HINSHAW

Alerts

# Get Ready for a Comprehensive U.S. Data Privacy and Protection Law at the Federal Level…Maybe

**July 26, 2022**
*Data & Cyber Law Decoded*

After years of inaction and watching other Western nations—and even some not so Western Nations, *e.g.*, China—enact data privacy and protection laws, it appears the United States (U.S.) may finally be getting into the game. While it might be too soon to update your list of legal acronyms, the proposed law, the American Data Privacy and Protection Act (ADPPA), is the first of its kind to show real promise at actually becoming a law. Since its release on June 3rd of this year the ADPPA has moved through the legislative process with bipartisan support at an almost meteoric clip, especially when compared to its many failed and forgotten predecessors.

What sets ADPPA apart? As they say, timing is everything. Just a few months ago, the European Union and the U.S. reached an "agreement in principle" for a "Trans-Atlantic Data Privacy Framework." Privacy advocates are already planning on challenging the framework, and a new U.S. privacy law could help act as a shield against the political and judicial scrutiny the framework will undoubtedly face. In addition, there was the leak of Supreme Court Justice Samuel Alito's draft opinion in *Dobbs* followed by the Court's holding in that case. Though seemingly unrelated, the case has serious privacy implications and helped highlight the growing concern of consumers about the collection and use of their personal and sensitive data. Finally, midterm elections are around the corner, and states continue to propose and enact their own laws, potentially complicating compliance for an already confused and anxious business community.

If passed into law, the ADPPA would regulate most organizations—including non-profits—that collect, process, or transfer "covered data." Covered data is defined as information that identifies or is linked to an individual or a device that identifies or is linked to an individual and may include derived data and unique identifiers. Notably, "Federal, State, Tribal, territorial, or local government" entities are excluded under the ADPPA, as are "service providers." Privacy advocates complain that this could result in problematic partnerships between public and private actors, such as Clearview AI and ID.me, and are asking legislatures to address this issue in any final draft of the law.

Another key provision of the ADPPA that has generated a lot of buzz concerns data minimization. Generally, covered entities would be prohibited from collecting any more data than is necessary for one of seventeen permitted purposes, such as to complete a transaction, comply with a legal obligation,

## Attorneys

Jason J. Oliveri

## Service Areas

Privacy, Security & Artificial Intelligence

and to prevent a harm. Targeted advertising is also identified as a permitted purpose, which some privacy advocates argue should be banned altogether. However, the ADPPA does impose limitations when it comes to children and sensitive data. It would also prohibit the collection of "information identifying an individual's online activities over time and across third-party websites or online services." In sum, some forms of targeting based on first-party data would remain, but a universal opt-out option is likely, curtesy of the Federal Trade Commission.

Other long called for provisions of the ADPPA address transparency standards, anti-discrimination, and cybersecurity requirements. By far though, the most hotly discussed provisions—and the ones that may prove to be the proverbial wrench—concern a private cause of action (no surprise there) and federal pre-emption. In its current form, the ADPPA would pre-empt most comprehensive state privacy laws, including the California Privacy Rights Act. This has garnered much debate. On the one hand, it is argued, pre-emption would mean that states would not be able to quickly address rapid changes in technology and could not pass laws more protective than the ADPPA. On the other hand, anything less than full pre-emption would mean a continued patchwork of privacy laws, exacerbating the acknowledged compliance problem.

Time will tell whether or not these issues can be resolved. One thing is certain. The ADPPA is unlikely to move forward if House Democrats from California and their allies are not satisfied, and they will not be satisfied unless their constituents enjoy protections that are equal to or better than what they currently enjoy. In any event, the ADPPA has demonstrated that parties on both sides of the aisle now widely recognize the need for a comprehensive data privacy and protection law. Even if it doesn’t become law, the debate over ADPPA will certainly inform any proposed law that comes after—and one will surely follow. In the meantime, stay tuned for more reporting on this topic.