DETAILED COMPARISON OF ADPPA VS. CALIFORNIA PRIVACY LAWS

	ADPPA	CCPA/CPRA	Compare
Covered Entities	● Any person or entity (excluding individuals acting in a non-commercial context) that (1) alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and (2) is covered under the FTC Act, is a common carrier, or is a non-profit organization. ● ADPPA places some extra requirements on “large data holders” and gives some exemptions and other special treatment to small businesses.	● Entities that: 1) have annual gross revenue in excess of $25M; or, (2) collect the personal information of 100,000 consumers; or, (3) derive 50% or more of its revenue from selling consumers’ personal information.	ADPPA coverage is broader. It covers any entity and then either adds or removes requirements depending on whether an entity is a large or small business. CCPA does not cover nonprofits.
Future Amendments	● Congress has the power to amend ADPPA in the future in ways that could strengthen or weaken privacy protections	● The CPRA ballot initiative provides that amendments to the CCPA must be in furtherance of the privacy intent of the measure, so the CA legislature cannot go below a “floor” of protections.	The CCPA/CPRA provide a protection against amendments that would weaken privacy.
Data Minimization & Privacy Protections			
Data minimization	● Imposes a baseline duty on all covered entities not to unnecessarily collect or use covered data, regardless of any notice or consent. ● Limits the collection, processing, and transfer of covered data unless limited to	● Limits the collection, use, retention, and sharing of a consumer’s data to what is reasonably necessary and proportionate to achieve the purposes for which it was collected or processed, or for another disclosed purpose that is compatible with	ADPPA’s data minimization requirements are more specific and provide more detailed restrictions. .

	what is reasonably necessary and proportionate to (1) provide or maintain a product or service requested by the individual, (2) deliver a reasonably anticipated communication, or (3) effect a expressly permitted purpose.	the original purpose.	
Heightened Protections and Sensitive Data	● Imposes stricter data minimization rules for sensitive covered data: it cannot be collected or used beyond strict necessity to provide service or for expressly enumerated purposes. ● Enumerated purposes include: processing necessary to provide service; internal operations, improving a product or service for which the relevant data was collected; user authentication; security, harm, and fraud prevention; to comply with legal obligations; product recalls; public interest research; and to deliver P2P communications. ● Sensitive covered data cannot be transferred to third parties w/o opt-in consent or a few narrow exceptions. ● "Sensitive covered data" includes govt. identifiers, health info, financial info, biometric and genetic info, location info, private communications, login credentials, sexual behavior info, intimate images, video streaming choices, and info about	● Heightened protections for sensitive data only apply when such data is collected/processed for "the purpose of inferring characteristics about a consumer." ● In such circumstances, a business may use sensitive data without consent as necessary to provide service, for security, for transient non-personalized first party advertising, internal operations, quality assurance, or other purposes authorized by rulemaking. ● In other circumstances, businesses can use sensitive data with notice to users and the option to opt-out. ● "Sensitive personal information" includes govt. identifiers; health info; financial info; biometric and genetic data; login credentials; location info; race, religion, or union membership; communications content; and sexual behavior info. ● The CA Privacy Protection Agency can add more categories by rulemaking.	ADPPA is more protective because (1) its restrictions apply in all circumstances, not just scenarios using inferences; (2) it does not allow additional uses with notice and choice; (3) it restricts third party transfers to opt-in; and (4) it requires opt-in consent to use browsing history for secondary purposes.

	kids. ● FTC can designate new categories by rulemaking. ● Aggregate browsing data cannot be collected, processed, or transferred w/o opt-in consent or for enumerated permissible purpose.		
Use and disclosure limitations and controls	● Data minimization provisions (see above) limit use and disclosure. ● Transfer of sensitive covered data to third parties is prohibited without opt-in consent. ● Collection, use, and transfer of aggregate browsing history is limited without opt-in consent. ● Right to withdraw previously given consents. ● Right to opt-out of covered data transfers to third parties. ● Right to opt-out of targeted advertising, including by global opt-out mechanism.	● Data minimization provisions (see above) limit use and disclosure but current regulations permit secondary uses with user express consent. ● Users have the option to opt-out of the sale or sharing of their personal information and can direct companies to limit the use of their “sensitive” personal data on an opt-out basis in some situations. ● Contemplates a global opt-out.	ADPPA is more protective because there are more explicit prohibitions on secondary uses, especially for sensitive data, and less reliance on user opt-outs..
Manipulative design restrictions	● Prohibits obtaining consent in ways that are misleading or manipulative (e.g., dark patterns). ● Prohibits deceptive advertising.	● CCPA regulations prohibit dark patterns that subvert or impair right to opt-out ● California UDAP law prohibits deceptive advertising	Roughly equivalent.
Privacy by design	● Covered entities have a duty to implement reasonable policies, practices, and procedures for collecting, processing,	● No relevant provisions in CCPA.	ADPPA is more protective.

	and transferring covered data, which should correspond to the entity's size, complexity, activities related to covered data, the types and amount of data the entity engages with, and the cost of implementation compared to the risks posed. ● Privacy by design must also take into account the particular privacy risks related to individuals under age 17.		
Bans take-it-or-leave-it terms and pay-for-privacy	● Covered entities may not deny, condition, or effectively condition the provision or termination of services or products to individuals by having individuals waive any privacy rights in the Act. ● Covered entities are not prevented from offering loyalty programs. ● Covered entities may offer incentives to participate in market research. ● Covered entities can offer different pricing or functionality if a user requests to delete their covered data.	● While the CCPA purports to prohibit businesses from discriminating against a consumer because the consumer exercised their rights (including by charging different prices or rates), it allows businesses to offer "financial incentives," including payments to consumers as compensation for the collection, sale, or retention of their personal information. ● It also allows businesses to offer a different price, rate, level, or quality of goods or services if the price is "reasonably related to the value provided to the business by the consumer's data."	Roughly equivalent. CCPA has some loopholes in its exceptions but ADPPA is not sufficiently clear as to what extent it restricts differential pricing.
Transparency	● All covered entities and service providers must have privacy policies that meet a certain standard.	● Covered businesses must provide privacy notices that meet a certain standard. ● CPPA authorized to issue regulations to	Roughly equivalent.

	- Large data holders must also provide short-form notices. - Material changes to privacy policies require opt-in consent.	ensure this notice may be easily understood by the average consumer.	
Civil Rights and Algorithmic Fairness			
Prohibits discriminatory uses of data	- Covered entities and service providers may not collect, process, or transfer covered data in a manner that discriminates on the basis of race, color, religion, national origin, sex, or disability. - Covers intentional discrimination and disparate impact. - Exempts self-testing and DEI programs.	- No relevant provisions in CCPA/CPRA. - California Unruh Civil Rights Act prohibits discrimination by businesses, but it applies only to intentional discrimination, not disparate impact.	ADPPA is more protective. *Note: All state civil rights laws are exempt from preemption under ADPPA.*
Algorithmic Impact Assessments	- Requires large data holders to conduct annual algorithmic impact assessments and submit to the FTC. - Algorithmic evaluations must also occur at the design phase of an algorithm, including evaluating any training data that is used to develop the algorithm. - Covered entities must test for disparate impact on the basis of protected characteristics. - Covered entities must test for bias in certain high-risk algorithms.	- No specific algorithmic impact assessments required, though privacy impact assessments may apply to some automated decision making.	ADPPA is more protective because it requires algorithmic impact assessments, focusing on algorithmic bias and the risks from discrimination, which feeds into ADPPA's prohibition of discriminatory practices.

Automated Decision Making Rights	● No opt-out right for automated decision making (but anti-discrimination provisions apply to automated decision making)	● CPPA can issue regulations regarding application of access and opt-out rights to automated decision making.	Roughly equivalent. Opt-out rights may apply to automated decision-making in CA, but ADPPA anti-discrimination provisions are stronger.
Enhanced Protections for Kids & Teens			
Kids/teens protections	● Targeted advertising is expressly prohibited to individuals under 17. ● Covered entities may not transfer the covered data of individuals between 13 and 17 years old to third parties without express affirmative consent. ● Establishes a Youth Privacy and Marketing Division at the FTC. ● Algorithmic impact assessments must assess and mitigate harms to kids and teens. ● Kids data is protected as sensitive data.	● Kids' data cannot be sold unless parents (for kids under 13) or teens (ages 13–15) opt-in to sale.	ADPPA is more protective because it has strict data minimization requirements and use limits and prohibits targeted advertising to kids and teens.
Data Brokers			
Data Broker Registry	● Data Brokers ("Third Party Collecting Entities") must register with the FTC. ● The FTC will create a national registry of data brokers so that individuals can find them and exercise their rights.	● A separate California law requires data brokers to register with the state. ● Data brokers are subject to CCPA opt-out and other protections.	Roughly Equivalent

	● Data brokers are also covered entities subject to the rest of the Act.		
Data Broker Opt-out	● Requires the FTC to establish a “Do Not Collect” mechanism where individuals may submit a single request to all registered data brokers to have their covered data deleted within 30 days.	● Data brokers are required to provide the same “Do not sell or share my information” link as other covered businesses.	ADPPA is stronger. Individuals do not know which data brokers hold their info, therefore CA link is insufficient.
Data Security and Corporate Accountability			
Data Security Requirements	● Covered entities and service providers must have reasonable data security practices and procedures, based on their size, nature and scope of processing, volume and sensitivity of data, current state of the art, and cost. ● Large data holders must conduct biennial audits to ensure compliance with all applicable laws and submit audit reports to the FTC upon request.	● Covered businesses must implement reasonable security procedures and practices appropriate to the nature of the personal information to protect from unauthorized or illegal access, destruction, use, modification, or disclosure. ● Covered businesses must conduct cybersecurity audits.	Roughly equivalent.
Executive Responsibility	● An executive must personally certify compliance with the Act.	● No requirement that an executive must personally certify compliance with the Act.	ADPPA is more protective.
Privacy Impact Assessments	● Large data holders must conduct biennial privacy impact assessments that weigh the benefits of data use against the potential adverse consequences to privacy.	● Covered businesses must conduct regular risk assessments weighing the benefits of their data processing against risks to consumers, with the goal of not engaging in practices whose risks	Requirements for assessments are roughly equivalent, but CCPA stronger because assessments must be

		outweigh their benefits. ● Must be submitted to CPPA. ● CPPA can issue regulations governing these risk assessments.	submitted to the CPPA.
Service Providers and Third Parties			
Service Providers	● Service providers can only collect, process, and transfer data to the extent strictly necessary to provide service. ● Service providers shall not collect, process, or transfer data if they have actual knowledge the covered entity violated the Act. ● Service providers cannot transfer data without opt-in consent. ● Requirements for service provider contracts, including a prohibition on commingling data from multiple covered entities. ● Covered entity not liable for service provider violations if, at time of transfer, they had no reason to know the service provider was likely to violate the Act. ● Service providers are not liable for covered entity violations of the Act if they received covered data in compliance with the Act. ● Covered entity must exercise reasonable due diligence in selection of service	● Service providers may not retain, use, or disclose the information outside of the direct business relationship. ● Requirements for service provider contracts, including a prohibition on commingling data from multiple businesses, or using data for purposes other than serving the business. ● Service providers receiving personal data from a business must provide the same level of protection as the original business was obligated to provide under the law ● Businesses not liable for service provider violations if, at time of data transfer, they did not have actual knowledge, or reason to believe, that the service provider intended to violate the Act. ● Grants CPPA rulemaking authority to define the business purposes for which businesses and service providers may use consumers' personal information "consistent with consumers'	ADPPA is slightly more protective because it has a narrower liability safe harbor for covered entities and prohibits a service provider from continuing to provide service if it knows the covered entity is violating the Act. Most provisions are equivalent otherwise.

	providers.	expectations”	
Third Parties	● Individuals can opt-out of covered data transfers to third parties. ● Third parties cannot process sensitive covered data beyond the purpose for which opt-in consent was obtained. ● Third parties cannot process non-sensitive covered data beyond purposes disclosed in the covered entity’s privacy notice as the reasons for which the covered entity transfers data to third parties. ● Covered entity must exercise reasonable due diligence in deciding to transfer data to third party. ● Third parties typically will also be covered entities subject to the bill’s requirements.	● Third parties may not sell or share personal information that has been sold to or shared with the third party by a business unless the consumer is given the opportunity to opt-out. ● Third parties must provide the same level of protection as the original business was obligated to provide under the law ● Businesses are not liable for third party violations if, at time of data transfer, they did not have actual knowledge, or reason to believe, that the third party intended to violate the Act.	ADPPA is stronger because it does not give covered entities a safe harbor from liability arising from third party violations and because it has greater protections for sensitive data processed by third parties.
User Rights			
Right to access, correct, and delete	● Grants rights to access/correct/delete and data portability. ● Establishes exceptions and gives FTC rulemaking authority.	● Grants right to access/correct/delete/port	Roughly equivalent.
Accessibility			
Language	● Covered entities are required to provide	● Statute grants CPPA rulemaking	Roughly equivalent.

Accessibility	notices and mechanisms in all languages it provides service in. ● FTC must also publish guidance documents in multiple languages.	authority to ensure that notices required under CCPA are available in the language primarily used to interact with the consumer.	
Disability Accessibility	● Covered entities are required to provide notices and mechanisms in a manner that is readily accessible and usable by individuals with disabilities. FTC as well.	● Statute grants CPPA rulemaking authority to ensure that notices required under CCPA are accessible to individuals with disabilities.	Roughly equivalent.
Enforcement			
Government Enforcement	● New Bureau of Privacy at FTC to enforce the Act. ● State AGs and state privacy agencies can also bring lawsuits. ● FTC can create “technical compliance programs” to guide businesses on compliance with the Act in certain areas, but it is not a safe harbor and doesn’t affect burden in enforcement.	● CA Privacy Protection Agency (CPPA) enforces and issues regulations. ● CPPA can get statutory civil penalties. ● CPPA has a Chief Privacy Auditor who can audit businesses to ensure compliance with the law. ● Violations of CCPA can also be enforced by over 60 district and city attorneys.	ADPPA has nationwide enforcement by FTC and state AGs and privacy agencies CPPA. California law cannot directly protect people outside California.
Private right of action	● PRA is available for violations involving sensitive covered data, pay-for-privacy, transparency, individual rights, consents and opt-outs, kids’ protections, data brokers, civil rights, data security, service providers, and third parties. ● PRA doesn’t start until four years after the Act takes effect. ● Persons or classes of persons may bring	● The CCPA only provides a private right of action for data breaches.	ADPPA has a stronger private right of action because it can be used to enforce a broader range of violations. CCPA does provide statutory damages for data breach; ADPPA does not provide

	a civil action in federal court seeking compensatory damages, injunctive relief, declaratory relief, and reasonable attorney’s fees and litigation costs. ● Limits on joint action waivers. ● Some procedural hurdles such as limits on pre-dispute monetary demands, a requirement to notify FTC and state AGs, and a right to cure for defendants.		statutory damages. *Note: ADPPA does not preempt CCPA’s data breach private right of action.*