving complicated disputes to providing the savvy legal counsel that keeps business moving forward.

Since the firm's founding in 1951, Paul Hastings has grown steadily and strategically along with our clients and the markets we serve. We established successful practices in key U.S. and European cities, creating a broad network of professionals to support our clients' ambitions. In addition, we were one of the first U.S. law firms to establish a presence in Asia, and today we continue to be a leader in the region. Over the past decade, we have significantly expanded our global network of lawyers to assist our clients in financial centers around the world, including the emerging markets of Latin America.

Today, we serve our clients' local and international business needs from offices in Atlanta, Beijing, Brussels, Century City, Chicago, Frankfurt, Hong Kong, Houston, London, Los Angeles, New York, Orange County, Palo Alto, Paris, San Diego, San Francisco, São Paulo, Seoul, Shanghai, Tokyo, and Washington, D.C.

Drawing on the firm's dynamic, collaborative, and entrepreneurial culture, our lawyers work across practices, offices, and borders to provide innovative, seamless legal counsel—where and when our clients need us.

Ranked among the Top 5 on the A-List of the most successful law firms in the U.S. six years in a row

— The American Lawyer

PAUL HASTINGS

GLOBAL RESOURCES

21 OFFICES *ACROSS THE AMERICAS, ASIA, AND EUROPE*

1 LEGAL TEAM *TO INTEGRATE WITH THE STRATEGIC GOALS OF YOUR BUSINESS*

THE AMERICAS

Atlanta
Century City
Chicago
Houston
Los Angeles
New York
Orange County
Palo Alto
San Diego
San Francisco
São Paulo
Washington, D.C.

ASIA

Beijing
Hong Kong
Seoul
Shanghai
Tokyo

EUROPE

Brussels
Frankfurt
London
Paris

PAUL HASTINGS

THE AMERICAS

Atlanta
1170 Peachtree Street, N.E.
Suite 100
Atlanta, GA 30309
t: +1.404.815.2400
f: +1.404.815.2424

Century City
1999 Avenue of the Stars
Los Angeles, CA 90067
t: +1.310.620.5700
f: 1.310.620.5899

Chicago
71 S. Wacker Drive
Forty-Fifth Floor
Chicago, IL 60606
t: +1.312.499.6000
f: +1.312.499.6100

Houston
600 Travis Street
Fifty-Eighth Floor
Houston, TX 77002
t: +1.713.860.7300
f: +1.713.353.3100

Los Angeles
515 South Flower Street
Twenty-Fifth Floor
Los Angeles, CA 90071
t: +1.213.683.6000
f: +1.213.627.0705

New York
200 Park Avenue
New York, NY 10166
t: +1.212.318.6000
f: +1.212.319.4090

Orange County
695 Town Center Drive
Seventeenth Floor
Costa Mesa, CA 92626
t: +1.714.668.6200
f: +1.714.979.1921

Palo Alto
1117 S. California Avenue
Palo Alto, CA 94304
t: +1.650.320.1800
f: +1.650.320.1900

San Diego
4747 Executive Drive
Twelfth Floor
San Diego, CA 92121
t: +1.858.458.3000
f: +1.858.458.3005

San Francisco
101 California Street
Forty-Eighth Floor
San Francisco, CA 94111
t: +1.415.856.7000
f: +1.415.856.7100

São Paulo
Av. Presidente Juscelino
Kubitschek, 2041
Torre D, 21º andar
São Paulo, SP, 04543-011
Brazil
t: +55.11.4765.3000
f: +55.11.4765.3050

Washington, DC
2050 M Street, N.W.
Washington, DC 20036
t: +1.202.551.1700
f: +1.202.551.1705

ASIA

Beijing
Suite 2601, 26/F
Yintai Center, Office Tower
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022, PRC
t: +86.10.8567.5300
f: +86.10.8567.5400

Hong Kong
21-22/F Bank of China Tower
1 Garden Road
Central Hong Kong
t: +852.2867.1288
f: +852.2523.2119

Seoul
33/F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu,
Seoul 04539, Korea
t: +82.2.6321.3800
f: +82.2.6321.3900

Shanghai
43/F Jing An Kerry Center
Tower II
1539 Nanjing West Road
Shanghai 200040, PRC
t: +86.21.6103.2900
f: +86.21.6103.2990

Tokyo
Ark Hills Sengokuyama Mori
Tower
Fortieth Floor
1-9-10 Roppongi
Minato-ku Tokyo 106-0032
Japan
t: +81.3.6229.6100
f: +81.3.6229.7100

EUROPE

Brussels
Avenue Louise 480
1050 Brussels
Belgium
t: +32.2.641.7460
f: +32.2.641.7461

Frankfurt
TaunusTurm – Taunustor 1
60310 Frankfurt am Main
Germany
t: +49.69.907485.000
f: +49.69.907485.499

London
100 Bishopsgate
London EC2N 4AG
United Kingdom
t: +44.20.3023.5100
f: +44.20.3023.5109

Paris
32, rue de Monceau
75008 Paris
France
t: +33.1.42.99.04.50
f: +33.1.45.63.91.49