CLIENT ALERTS & INSIGHTS

Privacy Surprise: Bipartisan Group Proposes Omnibus Data Protection Law that Preempts all US State Data Protection Laws

MAY 8, 2024

The American Privacy Rights Act of 2024 would establish a national, comprehensive data protection law unifying US businesses under one standard, preempting the well over a dozen U.S. states with laws already in effect.

Over the weekend, House Committee on Energy and Commerce Chair Cathy McMorris Rodgers (R-WA) and Senate Committee on Commerce, Science and Transportation Chair Maria Cantwell (D-WA) unveiled the American Privacy Rights Act (the "APRA").

The development is a surprise in light of the upcoming election cycle and past, failed attempts by members of congress to put forth a national, omnibus data protection law. The APRA is not unlike past iterations or proposed federal data protection legislation and brings in concepts that many businesses are now familiar with under the web of overlapping U.S. state data protection laws. Concepts such as data minimization, data privacy rights (access, correction, portability, deletion), sensitive personal data, targeted advertising opt-out, privacy notices requirements and much more are all addressed under the proposed APRA.

The biggest, topline takeaways, however, are that the APRA will act to preempt and supersede all the U.S. state data protection laws that have come into effect in recent years, such as those in California, Colorado, Virginia, and many more.

The APRA also creates a private right of action whereby the law, and violations of the law, can be enforced via action by the Federal Trade Commission, state attorneys general **or** via individual citizens filing claims against a business subject to the APRA. Unlike past iterations of federal data protection law proposals, the APRA only provides a grace period of 6 months from its effective date before the private right of action kicks in. Past iterations provided for longer periods (e.g., 1 year, 2 years, etc.).

Additionally increasing the potential for new litigation in the data protection context is that the APRA would **prohibit** a business from enforcing mandatory arbitration for "substantial privacy harm" or any claim related to the information of a minor.

It remains to be seen if Congress will act quick enough before the next election cycle to pass the APRA or a version thereof. However, some are hopeful this compromise proposal-that expands privacy rights and private rights of action, while also acting to clearly preempt all similar U.S. state data protection laws-could see a fast track to passage.

In the meantime, businesses still need to contend with the patch work system of U.S. state data protection laws.

Last year proved to be a huge year in U.S. state data protection law, ending with 13 U.S. states with comprehensive data protection laws on the books. And 2024 shows no sign of stopping or slowing that trend. To aid in the constant effort of keeping track of new U.S. state data protection laws-and while we all patiently await federal action on data protection-Benesch Friedlander Coplan and Aronoff and the Data Meets World blog now feature a "U.S. State Privacy Laws" landing page that offers a high level overview of all U.S. states with data protection laws in place and key requirements and takeaways from those laws. That page has now been updated to add Kentucky to the list.

The new webpage offers a continuously up to date snapshot of the U.S. state data protection landscape. To use the Data Meets World interactive U.S. Privacy Laws webpage, click here.

Scope of the America Privacy Rights Act

The scope of the proposed APRA is broad. Entities subject to the APRA would include any that (1) is subject to the FTC Act (including common carriers and certain subsets of nonprofits); and (2) collects, processes, retains, transfers, or otherwise uses personal data.

Covered entities under the APRA would not include certain types of small businesses or nonprofits whose primary mission is to prevent, investigate or deter fraud.

Additionally, the type of personal data covered under the APRA (deemed "covered data" under the APRA) is similarly broad. Covered data includes any information that identifies or is linked or reasonably linkable, along or in combination with other information, to an individual or a device that identifies or is linked or reasonably linked to one or more individuals. Covered data would not include de-identified data, employee information, publicly available information, and other narrow subsets of non-identifiable data.

Much like other omnibus data protection laws, both at the U.S. state level and globally in other jurisdictions, the APRA creates a subset of data considered sensitive that is subject to additional and heightened requirements. "Sensitive covered data" is defined much more broadly than in other data protection laws, and includes:

1. Government identifiers (e.g., social security number, passport number, driver's license number, etc.);
2. Physical or mental health information;
3. Genetic information;
4. Financial account numbers, debit card numbers, cred card numbers or any required security or access code, password or other credentials allowing someone to access financial accounts or cards;
5. Biometric information;
6. Precise geolocation information (locating to street-level location or to within a radius of 1,850 feet or less);

7. Private communications (e.g., emails, texts, etc. not addressed or intended for the covered entity);
8. Account or device log-in credentials;
9. Sexual orientation or sex life information;
10. Calendar information, address book information, phone or text logs, photos, audio recordings, or videos intended for private use;
11. A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual;
12. Information revealing the extent or content of any individual's access, viewing, or other use of any video programming described in section 713(b)(2) of the Communications Act of 1934;
13. Information that reveals the video content requested or selected by an individual;
14. Information revealing an individual's race, ethnicity, national origin, religion, or sex in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information;
15. Information revealing an individual's online activities over time and across websites or online services that do not share common branding or over time on any website or online service operated by a covered high-impact social media company; and
16. Information about an individual who is a covered minor (under the age of 17).

The APRA also institutes specific requirements for data brokers, including a new national data broker registry.

Under the APRA, a "data broker" includes any 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.

Conclusion

While the proof will be in whether Congress takes effective steps towards passing the ADPR, businesses will want to stay up to date on the latest as the ADPR-while similar in some respects to laws businesses commonly deal with today-would introduce new requirements and legal risks.

As the federal government moves forward with data protection legislation and rulemaking on a number of fronts-omnibus laws, financial services, children, healthcare, etc.-and businesses juggle the various new regimes, the Benesch Data Protection team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.