California's CCPA 2.0: Does the US finally have a data privacy Act?

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney

(2020) 168 *Privacy Laws & Business International Report*, 13-17, December 2020.

On the day of the US Presidential election, Californians voted to pass Proposition 24, enacting the *California Privacy Rights Act of 2020* (CPRA), in order to amend the current *California Consumer Privacy Act* (CCPA), which took effect earlier in 2020. The new law is known to some as 'CCPA 2.0' to indicate it is the combined effect of the CCPA as amended by the CPRA. Citations here are to sections of California's *Civil Code*, as amended by the CPRA. It will take effect on 1 January 2023, but will apply to data collected from 1 January 2022, except for the right of access. CCPA 2.0, in its combined effect, is the most ambitious US legislation affecting privacy more broadly than in a specific sector.[1]

For the past decade I have published in *Privacy Law & Business International Review* what has become a biennial analysis of how many countries have data privacy laws, the most recent edition of which (January 2019) counts 132 (now 144).[2] Some of the 'countries' accepted into this analysis are not States, but are regions which for various reasons have substantially autonomous capacity to enact a data privacy law, and have done so for their region.[3]

With the next edition of this review due in early 2021, where does California fit? I stress that this article is a *formal* analysis, based on the extent to which California's law can be mapped against the requirements of the three 'generations' of international data privacy instruments over the last forty years. It is not (and as yet, could not be) a *substantive* analysis of CCPA 2.0's effectiveness for privacy protection: how strong or weak are the interpretations of its provisions; how corrosive are its exceptions; how effective are its enforcement mechanisms; or how aggressive its enforcement authorities. At best, this analysis will help place CCPA 2.0 within the forty-year evolution of international standards, and in relation to the 144 national laws as yet enacted. But for how valuable a law it turns out to be, we must wait and see.

Is the CCPA 2.0 a data privacy law at all?

The criterion for inclusion that I have used is that a country (including a separate legal jurisdiction) is considered to have a 'data privacy law' if it has one or more laws covering the most important parts of its private sector, or its national public sector, or both. That law must provide a set of basic data privacy principles, which at least include almost all the principles (or standards) required by both the OECD privacy Guidelines (as at 1980) and Council of Europe data protection Convention 108 (as at 1981), plus some method(s) of officially-backed enforcement (i.e. not only self-regulation). Of these OECD/CoE principles that a law must include, the most important are individual participation (rights to access and correction), finality (uses and disclosures, and the extent of collection limited by the original purpose of

[1] Important Acts with only sectoral effects include the *Privacy Act of 1974*, affecting the federal public sector only; HIPAA affecting health and certain insurance information; FERPA regulating federally funded educational institutions; GINA regulating genetic data; and COPPA regulating information of children under 13.

[2] G. Greenleaf 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2019) 157 *Privacy Laws & Business International Report*, 14-18. Twelve other countries since then have enacted data privacy laws: G. Greenleaf, and Cottier, Bertil, '2020 Ends a Decade of 62 New Data Privacy Laws '163 Privacy Laws & Business International Report 24-26, documents 10, to which add Egypt and Jamaica.

[3] Examples are China's Special Administrative Regions (SARs) of Hong Kong and Macau, territories linked to the UK such as Jersey, Guernsey and Gibraltar, and even special economic zones such as Abu Dhabi Global Market (ADGM).

collection), and the obligation to provide data security. The rationale is that it was these two international instruments which, at the outset of the 1980s, provided the first international consensus on what is required for data privacy protection, sufficient to justify free flow of personal information between compliant countries.

I	1st Generation standards	C108 1981; OECD 1980	**CCPA 2.0**
1.01	*Collection* – limited (not excessive), lawful (for legitimate purposes) and by fair means	C108 5(a), (c); OECD 7	Collection is limited by compatible purposes, but with an exception for notice: 'A business shall not collect additional categories of personal Information… for additional purposes that are Incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section'. (1798.100(a)(1))
1.02	*Data quality* –relevant, accurate, up-to-date	C108 5(c) (d); OECD 8	No positive obligation to maintain relevant, accurate, or up-to-date personal data is provided, only obligations to correct inaccuracies, and delete data after intended use.
1.03	*Purpose specification* by time of collection	C108 5(b); OECD 9	Purpose must be specified before collection (implied by 1798.100(a)(1))
1.04	*Notice of purpose/rights* [assumed implied]	C108 5(b); OECD 9	Extensive notice before collection, of purpose and rights (1798.100(a))
1.05	*Uses limited* (including disclosures) to purposes specified or compatible	C108 5(b); OECD 10	Collection is limited by compatible purposes, but with an exception for notice: 'A business shall not … use personal information collected for additional purposes that are Incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section.' (1798.100(a)(1))
1.06	*Security* through reasonable safeguards	C108 7; OECD 11	Businesses 'shall implement reasonable security procedures' (1798.100(e))
1.07	*Openness* re personal data practices (not limited to data subjects)	C108 8(a); OECD 12	Businesses are required to publish (and update at least annually) considerable information about their privacy practices, either on a publicly accessible privacy policy, or on their Internet website. Access to this information is not restricted to persons on whom the business holds information ('reasonably accessible to consumers') (1798.130(a)(5)). Various other provisions assume the existence of a privacy policy.
1.08	*Access* – individual right of access	C108 8(b); OECD 13	'A consumer shall have the right to request that a business that collects personal information about the consumer disclose': categories collected; categories of sources; 'purpose for collecting, or selling, or sharing; 3rd party recipients; and 'specific pieces' collected (1798.110. (a)); also 1798.115, *Consumers' Right to Know What Personal Information is Sold or Shared and to Whom*
1.09	*Correction* – individual right of *correction*	C108 8(c), (d); OECD 13	Consumers have 'the right to request a business that maintains inaccurate personal information about the consumer correct such … information' (1798.106(a))

1.10	*Accountable* – identified data controller accountable for implementation	C108 8; OECD 14	There is no provision requiring a specific officer to be accountable, and for means to contact them to be made public. However, two or more contact mechanisms, with disclosed toll-free numbers, email address or website contact forms must be provided to facilitate access and correction requests (1798.130(a)(1)(A) and (B)).

The CCPA 2.0 therefore includes a sufficient number of the '1st generation' principles necessary for a data privacy law. Of the ten principles, implementation of only one is absent: the data quality principle. The 'Openness principle' in relation to personal data practices (not limited to data subjects, unlike the access principle) has a weak implementation. That principle is more often omitted than any other. The accountability principle is not fully implemented.

However, the scope of CCPA 2.0 may present problems with the somewhat imprecise requirement that it should cover the 'most important parts' of the jurisdiction's private sector, because of many exemptions. Other questions of coverage are whether the law protects a broad enough range of individuals, and whether enough information is protected.

The beneficiaries of the protections of CCPA 2.0 are limited to consumers[4] who are 'residents of California' (1798.140(i)), and do not extend even to residents of other US states (although some companies have extended the original CCPA rights to all with whom they deal: *de facto* 'CCPA creep'). This is not unusual: many data privacy laws limit protections to their own citizens or residents, although some extend them to any person (which is probably needed to obtain an EU adequacy finding).

'Personal information' is essentially defined in terms of 'identifiability' (1798.140(v)(1)), which is the case in almost all data privacy laws globally. Some personal information is excluded. The exclusion from 'personal information' of 'publicly available information'[5] (1798.140(v)(2)), is only found in a minority of data privacy laws (it is not excluded by the EU, or strongly EU-influenced laws), but it is by no means uncommon.[6] The exemption of 'de-identified or aggregate consumer information' (1798.145(a)(6); see 1798.140(b) and (m)), has its equivalents in many laws (eg Korea, Japan), including to some extent the EU's GDPR (only as an exemption for certain uses). It is everywhere susceptible to misuse.

The entities covered by the CCPA 2.0 are limited to 'businesses' (defined in 1798.140(d)(1)),[7] and thus do not normally include non-profit organisations such as clubs, churches, some schools, political parties etc. Limitation of data privacy laws to the business sector is also found in jurisdictions such as Malaysia. Exclusion of specific sectors of organisations is also common, such as political parties (Australia), churches (South Korea). Information collected by a business in its capacity as an employer is excluded (only until 1 January 2023: 1798,145(m)), but exclusion of employment information also occurs in some other jurisdictions (eg Australia). An entity is also only covered if it 'does business in the State of

[4] By complex means, the Act's protections are also to some extent extended to employees and 'independent contractors', but that is not dealt with here. The policy basis of the CPRA is that their privacy interests should also be protected (CPRA s. 3(8)).

[5] The section adds 'or lawfully obtained, truthful Information that is a matter of public concern', which is difficult to interpret.

[6] G. Greenleaf ' Private Sector Uses of 'Public Domain' Personal Data in Asia: What's Public May Still Be Private' (2014) 127 *Privacy Laws & Business International Report*, 13-15, https://ssrn.com/abstract=2438368

[7] There is also a complex extension of the CCPA 2.0 to 'contractors' (see 1798.140(j)), but this is not dealt with here.

California', so this law will not cover all US-based businesses, but such requirements of activity within the jurisdiction are typical of data privacy laws. There are also some exclusions in order to avoid inconsistency with US federal credit reporting laws, and some other laws (1798.145(d)-(g)),[8] another commonplace type of exclusion.

An additional important limitation is that a business in California will only be bound by the CCPA 2.0 if it meets one or more threshold conditions, one of which is that it 'had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year' (1798.140(d)(1)(A)). Such 'small business' exclusions are uncommon, but are found in Australia's law, and a version was previously found in Japan's law. The two other threshold tests (buying, selling or sharing personal information on 100,000 or more consumers; or deriving more than 50% of annual revenue from such selling or sharing) reduce the significance of this 'small business' exclusion. Businesses so exempted can 'opt-in' by voluntarily certifying to the CPPA that it complies with and agrees to be bound by the law (1798.140(d)(4)), which is unusual, but is also found in Australia's law.

None of these limitations on the scope of the CCPA 2.0 are therefore unprecedented (or even particularly unusual) in data privacy laws in other countries. This is still a Californian Act 'covering the most important parts of its private sector' (as my criteria require), so these limitations are no bar to CCPA 2.0 being considered a data privacy law.

Therefore, on the basis of both the principles that it includes, and its scope, we may conclude that CCPA 2.0 is a data privacy law. After 40 years, the US has a data privacy law implementing the OECD Guidelines of 1980 for a significant part of its private sector.

To what extent is CCPA a 2nd generation data privacy law?

A further stage of this analysis was to ask, in 2012,[9] to what extent the data privacy laws enacted outside Europe at that time similar to the European Union's data protection Directive of 1995 in the standards they embodied. Thirty three of the thirty nine data privacy laws in countries outside Europe at this time were analysed. The Directive included 10 requirements which were not found in both the 1980/81 OECD Guidelines and Convention 108 (although some were already in Convention 108). These ten requirements were as follows, compared with whether they are found in CCPA 2.0:

II	2nd Generation – 'European standards' – post-1995	EU DPD 1995	**CCPA 2.0**
2.01	*Minimum collection* necessary for purpose (data minimisation)	6(1)(b),(c), 7	'Collection, use, retention, and sharing' … 'shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed' (or for another disclosed and compatible purpose) … and not further processed In an incompatible manner. (1798.100(c))
2.02	*Destruction or anonymisation after purpose completed*	6(1)(e)	A business shall not retain personal information 'for longer than is reasonably necessary for that disclosed purpose' (1798.100(a)(3)).

[8] Some exclusion, such as of the *Gramm-Leach-Bliley Act*, have been argued to be against consumer interests: Robert Gellman 'Protect consumer privacy: Repeal GLBA's privacy provisions' IAPP website 30 July 2020 <https://iapp.org/news/a/protect-consumer-privacy-repeal-the-glbas-privacy-provisions/>

[9] G. Greenleaf 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' *International Data Privacy Law*, Vol. 2, Issue 2, 2012, https://ssrn.com/abstract=1960299

2.03	*Additional protections for sensitive data* in defined categories	8	'Sensitive personal information' is defined broadly (including 'precise geolocation') (1798.140(ae)). Additional notice is required (1798.100(a)(2)). See *Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information* (1798.121) and note that this limits first party use, not only sale or sharing (disclosure).
2.04	*Legitimate bases for processing defined*	7	No such requirement: only that purpose of collection must be disclosed, and processing limited by that. The limitations on uses for incompatible purposes do not constitute a positive requirement for legitimate bases for processing (as in the EU).
2.05	*Additional restrictions on some sensitive processing systems* (notification; 'prior checking' by DPA etc)	20	The Attorney-General shall issue 'regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security', to perform annual cybersecurity audits, and to submit to the CPPA on a regular basis a risk assessment which weighs up the benefits and risks involved (1798.185(15)).
2.06	*Limits on automated decision-making* (incl. right to know processing logic)	15, 12(a)	The Attorney-General shall issue 'regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to Include meaningful information about the logic involved in such decision making processes, as well as a description of the likely outcome of the process with respect to the consumer' involved (1798.185(16)).
2.07	*To object to processing on compelling legitimate grounds*	14(a), (b)	See 1798.120, Consumers' Right to Opt-Out of Sale or Sharing of Personal Information.
2.08	*Restricted data exports* requiring recipient country 'adequate', or alternative guarantees	25, 26	Not explicitly provided – Same requirements as for other disclosures of personal data, requiring transferees to offer the same level of protection (see 1798.140(i) re 'contractors'). Enforceability and other issues remain.
2.09	*Independent Data Protection Authority(-ies)* (DPA)	28	The California Privacy Protection Agency (CPPA) is established, comprised of a five member board (1798.199.10(a)). It is required to '*remain free from external influence, whether direct or Indirect, and shall neither seek nor take instructions from another'* (1798.199.15(c)), and also has other indicia of independence, including enforcement powers.
2.10	*Recourse to the courts* to enforce data privacy rights	22, 23	Nothing in CCPA 2.0 gives rise to a private right of action (1798.150(c)) to individuals, with the important exception of an action for recovery of damages for personal information security breaches. Recovery may be for actual damages, or statutory damages (limited to $750 per consumer per incident) (1798.150(a)).

The CCPA 2.0 therefore includes seven of the above ten stronger protections found in the 1995 Directive, but which were not included in the 1st generation instruments of the early 1980s. Those missing or partial are three of the most important '2nd generation' principles: defined

legitimate bases for processing (2.04), data export restrictions (2.08), and a private right of action (2.10) (except for data security breaches). Creation of an independent DPA, the CPPA, is a major advance (2.09), often regarded as the most important enforcement element in such laws.

The average number of these principles included in data privacy laws outside Europe in 2012 was also 7/10.[10] Informal estimates based on the much greater number of non-European countries that now have such laws are that approximately 7/10 of these principles are included.[11] The three important differences between CCPA 2.0 and the Directive are that CCPA 2.0 does not require a legitimate basis for processing; does not provide for individual actions before the courts, except for security breaches; and does not place explicit limits on exports of personal data (either outside California or outside the US).

We could therefore conclude that CCPA 2.0 is, considered overall, a law that approximates the current international standard for data privacy laws outside Europe: inclusion of almost all the 1st generation principles of the 1980s, and about 7 of the 10 additional principles embodied in the 1995 EU Directive and Convention 108.

What about 3rd generation principles?

The international standards for a data privacy law continue to evolve, and the new models for where such standards could be found have generally been regarded as the EU's General Data Protection Regulation (GDPR) and the CoE's 'modernised' Convention 108 (now known as '108+'). With the CCPA 2.0 so recently enacted, it is too early to say whether it will be another model.

Some additional rights in CCPA 2.0 have equivalents in the GDPR, others do not:

- *Administrative fines*: Any violations of CCPA 2.0 may make a business liable to an administrative enforcement action, where administrative fines may be up to $2,500 for each violation, or $7,500 where sensitive information, or customers known to be under 16 years old (1798.150(a)). Fines will go into a consumer privacy fund. Enforcement actions may be taken by the CPPA, the state A-G, and city and county attorneys.

- Sale or sharing *opt-out rights can be delegated to a privacy agent* who can exercise rights on behalf of individuals or groups of consumers. Software (eg Internet browser signals) is recognized as an opt-out agent.

- *Stronger deletion rights:* 'A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer' (1798.105 (a)). Notification to third party recipients is required. There are significant exceptions to the right (see 1798.105 (d)(2)).

- *No retaliation for exercise of rights:* 'A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title' (1798.125. (a) (1)). No direct GDPR equivalent, but Korean law includes such a provision.

- There is a *right to opt out of cross-context behavioral advertising*.

---

[10] Greenleaf 'The Influence of European Data Privacy Standards Outside Europe', above cited.

[11] G. Greenleaf, Graham, ''European' Data Privacy Standards Implemented in Laws Outside Europe' (2017) 149 Privacy Laws & Business International Report 21-23, https://ssrn.com/abstract=3096314

These innovations are significant, but CCPA 2.0 still only includes a small number of the twenty or more innovations found in the GDPR (the majority of which are also found in the 'modernised' Convention 108+) that were not in the earlier generations of European principles.[12]

Fifty years on

The CCPA 2.0 is not 'America's GDPR' as some have claimed,[13] and it would be an exaggeration to describe it as 'America's Data Protection Directive' given that it only embodies 7 of the 10 additional principles in the 1995 Directive. However, that puts it close to the current average of all data privacy laws outside Europe, a more modest but very valuable result, particularly given the importance of California and its law's extra-territorial effects.

Just as important, it is the first US law with more than a narrow sectoral scope[14] which can usefully be described as 'a data privacy law' rather than just 'a law including some privacy protections'. CCPA 2.0, even if its privacy protections are not as strong as many would wish,[15] is a genuine data privacy law that deserves to be compared with the privacy laws currently found in 144 countries.

Another important question is the extent to which CCPA 2.0 will be a major impetus toward, and influence on the content of, a US federal data privacy law. Some commentators argue that CCPA 2.0 sets a new high level of protection, which Congress must meet or exceed in any Bill, or it will face too much opposition (including from the very large Californian delegation in the House).[16] Although CCPA 2.0 has apparent geographical limitations, Californian standards have often become national (for example, car emissions).[17] Others argue that a federal data privacy law needs to be more ambitious in addressing the international position of the US, in light of the *Schrems II* decision, the common challenges from Chinese surveillance faced by the US and EU, and the desirability of the US enacting a law strong enough for it to accede to data protection Convention 108+ and accelerating it becoming a global data privacy treaty.[18]

Fifty years after the 1970 enactment of the first data privacy Act by the German state of Hesse, the US private sector finally has a broadly applicable data privacy Act, in the combined effect of the two Acts constituting CCPA 2.0. Its influence and significance should not take another 50 years to become apparent.

---

[12] For a brief account, see G. Greenleaf 'Convention 108+ and the Data Protection Framework of the EU (Speaking Notes for Conference Presentation) '*Convention 108+ Tomorrow's Common Ground for Protection*' (Council of Europe, Strasbourg, 21 June 2018)., < https://ssrn.com/abstract=3202606>.

[13] For example, S. Morrison 'California just strengthened its digital privacy protections even more' *Lexology* 4 November, 2020, describing CPPA 2.0 as 'giving California a law on a par with' the GDPR.

[14] The *Privacy Act of 1974* arguably has more than a narrow sectoral scope, as it covers the federal public sector, but is included under my criteria in any event.

[15] For example Electronic Privacy Information Center (EPIC) 'EPIC Analysis: California's Proposition 24' (undated) <https://epic.org/state-policy/ca-prop24/>; Lee Tien, Adam Schwartz and Hayley Tsukayama 'Why EFF Doesn't Support California Proposition 24', Electronic Frontier Foundation (EFF) 29 July 2020 <https://www.eff.org/deeplinks/2020/07/why-eff-doesnt-support-cal-prop-24>.

[16] C. F. Kerry and C. Chin 'By passing Proposition 24, California voters up the ante on federal privacy law' Brookings blog, 17 November 2020 <https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/>.

[17] For examples, see A. Chander, M. Kaminski, and W. McGeveran 'Catalyzing Privacy Law' (2019) *Minnesota Law Review*, Forthcoming <https://ssrn.com/abstract=3433922>.

[18] M. Rotenberg 'Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection'. *European Law Journal.* 2020;1–12. <https://onlinelibrary.wiley.com/doi/10.1111/eulj.12370>.

Information: Valuable comments and suggestions have been received from Robert Gellman, Chris Hoofnagle, Pam Dixon, James Rule, Marc Rotenberg and Woodrow Hartzog, but all responsibility for content remains with the author.