New Bipartisan Federal Privacy Bill – Breakthrough, Too Late, or Both?

Alexander I. Schneider

June 7, 2022

On Friday June 3, a bipartisan group of leaders from key House and Senate committees released a new "discussion draft" bill to establish nationwide standards for consumer privacy. The proposal (the American Data Privacy and Protection Act) builds on prior bills put forth by both Democrats and Republicans, as well as principles and provisions contained in the GDPR and State privacy laws. Of significance, the bill reflects bipartisan compromise on two thorny issues that have divided the parties for years – whether to preempt state privacy laws and/or include a private right of action. While the bill has been hailed as a "breakthrough," the prospects for passage are uncertain, particularly in this busy election year.

Why is this bill significant?

As most of our readers know, the US has no overarching federal privacy law – only sector-specific laws such as GLBA and COPPA. This patchy, confusing scheme has become even more complex with passage of the GDPR (which applies to US multinational companies) and five comprehensive State laws. While many federal bills have come and gone over the years, none reflect the high-level bipartisan compromise evident here – both on longstanding privacy concepts (notice, choice, access, security) as well as more specific concerns about discrimination, algorithms, platforms, data brokers, targeted ads, and corporate accountability. If passed, the bill would apply to virtually all companies doing business in the US.

Why is this happening now?

While many observers wish a bipartisan bill had been proposed earlier, the forces driving this bill forward have never been stronger. Passage of State laws is accelerating, the EU is exerting greater influence over privacy worldwide, and the FTC is planning to launch wide-ranging privacy rulemakings. In addition, Senator Wicker, one of the bill's authors and a longtime leader on privacy, may soon vacate his slot as Commerce's top Republican, motivating him to cement his legacy now. To cap it all off, while election year is indeed a difficult year to pass a bill like this, it's also creating pressure to make one last effort on privacy.

Key elements of the law

The law is extremely comprehensive and ambitious but, as expected, reflects compromise on certain issues. While we can't possibly summarize everything in a blogpost, here are some of the highlights:

- **Scope**: The bill covers entities subject to the FTC Act, as well as common carriers and non-profits. It applies to data that is linked or linkable to an individual or device (if linkable to one or

more individuals), including derived data and unique identifiers. There are exclusions for de-identified data, employee data, and publicly available data, but not for small businesses (though they're excluded from certain provisions). The net effect is that the bill covers virtually every company in the US and a good portion of their data.

- **"Standard" Provisions**: The ADPPA contains many elements that are now fairly standard in privacy laws and bills – privacy notices; the right to access, correct, and delete data, and to request it in a portable format; data minimization; privacy by design; data security; and corporate accountability. While these requirements differ in various ways from those in the State laws, the most notable departure is the strictness of the data minimization requirement (limiting the collection, processing, and transfer of data to what's necessary to provide a specific product or service requested by an individual, or to communicate in the context of the relationship). "Large data holders" (platforms and other large companies) must comply with enhanced notice and accountability requirements.
- **Duty of Loyalty**: The ADPPA includes several requirements in a section called "Duty of Loyalty" (a section that borrows its title, but not its contents, from a bill introduced by Senator Schatz). The notable requirements in this section include:
    - With certain exceptions, companies can't collect, process, or transfer SSNs or nonconsensual intimate images. They also can't transfer passwords.
    - With certain exceptions, companies can't collect, process, or transfer biometric or genetic data without affirmative express consent. (Unlike State privacy laws, these protections apply even when this data doesn't identify, or can't reasonably identify, an individual.)
    - With certain exceptions, companies can't transfer a person's precise geolocation, search or browsing history, or physical activity from their device without affirmative express consent.

Note that some of these provisions appear to overlap and/or conflict with other provisions of the bill. In particular, because biometric and genetic information, precise geolocation, online activities, and log-in credentials are defined as "sensitive covered data," they're also subject to the opt-in requirements discussed below. The restrictions on search and browsing data may also conflict with the law's purported opt-out regime for targeted advertising.

- **Rights to Consent & Object**: Like many privacy laws, the ADPPA requires opt in for certain practices and opt out for others.
    - Opt in is required before a company can process, collect, or transfer sensitive data. The bill defines sensitive data broadly and gives the FTC rulemaking authority to add new categories. Of note, the definition includes health, financial, biometric, genetic, and precise geolocation data; a person's private communications, media viewing history, and online activities; data revealing race, religion, or union membership (if such data isn't public); and the data of individuals under 17 (although the age is in brackets, indicating that it is still under discussion). As noted above, including "online activities" in here may conflict with the opt out for targeted advertising.
    - Opt out is required for data transfers to third parties (called "sales" in State laws) and targeted advertising (defined to exclude contextual advertising, ad reporting and measurement, and certain first party marketing). The bill also asks the FTC to study the feasibility of a unified opt-out mechanism (similar to Global Privacy Control in State laws)

and authorizes the FTC to implement it via rulemaking.

- **"Third Party Collecting Entities"**: The bill includes special requirements for "third party collecting entities" – companies (other than service providers) that derive their principal source of revenue from processing or transferring the data of individuals that the entity didn't collect directly from the individual. This provision is clearly designed to target data brokers and potentially ad networks or processors that operate behind the scenes. Such entities must register with the FTC and comply with a Do Not Collect mechanism allowing individuals to delete their data. Also, companies that share data with these entities must identify each of them *by name* in their privacy policies.

- **Children & Minors**: Building on recent concerns about harmful content directed at kids and teens, the bill would ban targeted advertising to minors under 17, as well as data transfers without consent. It also directs the FTC to create a division for Youth Privacy and Marketing, and asks the FTC's IG to assess the effectiveness of COPPA's safe harbor provisions. Here, the bill is clearly trying to address perceived weaknesses in COPPA – both its failure to protect teens and concerns that its safe harbor programs are inadequate.

- **Algorithmic Fairness:** To address rising concerns about the link between data collection and civil rights, the bill restricts collecting, processing, or transferring data in a manner that is discriminatory or that makes unavailable equal enjoyment of goods or services on the basis of race, religion, disability, or other protected categories. It would also require "large data holders" to conduct annual algorithmic impact assessments, and other entities to do design evaluations of their algorithms.

- **Service Providers & Third Parties:** In contrast to State laws and the GDPR, which use contractual requirements to control data use by service providers and third parties, the ADPPA regulates these entities directly. Service providers may only use data to perform services on behalf of covered entities, must promptly delete it thereafter, and may only transfer data to third parties with the affirmative express consent of the relevant individual (obtained via the covered entity). Third parties may not process data obtained from another entity contrary to individuals' reasonable expectations.

- **Federal and State Enforcement:** The bill authorizes FTC and State AG enforcement and sets forth a coordination scheme to prevent them from bringing duplicative actions. It also directs the FTC to establish a new Privacy Bureau; gives the FTC a wide array of rulemaking authority (sprinkled throughout the law); and authorizes it to approve compliance programs that "meet or exceed" the bill's requirements.

- **Private Right of Action:** The provision granting the private right of action is fairly complex, clearly reflecting extensive negotiations. It allows a person or class who suffers an injury due to a violation to bring a civil action in federal court but imposes a four-year delay until the PRA kicks in; bans mandatory arbitration clauses for minors only; and limits relief to compensatory damages, injunctions, and reasonable attorneys' fees and costs. For certain PRAs (those that seek an injunction, or that target smaller companies), there's a 45-day right to cure. Litigants also must notify the FTC and relevant State AG in advance, who may bring their own actions (but not, it appears, halt the private action). Finally, the bill directs the FTC to study the impact of the PRA on the economy.

- **State Preemption:** The preemption provision is similarly complex. It broadly preempts state laws that address the same issues as in the federal bill, and then claws back (i.e., preserves)

particular laws or types of laws, including California's data breach PRA (not the whole law, as has been mistakenly reported); Illinois' biometric and genetic privacy laws; employee and student privacy laws; laws that solely address facial recognition, surveillance, wiretapping, or phone monitoring; state breach notification laws; and a range of general purpose laws.

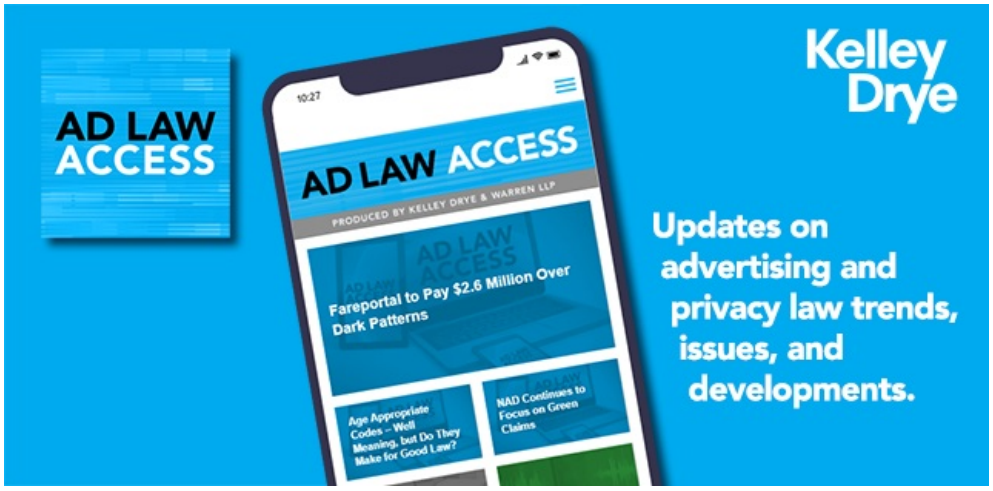
- **Other Federal Laws**: The bill generally preserves sector-specific privacy and data security laws like COPPA, GLBA and FERPA. One notable exception is that the bill prevents the FCC from using the Communications Act, or any rule issued under it, to take action against any covered entity for privacy violations. (Bracketed language would narrow the scope of this provision to satellite carriers, cable operator, or broadband providers.) The bill thus ousts the FCC of privacy jurisdiction in favor of the FTC, a move that some telecom groups have supported for years.

What's Next?

As we write this post, House Commerce has just announced that it will hold a hearing on the ADPPA on June 14, and we've heard that the Senate may hold a privacy hearing on the same day. However, time is short in this election year and Senator Cantwell (who chairs Senate Commerce) still supports her own bill, not the ADPPA, arguing that the PRA is too limited (even as industry members say it's too broad). Still, the bill has a chance; it's earned its "breakthrough" moniker; and if it doesn't pass this year, it will frame discussions moving forward.

Stay tuned as we continue to track progress on this bill.

* * *



Download our free App – *Ad Law Access* – a first-of-its kind, one-stop portal that provides updates and analysis on advertising, marketing, and privacy/data security law. The App is now available in the Apple App Store and Google Play, and can be used on iPhone, iPad, and Android devices.