The 10 Things Employers Need to Know About Sweeping New Federal Data Privacy Law Proposal

Insights
4.09.24

A bipartisan group of federal lawmakers just unveiled a sweeping proposal to pass the nation's first data privacy law and hand a significant amount of power to consumers, one that would bring about a massive change in the way that businesses treat customer data. While it would create a consistent framework across the country and eliminate the confusing patchwork of state laws that businesses now have to navigate, it would also expose more businesses to potential litigation and increase compliance obligations for tens of thousands of organizations. What are the 10 things you need to know about the proposal released this past weekend?

1. **Bipartisan proposal stands a chance of survival.**
   The proposal to pass the American Privacy Rights Act (APRA) is a bipartisan measure floated by Senate Commerce Committee Chair Maria Cantwell (D-Wash.) and House Energy and Commerce Committee Chair Cathy McMorris Rodgers (R-Wash.). Unlike past proposals, this one seems to have initial momentum due to leadership from both parties weighing in. It still will face an uphill battle due to the fractured nature of Congress and election year distractions – but it does at least stand a chance of passing in 2024.
2. **The proposal could mean the end of the CCPA as we know it and other state data privacy laws.**
   In its current form, the APRA would seemingly destroy most state data privacy laws, including much of California's landmark CCPA. While it would allow state laws that regulate certain kinds of data (such as financial, health, or employee data), these carve-outs would be few and far between. As you could imagine, the proposal has been met with a frosty reception by many California lawmakers who don't want to see their sweeping law largely cast into the dustbin. This dynamic could be enough to kill the APRA proposal – more on this later.
3. **Silver lining for employers: no additional workplace obligations.**
   Despite the many challenges businesses will face if the APRA is enacted, the one piece of good news you can celebrate is that you will not see your workplace obligations increase. As opposed to the broadest of state privacy laws (such as the CCPA), the law will not apply to data employers collect about their workers. There is an open question, however, as to whether California's CCPA employment obligations would survive the APRA – stay tuned for more on this dynamic as the proposal progresses through Congress.
4. **Consumers would have much more power over their data.**
   Turning to the proposal itself, the APRA would require businesses to give consumers the right to

access, delete, correct, and transport their data between digital services. Consumers would also have the ability to block businesses from transferring or selling their data. Businesses would need to obtain affirmative express consent before they transfer sensitive data to a third party.

5. **Businesses would need to provide opt-out rights to consumers.**
   Another key component of the APRA would be a provision giving users the right to opt out of certain data practices, including targeted advertising -- ads sent to people based on their personal data.

6. **Proposed law would create limitations on data gathering practices.**
   Next, businesses would be able to gather, retain, and use only as much information as they need in order to offer specific products and services to consumers under the proposed law. That would be a big shift from the current system that requires consumers to scroll through privacy agreements and respond to website pop-ups asking for data use and tracking permission. Further, companies that buy and sell personal data would have to register with the Federal Trade Commission (FTC).

7. **Proposed law will create anti-discrimination and other protections.**
   The APRA would prohibit businesses from using data they collect to discriminate against protected classes (such as race, gender, national origin, etc.). It would also allow consumers to opt out of a businesses' use of algorithms to make decisions about housing, employment, healthcare, credit opportunities, education, insurance, or access to places of public accommodation.

8. **Businesses will need to beef up their data protection practices.**
   Companies would also need to take affirmative steps to bolster their data privacy practices. First, they would need to appoint executive officers to their leadership teams deemed responsible for ensuring APRA compliance within the organization. They would also need to implement strong data security standards to prevent data from being hacked or stolen.

9. **Small businesses would be excluded from coverage.**
   Companies with under $40 million in annual gross revenue would be exempt from the proposed law. But companies with more than $250 million would face heightened obligations – such as the need to conduct regular privacy reviews.

10. **Expect to see a flood of new litigation.**
    Perhaps most troubling for businesses, people would have the power to file lawsuits against businesses that violate the law – and collect civil damages if they prevail. This would be a big change, as many state laws only allow for state officials to take action against alleged violations. Significantly, the law would also prevent arbitration agreements from being used to push many APRA disputes into arbitration settings. Among those excluded from arbitration: those with at least $10,000 in alleged damages, physical or mental injuries that require medical treatment, highly offensive intrusions into privacy, or alleged discrimination based on race, religion, or other protected classes. You can expect to see a cottage industry of plaintiffs' attorneys spring up to file lawsuits for privacy rights violations if the law is passed in its current form. The

proposed law would be regulated by a yet-to-be-developed bureau within the FTC, removing some power from the Federal Communications Commission.

What's Next?

- There's no need to panic – quite yet. After all, it is currently just a "discussion draft" that will allow the two committee chairs to gather feedback from their colleagues and third parties before it is formally introduced as a bill. And the proposal will face myriad obstacles.
- For example, as noted above, California lawmakers may fight against it to retain their state's own powerful law. You can also expect business advocacy organizations to fight against the proposal for going too far. And as earlier described, Congress may be too fractured and distracted by election year developments to pass such meaningful legislation.
- It also faces time pressure. Representative McMorris Rodgers plans on leaving Congress in January 2025, giving the APRA a small window of time to get pushed through with current leadership.
- That being said, we expect to see a formal bill introduced in the coming weeks. While some provisions may be reworked before introduction – for example, several lawmakers have already called for stronger protections for children – the final version will most likely appear very similar to the current proposal.
- One final warning: the time to comply with the proposed law would come rather soon if it is passed. As opposed to prior iterations of federal data privacy proposals, the APRA would take effect just six months after passage.

What Should You Do?

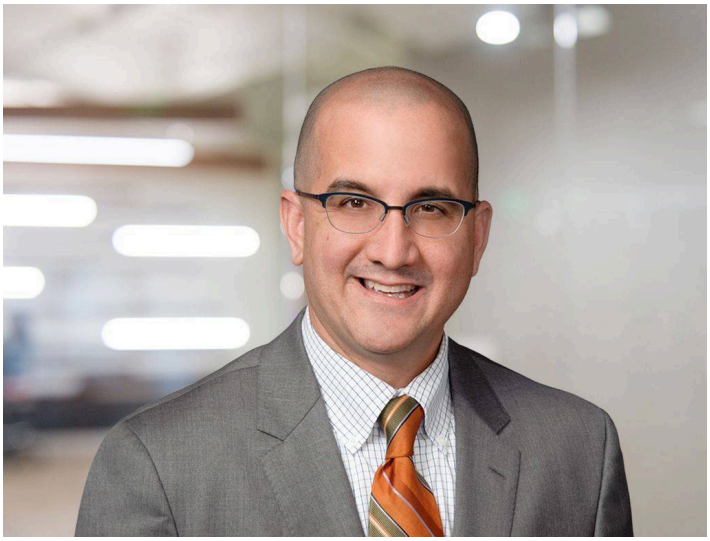
While this is the most significant development in the privacy rights arena in quite some time, there are no immediate steps for you to take other than to monitor the situation for more details as they evolve. You may also want to participate in advocacy efforts with your local business advocacy groups or industry-specific associations given the need for feedback about the practical impact of this proposal.

Conclusion

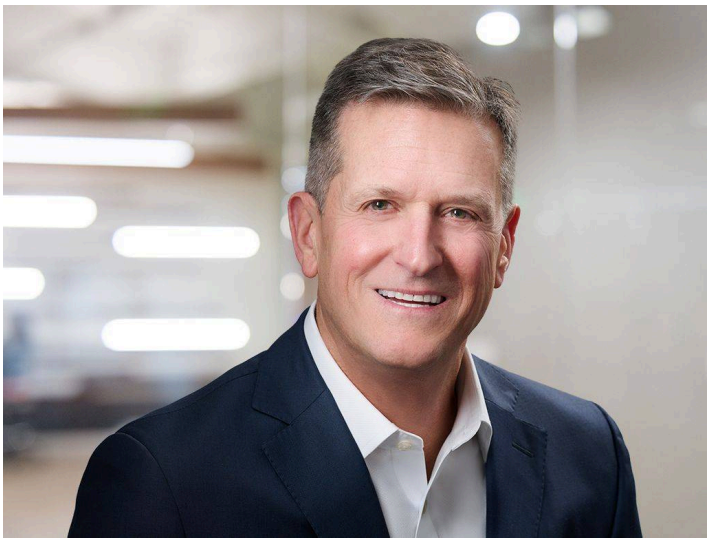
We will continue to monitor these developments and provide the most up-to-date information directly to your inbox, so make sure you are subscribed to Fisher Phillips' Insight System. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Privacy and Cyber Group or Government Relations Team.

Related People

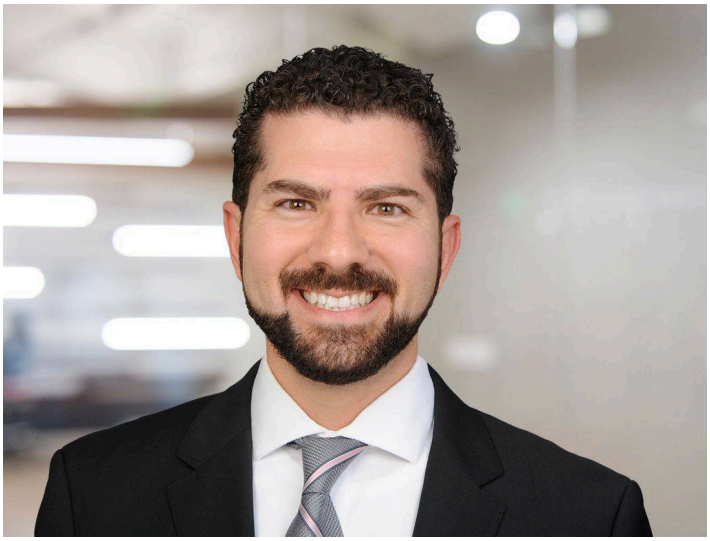
Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email



Benjamin M. Ebbink
Partner
916.210.0400
Email



Rick Grimaldi
Partner
610.230.2136
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Privacy and Cyber

Government Relations