CALIFORNIANS FOR CONSUMER PRIVACY

This analysis is meant as a detailed response by Californians for Consumer Privacy (CCP), to an analysis published by the Electronic Privacy Information Center (EPIC). CCP's comments are posted in the right-hand column: green for CPRA 'stronger,' salmon for ADPPA 'stronger,' and yellow for 'roughly equivalent.'

The points are presented in the order originally selected by EPIC. Sometimes we have inserted a comment that EPIC did not address, as with our comment on GDPR Adequacy, and in that case we have left the "Epic Comparison" column blank.

There is much to like in the proposed ADPPA, for many Americans. **But for Californians, it would weaken existing privacy law in far-reaching and important ways. California should not be forced to go backwards, and lose hard-won privacy rights, in return for the rest of the country getting privacy rights that are not nearly as strong as California's.** Big Tech is willing to accept a weak national privacy law, in return for eliminating the one law they fear—California's.

ADPPA should be a national privacy 'floor,' not a ceiling, and should not preempt the California Privacy Rights Act. This national model already exists with respect to other consumer protection legislation like the Fair Credit Reporting Act (FCRA); the Gramm-Leach-Bliley Act (GLBA); and the Health Insurance Portability and Accountability Act (HIPAA). ADPPA is attempting to preempt California's law in a departure from this national precedent, having bought into the tech narrative that 'privacy is different.'

There are many vital areas where ADPPA is weaker than CPRA, including that CPRA's protections can never be weakened by the California Legislature; the creation of an independent, standalone privacy agency, funded with indexed dollars that again cannot be reduced, and with the authority to audit; rights to opt out of automated decision making and profiling; and much broader access to, and control over, information governments are collecting on us.

We are saddened to have to oppose any efforts to give more Americans privacy rights, but the price the current version of ADDPA seeks to extract is too high—this is Big Tech's desperate attempt to neuter California's strong protections.

Our full post on ADPPA can be found here.

Items Not Included in EPIC's Original Review				
	ADPPA	**CCPA/CPRA**	**EPIC Notes**	**CCP Notes**
Adequacy		•Establishment of independent agency •Ability of consumers to file complaints/seek redress [1798.199.45] •Audit authority •Ability to opt-out of automated decision making and profiling •Inclusion of 'sexual orientation' in sensitive personal information		•CPRA Stronger •Our understanding is that ADPPA would need to address these issues to qualify for a GDPR 'adequacy' finding. We believe CPRA will qualify for GDPR adequacy.
Audit & Chief Privacy Auditor				•CPRA Stronger •ADPPA missing this important criterion.
Profiling	• No mention of profiling in ADPPA	•"Profiling" is a defined term referencing businesses analyzing and predicting aspects of a consumer's life and behavior.		•CPRA stronger •CPRA §1798.185(a)(16) requires businesses to disclose meaningful information about the logic involved in the profiling/automated decision-making, as well as a description of the likely outcome on the consumer. This is an incredibly powerful and useful tool and will only get more important with time.
Covered Data	•ADPPA §2(8)(A): "covered data…***may include*** derived data and unique persistent identifiers."	•CPRA §1798.140(v)(1)(A): "Personal information…***includes***…identifiers such as a…unique personal identifier..[and] (K) inferences drawn from any of the information identified in this subdivision" (i.e., your *smart phone*		•CPRA Stronger •CPRA requires the inclusion of unique personal identifiers and inferences into covered data/personal information.

EPIC 7-28-22 Analysis with Notes in Response by Californians for Consumer Privacy				
	ADPPA	**CCPA/CPRA**	**EPIC Notes**	**CCP Notes**
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 • Places some extra requirements on "large data holders" and gives some exemptions and other special treatment to small businesses, including exemption from the private right of action. • Carves out entities that provide assistance regarding missing and exploited children. • Excludes gov't service providers from the covered entity definition, but regulates them as service providers.	•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. •Any third party that receives data has to make representations and operate under a contract, so even entities that do not meet the "business" definition under CCPA are still subject to certain regulations.	•Roughly equivalent. ADPPA covers most entities that handle covered data and then either adds or removes requirements depending on whether an entity is a large or small business. CCPA excludes nonprofits and small businesses from its "business" definition but does impose certain rules and restrictions on third parties that handle data.	•CPRA stronger •ADPPA *excludes* all service providers to any "Federal, State, Tribal, territorial or local government entity" from having to respond to access/correction/deletion requests. CPRA permits citizens to access, delete and stop the sale by businesses that provide government surveillance. • The loss of control over what data government service providers are collecting about you, the ability to delete that or stop its sale, is especially troubling in world where governments routinely purchase data like location data (because it's easier than getting a warrant), or now are using social media to monitor women seeking reproductive health access, as recently happened in Nebraska, or access their search history to prove the were interested in abortion, as happened in Mississippi.

Future Amendments	•Congress has the power to amend ADPPA in the future in ways that could strengthen or weaken privacy protections •States would not be permitted to pass future laws covered by ADPPA and not explicitly preserved in the statute.	•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.	•CA law is stronger. The CCPA/CPRA provide a protection against amendments that would weaken privacy.	•We agree. The CPRA *is* much stronger •CPRA provides a 'forever' floor against weaker privacy in CA (unless via a weakening ballot measure). • **<u>This is THE most important distinction in this entire debate</u>**
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 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.	•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 the original purpose.	•ADPPA is stronger. ADPPA's data minimization requirements are more specific and provide more detailed restrictions. The CCPA section on use limits could be a basis for specific rules, but CPPA has not yet imposed such rules.	•Roughly equivalent •While the write-up says ADPPA is stronger because of more detailed restrictions on covered data, in fact ADPPA's "Permissible purposes" for collecting, processing or transferring covered data now would *specifically include* "Targeted Advertising" [§101(b)(17)]. The inclusion of this practice in federal law will have seriously negative consequences in terms of future efforts to impose limitations on the AdTech industry, given that industry will now be able to argue that the entire AdTech industry is a "<u>permitted use</u>" under ADPPA

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. •Transfer of sensitive covered data to third parties is prohibited without opt-in consent (with a few narrow exceptions). •Sensitive covered data cannot be transferred to third parties w/o opt-in consent or a few narrow exceptions.	•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. •Grants CA residents the right to limit the use of their "sensitive" personal data on an opt-out basis. • "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.	•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.	•CPRA stronger •ADPPA *excludes* 'sexual orientation' from sensitive personal information. •ADPPA excludes from SPI, consumers' precise geolocation obtained from security or surveillance cameras, including Automatic License Plate Readers. • §102(2): Consumers ***cannot stop*** the collection or processing of their SPI, if a business is using it for any of 14 uses enumerated in §101(b). One of these purposes is "to develop, maintain, repair or enhance or improve a product or service for which such data was collected." [§101(b)(2)(B)], which is a huge loophole. [Think of the pregnancy app sharing sensitive data with Facebook to 'improve' its product or offering]. •Finally, the criticism about the CPRA language governing SPI only applying when such data is collected/processed for "the purpose of inferring characteristics about a consumer," completely ignores §1798.185(a)(19)(C)(IV) which addresses this issue entirely.

	• "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 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.	•The CA Privacy Protection Agency can add more categories by rulemaking.		
Use and disclosure limitations and controls	•Data minimization provisions (see above) limit use and disclosure. •Collection, use, and transfer of information identifying an individual's online activities over time and across third party websites & services is limited, cannot be used for ads. •Right to withdraw previously given consents.	•Data minimization provisions (see above) limit use and disclosure but current regulations permit secondary uses with user express consent. •Right to withdraw previously given 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.	•Roughly equivalent. The CCPA includes several different opt-out mechanisms whereas ADPPA more directly limits uses by default and provides a right to	•CPRA Stronger •Under ADPPA, consumers ***cannot opt-out*** of the collection, processing or transfer of their covered data (§204(b)(2)); and ***cannot stop*** the collection or processing of their Sensitive Personal Information §102(2); if a business is using it for any of 14 uses enumerated in §101(b). One of these permitted purposes is a massive loophole: "to develop, maintain, repair or enhance or improve a product or service for which such data was collected." [§101(b)(2)(B)]

	•Right to opt-out of covered data transfers to third parties. •Right to opt-out of targeted advertising, including by global opt-out mechanism •Requires compliance with unified opt-out mechanisms.	•Requires compliance with unified opt-out mechanisms.	opt-out of both transfers to third parties and targeted advertising.	This loophole would allow, for example, Instagram to share data with third parties and argue it was to 'develop…enhance…or improve' its service. • •ADPPA always allows the transfer of sensitive personal information to "third parties" in certain circumstances [§102(3)], whereas CPRA in analogous situations only permits the transfer to "service providers," and prohibits SPI transfer to 'third parties' for users who have opted to limit the use of their SPI. [1798.121]
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.	•Agree, roughly equivalent
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. •Does allow covered entities to offer different pricing to individuals who request their data be deleted.	•Businesses may not discriminate against a consumer because the consumer exercised any of the consumer's rights. •However, CCPA allows businesses to offer "financial incentives," including payments to consumers as compensation for the collection, sale, or retention of their personal information. Such incentives may not be	CA law is slightly stronger as it places guardrails on financial incentives and discounts to ensure fairness.	•CPRA *much* stronger. •The most important concept in CPRA's anti-retaliation provision is 1798.125(b)(4): "A business shall not use financial incentive practices that are **unjust, unreasonable, coercive, or usurious in nature."** This idea is entirely lacking in ADPPA and will result in massive coercion to 'force' consumers to join loyalty programs that involve unlimited sale and exploitation of their purchases, or pay some ridiculous sum *(Sure, it only costs an extra $50/month to*

	•Covered entities are not prevented from offering bona fide 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	unjust, unreasonable, coercive, or usurious in nature. •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."		*choose the phone plan where we don't sell your personal information).* •Even worse, ADPPA §104(b)(5) explicitly allows a business to offer different pricing or functionality if a consumer requests that their data be deleted, all but ensuring that businesses will set up massive hurdles to data deletion *(Why yes, you *can* delete your data, but from then on every search will cost you $0.10)*
Transparency	•All covered entities and service providers must have privacy policies that meet a certain standard. •Large data holders must also provide short-form notices. •Entities must notify individuals affected of material changes to privacy policies & offer opportunity to withdraw consent.	•Covered businesses must provide privacy notices that meet a certain standard. •Covered businesses must notify consumers if they use data beyond the disclosed purpose. •CPPA authorized to issue regulations to ensure this notice may be easily understood by the average consumer.	•Roughly equivalent.	•CPRA Stronger •CPRA §1798.185(a)(16) requires businesses to include meaningful information about the logic involved in any automated decision making, including profiling—huge transparency benefit. ADPPA does not • CCPA Regs §999.336 requires businesses to enumerate the "value of the consumer's data" to the business, if they engage in any financial incentive program, in order to prevent discrimination. This is huge and will provide massive insight into the surveillance economy.

Civil Rights & 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.*	•Roughly equivalent •On one hand, yes, ADPPA is more protective in terms of traditional civil rights. • However, economic discrimination is linked integrally to race, given racial wealth gaps. ADPPA permits financial discrimination by *specifically excluding* CPRA's anti-discrimination language preventing businesses from using "financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature." [1798.125(b)(4)]. • This means under ADPPA, businesses will be allowed to offer financial incentives to collect, sell, share or retain personal information. This will promote price-based discrimination, and privacy will trend towards being a right enjoyed by the wealthy, who are so concentrated in certain racial groups. [Think of two phone plans, one is $75 less per month but the carrier gets to sell your geolocation data].
Algorithmic Impact Assessments	•Requires large data holders to conduct annual algorithmic impact assessments and submit to the FTC. •Impact assessments must include steps taken to mitigate harms related to minors,	•Covered businesses must conduct regular risk assessments weighing the benefits of their data processing (which includes using algorithms) against risks to consumers, with	•ADPPA is more protective because it requires algorithmic impact assessments, focusing on	• CPRA stronger • ADPPA Impact Assessment only applies to "large data holders"—CPRA covers all businesses. •CPRA *requires* businesses to include meaningful information about the logic involved in any automated decision making, as well as the likely outcome of the processing with respect to the

	disparate impact on basis of protected characteristics, life opportunities, etc. •Algorithmic evaluations must also occur at the design phase of an algorithm, including evaluating any training data that is used to develop the algorithm.	the goal of not engaging in practices whose risks outweigh their benefits. •Must be submitted to CPPA. •CPPA can issue regulations governing these risk assessments.	algorithmic bias and the risks from discrimination, which feeds into ADPPA's prohibition of discriminatory data uses.	consumer, and specifies this relates to a natural person's performance at work, their economic situation, health, personal preferences, interests, behavior, location, etc. •These rights come into effect in 2022, whereas ADPPA's will be delayed for 2 more years after its passage, depriving 40 million Californians of protection in those years.
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.	•CA offers a right to opt out of automated decision making that ADPPA does not. This right would not be preempted by ADPPA.	•CPRA stronger. •The analysis is incorrect: it is not *"can* issue," the statute specifies that the CPPA "***shall***…adopt regulations…to" govern access and opt-out *rights* with respect to automated decision making, including profiling. • CPRA gives consumers the *right* to opt-out of automated decision making and profiling. ADPPA does not.
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.	•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	• Agreed, ADPPA's prohibition on targeted advertising to minors is an excellent provision and CPRA does not have anything similar.

	•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.		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. •Data brokers are also covered entities subject to the rest of the Act.	•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	Agree, roughly equivalent.
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.	Agree, California does not yet have a "Do Not Collect" mechanism, this is one of the best parts of ADPPA.
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.	•CPRA infinitely stronger, because of CPRA private right of action enforcement provision: CPRA §1798.150 specifies a dollar figure per violation ($100-$750) *and does not require the consumer to show harm.* In ADPPA §403(a)(2)(A), ADPPA's private right of action for inadequate security only allows plaintiffs to seek "compensatory damages." The issue in data breach has always been, how do you prove that the data breach in April was linked to the identity theft in December? You can't, so the companies get away with a slap on the wrist, and don't invest in better security. Under CPRA, consumers are free of this construct, and do not have to prove damages: if the business did not have reasonable security practices and procedures in place at the time of the data breach, it is liable for the dollar penalty per violation.
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.	•Roughly equivalent. •CPRA gives the CPPA broad authority to implement the law, including what will be required for the impact assessments required under §1798.185(a)(15). A business will have to certify compliance, and how they do so will be subject to rulemaking. •Additionally, the Executive Compliance in ADPPA is only required for a relatively few "large data holders," whereas CPRA will require assessments and compliance

				from all businesses whose processing of PI presents significant risk to consumers' privacy.
Privacy Impact Assessments	•Covered entities (except small businesses) must conduct biennial privacy impact assessments that weigh the benefits of data use against the potential adverse consequences to privacy. •PIAs by large data holders must be approved by the entity's privacy protection officer.	•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 outweigh their benefits. •Must be submitted to CPPA. •CPPA can issue regulations governing these risk assessments. •Third parties whose data practices may pose a risk to consumers may also be required to implement PIAs.	•Requirements for assessments are roughly equivalent, but CCPA stronger because assessments must be submitted to the CPPA, improving transparency.	•Agree, CPRA stronger. The requirement to submit the PIA to the CPPA, by all businesses whose processing of PI presents significant risk to consumers' privacy, gives this concept teeth that are missing from ADPPA.
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 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	•Roughly equivalent	•CPRA Stronger •This provision dramatically weaker than CPRA. •ADPPA Sec. 2 (9)(B)(ii) *excludes* all service providers to any "Federal, State, Tribal, territorial or local government entity." •By design, CPRA specifically *includes* these entities. Because service providers are defined in CPRA as service providers *only* to businesses, not to government entities, when a service provider is acting on behalf of a

	•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 providers.	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' expectations."		government entity, then it itself becomes a 'business' subject to access, deletion and correction requests. So the cell phone provider selling geolocation information to a government agency, is not covered by ADPPA, but *is* covered by CPRA. This has massive implications in a politically volatile world: whether you think governments shouldn't be tracking attendees at protest rallies, seekers of abortions, or purchasers of guns, CPRA allows consumers to learn about government surveillance activity (with due exceptions for preventing criminal activity) by letting them query the service providers to governments. •CPRA specifically, intentionally gave these rights to 40 million Californians, and now ADPPA would eliminate them. ADPPA would represent a breathtaking diminution of Californian rights in this regard.
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 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. •Proposed regulations require that a business must have a contract with every	•Roughly equivalent. The proposed CCPA regulations would impose strict contract	•CPRA is stronger •Under ADPPA, consumers ***cannot opt-out*** of the collection, processing or transfer of their covered data (§204(b)(2)) to third parties if a business is using it for any of 15 uses enumerated in §101(b). •One of these permitted purposes is a massive loophole: "to develop, maintain,

	•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-party that receives data, ensuring there are no transfers to third parties that fall outside the scope of the law. •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.	requirements on all third parties that process personal information.	repair or enhance or improve a product or service for which such data was collected." [§101(b)(2)(B)] • Also, the analysis mentions "proposed CCPA regulations" but actually the *statute* [1798.100(d)(2)] imposes the requirement for third parties to provide the same level of privacy protections as the entity sharing or selling (contractually).
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.	•CPRA Stronger •First, consumers can access/correct/delete ***ALL*** their data post 1/1/22, not just the most recent 24 months. This is dramatically different coverage. •Additionally, ADPPA § 203(e)(3)(A)(v) contains an exception where businesses do not have to grant access, deletion, or correction requests if the business feels such activity would "result in the release of… confidential business information." So, a business merely has to deem the information it is collecting on consumers as 'confidential business information,'

				and then it doesn't have to disclose or delete it. Really? •§203(a)(1)(A): ADPPA allows businesses not to turn over data in "archival or back-up systems." If your data is in an archive, you no longer get that data when you make an access request and can no longer delete it. CPRA requires that as soon as the business restores the data (and is able to use it), they must fulfill your request.
Accessibility				
Language Accessibility	•Entities are required to provide notices and mechanisms in all languages it provides service in. •FTC must also publish guidance documents in multiple languages.	•Statute grants CPPA rulemaking authority to ensure that notices required under CCPA are available in the language primarily used to interact with the consumer.	•Roughly equivalent.	•Agree, roughly equivalent.
Disability Accessibility	•Entities are required to provide notices and mechanisms in a manner that is readily accessible and usable by individuals with disabilities.	•Statute grants CPPA rulemaking authority to ensure that notices required under CCPA are accessible to individuals with disabilities.	•Roughly equivalent.	•Agree, 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	•CA Privacy Protection Agency (CPPA) enforces and issues regulations. •CPPA can get statutory civil penalties. •CPPA has a Chief Privacy Auditor who can audit	•ADPPA has nationwide enforcement by FTC and state AGs and privacy agencies CPPA.	•Apples to oranges (entire country vs California) but California wins handily in enforcing *within* California •FTC would be given massive new responsibilities with no budgetary support. On an equivalent citizen: citizen ratio, the FTC would have to be

	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.	businesses to ensure compliance with the law. •Violations of CCPA can also be enforced by over 60 district and city attorneys.	California law cannot directly protect people outside California.	appropriated **$100M** in 2022 dollars; indexed to inflation forever; with zero ability by congress to ever reduce this amount (to compare to California's initiative protections). •§303(a) allows industry to propose technical compliance programs; requires the FTC to approve or deny the program; and gives industry the right to sue the Commission if it does not approve, amend or repeal a technical compliance program. Given the lack of resources allocated to the FTC under ADPPA, this section alone is a recipe for minimal regulation, since industry will be able to tie up the Commission in court for even the most minor change to a compliance program. •Highly unusually, ADPPA §401(c)(3) requires the FTC to choose either a cease-and-desist order, *OR* to bring a civil action alleging an act or practice violates this Act. In conversation with a former FTC commissioner, he stated he could not think of another statute the FTC enforces that has this provision, which will dramatically weaken the toolkit FTC has to enforce.
Ability to Audit Businesses	•No right of audit in ADPPA	• CPRA creates new statewide position of Chief Privacy Auditor, allows this person to audit businesses to ensure compliance with the Act. No right of audit in ADPPA		•CPRA stronger

Private right of action	•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 goes into effect after two years. •Persons or classes of persons may bring 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. •Small businesses are exempt from PRA.	•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 statutory damages. *Note: ADPPA does not preempt CCPA's data breach private right of action.*	• Yes, ADPPA's Private Right of Action covers more areas of law than CPRA's, but it is so weak that it is a Private Right of Action in name only. CPRA's is much narrower (data breach only) but will be much more powerful. • ADPPA plaintiffs have right to undefined "compensatory damages," [§403(a)(2)(A)], whereas CPRA *specifies* $100 - $750 per consumer per incident, and importantly, consumers do not have to show harm if their data was breached. Other issues: • FTC has 60 days to block actions by plaintiffs. • Industry-proposed "technical compliance program" under ADPPA §303 present a huge hurdle to effective PRA. •Right to Cure: §403(c): ADPPA Private Right of Action also has a right to cure granted to many businesses. For businesses with less than $41M in revenue, plaintiffs must first contact business before starting the lawsuit, and business then has 45 days to cure the problem. This is a fix-it ticket, not a speeding ticket. Not that this isn't useful public policy, but this is not a true 'private right of action' at all, since most businesses can merely wait until a problem is identified by a consumer, then 'fix' it, and have no liability.

Private right of action—ADPPA hurts CPRA PRA	Note: ADPPA claims it exempts CPRA PRA (§1798.150), but in fact since its passage, the CPRA PRA has been strengthened by adding genetic data to the list of information subject to §1798.150. ADPPA's passage would eliminate this item from CPRA's PRA, substantially weakening existing protections.			
Timing	•ADPPA gives the Federal Trade Commission 2 more years from date of passage, to promulgate regulations.	•CPRA's protections go into effect in 2023		•CPRA Stronger •CCPA actively being enforced TODAY by the CA DOJ, and soon a dedicated agency. 40 million Californians would have to wait 2 additional years to get, in many cases, weaker privacy protection.
Banks and other Financial Institutions	•ADPPA §2(9) (The term "covered entity…means any entity…that is subject to the Federal Trade Commission Act"). But the FTC Act excludes banks, savings and loan institutions, and federal credit unions.	•CPRA's approach is to exempt "personal information collected, processed, sold or disclosed subject to" various federal laws (FCRA, GLBA, etc—not the entities themselves.		•CPRA Stronger •CPRA begins coverage where federal laws like FCRA and GLBA leave off. • For example, a bank is constrained with respect to what it can do with your credit information; but if it also collected your geolocation, hair color or sexual identity, CPRA would constrain the bank from what it could do with that information. • CPRA stops banks from becoming commercial data brokers; ADPPA does not.
Preemption	•ADPPA preempts virtually all of CPRA—but none of the Illinois Biometric Privacy Act!			•ADPPA ignores the established provision of federal privacy law being a floor, not a ceiling: FCRA, GLBA, HIPAA are all floors not ceilings.