Data Minimization in the United States' Emerging Privacy Landscape: Comparative Analysis and Exploration of Potential Effects

August 2024

CIPL US State Privacy Laws Mapping Project
Discussion Paper

Data Minimization in the United States' Emerging Privacy Landscape: Comparative Analysis and Exploration of Potential Effects

The Centre for Information Policy Leadership ("**CIPL**") is publishing this discussion paper as part of a series on emerging privacy laws in the United States to offer analysis and recommendations to policymakers for safeguarding consumer data privacy and enhancing responsible data practices.

First, this paper analyzes the data minimization requirements in US state privacy laws[1] and the proposed American Privacy Rights Act ("**APRA**")—specifically, Section 102 of H.R. 8818 introduced on June 25, 2024.[2] Second, this paper explains, through case studies and examples from CIPL member organizations, how certain data minimization provisions in the APRA could affect business, research, government and other activities involving the collection and processing of personal data.

This analysis should be viewed in the context of our ongoing efforts to support a strong privacy ecosystem in the United States, where reasonable and beneficial data practices are promoted, and individuals' privacy is safeguarded.

1. Data Minimization Requirements at State and Federal Level

A. State Privacy laws

Most common approach at state-level—focus on processing purposes: Most US state privacy laws impose a duty of data minimization, limiting the *collection* of personal data by businesses to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.[3] With respect to *processing* personal data, these states also impose data minimization obligations not to process personal information for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes, unless the business obtains the consumer's consent. The obligations with respect to both collection and processing require that businesses identify and disclose processing purposes during the initial data collection. These obligations appear to enable

[1] While the chief focus of this paper is comprehensive privacy laws, we note that some privacy laws with narrower remit also address data minimization. For example, in 2024, New York adopted the New York Child Data Protection Act (NYCDPA), for which data minimization is a central concept. Washington's My Health My Data Act, which has sometimes been characterized as "quasi-comprehensive," is discussed further below.
[2] On June 27, 2024, the US House of Representatives cancelled the House Energy and Commerce Committee markup of the American Privacy Rights Act ("APRA") scheduled for that day. There has been no indication of when the markup will be rescheduled; however, House Energy and Commerce Committee Chairwoman Cathy McMorris Rodgers issued a statement reiterating her support for the legislation.
[3] Followed by Colorado, Connecticut, Delaware, Florida, Indiana, Kentucky, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas and Virginia.

future secondary and previously undisclosed processing purposes that are "compatible" with the disclosed purposes. However, since the concept of "compatibility" is not defined in most state privacy laws (except in California and Colorado), it can lead to legal uncertainty where it is not clear whether "compatibility" will be interpreted narrowly or broadly.[4] Additionally, these state privacy laws include in their Exclusions or Limitations chapters specific permissible purposes regardless of data minimization or other requirements. In other words, state privacy laws provide a list of permissible processing purposes as exceptions to their data minimization requirements (see Figure 1). Notably, the activities listed under Figure 1 resemble the permissible purposes under APRA's data minimization provision (*see* page 4), but there are some significant differences, e.g., the APRA does not include a "performing internal operations" exception among its permitted purposes.

Figure 1: Exclusions/Limitations to Obligations Imposed—Permissible Purposes Recognized Under State Privacy Laws*

- Comply with federal, state, local laws, rules or regulations
- Comply with a civil, criminal, regulatory inquiry, investigation, subpoena, summons by federal, state, local, government authorities
- Cooperate with law enforcement agencies (except Florida, Texas)
- Investigate, exercise, prepare for, or defend actual or anticipated legal claims
- Conduct internal research to improve, repair or develop products, services, technology (except in Maryland)
- Identify and repair technical errors that impair existing or intended functionality
- Perform internal operations reasonably aligned with consumer's expectation
- Effectuate a product recall
- Provide a product or service specifically requested by a consumer
- Perform a contract to which the consumer is a party or take steps prior to entering a contract
- Protecting an interest that is essential for the life or physical safety of an individual, and where the processing cannot be manifestly based on another legal basis
- Protect the vital interests of the consumer of another individual (only in Colorado)
- Protecting any person's health and safety (only in Oregon)
- Prevent, detect, protect against, respond to security incidents, identity theft, fraud, harassment, illegal activity
- Preserve integrity or security of systems
- Engage in public or peer-reviewed scientific or statistical research in the public interest—subject to conditions (except Colorado, Maryland, Oregon; also Minnesota and Utah include "historical research" within their scope of exclusions and Delaware exclude "statistical research" from its scope of exclusions)
- Process personal data for reasons of public interest in the area of public health (only in Colorado, Connecticut, Minnesota, Montana, New Hampshire, New Jersey, Rhode Island)
- Transfer personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller (only in Florida)
- Assist another controller, processor or third party with any of the obligations above

*Please note that certain language differences can be observed across states' laws.

[4] The situation in the European Union (EU) is different: The GDPR prescribes data minimization as a principle relating to processing of personal data. Accordingly, personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5/1/c GDPR). The GDPR's purpose limitation principle also clarifies that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Article 5/1/b GDPR). The concept of "compatibility" is specified further in Article 6(4) GDPR in the context of purpose limitation, providing a non-exclusive list of factors to be considered when assessing compatibility.

Utah's and Iowa's privacy laws don't prescribe data minimization as an obligation for data controllers but address the concept implicitly. First, both laws in their Limitations sections specify permitted purposes for processing personal data (see Figure 1), meaning that nothing in the regulations should be interpreted as restricting the ability to perform those specified activities. In addition, a degree of data minimization is also imposed through the Limitations section of the Iowa Consumer Data Protection Act, which further provides that personal data processed pursuant to permitted purposes must be: (a) reasonably necessary and proportionate to the listed purposes in the Limitations section and (b) adequate, relevant and limited to what is necessary in relation to those specific purposes.[5] Finally, one could argue that both laws imply a limited duty of data minimization for data security practices by requiring reasonable administrative, technical and physical practices (appropriate to the volume and nature of the personal data at issue) designed to protect the confidentiality, integrity and accessibility of personal data.

Reasonable expectation standard in California: California provides a slightly different data minimization framework. Organizations' collection, use, retention and/or sharing of consumer personal information must be reasonably necessary and proportionate to achieve:

(i) The purpose(s) for which the personal information was collected or processed—similar to the most common approach. A business may process personal information if the purpose is consistent with an individual's reasonable expectations.

OR

(ii) Another disclosed purpose that is compatible with the context in which the personal information was collected.[6]

California privacy regulations also include exemptions that allow businesses to process personal data for certain purposes without restrictions. Reading these exemptions in conjunction with the definition of "business purpose" under the CPRA,[7] these purposes are similar to those listed in Figure 1 but include some additional purposes[8] as well as certain exceptions.[9]

---

[5] Section 7 of 715D.7(6) Iowa Consumer Data Protection Act.

[6] Section 7002(a) California Consumer Privacy Act read in conjunction with Section 4. Section 1798.100(c) California Privacy Rights Act. Here, the statutory language and implementing regulations may create confusion regarding the need for a new secondary purpose to have been disclosed when the information was collected. In general, the concept of compatibility allows the processing of personal data for purposes other than those initially disclosed, as long as the new purposes are compatible with the original purposes for which the data were collected.

[7] Section 14. Section 1798.140(e) CPRA.

[8] For example, businesses can process personal data that is de-identified or aggregated, and they can process personal data if all commercial activities take place entirely outside of California (see Section 15. Section 1798.145(a)(6) and (7) CPRA).

[9] For example, there is also a permitted purpose for cooperating with a government agency if an individual is at risk of death or serious physical injury. However, unlike the approach followed by other states, this is subject to certain conditions in California: (a) the request is approved by a high-ranking agency officer for emergency access to a

Maryland and Washington—focus on necessity: While the proposed federal-level American Data Privacy and Protection Act ("**ADPPA**") of 2022 failed to pass in the House, its data minimization standards and language have influenced emerging state-level privacy rules. Notably, Maryland's Online Data Privacy Act and Washington's My Health My Data Act ("**MHMDA**") have adopted approaches to data minimization inspired by the ADPPA. These states limit collection of personal data (consumer health data in Washington's MHMDA) to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains. The language addressing data collection requirements differs from the most common approach in that it allows organizations to process data even if the processing purpose is not disclosed to a consumer in the privacy notices, as long as the processing is necessary for their products and services requested by the consumer. With respect to processing activities, Maryland incorporates the standard data minimization rule common in most states, i.e., organizations may not process personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed, as disclosed to the consumer. Importantly, Maryland's data minimization requirements are particularly strict with regard to sensitive data (discussed further below).

Additionally, the Maryland Online Data Privacy Act allows for permitted processing purposes similar to those in Figure 1, with certain exceptions. For instance, it does not list conducting peer-reviewed scientific or statistical research in the public interest, as well as conducting internal research to improve, repair or develop products, services, technology as permitted purposes.

B. Federal Legislative Proposal

The APRA's two-tiered approach: Section 102 of the APRA sets out a data minimization requirement. Similar to the ADPPA, under the APRA, a "covered entity" may not collect, process, retain or transfer "covered data" of an individual beyond what is necessary, proportionate and limited:

(i) to provide or maintain (a) a specific product or service requested by the individual to whom the data pertains (similar to emerging state trends) or (b) a communication, that is not an advertisement, to the individual reasonably anticipated within the context of the relationship;

OR

(ii) for a purpose expressly permitted under the APRA (17 in total—below).[10]

- (1) To protect data security, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs;
- (2) To comply with a legal obligation imposed by a Federal, State, Tribal, or local law that is not preempted;

consumer personal information; (ii) the request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis; (c) the agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted. Section 1798.145(a)(4) CPRA.

[10] We have not reproduced the full text of the permitted purposes in all instances. Please refer to the bill text for exact language.

- (3) To investigate, establish, prepare for, exercise or defend cognizable legal claims of the covered entity or service provider;
- (4) To transfer covered data to Federal, State, Tribal or local law enforcement pursuant to a lawful warrant, administrative subpoena, or other form of lawful process;
- (5) To effectuate a product recall pursuant to Federal or State law, or to fulfill a warranty;
- (6) To conduct market research;
- (7) With respect to covered data previously collected in accordance with this title, to process the covered data such that the covered data becomes de-identified data, including in order to: (a) develop or enhance a product or service of the covered entity or service provider; (b) conduct research or analytics to improve a product or service of the covered entity or service provider; (c) conduct research to investigate, establish, or improve the effectiveness or safety of medical care products, including drugs, biologics, and medical devices; (d) enable the effective delivery and administration of healthcare products and treatments to patients in compliance with Federal regulations, or (e) monitor the safety and efficacy of health care products and services administered to patients, in compliance with the Federal Regulations;
- (8) To transfer assets to a third party in the context of merger, acquisition, bankruptcy or similar transaction, with respect to which the third party assumes control, in whole or in part, of the assets of the covered entity, but only if the covered entity, in a reasonable time prior to such transfer, provides each affected individual with: (a) a notice describing such transfer, and (b) a reasonable opportunity to (i) withdraw any previously provided consent in accordance with the requirements of affirmative express consent under this title related to the covered data of the individual; and (ii) request the deletion of the covered data of the individual;
- (9) With respect to a covered entity or service provider that is a telecommunications carrier, or a provider of a mobile service, interconnected VoIP service or non-interconnected VoIP service (as such terms are defined in section 3 of the Communications Act of 1934), to provide call location information for emergency services;
- (10) To prevent, detect, protect against, investigate or respond to fraud, excluding the transfer of covered data for payment or other valuable consideration to a government agency;
- (11) To prevent, detect, protect against or respond to an ongoing or imminent security incident relating to network security or physical security, including an intrusion or trespass, medical alert or request for a medical response, fire alarm or request for a fire response, or access control;
- (12) To prevent, detect, protect against, or investigate or respond to an imminent or ongoing public safety incident (such as mass casualty event, natural disaster or national security incident), excluding the transfer of data for payment or other valuable consideration to a government agency;
- (13) Except with respect to health information, to prevent, detect, protect against, investigate or respond to criminal activity or harassment, excluding the transfer of data for payment or other valuable consideration to a government agency;
- (14) Except with respect to sensitive covered data, and only with respect to covered data previously collected in accordance with this title, to process or transfer such data to provide first-party advertising or contextual advertising, or to measure and report on marketing performance or media performance by the covered entity, including processing or transferring covered data for measurement and reporting of frequency, attribution and performance, including by independent entities, except that this paragraph does not permit the processing or transferring covered data for first-party advertising to a covered minor, as prohibited by Section 120;
- (15) Except with respect to sensitive covered data and only with respect to covered data previously collected in accordance with this title, to process or transfer such data to provide targeted advertising, direct mail targeted advertising or email targeted advertising (subject to the CAN-SPAM Act of 2003 and the regulations promulgated under such Act), or to measure and report on marketing performance or media performance, including processing or transferring covered data for measurement and reporting of frequency, attribution, and performance, including by independent entities, except that this paragraph does not permit the processing or transfer of covered data for targeted advertising to an individual who has opted out of targeted advertising pursuant to section 106, or to a covered minor as prohibited by Section 120;
- (16) To conduct a public or peer-reviewed scientific, historical, or statistical research project that is (a) in the public interest, (b) adheres to all relevant laws and regulations governing such research, including regulations for the

protection of human subjects, if applicable, (c) limits transfers to third parties of sensitive covered data to only those transfers as necessary, proportionate and limited to carry out the research, and (d) prohibits the transfer of covered data to a data broker; and,

- (17) To conduct medical research in compliance with applicable Federal regulations.

The APRA also allows the Federal Trade Commission to add more permitted purposes for collecting, processing, retaining or transferring covered data through a rulemaking process.[11]

C. Additional Safeguards Prescribed if Processing Involves Sensitive Data in State Privacy Laws and APRA

- **Opt-in mechanism**: Most state privacy laws require that businesses obtain affirmative opt-in consent to collect and process sensitive personal data.[12] Similarly, the APRA mandates that covered entities must secure affirmative express consent before transferring sensitive covered data to third parties, unless the transfer is pursuant to one of several of the permitted purposes. This requirement also applies to the collection, processing, retention or transfer of biometric and genetic information.

- **Opt-out mechanism**: The CCPA does not require opt-in consent to collect or process sensitive personal data. However, it recognizes that unauthorized use or disclosure of sensitive personal data poses a heightened risk of harm to consumers. Therefore, it requires organizations to provide a notice of the right to limit the use and disclosure of sensitive data. However, there are certain exceptions to this rule, such as preventing security incidents, maintaining product quality or processing data for purposes other than inferring characteristics about the individual.[13] Iowa's and Utah's state privacy laws also allow organizations to process sensitive data, provided that consumers are given clear notice and an opportunity to opt out of the processing.

- **Heightened standards**: Maryland state privacy law prescribes strict data minimization requirements for sensitive personal data. Controllers are prohibited from selling sensitive personal data and can only collect, process or share such data if it is "strictly necessary" to provide or maintain a requested product or service.

2. Potential Effects of APRA's Data Minimization Requirement

Section 102 of the APRA would prohibit covered entities from collecting, processing, retaining or transferring the covered data of an individual, or direct a service provider from collecting, processing, retaining or transferring covered data of an individual, beyond what is necessary, proportionate and limited to provide or maintain a specific product or service requested by the individual to whom the data

[11] Section 123 of the American Privacy Rights Act.
[12] Followed by Colorado, Connecticut, Delaware, Florida, Indiana, Kentucky, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas and Virginia.
[13] Section 7027 of the California Consumer Privacy Act Regulations.

pertains or another permitted purpose. In its current form, the data minimization provision is likely to affect common responsible data practices that underpin the modern digital economy. Examples include the following:

Impact on Product Improvement & Development and Artificial Intelligence ("AI")

- **Product improvement and impact on research**: Although APRA Section 102(d)(7) permits processing of data to "develop or enhance a product or service of the covered entity or service provider, as well as to conduct research or analytics to improve a product or service," it imposes two restrictions that undermine this allowance: (i) any product development or enhancement must use only de-identified data and (ii) it must use data "previously collected in accordance with the [APRA]." Organizations routinely gather information on how users interact with their services and collect feedback about which aspects of a product they like or dislike. Also, personal data is used to improve AI capabilities, such as email services that personalize writing style suggestions while drafting an email. Depending on the context in which the data is collected, the APRA's data minimization provision may significantly limit the use of such data for research, product improvement and the development of new products and services even if these purposes are compatible with the consumer's relationship with the covered entity. It is very unusual for a comprehensive privacy law to prohibit the use of personal data for product improvement, research or innovation. Additionally, as a practical matter, organizations may have difficulty meeting the high standard for de-identification set out in the APRA,[14] and data collected prior to the effective date of the APRA may not have been "previously collected in accordance with [the APRA]," bringing product development and enhancement work to a halt until sufficient compliant data can be collected.

- **Impact on artificial intelligence**:[15] Some AI developers have argued that the APRA would affect the development of AI by overly restricting the volume of data available to AI developers for responsible model training. Particularly for generative AI models, it is critical for models to be trained on large, diverse and high-quality datasets to ensure that models are robust, accurate, safe and non-biased. Also, in some circumstances, developing and testing AI products may involve the use of personal information that may not necessarily be considered "requested" by the individual but is still carried out appropriately with privacy safeguards and within the context of the consumer-business relationship. In this scenario, the permissible purpose of product or service development and improvement under Section 102(d)(7) would not be helpful because it only allows for such purposes using de-identified data. As a result, this provision would reduce the scope for collection and use of covered data for AI modeling and other product enhancements, and by extension, the development of AI models that use personal information.

[14] Section 101(18) of the American Privacy Rights Act.
[15] For further information, please see CIPL Response to the ICO's 4th Consultation on Engineering Individual Rights into Generative AI Models, available here.

Impact on Consumer Experience

- **Extra data collection**: Section 102(d)(8) of the APRA permits the transfer of assets to a third-party in the context of a merger or similar transaction, but only if the covered entity provides each "affected individual" with notice and a reasonable opportunity to withdraw any previously given consent. This provision may place an undue burden on commercial transactions without providing a corresponding benefit to consumers and may require the collection of additional customer data to provide notice.

- **Personalized services**: APRA's data minimization provision may impair companies' ability to offer certain personalized services by default (e.g., search results appearing in a person's native language), as far as these services may not be seen as specifically "requested" by the user. For instance, without personalized recommendation systems, platforms might have to use a reverse chronological index in search results, i.e., listing links from most recent ones to oldest, making content hard to find and the platform less user-friendly. Furthermore, bad actors could exploit this chronological ordering to spread low-quality or harmful content frequently and more easily.

- **Consent fatigue**: While the APRA data minimization provisions seem to have been designed, at least in part, to reduce reliance on consent, they may, paradoxically, increase reliance on consent. By limiting data collection to providing or maintaining a product or service "requested by the individual to whom the data pertains," the data minimization provision may cause organizations to make numerous and frequent consent requests to ensure compliance with these provisions, as consent could be viewed as a close proxy to documentation of a consumer request. This could lead to consent fatigue among individuals, ultimately eroding the meaning and function of consent.

Lack of Consideration for Unforeseen Needs

- **Need for a "reasonable processing" basis**: By adopting a "prohibited unless permitted" approach in the data minimization provision, the APRA lacks the flexibility for potential future processing of covered data that may become necessary but is not currently envisioned. For example, the use of personal data to conduct bias testing or to generate synthetic data is not explicitly contemplated as a permitted purpose. This, and other unanticipated but legitimate uses of data, would need to be added as permitted purposes, or "retrofitted" to align with purposes enumerated in the legislation. Organizations could benefit from a GDPR-like legitimate interest basis for data processing activities, which allows flexibility to address unforeseen needs while respecting the imperative to protect individuals' data privacy. Under the GDPR, an organizations' legitimate interest is a lawful basis for processing personal data so long as the rights of individuals do not override the interests pursued by the organization. Organizations would also benefit from the more flexible standard under some US state comprehensive privacy laws that require controllers to limit collection to what is reasonably necessary and proportionate to, as well as compatible

with, the purposes of processing as "disclosed to the consumer" or with their consent, rather than to specific purposes enumerated in the statute.

Limitations on Transfers to Government Entities for Fraud Detection, Public Safety and Addressing Criminal Activities

- **Fraud detection and prevention services**: Section 102(d)(10) of APRA recognizes an exception to the data minimization requirement if the purpose of the processing is to prevent, detect, protect against, investigate or respond to fraud. However, APRA excludes the sale of covered data to government entities to support this permitted purpose. Government entities often rely on the private sector, including data brokers, for data tools and services to support delivery of services and benefits to individuals while preventing fraud. Because this exclusion prevents private organizations from providing fraud detection and identity authentication tools to government entities on a commercial basis, agencies would need to develop alternative data sources to identify and address fraud. [16]

- **Private sector's involvement in responding to public safety incidents**: Similarly, Section 102(d)(12) excludes the sale of covered data to government entities from the permitted use of processing activities "to prevent, detect, protect against, investigate or respond to an imminent or ongoing public safety incident (such as a mass casualty event, natural disaster, or national security incident)." Federal agencies currently use data to deliver services, including disaster relief to victims of events like hurricanes and floods, as well as for national security matters, such as the screening of visitors to secured facilities. In addition, as part of the review of the COVID-19 pandemic response, agencies and Congress are considering how to better leverage private sector data tools to deliver relief more efficiently. APRA could necessitate different approaches for these efforts due to the prohibition on government purchasing data from organizations.

- **Private sector's collaboration with law enforcement in responding to criminal activity or harassment**: Section 102(d)(13) excludes the sale of covered data to government entities from the permitted use of processing activities "to prevent, detect, protect against, investigate, or respond to criminal activity or harassment, except with respect to health information." Some observers have argued that APRA could affect access to personal data-intensive investigative research services used by many law enforcement agencies. These agencies regularly use data that are critical for investigating a range of crimes, and these data are often sold to them by private organizations. These data services have developed over time to provide access for law enforcement agencies using a shared cost model that permits multiple agencies to each pay a

[16] Although the APRA has a narrow exception for "service providers" to government entities, covered entities such as data brokers would not qualify for this exception because they are not service providers processing data "on behalf of, and at the direction of" government entities. Instead, many data brokers operate independently and provide their tools and services to a variety of customers rather than only processing data "on behalf of, and at the direction of" a single entity.

portion of the cost of these systems where any agency might otherwise be unable to cover the expense of gathering data and maintaining these systems. There may not be equally practical and efficient alternatives to obtaining the same information.[17]

Impact on Advertising Ecosystem

- **Contextual advertising**: The data minimization provision prescribes a permitted purpose for contextual advertising under Section 102(d)(14) but limits it to covered data previously collected consistent with APRA and excludes sensitive covered data. Excluding the use of sensitive data for contextual advertising from the permitted purposes could affect small businesses and consumer experience. For example, local businesses often rely on precise geolocation information (considered as sensitive covered data) for effective advertising. With the current data minimization provision, these businesses may not be able to target users in specific neighborhoods. These provisions could also impact individuals' ability to discover local services during their online searches.

- **Ads measurement**: The APRA includes ad measurement as a permitted purpose under Section 102(d)(14) and (15). Ad measurement refers to reporting of information between advertisers and publishers to validate whether ad campaigns delivered results. In order for ad measurement to work efficiently, it must keep track of activity over time, even on the same page or app. However, the APRA includes "online activity profile"[18] in the definition of sensitive covered data, which is excluded from permitted uses for ad measurement. This exclusion will likely impact the ability of organizations, such as news publishers and streaming services, to conduct certain forms of ad measurement. These entities rely on ad measurement practices to ensure that ads reach consumers and are effective.

[17] Separate proposed legislation related to this topic passed the House of Representatives on April 17, 2024; the Senate had not taken action on it at the time of writing of this paper. The Biden Administration issued a Statement of Administration Policy indicating it "strongly opposes" the bill.

[18] The APRA introduced on June 25 defines "online activity profile" as covered data that identifies the online activities of an individual (or a device linked or reasonably linkable to an individual) over time and across third party websites, online services, online applications or mobile applications that do not share common branding, and that is collected, processed, retained or transferred for the purpose of evaluating, analyzing or predicting the behaviors or characteristics of an individual. *See* Section 101(41) APRA. The Bill also defines "online activity profile" as sensitive covered data. *See* Section 101(49)(A)(xv) APRA.