American Privacy Rights Act: A first glance at the US Congress's newest comprehensive privacy bill

Received: 6th June, 2024

Lothar Determann
Baker McKenzie, USA

Lothar Determann practises technology law at Baker McKenzie, Palo Alto, admitted in California and Germany. He teaches law at the Freie Universität Berlin and Berkeley School of Law and has authored more than 170 articles and six books including 'Determann's Field Guide to Data Privacy Law' (5th Edition, 2022, also available in Arabic, Chinese, French, German, Hungarian, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Turkish and Vietnamese), 'California Privacy Law — Practical Guide and Commentary on US Federal and California Law' (5th Edition, 2023), and 'Determann's Field Guide to Artificial Intelligence Law' (2024).

Baker McKenzie, 600 Hansen Way, Palo Alto, CA 94304, USA
Tel: +1 650 856 2400; E-mail: ldetermann@bakermckenzie.com

Brian Hengesbaugh
Partner & Chair, NA IP & Technology Practice, Baker McKenzie, USA

Brian is Chair of Baker McKenzie's Global Data Privacy and Security Business Unit, Chair of the North America IPTech Practice Group and a member of the firm's Global IP Tech Steering Committee. He is listed in The Legal 500 Hall of Fame and was recognised as a Regulatory & Compliance Trailblazer by the *National Law Journal*. He is also listed as a leading lawyer for cyber law (including data protection and privacy) in The Legal 500 and is ranked by Chambers. Brian provides advice on global data privacy, cybersecurity, artificial intelligence (AI), ad tech/social media and other data-related legal and regulatory issues. He focuses on these issues in the context of: (i) advisory matters, such as data privacy, cybersecurity and emerging AI laws and regulations (eg GDPR, CCPA, State Privacy Laws, NY DFS Cybersecurity Regulation, HIPAA, GLBA NIST AI Framework, EU AI Act, NIS2 and others), as well as technology transformations related to artificial intelligence, IoT, blockchain, synthetic data, mobile, cloud, data monetisation and other initiatives; (ii) transactional matters, such as mergers and acquisitions, sourcing, distributor, business partner and other third party arrangements; and (iii) crisis matters such as cybersecurity incidents, regulatory and governmental inquiries related to privacy and security issues, internal investigations and litigation-related matters.

NA IP & Technology Practice, Baker McKenzie, 300 E. Randolph Street, Suite 5000, Chicago, IL 60601, USA
Tel: +1 312 861 3077; E-mail: brian.hengesbaugh@bakermckenzie.com

Avi Toltzis
Knowledge Lawyer, Intellectual Property and Technology, Baker McKenzie, USA

Avi Toltzis is a knowledge lawyer in Baker McKenzie's Intellectual Property and Technology practice.

Intellectual Property and Technology, Baker & McKenzie LLP, 300 East Randolph Street, Suite 5000, Chicago, IL 60601 USA
Tel: +1 312 861 8000, Fax: +1 312 861 2899; E-mail: avi.toltzis@bakermckenzie.com

Abstract The recently introduced the American Privacy Rights Act (APRA) represents the latest attempt to pass a comprehensive federal privacy law in the US that would vern privacy generally across the country. The draft bill proposes novel compromises on controversial topics such as federal pre-emption and rights of private action, which need refinement and are likely to be changed in the legislative process. The attempt to cover

not-for-profit entities without accounting for their different purposes seems ill conceived and raises constitutional concerns. This paper examines the APRA in its constitutional, historical and policy contexts.

KEYWORDS: APRA, American Privacy Rights Act, pre-emption, right of private action, CCPA, GDPR, data privacy, consumer privacy, United States, federal, DSARs, transparency, privacy notice, privacy compliance

DOI: 10.69554/WUNF9400

INTRODUCTION

Although legislative affairs typically require a particular kind of fortitude — only about 7 per cent of bills that are introduced survive to become law — observers may wonder if US Congress's new attempt to enact a federal comprehensive privacy law is a case of doing the same thing over and over but expecting different results. On 7th April, 2024, Senator Maria Cantwell, joined by Representative Cathy McMorris Rodgers jointly released a discussion draft of the American Privacy Rights Act (APRA).[1] On 23rd May, 2024 the House Energy & Commerce Committee unveiled an updated version.[2] The APRA is the latest in a line of proposals seeking to bring a uniformity to the confusing patchwork that has defined American privacy law and comprehensive data processing regulation in recent years. Like its predecessors,[3] the APRA faces fierce opposition on controversial topics such as private rights of action and pre-emption of state laws, which may stymie its progress through the legislative process.

BACKGROUND: EXISTING US PRIVACY REGULATION

The APRA enters an already complex regulatory and legislative environment — indeed, one of the stated objectives of the APRA is to 'eliminate[. . .] the existing patchwork of [. . .] data privacy laws.'[4] According to a 2006 survey of US privacy laws, the US has 'hundreds of laws pertaining to privacy: the common law torts, criminal law, evidentiary privileges, constitutional law, at least twenty federal statutes, and numerous statutes in each of the fifty states.'[5] Since the 1970s, countless new privacy laws have been added each year. To appreciate how the field became so congested with competing mandates — and how the APRA proposes to bring some measure of harmony to this disorder — it is first necessary to consider the unique legislative framework of the US.

Law in the US can be created at either the federal, state or local levels. The allocation of authority to enact laws between the state and federal levels is governed by the US Constitution. The US Congress, the legislative body of the federal government, is empowered to pass laws only in areas specifically enumerated by the Constitution, while all other authority is reserved to the states.[6] Generally speaking, federal authority to legislate in the area of data privacy derives from the Commerce Clause, which imparts to Congress the power 'to regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes.'[7]

US states typically have broad authority to legislate as established by their respective constitutions. In many instances, federal and state legislative authority may overlap, where they are said to have 'concurrent powers.' However, where such overlapping authority exists and Congress has enacted legislation that conflicts with a state law, the federal law prevails and it may pre-empt (ie replace, supersede and/or invalidate) the state law.[8] State law can be pre-empted by a federal law

either expressly (ie by a pre-emption clause that specifically states Congress's intent to pre-empt state law) or implicitly (ie by enacting a law that conflicts with or 'occupying a field' of state legislation).[9] One of the main benefits of the pre-emption doctrine is that it promotes uniformity of the law across the nation, making it easier and more predictable to conduct business across state lines.[10]

However, it is also possible that a federal law expressly or impliedly accepts that state laws may be stricter or different. For example, financial services regulations like under the Gramm–Leach–Bliley Act (GLBA) do not generally pre-empt state laws that provide greater privacy protections[11] and the federal Computer Fraud and Abuse Act (CFAA) does not pre-empt state law equivalents.[12] Under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), covered entities and their business associates must comply with numerous, detailed data privacy and security requirements, including the Security and Privacy Rules, as amended by the omnibus rule issued by the US Department of Health and Human Services in 2013;[13] but HIPAA and these rules set only a minimum standard and do not pre-empt more stringent state law.[14]

When European countries started enacting data protection laws in the 1970s, the US also considered this option but decided against comprehensive regulation of data processing. Congress felt it was too early to appropriately identify and address potential privacy harms and balance privacy interests with freedom of information, innovation and economic freedoms.[15] Therefore the US instead resolved to pass sector, situation and harm-specific privacy laws, as the need should arise, at the state and federal level. This allowed information technology companies in the Silicon Valley to grow and become industry leaders in semiconductor technologies, software, e-commerce, cloud computing, social media, big data and other data-intensive products and services.[16] But this also resulted in hundreds of diverging and constantly evolving privacy laws across the US. Companies and government agencies find it increasingly difficult to navigate the maze of US privacy laws. Businesses are particularly concerned about the California Consumer Privacy Act of 2018 (CCPA), which adds extensive new disclosure requirements and individual rights to existing laws in order to rein in perceived risks emanating from data selling or sharing, and that applies comprehensively to personal information about individual consumers, households, employees, business contacts and other natural persons.[17] The surplus of distinct and sometimes overlapping privacy mandates has led to compliance challenges, public confusion and rising calls for Congress to intervene.

Although no comprehensive federal privacy law currently exists, sectoral privacy legislation at the federal level abounds. Despite the relatively modern vintage of most of the statutes crowding the field, the notion of governmental regulation of privacy can be traced back to the nation's founding and beyond. Privacy interests are said to be woven into many of the constitutional amendments in the Bill of Rights.[18] And in their seminal 1890 article, 'The Right to Privacy', Warren and Brandeis tethered the right to common law foundations.[19]

Yet the conditions giving rise to the present abundance of privacy laws emerged in earnest in the 20th century. The expansion of mass media, new communication technologies, innovations in consumer finance and the rise of the administrative state created a perfect storm. Many of federal privacy laws were enacted in direct response to, or as a consequence of, these factors.

The Fair Credit Reporting Act of 1970, for example, restricts the disclosure of certain information collected by creditors and allows borrowers to correct erroneous information.[20] The Privacy Act of 1974 regulates the use of records about individuals

collected by federal agencies by restricting their disclosure and allowing individuals to request access to records about them.[21] The Electronic Communications Privacy Act of 1986 (ECPA) amended the federal wiretapping statute (which itself dates to the 1960s) to apply to a wider range of electronic communications.[22] HIPAA, along with its companion legislation the Health Information Technology for Economic and Clinical Health Act, regulates use of health data by health plans, healthcare clearinghouses, healthcare providers and their 'business associates.'[23] Financial institutions must comply with privacy requirements contained in 1999's GLBA. The Children's Online Privacy Protection Act 1998 (COPPA) places certain obligations on websites that are aimed at children younger than 13 years old or those that knowingly collect personal information from children under 13 years of age.

These laws, and scores of others, cumulatively regulate almost every imaginable scenario. Yet a comprehensive federal privacy statute — that is, a law that governs all varieties of personally identifiable information and applies to any entity handling such information, irrespective of industry or posture — has remained elusive.

Turning to the states, the situation is no less convoluted. As at the federal level, a staggering volume of industry and use-specific privacy legislation has emerged. In many instances these coexist with similar federal laws, despite the constitutional doctrines on pre-emption. For example, although the ECPA establishes federal protections for privacy in electronic communications, every US state has enacted its own wiretapping statute. These laws may coexist with the ECPA because the ECPA does not explicitly pre-empt state legislation nor does it express the 'intent by Congress to occupy the entire field involving the interception of communications.'[24] Because of the permissive approach to pre-emption, state privacy laws have proliferated even in subject areas which substantially overlap with federal legislation.

In addition to these sectoral privacy laws, in recent years a growing cohort of states have enacted comprehensive privacy legislation. The first such law, the CCPA[25] was passed soon after, and in apparent response to, the EU's General Data Protection Regulation (GDPR).[26] In the years since, many states have followed California's lead by enacting their own comprehensive privacy laws loosely modelled on the CCPA — as of May 2024, 17 states had enacted such statutes, with more in advanced legislative stages.

Although these laws tend to have similar overall features, they impose disparate, and often difficult to reconcile, requirements. An organisation may need to display different privacy notices, afford consumers different rights or abide by different restrictions on sharing data, depending on which law applies. Simply identifying which of these laws apply to a specific organisation can itself be a significant, costly exercise. Consumers themselves are also poorly served by this situation, with little public understanding of what rights privacy laws confer on them.

For these reasons, the US privacy regulatory landscape has often been characterised as a 'patchwork'. Both industry and privacy advocates have called for federal action to streamline this ever-more byzantine and inscrutable system.

LEGISLATIVE HISTORY: PAST ATTEMPTS TO PASS COMPREHENSIVE FEDERAL PRIVACY LEGISLATION

The APRA is not the first proposal to standardise privacy requirements nationwide through federal legislation. As far back as May 2000, the Federal Trade Commission (FTC), the primary consumer protection agency in the US, entreated 'Congress [to] enact legislation to ensure adequate protection of consumer privacy online.'[27]

The FTC's proposal for legislation centred around four pillars that endure and continue to form the basis of much privacy legislation nearly 25 years later: (1) notice; (2) choice; (3) access; and (4) security.

In 2012, a comprehensive privacy law was back on the legislative docket, with the Obama administration urging Congress to codify its 'Consumer Privacy Bill of Rights.' This effort foundered, and was ultimately shelved, after years of debates between industry representatives and privacy rights groups.[28]

Privacy legislation re-emerged on the congressional agenda in 2019, with the passage of the GDPR prompting renewed calls for federal privacy legislation and bringing several diverse proposals. In April, Senator Edward Markey tabled the Privacy Bill of Rights Act, which proposed an opt-in consent regime.[29] In November, Democratic Senator Maria Cantwell and her Republican counterpart, Roger Wicker, introduced competing proposals in their respective Consumer Online Privacy Rights Act (COPRA)[30] and discussion draft of the US Consumer Data Privacy Act (USCDPA).[31] The bills established similar frameworks but diverged on key sticking points, including the availability of private enforcement and the pre-emption of state laws.[32] These attempts stalled as compromise on these issues proved elusive — much as it has in the years since — and as 'response to the COVID-19 pandemic [. . .] necessarily consumed most of the available bandwidth in Congress.'[33]

In 2022, with several states having already taken the initiative by passing their own consumer privacy laws, Representative Frank Pallone introduced the American Data Privacy and Protection Act (ADPPA).[34] The ADPPA is notable in that it borrows some features from the state laws that preceded it, but it also departs from those precedents in other key areas.

Like existing state privacy legislation[35] (and like the GDPR before it), the ADPPA would confer certain rights on consumers to dictate how their data used, such as the rights to access, correct and delete their data.[36] Controllers would be required to recognise universal opt-out mechanisms expressing a consumer's preferences for how their data is to be used.[37] Additionally, the ADPPA espouses data minimisation principles that have become ubiquitous in privacy legislation.[38]

But the ADPPA differs from its state law predecessors in very significant ways. The ADPPA introduced a 'duty of loyalty' that controllers would owe to consumers, notionally derived from the fiduciary duties that shareholders are due from corporations.[39] Similarly, the ADPPA included corporate governance requirements, such as the appointment of a privacy protection officer, which is absent from prevailing state laws (but present in the GDPR).[40]

Even more consequential than these provisions, was the ADPPA's approach to enforcement. Primary enforcement authority would be shared by the federal FTC and by state authorities.[41] However, the ADPPA also established a private right of action, allowing individuals to bring lawsuits for violations of the ADPPA.[42] The prospect of private enforcement, notably absent from the majority of state privacy legislation,[43] is significant because it allows for the possibility of costly — and, in the estimation of many defendants, frivolous — class action litigation. Although the private right of action provision would have a sunrise period[44] and would require private litigants to inform the FTC and state authorities to afford them an opportunity to intervene, many businesses consider private enforcement a non-starter for any legislative proposal.[45]

Another controversial aspect of the ADPPA was its approach to pre-emption. As noted above, under the US federal system, under the doctrine of pre-emption, the federal law prevails when it either expressly or impliedly pre-empts a state counterpart, rendering the state law a nullity.[46] This has

the effect of promulgating a single uniform standard across the nation. The ADPPA pre-empted state laws 'covered by the provisions of [the ADPPA]' but included myriad carve-outs, including for laws that address financial data and health information, as well as exceptions for specific state laws including Illinois' Biometric Information Privacy Act (BIPA) and the CCPA's private enforcement provision.[47] The pre-emption of state privacy laws provoked the ire of state lawmakers and regulators, who viewed pre-emption as an unwanted encroachment on states' prerogative to protect their constituents.[48] On the other hand, many businesses felt that the ADPPA's piecemeal approach to pre-emption did not act strongly enough to establish a streamlined compliance environment.[49]

In July 2022, the ADPPA was reported out of the House Committee on Energy & Commerce by an overwhelming vote (53:2), the first comprehensive federal bill to be voted out of committee.[50] Although the ADPPA was formally scheduled for a full floor vote in the House of Representatives, a major step in the federal legislative process, it subsequently languished and a floor vote never transpired.

April 2023 saw another comprehensive privacy bill, the Online Privacy Act of 2023, introduced by Democratic Representative Anna Eshoo in the House Committee on Energy & Commerce.[51] This proposal, which echoes legislation proposed by Representative Eshoo in 2019 and 2021, features many of the familiar components of other consumer privacy legislation — mandatory notice, the establishment of consumer rights, and so on — but also envisages the establishment of a new federal agency to police online privacy, the Digital Privacy Agency.[52] The Online Privacy Act did not even proceed to a committee vote.

With this history of false starts as prologue, on 7th April, 2024, Senator Cantwell — who had been deeply involved in the formulation of past draft privacy legislation, as well as a vocal opponent of the ADPPA[53] — and Republican Representative Cathy McMorris Rodgers introduced the APRA. The APRA shares many features with past attempts to pass federal omnibus privacy legislation. The following sections will explore how the APRA is structured and dig deeper into several of its most significant provisions.

STRUCTURE OF THE APRA

Key concepts and terminology

Broadly speaking, the APRA places restrictions and requirements on how 'covered entities' use 'covered data.' A covered entity is one that, 'alone or jointly with others, determines the purposes and means of collecting, processing, retaining, or transferring covered data.'[54] This formulation closely aligns with that of the 'controller' in other data privacy legislation, including the GDPR and many state consumer privacy statutes.[55]

In a stark departure from nearly all existing US privacy laws (though in common with the ADPPA), the proposed law would explicitly apply to non-profit organisations.[56] The inclusion of churches, charities and other non-profit organisations seems particularly problematic because the substantive provisions and regulatory concepts of the APRA are tailored to businesses and do not take the special purposes and situation of non-profits into account.[57] The policy implications of subjecting non-profits to business regulation, liability and enforcement at the expense of their ability to serve their non-profit purposes do not seem to have been sufficiently considered.

The APRA further defines two subcategories of covered entities, 'large data holders' and 'data brokers', who are subject to heightened requirements.[58] This approach contrasts somewhat from the prevailing trends in state consumer privacy legislation, which generally only apply to entities

that meet set revenue and data processing thresholds.[59] The base provisions of the APRA would apply to all covered entities, reserving stricter requirements for the large data holders meeting threshold criteria.

Some provisions of the APRA also apply to 'service providers', which are entities that 'collect[. . .], process[. . .], retain[. . .], or transfer[. . .] covered data for the purpose of performing 1 or more services or functions on behalf of, and at the direction of, a covered entity.'[60] The concept of service providers tracks that of 'processors' in many other privacy laws.[61]

Covered data refers to 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 1 or more individuals.'[62] Again, this definition is broadly analogous to 'personal information' or 'personal data' in other laws, though it is potentially broader insofar as it may encompass information linked to a device.[63] As with most state comprehensive privacy laws, the APRA excludes employee data.[64]

Consistent with many other laws, the APRA imposes stricter requirements on the use of sensitive data (or in the case of the APRA, 'sensitive covered data'), which includes: government-issued identifiers, information that describes or reveals the past, present or future physical health, mental health, disability, diagnosis or healthcare condition or treatment of an individual; genetic information; financial account information; precise geolocation information; private communications; account or device login credentials; information revealing a person's sexual behaviour; calendar information; media showing the naked or undergarment-clad private area of an individual; information revealing the extent or content of any individual's access, viewing or other use of any video programming.[65] This partial list suggests that while the APRA's conception of sensitive information overlaps significantly with that in existing laws, it is rather broader in that it extends to categories of information that relate to a person's conduct, not simply their identity.[66] Like other privacy laws, the APRA uses new terminology, compared in the Table 1 with excerpts from the CCPA, GDPR and India's Digital Personal Data Protection Act (DPDPA). The complexity, diversity and prescriptiveness of terminology makes it particularly difficult for global organisations to operationalise compliance with data privacy laws.[67]

Data subject rights

The APRA would establish a familiar set of consumer rights that individuals may exercise over their data: rights to access, correct and delete their covered data and the right to its portability.[68] Covered entities will have 30 days to respond to data requests; large data holders will need to respond within 15 days.[69] The APRA also empowers individuals to opt out of transfers of their data, as well as targeted advertising.[70] The law requires the FTC to promulgate regulations on the establishment of a universal opt-out mechanism standard.[71]

Transparency

The APRA would require a covered entity or service provider to publish a privacy policy that offers 'a detailed and accurate representation of the covered entity or service provider's data collection, processing, retention, and transfer activities.'[72] The policy must provide the identity and contact information for the covered entity or service provider, the categories of covered data collected, processed or retained, the processing purposes for each data category, categories of service providers to whom the data is transferred, the names of data brokers to whom data is transferred, the purposes of the transfers, the duration for which data is retained, instructions for invoking data subject rights and opt out requests, a general

Table 1: Comparison of APRA Terminology with that of the CCPA, GDPR and DPDPA

APRA	CCPA	GDPR	DPDPA
The term *'covered entity'* means any entity that, alone or jointly with others, determines the purposes and means of collecting, processing, retaining, or transferring covered data and — (i) is subject to the Federal Trade Commission Act; (ii) is a common carrier subject to title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.); or (iii) is an organization not organized to carry on business for its own profit or that of its members.	*'Business'* means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: [. . .] [CCPA exempts smaller companies that are not focused on selling personal information]	*'Controller'* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	*'Data Fiduciary'* means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
The term *'large data holder'* means a covered entity or service provider that, in the most recent calendar year, had an annual gross revenue of not less than $250,000,000 and, subject to subparagraph (B), collected, processed, retained, or transferred — (i) the covered data of — (I) more than 5,000,000 individuals; (II) more than 15,000,000 portable connected devices that identify or are linked or reasonably linkable to or more individuals; or (III) more than 35,000,000 connected devices that identify or are linked or reasonable linkable to 1 or more individuals; or (ii) the sensitive covered data of — (I) more than 200,000 individuals; (II) more than 300,000 portable connected devices that identify or are linked or reasonable linkable to 1 or more individuals; or (III) more than 700,000 connected devices that identify or are linked or reasonably linkable to 1 or more individuals.	[CCPA does not contain a comparable term but exempts smaller companies altogether and a separate California law regulates data brokers].	N/A	*'Significant Data Fiduciary'* means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10.

(*Continued*)

Table 1: Comparison of APRA Terminology with that of the CCPA, GDPR and DPDPA (*continued*)

APRA	CCPA	GDPR	DPDPA
The term *'service provider'* means an entity that collects, processes, retains, or transfers covered data for the purpose of performing 1 or more services or functions on behalf of, and at the direction of, a covered entity or another service provider.	*'Service provider'* means a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract.	*'Processor'* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	*'Data Processor'* means any person who processes personal data on behalf of a Data Fiduciary.
The term *'covered data'* means information, including sensitive covered data, 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 1 or more individuals.	*'Personal information'* means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. [CCPA contains a long list of examples of categories of personal information and requires companies to use the statutory terminology in their privacy policies]	*'Personal data'* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	*'Personal data'* means any data about an individual who is identifiable by or in relation to such data.

description of data security policies, and the policy's effective date.[73]

Prohibited conduct

The APRA also contains several broad prohibitions on covered entity conduct. Covered entities may not use dark patterns to distract from their privacy notice, to hinder the assertion of a data subject's rights or to obtain an individual's consent for any APRA purpose.[74] Covered entities are also barred from retaliating against an individual for exercising data subject rights, such as by denying products or services or by charging different prices.[75] Collecting, processing, retaining or transferring covered data in a discriminatory manner is also prohibited.[76]

Data security

Covered entities and service providers must establish, implement and maintain reasonable data security practices.[77] The APRA grants the FTC rulemaking authority to establish standards under which reasonable security practices may be assessed.[78]

Notably, the APRA does not address data security breach notification requirements, but specifically excludes data security breach notification laws from pre-emption.[79] This is unfortunate, because the myriad different federal and state laws that require companies and public sector entities to notify breaches are substantively fairly similar and unnecessarily complicate the process of notifying data subjects and authorities. When organisations experience ransomware attacks and security breaches, they have to act quickly to protect data, privacy and their operations. Every minute counts, but in practice, much time is wasted on sifting through slightly different definitions, formal requirements and details that must and that may not be addressed in notifications. This places an unnecessary burden on organisations and does not benefit individual privacy or security.[80] Few controversies exist from a policy perspective and the great volume of disparate laws seems to be caused solely by legislative dysfunctionality. Harmonising, improving and simplifying data security breach notification laws should be a particularly low-hanging fruit for federal pre-emption.

Data governance

Unlike most US federal and state privacy laws, but in common with the GDPR, the APRA would require covered entities and service providers to appoint either a privacy officer or data security officer.[81] Large data holders would need to appoint individuals in each of these roles and would also be required to undertake annual certifications for the FTC affirming compliance with the APRA.[82] Large data holders would also be required to conduct privacy impact assessments biennially.[83] In contrast to existing state laws, the privacy impact assessment requirement would not be triggered by engagement in high risk processing but would apply to all large data holders irrespective of their activities.

Use of algorithms

Large data holders that use algorithms that make a decision or facilitate human decision making by using covered data in such a manner that poses a consequential risk of harm will also need to conduct annual algorithm impact assessments.[84] And any covered entity that uses algorithms to make or facilitate consequential decisions must publish notice to affected individuals of such use and provide them with an opportunity to opt out of such use.[85]

KEY FEATURES OF THE APRA: IN DETAIL

Several specific provisions of the APRA merit special examination. This section will take a closer look at the APRA's approach

to pre-emption, data minimisation and enforcement.

Pre-emption of state laws

The APRA's pre-emption clauses are derived from those in the ADPPA[86] but include several key differences. Like its predecessor, the APRA would trump 'any [state] law, regulation, rule, or requirement covered by the provisions of [the APRA]'.[87] The APRA also includes a number of carve-outs to the pre-emption provision, allowing certain state laws to coexist. The APRA contains fewer exceptions from pre-emption than ADPPA, but there are still a number of significant exceptions, including for employee privacy laws[88] and health privacy laws.[89] With respect to the BIPA, Illinois' biometric privacy statute, APRA does not contain a complete carve-out from pre-emption (as ADPA did) but allows courts to award to a plaintiff 'for a violation involving biometric information, the same relief as set forth in section 20 of the Biometric Information 11 Privacy Act (740 ILCS 14/20), as such statute read on January 1, 2024' if the conduct underlying the violation 6 occurred primarily and substantially in Illinois.[90] This is highly problematic for companies doing business in Illinois, given the excessive damages awards under BIPA by courts in Illinois and the fact that the Illinois state legislature recently reformed the law to reduce exposure for businesses.[91] APRA protects biometric information somewhat comparable to the substantive requirements codified in BIPA.[92] Yet, APRA's private enforcement provisions would allow plaintiffs alleging a violation of the APRA biometric information requirements to recover the same relief as provided under BIPA if a case relates to Illinois.[93] Although these features purportedly attempt to strike a balance between preserving protection available under existing law and creating a uniform regulatory environment, they are difficult to justify in a comprehensive, federal privacy law and could stir confusion and contention. Similar concerns apply with respect to a California-specific provision in the APRA[94] according to which 'the court may award a plaintiff who is a resident of California the same relief as set forth in section 1798.150 of the California Civil Code, as such statute read on January 1, 2024'.

Another aspect of the APRA pre-emption scheme is likely to foment uncertainty. Like the ADPPA, the APRA has a provision disapplying pre-emption for 'provisions of laws that protect the privacy of health information.'[95] Although this passed without significant comment over the course of the ADPPA's brief lifetime, the developments in the field of health privacy render these provisions increasingly vague and problematic. For instance, some nominally consumer privacy laws have since been amended to add significant health data protections.[96] Conversely, a recent health data law, Washington state's My Health My Data Act defines 'consumer health data' extremely broadly to include information 'derived or extrapolated from nonhealth information'.[97] This blurring of health data and consumer data casts significant doubt on the scope and effect of this pre-emption carve-out. If a final version of the APRA bill does not contain broad and clear pre-emption provisions, then APRA will end up as just another federal privacy bill, adding to the suffocating compliance burden on businesses and confusion for consumers, regulators and law enforcement authorities.

Data minimisation

Although data minimisation requirements have become commonplace in contemporary privacy legislation — all but two of the existing state consumer privacy laws mandate some form of minimisation — these rarely amount to

anything more than a broad, aspirational statement that data collection should be 'adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes'.[98] By comparison, the data minimisation requirements of the APRA are much more prescriptive. The APRA minimisation provision can be broken into two overall requirements. The first limits the collection, processing, retention or transfer of covered data to that which is necessary, proportionate and limited to provide a specific product or service to the individual or to communicate with the individual.[99]

The minimisation principle also dictates that the collection, processing, retention or transfer must be for an expressly permitted purpose.[100] These purposes include: the protection of data security; complying with a legal obligation; the investigation or defence of legal claims; to comply with a subpoena; to effect a product recall; to conduct market research; to deidentify data; to transfer assets in the context of a merger or similar transaction; to provide call location information (if the covered entity or service provider is a telecommunications carrier); to prevent, detect, protect against, investigate or respond to fraud or harassment; to prevent, detect, protect against or respond to a data security incident or public safety incident; to prevent, detect, protect against, investigate or respond to criminal activity; to provide first-party or contextual advertising; to provide targeted advertising to an individual who has not opted out; or to conduct public or peer-reviewed research.[101]

Although the lifting of the minimisation principle from a mere formality to a meaningful requirement may be welcomed by privacy advocates, the use limitations and permitted purposes reflect neither the commercial realities of the existing data ecosystem nor the reasonable expectations of consumers.[102] Moreover, the exceptionally broad application of the APRA, including to non-profit organisations that may have entirely legitimate processing purposes outside those listed in the APRA, creates a real risk that the law may have chilling effects that curtail constitutionally protected expression. For example, APRA §102(d) contains a list of 'permitted purposes' (which, as a term and concept, already raises red flags under the 1st Amendment of the US Constitution, which protects freedoms of speech and information, as well as other civil rights). On the 'permitted purposes' list are market research, product development, mergers and acquisitions, harassment prevention and targeted advertising. However, APRA would not grant permissions to the core purposes of churches, charities and other non-profits. This is in stark contrast with the EU GDPR, for example, which allows data processing if it is 'carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim'. An EU-style limited exception for religious organisations could create equally significant tensions with US constitutional protections against content-based regulation of speech and information access as the principle of 'data minimisation' as such, which seeks to broadly limit access to information. To reduce the risks of constitutional violations, the proponents of APRA should consider removing non-profit entities from the scope of the law (as nearly all US privacy laws already do with the one notable exception of the relative new Colorado Privacy Act)[103] and data minimisation as an overly broad, hardly justifiable restraint on freedom of speech and information.[104]

Enforcement of the APRA

As was the case with the ADPPA, the APRA provides for a sprawling, decentralised enforcement scheme through which violations of individuals' rights can be vindicated.[105]

The APRA grants the FTC broad authority to enforce infringements of the APRA and proposes the establishment of a new bureau for this purpose.[106] The grant of enforcement authority is also notable in that it extends to organisations that would typically fall outside the FTC's jurisdiction — common carriers subject to the Federal Communications Commission's authority, as well as non-profit organisations.[107]

Coexisting with the FTC's authority is that of state attorneys general and other state agencies to enforce violations of APRA committing against residents of their respective states.[108] Before initiating an enforcement action under the APRA, state authorities must notify the FTC if it is feasible to do so.[109]

Lastly, and most controversially, the APRA provides for private enforcement by individuals alongside enforcement by the FTC and by state authorities.[110] However, unlike the FTC or state authorities, who are empowered to enforce any violation of the APRA, the private right of action only applies to a list of specific APRA provisions. This is bound to cause confusion, as it has in the context of the CCPA's private right of action, which has attracted claims based on violations of CCPA provisions outside of Cal. Civ. Code 1798.150.[111] If anything, the uncertainty regarding the scope APRA's private right of action will be considerably worse than for the CCPA — the private right of action clause cross-refers to more than a dozen other APRA provisions. The lack of clarity also invites the risk that some claimants may cite violations included in the private enforcement clause simply to cause a nuisance to defendants in order to extract a quick settlement.

Significantly, the APRA also eschews the ADPPA's prerequisite that authorities be notified before a private action is commenced.[112] The removal of this requirement increases the risk that businesses will be subject to unnecessarily burdensome and duplicative proceedings.

CONCLUSION

Outlook for the APRA

The APRA has already attracted more public attention than any previous federal privacy bill. Because it has received bipartisan and bicameral sponsorship, there is optimism in some quarters that the APRA will succeed where so many others have already failed. At a committee hearing following the bill's introduction, Republican Representative Gus Bilirakis asked the panel: 'Do you think this is the best chance we have to getting something done on comprehensive data privacy?' Each of the six witnesses answered in the affirmative.[113]

The progress of the bill so far has validated this optimism, with the bill having recently passed a voice vote to clear the House Committee on Energy and Commerce Subcommittee on Data, Innovation and Commerce.[114] Still significant — probably intractable — obstacles remain. Unsurprisingly, the California Privacy Protection Agency (CPPA), charged with enforcement of the CCPA, has sharply criticised the bill, as California had done previously with the ADPPA.[115] As before, the CPPA's criticisms centre around APRA's pre-emption of laws like the CCPA, arguing that any federal legislation should set 'a floor, not a ceiling on those rights' afforded by state acts. Such resistance is likely to grow exponentially as more and more states invest in the enactment of privacy laws and regulations, the establishment of departments and institutions dedicated to enforcement of state privacy laws and, by extension, new jobs, career paths and economic opportunities for attorneys, privacy professionals, consultants, technology providers and others.

Yet, pre-emption of state privacy legislation, and the uniformity and predictability that would follow, are likely to be firm prerequisites to any industry support for a comprehensive federal privacy solution. The US Chamber of Commerce, representing the US business community,

has expressed concern over the APRA's tentative approach to pre-emption.[116] If a final version of the APRA bill does not contain broad and clear pre-emption provisions, then the APRA will end up as just another federal privacy bill, adding to the suffocating compliance burden on businesses and confusion for consumers, regulators and law enforcement authorities. The claim that a 'federal floor' for privacy laws is necessary does not seem very plausible, given that most businesses already have to comply with the many state privacy laws, including the newer comprehensive consumer privacy bills that 17 states have already enacted, and the fact that the FTC has been building a robust framework of federal privacy law by actively providing guidance and enforcement actions based on federal unfair competition law.

Adding to the uncertain fate of the APRA, recent amendments seem to have cooled some lawmakers' support for the bill, particularly the hasty addition of amendments to overhaul the US's children's privacy statute, COPPA.[117] The various critical comments make clear that despite the unprecedented buzz surrounding the APRA, it faces a long, bumpy path to becoming a law, even though many scholars, policymakers, practitioners and business representatives agree that APRA could be a step in the right direction if it simplifies, harmonises and fortifies privacy protections in the US.

References and notes

1. American Privacy Rights Act (Discussion Draft MUR24230L4H) (7th April, 2024), available at https://www.commerce.senate.gov/services/files/3F5EEA76-5B18-4B40-ABD9-F2F681AA965F (accessed 25th June, 2024).
2. *See* American Privacy Rights Act (Updated House Draft) (23rd May, 2024), available at https://d1dth6e84htgma.cloudfront.net/PRIVACY_04_xml_d1d6b82f10.pdf (accessed 25th June, 2024); see also Congressional Research Service (31st May, 2024) 'The American Privacy Rights Act', available at https://crsreports.congress.gov/product/pdf/LSB/LSB11161#:~:text=The%20House%20Energy%20%26%20Commerce%20Committee%20unveiled%20an%20updated%20version%20 (accessed 25th June 2024).
3. See the section on legislative history below.
4. United States Senate Committee on Commerce, Science & Transportation (7th April, 2024) 'Press Release: Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation', available at https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation (accessed 25th June, 2024).
5. Solove, D. (2006) 'A Brief History of Information Privacy Law' in 'Proskauer on Privacy', at § 1:1, available at https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications (accessed 25th June, 2024).
6. US Constitution, amend. X. ('The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.').
7. US Constitution, art. 1, sec. 3, cl. 8. See also, H.R. 7891, § 20(a)(1) ('The purposes of this Act are to establish a uniform national data privacy and data security standard in the United States to prevent administrative costs and burdens placed on interstate commerce[.]').
8. US Constitution, art. IV, cl. 2.
9. *See* eg *Altria Grp., Inc. v. Good*, 555 U.S. 70, 87, 129 S. Ct. 538, 549 (2008).
10. *See* eg *Aloha Airlines v. Ahue*, 12 F.3d 1498, 1501 (9th Cir. 1993) ('To ensure uniformity and consistency in such laws throughout the states, Congress included within ERISA one of the broadest preemption clauses ever enacted by Congress.').
11. 15 U.S.C. § 6807(b); Cal. Fin. Code §§ 4050–4060.
12. *Hecht v. Components Int'l, Inc.*, 867N.Y.S.2d 889, 898 (NY Sup. Ct. 2008) ('It appears that the CFAA is not intended to preempt state law claims based on unauthorised access to a computer such as trespass to chattel, conversion, or fraud.'); *Pacific Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1194 (ED Wash. 2003).
13. *See* 78 Fed. Reg. 5566 (25th January, 2013) available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf (accessed 25th June, 2024); 45 C.F.R. §§ 164.102–164.534.
14. *See* 45 C.F.R. §§ 160.201–160.205.
15. Schwartz, P. (2008) 'Preemption and Privacy', *Yale Law Journal*, Vol. 118, pp. 910–16.
16. Chander, A. (2014) 'How Law Made Silicon Valley', *Emory Law Journal,* Vol. 63, No. 3, pp. 639–693, available at https://ssrn.com/abstract=2340197 (accessed 25th June, 2024).
17. Determann, L. (2018) 'California Privacy Law, Practical Guide and Commentary - U.S. Federal and California Law: CCPA Supplement', IAPP, Portsmouth, NH.
18. *Griswold v. Connecticut*, 381 U.S. 479, 85 S. Ct. 1678 (1965).

19. Warren, S. D. and Brandeis, L. D. (1890) 'The Right to Privacy', *Harvard Law Review*, Vol. 4, No. 5, pp. 193–220.
20. 15 U.S.C. 1681 *et seq*.
21. 5 U.S.C. § 552a.
22. 18 U.S.C. § 2510 *et seq*.
23. 42 U.S.C. § 1320d.
24. *Valentine v. NebuAd, Inc.,* 804 F. Supp. 2d 1022, 1029 (N.D. Cal. 2011).
25. Cal. Civ. Code § 1798.100 *et seq*. See above.
26. *See* Determann, L. and Tam, J. (2021) 'The California Privacy Rights Act of 2020: A Broad and Complex Data Processing Regulation That Applies to Businesses Worldwide', *Journal of Data Protection & Privacy*, Vol. 4, No. 1, p. 7.
27. Federal Trade Commission (2000) 'Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress', available at https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report (accessed 25th June, 2024).
28. Singer, N. (29th February 2016) 'Why a Push for Online Privacy Is Bogged Down in Washington', *The New York Times*, available at https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html (accessed 25th June, 2024).
29. S.1214, 116th Congress (2019).
30. S.3456, 116th Congress (2019).
31. Senate Committee on Commerce, Science and Transportation (3rd December, 2019) Fact Sheet: Chairman Wicker's Discussion Draft The United States Consumer Data Privacy Act, available at https://www.commerce.senate.gov/2019/12/chairman-wicker-s-discussion-draft-the-united-states-consumer-data-privacy-act (accessed 25th June, 2024).
32. Congressional Research Service (3rd April, 2020) 'Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress', available at https://crsreports.congress.gov/product/pdf/LSB/LSB10441 (accessed 25th June, 2024).
33. Kerry, C., Morris, J., Chin-Rothman, C. and Turner Lee, N. (3rd June, 2020) 'Bridging the Gaps', Brookings Institution, available at https://www.brookings.edu/articles/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/ (accessed 25th June, 2024).
34. H.R. 8152, 117th Congress (2022).
35. See the section on background above.
36. § 203.
37. § 210.
38. § 101.
39. §§ 101–104.
40. § 301(C).
41. §§ 401–402.
42. § 403.
43. *But see* California Civil Code 1798.150 (providing private right of action under the CCPA for a business's failure to secure personal information resulting in unauthorised access).
44. § 403(a)(1). The sunrise period of four years in the initial draft was shortened to two years in subsequent versions of the bill.
45. *See* eg Castro, D., Dascoli, L. and Diebold, G. (24th January, 2022) 'The Looming Cost of a Patchwork of State Privacy Laws', Information Technology & Innovation Foundation, available at https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/ (accessed 25th June, 2024).
46. See the section on background above.
47. § 404(b).
48. *See* eg Newsom, G. (28th February, 2023) 'Governor Newsom, Attorney General Bonta and CPPA File Letter Opposing Federal Privacy Preemption', Governor of California, available at https://www.gov.ca.gov/2023/02/28/governor-newsom-attorney-general-bonta-and-cppa-file-letter-opposing-federal-privacy-preemption/ (accessed 25th June, 2024).
49. Cummings, J. (25th August, 2022) 'A Possible Move toward Comprehensive Federal Privacy Legislation', EDUCAUSE Review, available at https://er.educause.edu/articles/2022/8/a-possible-move-toward-comprehensive-federal-privacy-legislation (accessed 25th June, 2024).
50. Zhao, Q. (19th October, 2022) 'American Data Privacy and Protection Act: Latest, Closest, Yet Still Fragile Attempt toward Comprehensive Federal Privacy Legislation', JOLT, *Harvard Journal of Law & Technology*, available at https://jolt.law.harvard.edu/digest/american-data-privacy-and-protection-act-latest-closest-yet-still-fragile-attempt-toward-comprehensive-federal-privacy-legislation (accessed 25th June, 2024).
51. H.R.2701, 118th Congress (2023).
52. § 301.
53. IAPP (26th July, 2022) 'Sen. Cantwell holds firm on American Data Privacy and Protection Act opposition', available at https://iapp.org/news/b/cantwell-holds-firm-american-data-privacy-and-protection-act-opposition (accessed 25th June, 2024).
54. § 101(13)(A). Section references to the APRA are to the May 2024 draft cited at ref 2 above.
55. *See* eg Colo. Rev. Stat. § 6-1-1303(7) (defining 'controller' as 'a person that, alone or jointly with others, determines the purposes for and means of processing personal data.').
56. § 101(13)(A)(iii).
57. See the section on key features of the APRA below.
58. A large data holder is a covered entity that meets certain revenue and data processing thresholds. §101(32)(A). A data broker is 'a covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to such covered data'. § 101(17)(A).
59. *See* eg Cal. Civ. Code § 1798.140(d)(1).
60. § 101(42)(A).
61. *See* eg Colo. Rev. Stat. § 6-1-1303(19) (defining 'processor' as one 'that processes personal data on behalf of a controller').
62. § 101(12)(A).

63. Colo. Rev. Stat. § 6-1-1303(17) ('"Personal data" means information that is linked or reasonably linkable to an identified or identifiable individual.').
64. § 101(12)(B)(ii).
65. § 101(41)(A).
66. *Compare with* Colo. Rev. Stat. § 6-1-1303(24) (defining 'sensitive data' as 'Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or Personal data from a known child.').
67. For more information on statutory definitions and recommendations for operationalising, see Determann, L. (2023) 'California Privacy Law', IAPP, Portsmouth, NH; Determann, L. and Gupta, C. (2019) 'Indian Personal Data Protection Act of 2018: Draft bill and Its History, Compared to GDPR and California Privacy Law', *Berkeley Journal of International Law*, Vol. 37, p. 481; Singh, S., Determann, L., Engfeldt, H. and Tam, J., (2023) 'India Enacted the Digital Personal Data Protection Act: What Should U.S. Companies Do Now?', Bloomberg Law: Data Privacy & Security, available at https://www.bloomberglaw.com/external/document/X68LPEPK000000/international-data-privacy-compliance-professional-perspective-i (accessed 25th June 2024); and, generally, Determann, L. (2022) 'Determann's Field Guide to Data Privacy Law', Edward Elgar, Cheltenham.
68. §§ 105(a)(1)-(4).
69. § 105(c).
70. §§ 106(a)(1)-(2).
71. § 106(b)(1).
72. § 104(a).
73. § 104(b).
74. § 107(a).
75. § 108(a).
76. § 113(a)(1).
77. § 109(a)(1).
78. § 109(c).
79. § 120(a)(3)(E).
80. For practical guidance see Determann, L. (2022) 'Determann's Field Guide to Data Privacy Law', Edward Elgar, Cheltenham.
81. § 110(a)(1).
82. § 110(b).
83. § 110(4).
84. § 113(b)(1).
85. §§ 114(a)-(b).
86. See the section on legislative history above.
87. § 120(2).
88. Sec. 20(a)(3)(C).
89. Sec. 20(a)(3)(N).
90. APRA § 119(a)(2)(B).
91. On 23rd May, 2024, the Illinois House of Representatives approved Senate Bill 2979, which overrules the Illinois Supreme Court's interpretation of BIPA in a 2023 decision (*Cothron v. White Castle Systems*) whereby plaintiffs could recover liquidated damages of US$1,000 (or US$5,000) for each act of processing their biometric identifier in violation of the law. Poell, D. (23rd May, 2024) 'BIPA Reform Watch – Illinois Legislature Eliminates "Per-Scan" Damages', JD Supra, available at www.jdsupra.com/legalnews/bipa-reform-watch-illinois-legislature-2401526/ (accessed 25th June, 2024).
92. § 102(c). For example, the APRA has no requirement that an individual receive written notice prior to the collection or storage of biometric information.
93. § 119(a)(2)(B)(i). The APRA has a similar provision allowing relief equivalent to the CCPA private right of action (as with BIPA, the APRA contains no pre-emption carve-out for the CCPA).
94. APRA § 119(a)(2)(C).
95. § 120(a)(3)(N).
96. See eg Ct. SB 3 (2023).
97. § 3(8)(b)(xiii).
98. *See* eg Colo. Rev. Stat. § 6-1-1308(4). See also the section on legislative history above.
99. § 102(a)(1).
100. § 102(a)(2).
101. § 102(d)(1)-(16).
102. *See* Hendrix, J. and Lennet, B. (11th April, 2024) 'Experts Provide Early Analysis of the American Privacy Rights Act', TechPolicy.Press, available at https://www.techpolicy.press/experts-provide-early-analysis-of-the-american-privacy-rights-act/ (accessed 25th June, 2024) ('Furthermore, a strict reading of the proposed minimisation requirements of the APRA discussion draft could curtail certain socially beneficial practices, such as processing for research carried out in the public interest.').
103. *See* eg Conn. Gen. Stat. § 42–517(a)(3).
104. *See* Rosen, J. (2012) 'The Right to Be Forgotten', *Stanford Law Review Online*, Vol. 64, p. 88; Bambauer, J, 'Is Data Speech?', *Stanford Law Review*, Vol. 66, p. 57; Solove, D. J. (2023) 'The Limitations of Privacy Rights', *Notre Dame Law Review*, Vol. 98, No. 3, pp. 975–1036.
105. See the section on legislative history above.
106. § 117(a)(1).
107. § 117(b)(3).
108. § 118(a)(1).
109. § 118(b).
110. § 119(a).
111. *See* eg *Cullen v. Zoom Video Communications, Inc.*, Civil Docket No. 5:20-cv-02155-LHK (N.D. Cal.).
112. See the section on legislative history above.
113. House Committee on Energy and Commerce (17th April, 2024) 'Subcommittee Chair @RepGusBilirakis Just Asked If the American Privacy Rights Act Is the Best Chance We Have at Accomplishing Comprehensive Data Privacy. Without hesitation, every witness Answered YES', available at https://x.com/HouseCommerce/status/1780623091992854530 (accessed 25th June, 2024).
114. Duball, J. (23rd May, 2024) 'Proposed American Privacy Rights Act Clears US House Subcommittee', IAPP, available at https://iapp.org/news/a/proposed-american-privacy-rights-act-clears-us-house-subcommittee (accessed 25th June, 2024).
115. Soltani, A. (16th April, 2024) 'Letter Re: American Privacy Rights Act Discussion Draft', California

Privacy Protection Agency, available at https://cppa.ca.gov/pdf/apra_discussion_draft.pdf (accessed 25th June, 2024).
116. Crenshaw, J. (17th April, 2024) 'U.S. Chamber Letter on the American Privacy Rights Act', US Chamber of Commerce, available at https://www.uschamber.com/technology/data-privacy/u-s-chamber-letter-on-the-american-privacy-rights-act (accessed 25th June, 2024).
117. Duball, J. (23rd May, 2024) 'Proposed American Privacy Rights Act Clears US House Subcommittee', IAPP, available at https://iapp.org/news/a/proposed-american-privacy-rights-act-clears-us-house-subcommittee (accessed 25th June, 2024).