UNSW SYDNEY

*UNSW Law & Justice Research Series*

# Proposed US Federal Data Privacy Law Offers Strong Protections But Only to US Residents

**Graham Greenleaf**

[2022] *UNSWLRS* 50
(2022) 179 *Privacy Laws & Business International Report* 1, 3-74

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

**E:** LAW-Research@unsw.edu.au
**W:** http://www.law.unsw.edu.au/research/faculty-publications
**AustLII:** http://www.austlii.edu.au/au/journals/UNSWLRS/
**SSRN:** http://www.ssrn.com/link/UNSW-LEG.html

# Proposed US federal data privacy law offers strong protections but only to US residents

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

Published in (2022) 179 *Privacy Laws & Business International Report* 1, 3-7

13 September 2022

To the surprise of most observers, businesses and privacy advocates, the United States is closer than it has ever been to enacting a national data privacy law for its private sector, the *American Data Privacy and Protection Act* (ADPPA).[1] The proposed Act has strong bipartisan support, as shown in a 53-2 vote in its favour by the US House Energy and Commerce Committee on 20 July. It will now be subject to a vote by the full House (itself a first), before going to the Senate. US commentators are split over whether the legislation could or should be enacted before the current Congress completes its term in January 2023.

The existing position in the US is that the current *California Consumer Privacy Act* (CCPA), in effect since 2020, was amended by the *California Privacy Rights Act of 2020* (CPRA) which will take effect on 1 January 2023. The amended law, referred to as 'CCPA 2.0' to indicate it is the combined effect of the CCPA as amended by the CPRA, is the most ambitious US legislation affecting privacy more broadly than in a specific sub-sector.[2] Four other states have enacted bills affecting the private sector, but none are regarded as being as strong as CCPA 2.0.[3]

The main purpose of this article is to ask where will the ADPPA fit in the existing global landscape of 159 countries[4] with data privacy laws, if it is enacted in its current form? This can only be a formal analysis ('the law on the books') until the law is in effect.[5] At best, this analysis will help place the ADPPA within the forty-year evolution of three generations of international standards ((i) OECD Guidelines/Convention 108 of 1980/81; (ii) EU Directive of 1995; and (iii) EU GDPR of 2016), and the half-century of enactment of national laws influenced by these standards. But for how valuable a law it turns out to be, we must wait and see.

---

[1] H.R.8152 - American Data Privacy and Protection Act 117th Congress (2021-2022) https://www.congress.gov/bill/117th-congress/house-bill/8152

[2] 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.

[3] 'Five states — California, Colorado, Connecticut, Utah and Virginia — have enacted comprehensive consumer data privacy laws.': 'State Laws Related to Digital Privacy' on National Conference of State Legislatures website, https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#Comprehensive

[4] See G. Greenleaf 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 P*rivacy Laws & Business International Report,* 1, 3-5; G. Greenleaf 'Now 157 Countries: Twelve Data Privacy Laws in 2021/22' (2022) 176 *Privacy Laws & Business International Report* 1, 3-8 ; plus eSwatini (until 2018 known as Swaziland), and Cuba, the 158th and 159th laws.

[5] I stress that this is a *formal* analysis, based on the extent to which the ADPPA 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 the Act'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.

By 2023, fifty years after the enactment of the world's first national data privacy law, the *Swedish Data Act* of 1973, the US may finally enact a broadly applicable data privacy Act for its private sector. Its influence and significance should be major and immediate.

My analysis of California's CCPA 2.0 concluded[6] that it did meet the 'first generation' requirements for being considered to be a 'data privacy law'. In comparison with the 'second generation' standards set by the EU's Data Protection Directive (EU DPD), I concluded that CCPA 2.0 approximated the then-current international standard for data privacy laws outside Europe, by inclusion of about 7 of the 10 additional principles found in the EU DPD of 1995. However, I also concluded that CCPA 2.0 only includes a small number of the twenty or more innovations found in the EU's General Data Protection Regulation (GDPR) of 2016 – the 'third generation' principles. The CCPA 2.0 was therefore not 'America's GDPR' as some had claimed – but it is a good quality data privacy law by international standards.

In this article I aim to answer the same questions in relation to the ADPPA. Statutory references are to the ADPPA unless specified otherwise.

## Differing views from a national perspective

Within the US there are differing views about whether ADPPA should be supported, with strong differences even between consumer-oriented organisations who support such a law in theory.[7] Some key differences are: (i) ADPPA includes pre-emption provisions which prevent any State enforcing legal provisions covering the same issues as ADPPA, but still leaves significant exceptions within which State laws may operate; (ii) Balanced against this, ADPPA does provide a private right of action (see below), a major improvement on earlier federal Bills, but some still regard this right as too weak; and (iii) The principles included in ADPPA are regarded as having too many loopholes, including for transfers between the public and private sectors. Of these, the pre-emption issue is the most important and pervasive: many flaws in ADPPA will not be able to be exposed by better state laws that remedy the defect.

## Does the scope of the ADPPA qualify it as a national data privacy law?

The scope of ADPPA raises issues around the somewhat imprecise requirement that a national law should cover the 'most important parts' of the jurisdiction's private sector, because of ADPPA's many exemptions from the definition of 'covered entities'. Other questions of coverage are whether the law protects a broad enough range of individuals, and whether enough information is protected under the definition of 'covered data' and exemptions.

Obligations under the ADPPA apply only to 'covered entities' and expressly exclude 'a Federal, State, Tribal, territorial or local government entity', or any body that is collecting processing or transferring data for such an entity (s. 2(9)(B)). Such limitations of coverage to the private sector only are found in a small minority of data privacy laws (Singapore and Malaysia are examples), and in any event the US Federal *Privacy Act of 1974* does provide some coverage.

Otherwise, the ADPPA applies to any 'covered entity' which includes 'any entity or any person other than an individual acting in a non-commercial context' that alone or jointly with others determines processing of 'covered data' (much like a 'controller' under the GDPR) and is either subject to the Federal Trade Commission (FTC) Act, or to the Communications Act of 1934, or is a non-profit organization (s. 2(9)(A)). Limitation of data privacy laws to the business sector is also found in

[6] G. Greenleaf 'California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?' (2020) 168 *Privacy Laws & Business International Report*, 13-17.

[7] Compare, for example, the views of the Electronic Privacy Information Centre (EPIC) and the Electronic Frontiers Foundation (EFF): A. Butler (EPIC) 'Evaluating the American Data Privacy and Protection Act' 8 August 2022 https://techpolicy.press/evaluating-the-american-data-privacy-and-protection-act/ ; H. Tsukayama et al (EFF) 'Americans Deserve More Than The Current American Data Privacy Protection Act' 24 July 2022 https://www.eff.org/deeplinks/2022/07/americans-deserve-more-current-american-data-privacy-protection-act

jurisdictions such as Malaysia. Exclusion of specific sectors of organisations is also common, such as political parties (Australia), churches (South Korea).

Unlike California's law, there is no exclusion of employment information (temporary), or threshold conditions which exempted smaller businesses, or requirement to do business within California. Some ADPPA requirements on covered entities are relaxed for 'small and medium size businesses' (SMEs) (s. 209). Australia goes so far as to completely exempt 'small businesses' (annual turnover of less that AUD$3M) from its Act. Japan previously had a very broad exemption. In contrast, some entities defined as 'large data holders' or 'service providers' using data on behalf of other entities will have additional obligations (s.206, 207).

ADPPA protections are limited to 'individuals', meaning 'a natural person residing in the United States' (s. 2(19)), and do not extend to residents of other countries even though their data is being processed in the US. This makes the ADPPA irrelevant to any consideration of whether the ADPPA provides 'adequate' protection under the GDPR, because it provides no protection to Europeans, except those residing in the US. A few other national laws have or have had similar limitations. US experts point out that limiting benefits to 'residents' is not found in most other US consumer protection laws, and consider this a strange and counter-productive limit.[8]

'Covered data' (s. 2(8)) is the term used to indicate personal information that is protected. 'Covered data' is essentially defined in terms of 'identifiability',[9] which is the case in almost all data privacy laws globally. There are four exclusions (s. 2(8)(B)):

(i) 'de-identified data' – This has its equivalents in many laws (e.g. Korea, Japan, California), including to some extent the EU's GDPR (only as an exemption for certain uses). It is susceptible to misuse everywhere.
(ii) 'employee data', further defined in section 2(8)(C) as five limited categories.
(iii) 'publicly available information' – This exclusion 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.[10]
(iv) Although 'derived data' (undefined) is included in 'covered data', there is an exemption for 'inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual'.

None of these limitations on the scope of the ADPPA are therefore unprecedented (or even particularly unusual) in data privacy laws in other countries. We must conclude that this is an American national Act 'covering the most important parts of its private sector' (as my criteria require), so these limitations are no bar to it being considered a data privacy law.[11]

## Do the ADPPA's principles meet the 'first generation' minimum requirements?

The criterion that I have used since 2011 as to whether a country (including a separate legal jurisdiction) is considered to have a 'data privacy law' is as follows. It must have one or more laws covering the most important parts of its private sector, or its national public sector, or both. The law must provide a set of basic data privacy principles, which at least include almost all the principles (or

[8] Personal correspondence from Marc Rotenberg, former head of the Electronic Privacy Information Center (EPIC).

[9] 'The term 'covered data' means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers' (ADPPA s. 2(8)).

[10] 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.

[11] However, the exclusion from coverage of both the finance sector and the health sector because they already have privacy laws is a significant diminution of coverage, because those laws are so weak: R. Gellman 'Protect consumer privacy: Repeal GLBA's privacy provisions' *iapp privacy perspectives* 30 July 2020 https://iapp.org/news/a/protect-consumer-privacy-repeal-the-glbas-privacy-provisions/

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 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.

The following Table applies these criteria to the ADPPA. *[Italicised data in brackets is a comment.]*

| I | 1st Generation standards | C108 1981; OECD 1980 | **ADPPA** |
|---|---|---|---|
| ***1.01*** | *Collection* – limited (not excessive), lawful (for legitimate purposes) and by fair means | C108 5(a), (c); OECD 7 | Collection, processing etc. is limited to what is reasonably necessary and proportionate to (1) provide/maintain a service requested by the individual, or (2) effect on of 17 specified services/purposes (s. 101(a)) [see 2.04 legitimate bases for processing.] |
| ***1.02*** | *Data quality* –relevant, accurate, up-to-date | C108 5(c)(d); OECD 8 | No positive obligation is provided in ADPPA to maintain relevant, accurate, or up-to-date personal data, only obligations to correct inaccuracies, and delete data after intended use. |
| ***1.03*** | *Purpose specification* by time of collection | C108 5(b); OECD 9 | The categories of covered data that are collected and their purpose must be specified in a privacy policy (s. 202(b)(2) and (3)). |
| ***1.04*** | *Notice of purpose/rights* [assumed implied] | C108 5(b); OECD 9 | Notice of material changes to privacy policy or practices required, with opportunity to opt out in relation to further processing of newly-collected data or previously collected data (s. 202(e)(1)). |
| ***1.05*** | *Uses limited* (including disclosures) to purposes specified or compatible | C108 5(b); OECD 10 | Affirmative express consent required as in s. 202(e)(1)). |
| ***1.06*** | *Security* through reasonable safeguards | C108 7; OECD 11 | Covered entities must establish and maintain reasonable security practices (s. 208(a)(1)). Consideration for evaluating what is adequate are set out. |
| ***1.07*** | *Openness* re. personal data practices (not limited to data subjects) | C108 8(a); OECD 12 | Covered entities must make a privacy policy publicly available, with details specified (s. 202). Access to this information is not restricted to persons on whom the business holds information ('publicly available'). FTC can also specify short-form notices (less than 500 words) by large data holders (s. 202(f)). FTC must submit a report to Congress five years after individual civil actions commence, and annually thereafter (s. 403(5). |
| ***1.08*** | *Access* – individual right of access | C108 8(b); OECD 13 | '…a covered entity shall provide an individual, after receiving a verified request from the individual, with the right to – (1) access – … the covered data … of the individual … that is collected, processed, or transferred by the covered entity, or any service provider of the covered entity within 24 months preceding the request' (203(a)(1)(A)). Also (B) categories of third parties (and names on request) plus categories of service providers to whom covered entity has transferred individual's covered data for profit. Also (C) description of purpose of such transfers. |
| ***1.09*** | *Correction* – individual right of *correction* | C108 8(c), (d); OECD 13 | Obligation to 'correct any verifiable substantial inaccuracy' and make reasonable efforts to inform 3rd party recipients' (s. 203(a)(2)). |
| ***1.10*** | *Accountable* – identified data controller accountable for implementation | C108 8; OECD 14 | Privacy policy must contain identity and contact information for privacy and data security enquiries (s. 202(b)(1)). Employee(s) to be designated to carry out disposal of data (s. 208(a)(6)). |

The ADPPA therefore includes equivalents of nine of the ten '1st generation' principles necessary for a data privacy law, except 1.02 (data quality). California's law has the same omission.

Therefore, on the basis of both the principles that it includes, and its scope, we may conclude that ADPPA is a data privacy law. If it is enacted, then after 40 years, the US will have a national data privacy law implementing the OECD Guidelines of 1980 for most of its private sector, but with significant gaps in coverage.

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

The second stage of the analysis I undertook in 2012 was to ask,[12] to what extent do the data privacy laws enacted outside Europe up to 2012 embody principles similar to the European Union's data protection Directive of 1995. 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). Thirty-three of the thirty-nine data privacy laws in countries outside Europe were analysed at this time.

These ten requirements were as follows, compared with whether they are found in the ADPPA. *[Italicised text in brackets is a comment.]*

| II | 2nd Generation – 'European standards' – post-1995 | EU DPD 1995 | **ADPPA** |
|---|---|---|---|
| ***2.01*** | *Minimum collection* necessary for purpose (data minimisation)[13] | 6(1)(b),(c), 7 | Collection, processing etc. is limited to what is reasonably necessary and proportionate to permissible purposes (s. 101). FTC shall issue guidance on what is 'reasonably necessary and proportionate' (s. 101(c)). *[This could in practice amount to data minimization.]* |
| ***2.02*** | *Destruction or anonymisation after purpose completed* | 6(1)(e) | Disposing of covered data is required when it is no longer necessary for the purpose for which it was collected (s. 208(a)(4)). Methods of disposal are set out. On request it is required to 'delete covered data' and make reasonable efforts to notify all 3rd party recipients (s. 203(a)(3)). |
| ***2.03*** | *Additional protections for sensitive data* in defined categories | 8 | 'Sensitive covered data' is defined to include an exceptionally broad list of 16 categories (s. 2(28)).[14] *['Sensitive data' is radically broader than in the GDPR, particularly (vi), (vii) and (xv)– see footnote.]*<br><br>The collection or processing of sensitive covered data must be 'strictly necessary' (not only 'reasonably necessary and proportional) for one of the permitted purposes (except (13), (16) or (17) where it is not allowed at all) (s. 102(2)). The conditions under which sensitive covered data may be transferred to a third party are also more limited than with other covered data. |

[12] 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

[13] Both EU DPD and C108 use 'not excessive', but EU DPD adds 'necessary', except for processing with unambiguous consent. C108+ 5(c) retains 'not excessive' but EM [52] states this means minimal collection and anonymity where possible. GDPR 1(c) 'data minimisation' says 'limited to what is necessary'.

[14] Sensitive covered data includes information revealing: (i) government-issued IDs, not requiring public display; (ii) physical health, mental health, disability, diagnosis, or healthcare condition or treatment; (iii) financial data revealing income level or bank balances; (iv) biometric information; (v) genetic information; (vi) precise geolocation information; (vii) private communications; (viii) log-in credentials / codes; (ix) sexual behavior; (x) calendar information; (xi) photos etc. of naked/semi-clad people; (xii) video content preferences; (xiii) known minors (under 17); (xiv) race, color, ethnicity, religion, or union membership; (xv) online activities over time and across 3rd party websites or online services; and (xvi) covered data collected so as to identify sensitive data in categories (i)-(xv).

| | | | |
|---|---|---|---|
| ***2.04*** | *Legitimate bases for processing defined* | 7 | 17 legitimate bases for collection, processing etc ('permissible purposes') specified (s101(b)). *[Purposes (16) and (17) concern first party advertising and targeted advertising.]* |
| ***2.05*** | *Additional restrictions on some sensitive processing systems* (notification; 'prior checking' by DPA etc) | 20 | 'Third party collecting entities must display specified information on their websites, and must be registered (s. 206). |
| ***2.06*** | *Limits on automated decision-making* (incl. right to know processing logic) | 15, 12(a) | A large data holder that uses a covered algorithm in a manner that poses a consequential risk of harm to an individual or group, must conduct an impact assessment (s. 207(c)). Users of such algorithms must re-design them to reduce the risk of potential harms (s. 207(c)(2)). |
| **2.07** | *To object to processing on compelling legitimate grounds* | 14(a), (b) | There must be an 'easy to execute' right to withdraw consent in relation to use of covered data (ADPPA s. 204(a)). There must also be a right to opt out of covered transactions (s. 204(b)). The FTC must establish or recognize one of more centralized mechanisms, including browser or device privacy settings, and registries, to allow individuals to exercise all such opt-out rights through a single interface (s. 210). |
| ***2.08*** | *Restricted data exports* requiring recipient country 'adequate', or alternative guarantees | 25, 26 | Not explicitly provided, same conditions as for transfers within US: see s101(a); right to opt out in some cases (s. 204(b)). Transfer of sensitive covered data requires affirmative express consent (s. 102(3)). Notice required if covered data will be processed in or otherwise accessible to the People's Republic of China (PRC). Russia, Iran or N. Korea (s. 202(b)(9)). |
| ***2.09*** | *Independent Data Protection Authority(-ies)* (DPA) | 28 | A 'Bureau of Privacy' is to be established within the FTC. Breaches of FTC regulations shall be treated as unfair or deceptive acts or practices. (ADPPA s. 401). *[The independence of the Bureau will reflect that of the FTC, which is an independent agency.]* |
| ***2.10*** | *Recourse to the courts* to enforce data privacy rights | 22, 23 | Civil actions for breaches of the Act or a regulation may be brought by a person or class of persons, two years after the Act takes effect (s. 403). *[In addition, the FTC or a State Privacy Authority may enforce through civil actions, as explained below.]* |

The FTC will establish a Victims Relief Fund which will receive any civil penalties paid to the FTC by covered entities and may use it to provide compensation etc. to victims (s. 401(5)). This is not a private right of action but may have some of the same effects, if it is in fact used for compensation (a similar provisions in the HIPAA resulted in the FTC keeping the money). A State attorney-general or State Privacy Authority may bring a civil action in the Federal district court to enforce the Act, including obtaining compensation etc on behalf of State residents (sec. 402(a)). Cooperation between the FTC and State Privacy Agencies is required, and the FTC can intervene in such actions (sec. 402(b)). States can also intervene in FTC-initiated actions (s. 402).

The ADPPA therefore includes nine 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. The missing principle is that of data export restrictions (2.08). The private right of action is delayed two years, but that is not unusual, world-wide. California's law also omits two other important '2nd generation' principles: defined legitimate bases for processing (2.04); and a private right of action (2.10). Creation of an independent DPA, the Bureau of Privacy, is a major advance (2.09), often regarded as the most important enforcement element in such laws.

The average number of these 2nd Generation principles included in data privacy laws outside Europe in 2012 was 7/10.[15] Informal estimates, taking into account the much larger number of non-European data privacy laws since then, are that it is still the case that approximately 7/10 of these principles are included.[16] The ADPPA's inclusion of 9/10 of these principles, if enacted, would make it one of the stronger laws outside Europe, and above the international average.

## Which of the GDPR's 3rd generation principles are included?

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 GDPR and the Council of Europe (CoE) 'modernised' Convention 108 of 2018 (now known as '108+').

'Third generation' principles included (at least in part) in the ADPPA include:

- A right of data portability (s. 203(a)(4)) – equates to GDPR art. 20.
- Attempts to interfere with the autonomy of individuals by attempting to condition the exercise of their rights, including by the manipulation of interfaces`, are illegal (s. 203(b)(4)) – overlaps GDPR art. 5(2).
- Retaliation against individuals for exercising any of their rights under ADPPA, including by denial or differential pricing of goods or services, is illegal (s. 104).
- Biometric and genetic data are included as sensitive data (s. 2(28)) – included in GDPR art. 6(1).
- Although data breach notifications are not included in the ADPPA, every US State or Territory has legislation requiring such notifications – equivalent to GDPR, arts. 33 and 34).
- 'Privacy By Design' is required (s. 103), with guidelines as to factors covered entities and service providers must consider. The FTC is required to issue guidance on what is reasonably required, within one year following enactment. The GDPR's implementation of 'Data Protection by Design and by Default' (GDPR art. 25) is much stronger and is potentially actionable for breaches, whereas the ADPPA version is only guidelines as yet.
- Individuals have strong consent-based rights: (i) to withdraw any previous affirmative express consent (s. 204(a)); (ii) to opt out of the transfer of their data by a covered entity to a third party (s. 204(b)) by an opt-out mechanism in s. 210; and (iii) to opt out of targeted advertising (s. 203(c)), by use of a general opt-out mechanism.

These inclusions are significant, but ADPPA still only includes a handful 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.[17] This is still a reasonably high take-up of these GDPR principles, compared with other recent new or revised laws globally.

## Additional principles: Going beyond the GDPR

Although the European Union has been the main source of innovations (and emulation) in data privacy laws since the mid-90s, there is every reason to expect that a strong national data privacy law in the US should become a new source of innovations and be emulated by other countries. Whether it can supplant the GDPR as the 'gold standard' for emulation by other countries remains to be seen.

Some examples of innovations in ADPPA include:

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

[16] G. Greenleaf, Graham, ''European' Data Privacy Standards Implemented in Laws Outside Europe' (2017) 149 *Privacy Laws & Business International Report* 21-23.

[17] 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>.

- The whole of Title 1 is called 'Duty of Loyalty', a new concept for data privacy laws. It encompasses data minimization (s. 101), other loyalty by which deceptive advertising or marketing is banned (s. 102), privacy by design (s. 103) and loyalty concerning pricing (s. 104). One analysis of the concept sums it up as 'Data loyalty is the simple idea that the organizations we trust should not process our data or design their tools in ways that conflict with our best interests.'[18] 'Data loyalty' could emerge as a US innovation.
- As part of data loyalty, ADPPA prohibits cross-contextual behavioural advertising, whereas California's law only allows consumers to opt out of such advertising.
- ADPPA embeds 'algorithmic accountability' and other civil rights aspects of algorithms in much more details than the EU approach which puts more emphasis on separate AI laws, rather than incorporating these details in the GDPR.
- There will be additional protections for those under 17, including a prohibition on targeted advertising, and a Youth Privacy and Marketing Division will be established at the FTC.
- Third party collecting entities will have extra obligations, including registration (s. 206). They must place legislatively specified notices on their website. The must register with the FTC, and have their details included in a public register. They must comply with a 'Do Not Collect' registry link and mechanism by with an individual may easily submit a request to all registered 3rd party collecting entities (other than consumer reporting agencies), to delete all data held which was not collected directly from the individual. The data must be deleted within 30 days.
- Covered SMEs would have some different obligations, including the option of deleting individual data instead of responding to a correction.
- The explicit requirement that large data holders provide short form privacy notices of not more than 500 words (s. 203(f)) goes beyond GDPR requirements.

## Conclusions from an international perspective

The ADPPA is not 'America's GDPR' since few GDPR principles are included. It would be more accurate to describe it as 'America's Data Protection Directive' given that it embodies 9 of the 10 additional principles in the 1995 Directive. It is a very strong '2nd Generation' law.

There is much about the ADPPA which makes it very innovative and worth comparing to the strongest data privacy laws. In particular, it establishes a unique relationship between federal and state enforcement authorities, which may turn out to be comparable to the relationship between national DPAs and the European Data Protection Board (EDPB) in the EU. Its use of automated 'Do Not Collect' links may develop innovative ways in which individual agency can control the use of personal data in ways which the 'notice and consent' model failed to do.

However, ADPPA also has very significant limitations from an international perspective. First, its benefits extend only to US residents, which destroys the role it could play in establishing a reciprocal basis for free flow of personal information. Second, it does not place limits on the export of personal data to countries with very low privacy standards (except in the new 'axis of evil': People's Republic of China (PRC). Russia, Iran or N. Korea (s. 202(b)(9))).

For maximum global effect, a US federal data privacy law needs to be more ambitious in addressing:

1. the international position of the US, particularly government access to private sector data, in light of the *Schrems II* decision,
2. the common challenges from Chinese surveillance faced by the US and EU;
3. the desirability of an EU decision that data protection in the whole US private sector is 'adequate'; and

[18] W. Hartzog and N. Richards 'Legislating Data Loyalty (June 8, 2022). 97 *Notre Dame Law Review Reflection* 356 (2022), https://ssrn.com/abstract=4131523

4. 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.[19]

*Information: Valuable comments and suggestions have been received from Marc Rotenberg, (president of the Center for A.I. and Digital Policy), ), Woodrow Hartzog (Boston University School of Law) and Robert Gellman (US Privacy and Information Policy Consultant), but all responsibility for content remains with the author.*

*4,800 words*

[19] 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>.