PILLAR LEGAL

The California Privacy Protection Agency Talks Rulemaking—Are Businesses Ready for New California Data Privacy Rules?

U.S. TECH LAW UPDATE[1]

September 29, 2021
By: Greg Pilarowski | Alexandra Ashbrook | Ziwei Zhu

I. Introduction

On November 3, 2020, California voters passed Proposition 24 enacting the California Privacy Rights Act ("CPRA" or "2020 Act").[2] The CPRA becomes effective January 1, 2023 and will be enforced by the newly created California Privacy Protection Agency and the California Attorney General starting July 1, 2023. In accordance with California privacy activists' efforts to strengthen the California Consumer Privacy Act of 2018 ("CCPA" or "2018 Act," with the 2020 Act the "Privacy Acts"), the 2020 Act substantively amends and expands the 2018 Act.

The battle to define Californian consumers' privacy rights continued after then-California Governor Jerry Brown signed the CCPA into law in June of 2018. In October of 2019, California Governor Newsom signed five amendments to the 2018 Act and an amendment to California's data breach law.[3] The following month, privacy activists submitted Proposition 24 to the California Attorney General, which noted that throughout 2019 the California legislature considered many more amendments to the CCPA, "some of which would have significantly weakened it."[4] In November of 2020, California voters passed Proposition 24 with over 9.3 million votes, the sixth most votes for any ballot initiative in California history.[5] The 2020 Act includes a provision that explicitly limits amendments to only those that are consistent with and further the intent and purpose of the Privacy Acts in order to safeguard against similar attempts to weaken Californian consumer protections in the future.[6]

Pursuant to the 2020 Act, Californian consumer's privacy rights will now be safeguarded by a newly founded body: the California Privacy Protection Agency ("CPP Agency" or "Agency"). The 2020 Act vests the Agency with full administrative power, authority and jurisdiction to implement and enforce the Privacy Acts.[7] The CPP Agency is governed by a five-member board comprised of Californians with expertise in privacy, technology, and consumer rights.[8]

---

[1] This U.S. Tech Law Update is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This U.S. Tech Law Update may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-474-3258 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: info@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] The full text of Proposition 24 is available here.

[3] *Governor Newsom Issues Legislative Update 10.11.19*, OFFICE OF GOVERNOR GAVIN NEWSOM (Oct. 11, 2019).

[4] See Proposition 24, Section 2(D).

[5] *California Privacy Rights Act*, CALIFORNIANS FOR CONSUMER PRIVACY.

[6] See Proposition 24, Section 25.

[7] Cal. Civ. Code § 1798.199.10(a).

[8] *California Officials Announce California Privacy Protection Agency Board Appointments*, OFFICE OF GOVERNOR GAVIN NEWSOM (Mar. 17, 2021).

On September 7 and 8, 2021, the board of the CPP Agency hosted a public virtual meeting to address its rulemaking responsibilities under the 2020 Act.[9] At the meeting, members of the board announced the CPP Agency shall begin the rulemaking after it gives notice to the Attorney General and intends to submit its proposed regulations by mid-May 2022.[10] When proposing its regulations, the Agency is empowered to add to, amend, or repeal any regulation that the Attorney General enacted with respect to the Privacy Acts. More information on the CPP Agency is provided below.

The 2020 Act will affect many businesses operating in California, as key changes introduced affect the scope of businesses and personal information covered by the Privacy Acts, consumers' privacy rights, required privacy notices and disclosures, and employer obligations. This Tech Law Update summarizes the 2020 Act's key changes, and also provides a table that compares the key provisions of the Privacy Acts against the European Union's General Data Protection Regulation ("GDPR") and the Personal Information Protection Law ("PIPL") adopted by the People's Republic of China ("China").[11]

II. Key 2020 Act Changes

a. Important Definitions

1. *"Sensitive Personal Information"*

The 2020 Act adds a new category of personal information protected under the Privacy Acts. "Sensitive Personal Information" is a type of personal information that includes a consumer's social security number, driver's license, financial account, login information, race, ethnicity, religious or philosophical beliefs, and the contents of nonpublic communications.[12] Recognizing that misuse of Sensitive Personal Information may be more harmful than misuse of other types of personal information, the 2020 Act imposes new restrictions on and consumer rights in the collection, processing, and sharing of Sensitive Personal Information, as addressed below.

The introduction of Sensitive Personal Information into the Privacy Acts means that covered businesses must take extra precautions when handling this type of data and comply with consumer rights surrounding the data. Moreover, businesses that intend to store Sensitive Personal Information of California consumers will be required to comply with disclosure obligations, and provide new links on their websites enabling consumers to restrict the processing of their Sensitive Personal Information.[13]

2. *"Cross-Context Behavioral Advertising"* and *"Sharing"*

[9] *September 7-8, 2021 Board Meeting*, CALIFORNIA PRIVACY PROTECTION AGENCY (Sept. 7, 2021).
[10] *California Privacy Protection Agency Board Meeting Minutes*, CALIFORNIA PRIVACY PROTECTION AGENCY (Sept. 7, 2021).
[11] For a brief overview on the CCPA as first-enacted, please see our US Tech Law Update "California Consumer Privacy Act 2018 – California's GDPR?", published on November 6, 2018. For a brief overview on China's evolving privacy laws, please see our China Regulation Watch, "China's Evolving Personal Information Protection Rules," published September 28, 2020.
[12] Cal. Civ. Code § 1798.140(ae).
[13] Cal. Civ. Code § 1798.135.

The 2020 Act introduces limitations related to "cross-context behavioral advertising," defined under the law as the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.[14] In addition, while the 2018 Act applied to the sale of personal information, the 2020 Act amends the law to also apply to the "sharing" of personal information with another third party for the purpose of "cross-context behavioral advertising," even where nothing of monetary value is exchanged.[15] The definition of "sharing" was included to address conventional tracking-based advertising technology methods, such as syncing and the broadcasting of real-time bidding requests.[16] In addition to restrictions on the sharing of personal information, California consumers will now have the right to opt-out of cross-context behavioral advertising altogether.[17]

In practice, these limitations will have a significant impact on online advertisement businesses (often referred to as "adtech"). Particularly, companies utilizing cookies to track users across internet domains to determine which advertisements should be shown to a particular consumer are now not only fully brought under the Privacy Acts but will also be obligated to allow California consumers to opt-out of such tracking. Previously, adtech companies and other tech industry giants such as Facebook and Google relied on the ambiguous definition of "sale" under the 2018 Act to avoid compliance obligations.[18] Early data suggests that most users will opt-out of tracking for cross-context behavioral advertising when given the choice.[19]

b. Introduction of the CPP Agency

As mentioned above, the 2020 Act established the CPP Agency. Prior to the 2020 Act, the California Attorney General retained enforcement authority under the 2018 Act.[20] Following the adoption of the 2020 Act, the CPP Agency is now poised to become the primary educational and enforcement authority of the Privacy Acts, although the state Attorney General will retain the authority to coordinate with the CPP Agency and to impose civil penalties.[21] Similar to the European Union's Data Protection Authorities, which supervise the application of the GDPR through investigative and corrective powers, provide guidance on data protection issues, and handle complaints lodged against violations of the GDPR in each member-state, the CPP Agency operates as the central point of contact for businesses and citizens engaging with personal information or privacy rights.

In its enforcement capacity, the CPP Agency will appoint a chief privacy auditor to oversee audits ensuring business compliance with the Privacy Acts.[22] The CPP Agency will also be responsible for coordinating regulatory activities with privacy agencies from other states and

[14] Cal. Civ. Code § 1798.140(k).
[15] Cal. Civ. Code § 1798.140(ah)(1).
[16] Johnny Ryan, *California Privacy Rights Act to define and limit "cross-context behavioral advertising"*, LINKEDIN (June 22, 2020).
[17] Cal. Civ. Code § 1798.140(ah)(1).
[18] Elise Feikje van der Berg, *Web tracking giants Facebook and Google don't consider themselves data-sellers under CCPA*, DATAWALLET (Feb. 3, 2020).
[19] Samuel Axon, *96% of US users opt out of app tracking in iOS 14.5, analytics find*, ARSTECHNICA (May 7, 2021).
[20] *CCPA Enforcement Case Examples*, CALIFORNIA OFFICE OF THE ATTORNEY GENERAL (accessed September 20, 2021).
[21] Cal. Civ. Code § 1798.199.10.
[22] Cal. Civ. Code § 1798.199.40(f).

jurisdictions.[23] In its rulemaking and educational capacities, the CPP Agency will provide guidelines for consumers regarding their rights and guidelines for businesses regarding their obligations under the Privacy Acts, as well as award grants from its budget for educational purposes.[24] An additional responsibility of the CPP Agency will be to provide advice to the California legislature with respect to any future privacy-related legislation, and to keep abreast of any new developments in the field of data privacy.[25]

Notably, the CPP Agency's role in rulemaking and enforcement marks a significant change from the 2018 Act. The Agency may investigate businesses, service providers, contractors, or individuals for violating the Privacy Acts, and impose administrative fines upon businesses that fail to cure such violations.[26] Creation of the CPP Agency indicates regulations, investigations, and enforcement actions will likely increase as responsibility shifts away from the Attorney General, which has complained of the "unworkable obligations and serious operational challenges upon the Attorney General's Office" imposed by the 2018 Act. After all, California's Office of the Attorney General is designed to operate as the state's top lawyer and law enforcement official—not a rulemaking body. Whereas the California Attorney General's obligations under the 2018 Act were in competition with the office's many other responsibilities, the CPP Agency can focus on both the original obligations imposed under the 2018 Act and any new ones imposed by the 2020 Act. Under the 2020 Act, the CPP Agency will have an annual budget of $10 million for its administrative, enforcement, and educational functions.[27]

c. Scope of Businesses Covered

While the 2018 Act's existing monetary threshold remains an annual gross revenue over $25 million, the 2020 Act doubled the 2018 Act's consumer threshold from 50,000 California consumers to 100,000 California consumers.[28] Moreover, the 2020 Act expanded the definition of covered businesses to include entities that share branding with a covered business, and joint ventures or partnerships composed of other covered businesses that have at least a forty percent (40%) stake in the entity.[29] The 2020 Act also updated the 2018 Act's annual revenue thresholds to include sharing of personal information.[30] Thus, following the implementation of the 2020 Act, the Privacy Acts now apply to (1) any business with gross revenues in excess of $25,000,000, (2) any business that annually buys, sells, or shares the personal information of 100,000 or more consumers or households, and (3) any business that derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

d. New Consumer Privacy Rights

Under the 2020 Act, Californian consumers are explicitly granted rights not available under the original 2018 Act. These new privacy rights are similar to those enumerated under

[23] Cal. Civ. Code § 1798.199.40(i).
[24] Cal. Civ. Code § 1798.199.40(d), (f).
[25] Cal. Civ. Code § 1798.199.40(g), (h).
[26] Cal. Civ. Code § 1798.199.45.
[27] Cal. Civ. Code § 1798.199.95(a).
[28] Cal. Civ. Code § 1798.40(d)(1)(B).
[29] Cal. Civ. Code § 1798.40(d)(1)(C).
[30] Cal. Civ. Code § 1798.40(d)(1)(C).

Europe's GDPR. Beginning January 1, 2023, consumers will be able to exercise the following new rights regarding the use of their personal information:

NEW CONSUMER PRIVACY RIGHTS UNDER THE 2020 ACT	
The Right to Correct	A consumer may now require a business to correct their personal information if the information is inaccurate.[31] Similar to consumer right obligations under the 2018 Act, businesses are required to disclose this right to the consumer.[32]
The Right to Opt-Out of Automated Decision-Making Technology	A consumer may now opt-out of the use of automated decision-making technology in line with the consumer's other opt-out rights.[33] These technologies include profiling or any other form of automated processing that evaluates a natural person to analyze or predict aspects concerning that person's behavior at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.[34] This consumer right also includes the ability to request information regarding the logic of the decision-making process behind the technology, as well as a description of the likely outcome of such a process.[35]
The Right to Restrict Sensitive Personal Information Processing	The 2020 Act introduces a list of restrictions on the usage of Sensitive Personal Information (defined above), including a new opt-out right to prohibit the selling or sharing of Personal Sensitive Information.[36] Businesses who use, sell, or share Sensitive Personal Information are also subject to disclosure obligations under the Privacy Acts.[37]
The Right to Data Portability	A consumer may now require a business to transmit the consumer's personal information in a structured, commonly used, and machine-readable format.[38] This right allows a consumer to receive his or her information in a format that easily allows the consumer to port the information from one platform or service to another. Alternatively, the consumer may request the business transmit the consumer's information to another platform or service on the consumer's behalf.

e. Changes to Existing Consumer Privacy Rights

[31] Cal. Civ. Code § 1798.106(a).
[32] Cal. Civ. Code § 1798.130(a)(5)(a)
[33] Cal. Civ. Code § 1798.185(a)(16).
[34] Cal. Civ. Code § 1798.140(z).
[35] Cal. Civ. Code § 1798.185(a)(16).
[36] Cal. Civ. Code § 1798.135(c).
[37] Cal. Civ. Code § 1798.135(a); *see also* Cal. Civ. Code § 1798.135(b) for exceptions.
[38] Cal. Civ. Code § 1798.130(a)(3)(B)(iii).

In addition to introducing new consumer privacy rights, the 2020 Act strengthened some consumer privacy rights available under the 2018 Act. Beginning January 1, 2023, Californian consumers will be able to exercise the updated enumerated rights below:

CHANGES TO EXISTING CONSUMER PRIVACY RIGHTS UNDER THE 2020 ACT	
The Right to Know	Under the 2018 Act, a consumer was given the right to request knowledge of what personal information a business collects regarding that consumer.[39] Related to this right, businesses were obligated to provide the consumer with a description of all personal information collected about consumers within the twelve-month period preceding the request, the categories of sources from which such information was collected, whether such information was sold and to whom it was sold, amongst various other disclosures.[40] The 2020 Act expands a business' obligations in relation to this right. In particular, the business must also disclose what personal information is shared and to whom it is shared.[41]
The Right to Delete	Under the 2018 Act, consumers were authorized to require businesses to delete their personal information, and businesses were obligated to comply with the request.[42] The 2020 Act expands a business' compliance obligations. A business in receipt of a consumer request to delete must also notify third parties to delete any personal information sold or shared by the business (unless impossible or disproportionately difficult).[43]
The Right to Opt-Out	The 2020 Act extends the protections of the 2018 Act to apply to the sharing of personal information in addition to the sale of personal information. Correspondingly, the 2020 Act also extends the right to opt-out of the sale of

[39] Cal. Civ. Code § 1798.110.
[40] Cal. Civ. Code § 1798.130(a)(2)(B).
[41] Cal. Civ. Code § 1798.115.
[42] Cal. Civ. Code § 1798.105.
[43] Cal. Civ. Code § 1798.105(c)(1).

	their personal information to also apply to the sharing of their personal information.[44]
The Right to Opt-In for Minors	The 2018 Act created an "opt-in" right for consumers less than sixteen years of age. If a minor consumer does not opt-in to the sale or sharing of their personal information, the 2020 Act now requires businesses wait at least twelve months before again requesting that the minor consumer opt-in to the sale or sharing of their personal information.[45]

III. What Businesses Need to Know

a. Workforce Personal Information Exemptions Expiring in 2023

The original 2018 Act exempted some types of workforce personal information from the Privacy Acts' scope. The 2020 Act extends such exemptions until January 1, 2023. Beginning in 2023, the Privacy Acts will apply to the personal information a business collects about employees, job applicants, owners, directors, officers, medical staff members, and independent contractors of the business as such information relates to that person's role, emergency contact information, and/or benefits.[46] Accordingly, workforce members will also be entitled to exercise the same rights as any consumer under the Privacy Acts. Workforce members are also provided a new right that prohibits businesses from retaliating against them for exercising any of their rights under the Privacy Acts.[47]

b. New Third-Party Service Provider Requirements

The 2020 Act significantly expands contracting requirements for businesses that collect personal information. While the 2018 Act covered "service providers" (i.e., any person or entity that receives or processes personal information on behalf of a business), the 2020 Act also subjects "contractors" and "third-parties" to coverage under the Privacy Acts.

Service Provider	An entity that processes personal information from or on behalf of the business pursuant to a written contract.[48]
Contractor	An entity that receives personal information for a business purpose pursuant to a written contract.[49]

[44] Cal. Civ. Code § 1798.135(c)(4).
[45] Cal. Civ. Code § 1798.135(c)(5).
[46] Cal. Civ. Code § 1798.145(m)(1).
[47] Cal. Civ. Code § 1798.125(a)(1)(E)
[48] Cal. Civ. Code § 1798.40(ag)(1).
[49] Cal. Civ. Code § 1798.40(j)(1).

Other Third-Party	Any person or entity that is not a service provider or contractor but receives personal information from the business.[50]

The annotated version of the 2020 Act highlights that a contractor essentially functions identically to a service provider, with the distinction that service providers process personal information received "from or on behalf of" a business, whereas contractors use personal information "disclosed by" a business."[51] Notably, the 2020 Act explicitly requires businesses to have contracts in place with all types of recipients of personal information, and requires those contracts to include provisions that:

- State that the business sells or disclose the personal information only for limited and specific purposes.

- Obligate the third party, service provider, or contractor to comply with the Privacy Acts and require them to provide the same level of privacy protection the Privacy Acts require.

- Grant the businesses rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information in a manner consistent with the business's obligations under the Privacy Acts.

- Require the third party, service provider, or contractor to notify the business if it determines that it can no longer meet its obligations under the Privacy Acts.

- Grant the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.[52]

Businesses working with the personal information of Californian consumers should ensure the above provisions are addressed in all contracts under which the business provides personal information to a service provider, contractor or other third-party. Considering the exponential rise in cyber threats, ensuring contractual compliance with the Privacy Acts may help to minimize security risks associated with sharing personal information outside of a business' closed ecosystem.[53]

c. Updating Notices, Disclosures, and Polices

Similar to many other recent iterations of privacy legislation introduced around the country and world, the 2020 Act requires businesses to adjust their notices, disclosures, and policies in accordance with the law's provisions.

1. *Notice at Collection*

[50] Cal. Civ. Code § 1798.40(ai).
[51] The California Privacy Rights Act of 2020, comment CCP7, *available at* https://uploads-ssl.webflow.com/5aa18a452485b60001c301de/5d8bc3342a72fc8145920a32_CPREA_2020_092519_Annotated_.pdf.
[52] Cal. Civ. Code § 1798.100(d).
[53] *Global Security Insights Report 2021: Intelligence from the Global Cybersecurity Landscape*, VMWARE (2021).

The 2018 Act required businesses provide a "notice at collection" when they intend to collect personal information directly from a Californian consumer. The 2020 Act expands the amount and type of information that must be provided in the notice. In addition to the categories of personal information collected, businesses must also disclose the commercial purpose for collecting the information, how to opt-out of the sale of personal information, and information on how to find the company's privacy notice. In addition, the Privacy Acts now require disclosure of whether Sensitive Personal Information is collected and the length of time the business intends to retain each category of personal information.[54]

2. *Privacy Policy*

When the 2018 Act came into effect, many businesses were required to implement new privacy policies or bring existing ones into compliance.[55] The Privacy Acts now require businesses to update their privacy policies again. Before a business next reviews and updates its privacy policy—and no later than January 1, 2023—it may consider implementing new disclosures mandated under the 2020 Act, including:

- The retention period or retention criteria for each category of personal information collected.

- Details about the business' processing of Sensitive Personal Information.

- Californian consumer's new privacy rights (above).

- Whether the business sells or shares personal information. [56]

d. Adoption of GDPR-Inspired Practices

The GDPR was adopted by the European Union in 2016. Since then, many other territories borrowed from the concepts first enumerated in the GDPR to draft their own data privacy regulations. While California's 2018 Act included many GDPR-inspired provisions, the 2020 Act further harmonizes California's Privacy Acts with the European Union's GDPR.

1. *Audit Obligations*

The 2020 Act introduces audit obligations for certain businesses. Under the GDPR, businesses are required to conduct "Data Protection Impact Assessments" when engaging in high-risk processing.[57] Now, businesses that use the personal information of Californian consumers will have similar requirements. Businesses whose processing of personal information presents a significant risk to consumers' personal information and privacy must perform annual audits and submit risk assessments to the CPP Agency for review.[58] Although the CPP Agency

[54] Cal. Civ. Code § 1798.100(a)(2),(3).
[55] Cal. Civ. Code § 1798.130(a)(5).
[56] Cal. Civ. Code § 1798.115(b)(5).
[57] GDPR Art. 35.
[58] Cal. Civ. Code § 1798.185(a)(15)(A), (B).

has yet to establish the factors to be considered in determining when processing results in a significant risk, businesses engaged in "high-risk processing" under the GDPR are encouraged to prepare for similar audit obligations under California's Privacy Acts.

2. *Data Minimization and Purpose Limitation*

Similar to the GDPR, the 2020 Act introduces the concept of "data minimization" to California's data privacy regime. The Privacy Acts will now prohibit the collection, use, retention, and sharing of a consumer's personal information that is not reasonably necessary and proportionate to achieve the purposes for which it was collected, processed, or disclosed.[59] In addition, the 2020 Act specifies that personal information cannot be used for additional purposes that are incompatible with the disclosed purpose for which the personal information was first collected.[60] Businesses engaging with consumer personal information will need to limit their collection to only the personal information required for the business' disclosed purpose(s) and ensure they do not use the personal information in any way inconsistent with the purpose(s) previously disclosed.

3. *Retention Period Limitation*

Provisions of the 2020 Act provide for a new retention period limitation. This limitation was absent from the original 2018 Act but is a familiar concept under the GDPR and other similar privacy laws. When the 2020 Act enters into force, businesses can no longer retain a consumer's personal information or Sensitive Personal Information longer than reasonably necessary to achieve the purpose disclosed to the consumer.[61] Businesses in possession of personal information after such information has served its purpose must ensure this data is ultimately purged.

4. *Data Security*

Throughout the GDPR, the law calls for "appropriate technical and organizational measures" to ensure data security. Following the adoption of the 2020 Act, California's Privacy Acts will similarly include explicit requirements for businesses to implement "reasonable security procedures and practices" appropriate to the nature of the personal information being handled. These procedures and practices must protect consumer personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.[62] The 2020 Act does not, however, define what constitutes reasonable security procedures under California's privacy regime. Without further guidance from the CPP Agency, businesses may consider California's 2016 Data Breach Report, which recommends the 20 controls in the Center for Internet Security's Critical Security Controls as the minimum level of information security a business that collects or maintains personal information should meet.[63]

e. Increased Penalties

[59] Cal. Civ. Code § 1798.100(c).
[60] Cal. Civ. Code § 1798.100(a)(1).
[61] Cal. Civ. Code § 1798.100(a)(3).
[62] Cal. Civ. Code § 1798.100(e).
[63] Kamala Harris, Attorney General, California Data Breach Report 2012-2015, CALIFORNIA DEPARTMENT OF JUSTICE (Feb. 2016).

Businesses in possession of personal information should also be aware of the increases in penalties for violations established by the 2020 Act.

CHANGES TO PENALTIES UNDER THE 2020 ACT	
Minors' Data	Fines for violations involving the personal information of consumers known to be under 16 years of age are tripled from US$2,500 to US$7,500 under the 2020 Act. The CPP Agency may bring an administrative enforcement action for this fee against any entity found in violation of minors' rights under the Privacy Acts.[64]
Theft of Log-In Information	The 2020 Act explicitly authorizes a private civil cause of action for unauthorized access and exfiltration, theft, or disclosure of an email address in combination with a password or security question that would permit access to an account due to failure to implement and maintain reasonable security procedures and practices.[65] Previously, this private civil cause of action was only applied to nonencrypted or nonredacted personal information.

IV. Looking Ahead

The CPP Agency met for the first time in June of 2021. Since then, the CCP Agency has met with increasing frequency in preparation for July 1, 2022, when its guidance on certain provisions of the Privacy Acts is expected to be finalized.[66] Amongst its other obligations, the CPP Agency is expected to:

- Establish standards on the consumer's right to correct and right to delete.[67]

- Establish standards surrounding service provider and contractor use of personal information received pursuant to a contract.[68]

[64] Cal. Civ. Code § 1798.155(b).
[65] Cal. Civ. Code § 1798.150(a)(1).
[66] Cal. Civ. Code § 1798.185(a).
[67] Cal. Civ. Code § 1798.185(a)(7), (8).
[68] Cal. Civ. Code § 1798.185(a)(10), (11).

- Issue regulations on mandatory cybersecurity audits and risk assessments for processing activities entailing significant risks.[69]

- Provide technical specifications and standards for "opt-out preference" signals sent by a platform, technology, or mechanism.[70]

- Clarify privacy protections governing use and disclosure of Sensitive Personal Information.[71]

Ultimately, the 2020 Act will become operative on January 1, 2023. When it does, consumers will be entitled to exercise their new rights related to their personal information obtained all the way back to January 1, 2022! Preparing for California's compliance obligations early will ensure businesses are ready on July 1, 2023, when the CPP Agency will begin enforcing the 2020 Act. Now is the time for a business subject to California's Privacy Acts to consider reviewing agreements with third parties, updating notifications, disclosures, and policies, and conducting internal data audits.

[69] Cal. Civ. Code § 1798.185(a)(15).
[70] Cal. Civ. Code § 1798.185(a)(19)(A), (B).
[71] Cal. Civ. Code § 1798.185(a)(19)(C).

V. Comparison Table

COMPARISON TABLE: California, Europe and China			
	California[72]	**Europe**	**China**
Protects	"**Consumers**" who are California residents that are either: • In California for other than a temporary or transitory purpose; or • Domiciled in California but currently outside the state for a temporary or transitory purpose. **"Households"**, i.e., a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common device(s) or service(s). **Cal. Civ. Code** § 1798.140(i) **Cal. Civ. Code** § 1798.140(q) **11 C.C.R.** § 999.301(k)	"**Data subjects**" who are in the European Union that can be identified by reference to an identifier such as a name, an identification number, location data, online identifiers, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. **GDPR** Article 3	Personal information rights and interests of any "**natural person**". **PIPL**[73] Article 2
Regulates	"**Businesses**" that: • Have annual gross revenues in excess of US$25,000,000; • Annually buy, sell, or share the information of 100,000	"**Controllers**" located both inside and outside of the European Union who are natural or legal people, public authorities, agencies, or bodies which determines the purpose and means of	"**Personal information processors**" that: • Process personal information in China; or • Process personal information of any natural

[72] This column of the Comparison Table represents the California Privacy Acts, including the 2018 Act as amended by the 2020 Act.
[73] PIPL was passed into law in China on August 20, 2021, and will become effective November 1, 2021.

	or more consumers or households; or • Derive 50% or more of annual revenues from selling or sharing consumers' personal information.	processing of personal data of data subjects. "**Processors**" located both inside and outside of the European Union who are natural or legal people, public authorities, agencies, or bodies which process personal data of data subjects on behalf of a controller.	person located in China **from overseas**, with the purpose of (i) providing product or service to natural person located in China; or (ii) analyzing the behavior of natural person located in China. **"Activities of processing personal information"** including the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information.
	Cal Civ. Code § 1798.140(d)	**GDPR** Article 24 **GDPR** Article 28	**PIPL** Article 3 **PIPL** Article 4
Types of Data	"**Personal information**" that identifies, relates to, describes, or is capable of being linked to or associated with a particular consumer or household. Non-exhaustive examples include: • Commercial information • Internet or electronic network activity information • Audio, electronic, visual, thermal, olfactory, or similar information	"**Personal data**" that relates to an identified or identifiable data subject. "**Pseudonymized data**" that is processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information when the business also: • Keeps any additional information separately; and • Implements technical and organizational measures to ensure personal data is not	"**Personal information**" meaning any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized. "**Anonymization**" refers to the process in which any personal information is processed to the extent that it cannot identify a specific natural person and cannot be restored to its original state.

	• Professional or employment-related information • Education information • Inferences drawn from information "**Deidentified**" information refers to information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer. "**Sensitive personal information**", a subcategory of personal information that includes but is not limited to: • Identifiers such as name, postal address, online identifier, IP address, email address, social security number, and other similar identifiers • Characteristics of protected classifications under California or federal law • Biometric information • Precise geolocation	attributed to an identified or identifiable data subject. "**Special categories of data**" revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.	"**Sensitive personal information**" refers to personal information that, once leaked or illegally used, will easily lead to infringement of personality rights or harm personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical and health, financial account, personal location tracking and other information of a natural person, as well as any personal information of a minor under the age of 14.
	Cal. Civ. Code § 1798.140(o) **Cal. Civ. Code** § 1798.140(m) **Cal. Civ. Code** § 1798.140(ae)	**GDPR** Article 3 **GDPR** Article 9	**PIPL** Article 4 **PIPL** Article 73 **PIPL** Article 28

Required Notices	"**Privacy policy**" made available to consumers describing the business' practices regarding the collection, use, disclosure, and sale of personal information, and the rights of consumers regarding their own personal information. "**Notice at collection**" given by a business to a consumer at or before the point at which the business collects personal information. "**Notice of right to opt-out**" given by a business informing consumers of their right to opt-out of the **sale or sharing** of their personal information and/or sensitive personal information, including in an interactive form accessible via a clear and conspicuous link titled "**Do Not Sell or Share My Personal Information**" on the business's website or mobile application. "**Notice of right to limit use and disclosure of sensitive personal information**" given by a business informing consumers of their right to limit the use and disclosure of sensitive personal information, including in an interactive form	Controllers must **provide information** to the data subject, in situations where personal data is collected from the data subject or a third-party.	Prior to processing activities, personal information processors must inform the individual of: • The processor's name and contact information; • The processing purpose, method, information type, retention period; and • The procedure of exercise individual's rights under PIPL. Any change to the above-mentioned matters must be conveyed to the individual. Prior to the **processing sensitive personal information**, processors must also inform the individual of the **necessity** and the **impact on the individual's rights and interests.**

	accessible via a clear and conspicuous link titled "**Limit the use of My Sensitive Personal Information**" on the business's website or mobile application. **"Notice of financial incentive"** given by a business explaining each financial incentive or price or service difference related to providing personal information.		
	11 C.C.R. §§ 999.308 **11 C.C.R.** §§ 999.305 **11 C.C.R.** §§ 999.306 **11 C.C.R.** §§ 999.307 **Cal. Civ. Code** § 1798.120 **Cal. Civ. Code** § 1798.121	**GDPR** Articles 13 – 14	**PIPL** Article 17 **PIPL** Article 30
Minors	Businesses with personal information of **minors under 13 years of age** must establish, document, and comply with a reasonable method for determining and receiving affirmative authorization from the minor's parent or guardian to opt-in to the sale or sharing of their personal information. Businesses with personal information of **minors at least 13 and less than 16 years of age** shall establish, document, and comply	Processing of personal data of **minors below 16 years of age** must be consented to by the minor's parent or guardian.	Processing of personal information of **minors below 14 years of age** must be consented to by the minor's parent or guardian. Personal information processors must establish **special rules** for processing personal information of minors under the age of 14.

	with a reasonable process for allowing such minors to opt-in to the sale or sharing of their personal information.		
	11 C.C.R. §§ 999.330 **11 C.C.R.** §§ 999.331 – 999.332	**GDPR** Article 8	**PIPL** Article 31
Third Parties	**Third party contracts** that involve **selling, sharing, or disclosing personal information** are required to include terms and provisions compliant with procedure under the Privacy Acts. Required contract terms must include provisions that: • State that the business sells or discloses the personal information only for limited and specified purposes; • Obligate the third party to comply with California's Privacy Acts and require them to provide the same level of privacy protection the Privacy Acts require; • Grant the business rights to take reasonable and appropriate steps to help ensure that the third party uses the personal information in a manner consistent with California's Privacy Acts; • Require the third party notify the business if it determines that it can no longer meet its privacy obligations; and • Grant the business the right to take reasonable and appropriate steps	Once personal data is **transferred or shared**, the receiving party will become a data controller, and therefore will be required to comply with all the requirements applicable to a controller under GDPR. "**Engaging a processor to process**" data on behalf of a controller must be governed by a data processing agreement between the controller and the processor, which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The obligations of a processor that must be set forth in a data processing agreement include: • Process the personal data on instructions from the controller; • Ensure that persons authorized to process the personal data are under an appropriate statutory obligation of	When **providing** personal information **to a third party**, personal data processors shall: • Provide the individual with detailed information of the receiving party and the processing activities involved; • Obtain specific consent from the individual; and • Conduct a personal information protection impact assessment. When **engaging a third party** to process personal information, personal information processors shall: • Reach an agreement with the third party on the purpose, period, and method of the processing, the type of personal information to be processed, any protection measure to be taken, and

	to stop and remediate unauthorized use of personal information.	confidentiality; • Take all measures required for data security; • Assist the controller to respond to requests for exercising the data subject's rights; and • Delete or returning all the personal data to the controller after the processing service ends.	the rights and obligations of both parties, and • Supervise third party's processing activities.
	Cal. Civ. Code § 1798.100(d)	**GDPR** Article 28	**PIPL** Article 23 **PIPL** Article 55 **PIPL** Article 21
Cross-Border Transfers	No prohibitions on cross-border transfers of personal information.	In cases of transfer of personal data **within the EU**, the GDPR does not impose any additional requirements. In the case of transfer of personal data **outside of the EU**, the GDPR requires the recipient's country to be covered by an **adequacy decision** by the EU commission or the transfer to be subject to **appropriate safeguards**.	Before providing personal information **to an overseas recipient**, a personal information processor must fulfill at least one of the following conditions: • Pass the security assessment conducted by Cyberspace Administration of China ("CAC"); • Undertake personal information protection certification conducted by professional agencies; • Sign a contract with the overseas recipients in accordance with the standard contract provided by CAC. Additionally, personal information processors shall:

			• Provide individuals with detailed information of the overseas recipient, the processing activities involved, and the procedure of exercising individual's rights under PIPL; • Obtain specific consent from the individual; and • Conduct a personal information protection impact assessment. Personal information processors whose processing of personal information reaches the **threshold amount** prescribed by CAC, must pass the **security assessment** conducted by CAC before providing personal information to an overseas recipient. An overseas personal information processor who **provides a product or service** to a natural person located in China or **analyzes the behavior** of natural person located in China, shall: • Establish a special agency or appoint a representative in China to be responsible for personal information

			protection-related affairs; and • Submit the name and contact information of its agency or representative to relevant government authorities.
		GDPR Article 44 **GDPR** Article 45 **GDPR** Article 46	**PIPL** Article 38 **PIPL** Article 39 **PIPL** Article 55 **PIPL** Article 40 **PIPL** Article 53
Automated Decision Making and Profiling	California consumers will be able to **opt-out of automated decision-making technology**, and to access the logic involved in the decision-making process and a description of the process's likely outcome.	Data subjects have the right to not be **subject to a decision based solely on automated processing**, including profiling, which produces legal or other significant effects.	For push-based information and business marketing provided to individual based on automated decision-making technology, personal information processors must provide the individuals with: • An **option** not targeting the personal characteristics of the individual; or • An **easy way to refuse** to receive such information generated by automated decision-making. No unreasonable **differential treatment** of individuals in terms of **transaction prices** or other **transaction terms** should be implemented when using

			automated decision-making technology.
	Cal. Civ. Code § 1798.185(a)(16)	**GDPR** Article 22(1)	**PIPL** Article 24
DATA SUBJECT RIGHTS			
Right(s) to…	**California**	**Europe**	**China**
Know	The right to know **what personal information is sold and shared** and to whom. **Cal. Civ. Code** § 1798.115	The right to **receive detailed information** about a Controller's data collection and protection activities, including the legal basis for processing, and how to exercise data rights under the GDPR. The right to know what data is **shared with third parties.** **GDPR** Article 13 **GDPR** Article 14	The right to receive detailed information of the personal information processor, the processing activities, the procedure for the individual to exercise rights under PIPL, and any change to the processing rules. The right to know any provision of personal information to a **third party** or an **overseas recipient**. **PIPL** Article 17 **PIPL** Article 23 **PIPL** Article 39
Access	The right to **access personal information** and to know what personal information is being collected or has been collected about the consumer or household and to whom the personal information has been disclosed. **Cal. Civ. Code** § 1798.110	The "**right of access**" to obtain confirmation from the controller as to whether the data subject's personal data is being processed, as well as the data subject's right to obtain access to the personal data in a readable format. **GDPR** Article 15	The **right to access** or **make copies** of their personal information. **PIPL** Article 45
	The right to **correction** of personal information that is not accurate.	The "**right to rectification**" by the data subject to obtain from the	The **right to request** personal information processors to **correct**

Correct		controller the rectification of inaccurate personal data.	**or complete** their personal information.
	Cal. Civ. Code § 1798.106(a)	**GDPR** Article 16	**PIPL** Article 46
Delete	The right to **request to delete** personal information about the consumer or household that the business has collected from the consumer. **Cal. Civ. Code** § 1798.105	The "**right of erasure**" to obtain from the controller the erasure of personal data concerning the data subject without delay, subject to certain conditions. **GDPR** Article 17	The **right to request** personal information processors to **delete** personal information by withdrawing consent. **PIPL** Article 47
Restrict Processing	In accordance with the ability to limit the use and disclosure of sensitive personal information (see above), the right to restrict **sensitive personal information** to only the purpose for which the consumer disclosed the information. **Cal. Civ. Code** § 1798.135(2)	The "**right to restrict processing**" of personal data so that the controller can only continue to process the data subject's personal data with the data subject's consent, subject to certain conditions. The "**right to object**" by the data subject to particular types of processing. **GDPR** Article 19 **GDPR** Article 21	The **right to restrict or deny** personal information processors from the processing of their personal information. **PIPL** Article 44
Data Portability	Businesses must disclose and deliver information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer in a **readily useable format** that allows the consumer to transmit the information **from one entity to another entity without hindrance**.	The "**right to data portability**" whereby the data subject may request to transmit the data subject's personal data provided to a controller to another controller without hindrance.	Personal information processors must provide a way to transfer personal information to another personal information processor as designated by the individual.

	Cal. Civ. Code § 1798.130(a)(2)	**GDPR** Article 20	**PIPL** Article 45
No Retaliation/ Against Discrimination	Businesses **cannot discriminate** against consumers for exercising their privacy rights under California law. **Cal. Civ. Code** § 1798.125(a)(1)	Data subjects must be **protected from discriminatory consequences** derived from the processing of their personal data. **GDPR** Article 5 **GDPR** Article 22	Personal information processors **cannot refuse to provide service** to individuals that do not consent to the processing of their personal information, unless such personal information is necessary for providing the service. **PIPL** Article 16
Complain	Implied right to lodge a **sworn complaint** with the CPP Agency. **Cal. Civ. Code** § 1798.199.45	The "**right to lodge a complaint with a supervisory authority**" by the data subject **GDPR** Article 77	The right to **file a complaint or report** about any illegal activity of processing of personal information **with an authority performing personal information protection duties**. **PIPL** Article 65
Request Verification	Businesses must establish, document, and comply with, a reasonable method for verifying that the person making a request is the consumer about whom the business has collected information. **11 C.C.R.** §999.323	No specific request verification procedures. Controllers must use all reasonable measures to verify the identity of a data subject who requests access. **GDPR** Recital 64	No specific request verification procedures.
PRIVACY COMPLIANCE OBLIGATIONS			
	California	**Europe**	**China**
Internal Requirements	All businesses handling personal information must: • Inform individuals responsible for handling consumer	Controllers must maintain records of all processing activities under their responsibility. Processors must maintain a record of all categories of	Personal information processors shall conduct "**compliance reviews**" for their processing activities on a regular basis.

	inquiries about the requirements under California's Privacy Acts and how to direct consumers to exercise their rights; and • Maintain records of consumer requests made pursuant to California's Privacy Acts and how the business responded for at least 24 months. A business whose processing of consumers' personal information presents a significant risk to consumers' privacy or security must conduct a **cybersecurity audit** and submit a **risk assessment** to the CPP Agency with respect to their processing of the personal information. A business that reasonably should know that it buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year must: • Compile metrics for the previous calendar year as listed in 11 C.C.R. § 999.317(g)(1); • Disclose such metrics by July 1 of every calendar year; and • Establish, document, and comply with a training policy	processing activities carried out on behalf of a controller. Controllers and processors must conduct a **"data protection impact assessment"** where a type of processing uses new technologies and is likely to result in a high risk to data subjects. Controllers and processors must appoint a "**data protection officer**" in cases where: • The processing is carried out by a public authority or body; • The core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or • The core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offenses.	Personal information processors shall conduct a **"personal information protection impact assessment"** when: • Processing sensitive personal information; • Using personal information in automated decision-making; • Providing or disclosing of personal information to third party; or • Providing personal information to overseas recipient. Personal information protection impact assessment reports and relevant processing records shall be **retained for at least 3 years**. Personal information processor whose processing of personal information **reaches the threshold amount** prescribed by CAC shall appoint a **"personal information protection officer",** and such officer's name and contact information shall be disclosed to the public and submitted to the authorities in charge of personal information protection.

	for all individuals responsible for handling consumer requests and privacy law compliance.		If a network operator collects or processes the data of minors below the age of 14, it must appoint a **"specific person"** in charge of the minors' personal information protection.
	11 C.C.R. § 999.317 **Cal. Civ. Code** 1798.185(15)	**GDPR** Article 30 **GDPR** Article 35 **GDPR** Article 37	**PIPL** Article 54 **PIPL** Article 55 **PIPL** Article 56 **PIPL** Article 52 **Minor Personal Information Protection Provisions** Article 8
Security Requirements	Businesses must implement **reasonable security procedures and practices** appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.	Controllers and processors must implement **appropriate technical and organizational measures** to ensure a level of security appropriate to risk, including as appropriate: • Pseudonymization and encryption of personal data; • The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services; • The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical accident; and • A process for regularly testing the effectiveness of technical and organizational measures for ensuring processing security.	Network operators shall take **technical measures and other necessary measures** to ensure the security of personal information collected and to prevent information leakage, damage, and loss. Personal information processor shall implement the following measures where appropriate to ensure the security of personal information: • Making plans for internal administration and operation; • Classifying personal information;

		Controllers and processors may demonstrate compliance with security requirements by adhering to an **approved code of conduct** or an **approved certification mechanism.**	• Taking appropriate technical security measures such as encryption and de-identification; • Determining authority of employees in charge, and training employees on a regular basis; and • Making emergency plans for personal information security incidents.
	Cal. Civ. Code §1798.100(e) **Cal. Civ. Code** § 1798.150	**GDPR** Article 32 **GDPR** Article 40 **GDPR** Article 42	**Cyber Security Law** Article 42 **PIPL** Article 51
Data Breaches	A business must notify any California resident whose unencrypted and unredacted personal information was acquired by an unauthorized person. Any entity required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification to the Attorney General. **Cal. Civ. Code** § 1798.29(a), (e) **Cal. Civ. Code** § 1798.82(a), (f)	Controllers and processors must notify the supervisory authority. When the data breach is likely to result in a high risk to the rights and freedoms of the data subject, the controller must communicate information about the breach to the data subjects. **GDPR** Articles 33 – 34	For any leakage of, tampering with, or loss of personal information that occurs or may occur, a personal information processor shall take timely remedial measures, and notify the authorities in charge of personal information protection and any individual concerned. **PIPL** Article 57

Valuing Data	Businesses offering financial incentives or price or service differences in exchange for the sale or sharing of consumer personal information must use and document a reasonable and good faith method for calculating the value of the consumer's data. **Cal. Civ. Code** § 1798.125 **11 C.C.R.** § 999.337	The GDPR does not require controllers or processors to calculate the value of personal data.	The PIPL does not require the calculation of personal data values.
Legal Liability	A consumer whose nonencrypted and nonredacted personal information, or whose email address in combination with a password or security question and answer, is subject to a data breach may institute civil action to recover damages between **US$100 and US$750** per consumer per incident, or **actual damages**, whichever is greater. Any entity that violates California's Privacy Acts is subject to an injunction and liable for **a civil penalty** of not more than **US$2,500** for each violation and **US$7,500** for each intentional violation and each violation involving the personal information of minors.	Infringement of GDPR that causes material or non-material damage to a data subject entitles the data subject to compensation for the damages suffered from the controller and/or processor. Supervisory authorities may also impose **administrative fines** dependent upon the circumstances of each individual case. Fines for lesser violations are subject to fines up to **10,000, 000 EUR** or up to **2% of total worldwide annual turnover** for the preceding financial year, whichever is higher. Fines for larger violations may reach as high as **20,000,000 EUR** or up to **4% of total worldwide annual**	Violators will be ordered to **make a correction**, given a **warning**, ordered to **suspend or terminate** its services, and any illegal gains shall be **confiscated**, for a violation of PIPL. If the required correction is not made, a **fine** of up to **RMB1,000,000** will be imposed on the violator; and a fine between **RMB10,000 and RMB100,000** will be imposed on the person in charger or directly liable for the violation. If the violation is of a grave nature: • The violator will be ordered to make correction, confiscated of illegal gains, and fined up

		turnover for the preceding financial year, whichever is higher.	to **RMB 50,000,000 or 5% of last year's annual revenue**; and may also be ordered to **suspend any related business** for rectification, or have its business permit or business license cancelled; and • Its person in charge or directly liable for the violation will be fined between **RMB100,000 and RMB1,000,000**, and also be **banned** for a certain period from serving as a director, supervisor, senior officer or personal information protection officer of certain enterprises. Any violation under PIPL will be recorded into **credit files** and **disclosed to the public**. Where any damages are caused due to an infringement of personal information rights and interests, the personal information processor **shall bear tort liability**.
			PIPL Article 66

	Cal. Civ. Code §1798.150 **Cal. Civ. Code** § 1798.155	**GDPR** Article 82 **GDPR** Article 83	**PIPL** Article 67 **PIPL** Article 69